Cisco Digital Network Architecture
CCIE Technical Series Webinar

Jerome Henry
jerhenry@cisco.com
June 2016
CCIE Webinar Series

- Technical Sessions – focused on new technologies
- 4 – 6 Sessions per year
- OpenStack – May 2015
- Fog Architecture – August 2015
- Cisco NetFlow and Big Data Analytics for Cybersecurity – October 2015
- OpenStack Neutron Deep Dive – February 2016
- DNA Deep Dive – June 2016

https://learningnetwork.cisco.com/community/archived_events/ccie-community-events
Never Received an Invitation? Opt-In

http://mkto.cisco.com/CCIE-Opt-In.html
Cisco DNA: Deep Dive
Cisco Digital Network Architecture

Network-enabled Applications

Cloud Service Management
- Policy | Orchestration

Automation
- Abstraction & Policy Control from Core to Edge

Analytics
- Network Data, Contextual Insights

Virtualization
- Physical & Virtual Infrastructure | App Hosting

Open & Programmable | Standards-Based

Open APIs | Developers Environment

Cloud-enabled | Software-delivered

Principles

Insights & Experiences

Automation & Assurance

Security & Compliance

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
What’s New: Cisco DNA Innovations

**APIC-EM Automation Platform**
- Completely New Platform
  - Available Now
- Base Automation: **Plug and Play**
  - Available Now
  - *Cloud version Controlled Availability, May 2016*
- Policy Services: **I WAN App & Easy QoS**
  - Available Now | March 2016, respectively

**Enterprise NFV**
- Branch Service Virtualization
  - Controlled Availability, March 2016

**CMX Cloud**
- Presence Analytics and Connect
  - Available Now, globally as local laws permit

Available on DNA-Ready Infrastructure through Cisco ONE Software
Evolution to a Policy Model

- **Express Business Intent**
- **Translate** into device specific policy/configuration
- **Leverage Abstraction** (the controller knows about the device specifics)
- **Automate the Deployment** across the Network
- **Insure Fidelity to the Expressed Intent** (keep everything in sync)

User policy based on user identity and user-to-group mapping

De-coupling of **User Identity** and **Topology**

Much easier to translate **business objectives** to network functionality—**Lowers TCO**

**Policy based Configuration**—**Dynamic**, able to be automated** by the Controller

**Over time—Policy grows, static shrinks**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Today</th>
<th>Controller-based Automation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
Controller-Led Networking
Bridging the Gap to Increased Success in Network Deployment and Use

Any given “custom” configuration has a very high probability of not being tested exactly as deployed “individually—as a one off…” which introduces potential issues...

The automated configuration deployed by the controller will have gone through...

- **Joint development** by the Cisco Product Teams, the Architects developing Best Practices, and the Controller Team—“Blessed Configurations”
- **Testing by Cisco’s Solution, System, and Devtest teams** against the deployment use cases developed jointly, above
- And will be deployed by 1000’s, with any unforeseen situations addressed ASAP due to widespread and standardized deployment

**Automation**
Controller-Led Networking Deployment

- **Risk**
- **Bugs**
- **Uncertainty**
- **Trust**
- **Problems**
- **Combinatorial Issues…**

Greatly increased probability of success
Deploy, Report, Measure, Adjust, Repeat

Applications
Network
Endpoints

Automated Deployment

Instrumentation Telemetry Correlation
Run Reports
Deliver relevant content
Discover user insights

Analytics

Measure and Adjust
Click here to Correct
Always Correct this way (and never ask me again)
Embracing Tools

- Python
- Linux Applications
- Saltstack
- Openstack
- Ansible
- Chef
- Puppet
- OpenTSDB
- Splunk
- Tcollector

DevOps Orchestration  Automation  Monitoring/Analytics
What does this mean for You? (if you are old school networking)

- Hardware is specialized
- SW is tailored for specialized HW and functions
- Each device, each function is configured individually (and manually)

Hardware company spirit:
What does this mean for You?

(if you are old-school networking)

- Network has places and functions
- Still need efficient HW, but:
  - Functions need to be flexible (add a function, not a box)
  - Well-known tasks should be automated (tell me your business intent, the tool takes care of the details)
  - Visibility into the flows allows you to improve your operations
  - Deploy and manage as your business needs (centralized, distributed, standalone)

Most customers just want a coffee:
Choose your function, press, done.
DNA Under-the-Hood
Automation: Plug and Play

Cloud-Based Plug and Play

Order
Plug in and Cloud Provision
Controller-Based Management

Lower deployment costs

79%

“Plug and play means no more IT engineers in the field – faster time to market and dramatically lowered costs.”

Eliminates

Staging
Truck Roll

New!

Cisco ONE Foundation

PnP Available Now
PnP Cloud May 2016
(controlled availability)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
PnP: Pre-provision & Discover

1. Pre-provision
   N-PnP App pre-provisioned w/ device SR#
   N-PnP app on APIC-EM

2. Discovery
   Configure device discovery
   • DHCP Option-43 or DNS

3. Secure Deployment
   • Installer powers-on devices
   • Devices securely downloads Image and Configuration

1. Discovery
   Configure device discovery
   • DHCP Option-43 or DNS

2. Un-claimed Devices
   Installer powers-on devices
   • Devices securely connects to APIC-EM Server, waiting to be ‘Claimed’

3. Secure Deployment
   • Network admin claims devices based on device information
   • Device downloads Image and configuration

Plug & Play
Enterprise-wide Scale
Automated workflow
1. Pre-provisioning
Step 1a: Create Site

Step 1a. The network admin creates a site for any new deployment on the Cisco® APIC-EM PnP app.

Name the site and click “Create”
1. Pre-provisioning

Step 1b: Upload IOS Image File

“Upload” allows to save the image in APIC-EM. Once uploaded, the image is available across sites.

“Images” tab allows to upload/manage images for the devices.

All available images, previous uploads, and new uploads will be listed here.
1. Pre-provisioning

Step 1c: Upload Configuration File

“Upload” saves the configuration in APIC-EM. Once uploaded, the configuration is available across sites.

“Configurations” tab allows to upload/manage the configurations for the devices.

All available configurations, previous uploads, and new uploads will be listed here.
1. Pre-provisioning

Step 1d: Create device entry

- If any external TFTP server is used for configurations and images, for a given site information must be entered here. This is not recommended.

- Drag and drop the device configuration here as a txt file or select from uploaded configurations.

- Select the image from an available list already loaded into the APIC-EM.

- Step 1d.
  - Create a device entry for the site created
  - Add device Serial number
  - Map Image (Optional) and Configuration file
3. Device Deployment
Step 3a: DHCP based server discovery

- The device after authentication & authorization establishes Secure communication with PnP server
- The network admin remotely monitors the status of installation while in progress

Remote Installer
- Mount and cable devices
- Power on

The device receives PnP Server (APIC-EM) IP from DHCP option 43
3. Device Deployment

Step 3a: Optional - DNS based server discovery

- The network admin remotely monitors the status of installation while in progress.
- Optionally, devices resolve hostname ‘pnpserver.localdomain’ to get PnP Server (APIC-EM) IP address.
- The device after authentication & authorization establishes secure communication with PnP server.

Installer

- Mount and cable devices
- Power on

Remote Installer

- DNS Server
- PnP Server
3. Device Deployment

Step 3b: Monitor device installation

Click on “Details” to see full workflow details in APIC-EM

Step 3b. Verify installation of devices

Once devices get config, image, and certificates, the APIC-EM will show the device as provisioned.
APIC-EM IWAN is more than PnP

**Day 0**
**Plug-and-Play App**
Zero touch deployment of routers / switches / APs
Accelerated roll-out: Eliminates tech visits and shrinks deployment from months to minutes

**Day 1**
**Cisco IWAN App**
Guided, fast auto-provisioning of IWAN solution with Cisco experts’ best practices
From 1000 CLI commands to 10 GUI clicks per branch

**Day 2**
**Path Trace App**
Discover path between two end points based on 5-tuple flow
Rapidly troubleshoot network issues and lower OPEX for trouble tickets
Applications can ALSO interact with APIC-EM via Northbound APIs, informing the network of application-specific and dynamic QoS requirements.
New: APIC-EM QoS Automation - Easy QoS

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Client A calls Client B</td>
</tr>
<tr>
<td>2.</td>
<td>CUCM calls APIC-EM to setup Policy</td>
</tr>
<tr>
<td>3.</td>
<td>QoS Policy enabled on network device</td>
</tr>
</tbody>
</table>

**Optimal Experience**

Dynamic QoS in 250 ms
Reduce voice jitter by 300%
50% improvement for video traffic
Determining Business Relevance

How Important is an Application to Your Business?

Relevant
- These applications directly support business objectives
- Applications should be classified, marked and treated marked according to industry best-practice recommendations
  - RFC 4594

Default
- These applications may/may not support business objectives (e.g. HTTP/HTTPS/SSL)
- Applications of this type should be treated with a Default Forwarding service
  - RFC 2474

Irrelevant
- These applications do not support business objectives and are typically consumer-oriented
- Applications of this type should be treated with a “less-than Best Effort” service
  - RFC 3662
EasyQoS GUI

Step 1: Select a Scope for Policy Application
EasyQoS GUI

Step 1: Select a Scope for Policy Application
EasyQoS GUI

Step 2: (Optional) Change Application Business-Relevance
EasyQoS GUI

Step 3: (Optional) Add Custom Applications
Security: StealthWatch and ISE

Extend Security Everywhere

Wi-Fi  Core  WAN  Cloud

Network as a Sensor:
Real-time situational awareness and rapid threat detection everywhere

Infrastructure-Enforced Policy

Network as an Enforcer:
Software-defined segmentation with TrustSec® for assurance and compliance

Rapid Threat Containment

Quickly detect and stop threats
Scales to handle dramatic threat increase

“The network touches every element of the digital enterprise – every business process, device, customer, employee – and therefore has the unique ability to detect, analyze, and prevent new forms of attack by flagging unusual network behavior.”
Network as a Sensor (NaaS) Solution overview

Collection & Behavior Analysis

The StealthWatch FlowCollector collects and analyzes data from various flow sources.

Enrichment with Global Threat Intelligence

Correlated flow data collected in (1) with a global threat feed (SLIC)

Unmatched Threat Protection

Additional threat context by revealing what infected hosts are doing within the network.
Flexible Netflow = Wealth of Information

Router# show flow monitor CYBER-MONITOR cache

... IPV4 SOURCE ADDRESS: 192.168.100.100
IPV4 DESTINATION ADDRESS: 192.168.20.6
TRNS SOURCE PORT: 47321
TRNS DESTINATION PORT: 443
INTERFACE INPUT: Gi0/0/0
IP TOS: 0x00
IP PROTOCOL: 6
tcp flags: 0x1A
interface output: Gi0/1.20
counter bytes: 1482
counter packets: 23
timestamp first: 12:33:53.358
timestamp last: 12:33:53.370
ip dscp: 0x00
ip ttl min: 127
ip ttl max: 127
application name: nbar secure-http
...
Enable Netflow in 3 easy steps

1. Configure Exporter
   **Where to Send**
   This is usually IP Address of StealthWatch FlowCollector

2. Configure Flow Record
   **What to Send**
   Traffic flow record can be customized to include certain fields from flow record

3. Configure Monitor
   **Apply to Send**

Router(config)# flow exporter my-exporter
Router(config-flow-exporter)# destination 172.27.1.1

Router(config)# flow record my-record
Router(config-flow-record)# match ipv4 destination address
Router(config-flow-record)# match ipv4 source address
Router(config-flow-record)# collect counter bytes

Router(config)# interface s3/0
Router(config-if)# ip flow monitor my-monitor input
Locating Services and Application

Search for assets based on transactional data:
Ex. Protocol (HTTP Servers, FTP Server, etc)

Identify servers and assets
Full Context Visibility

Username

Active directory details

View Flows

Devices and sessions
NaaE (TrustSec)

Segmentation based on roles
• Not based on IP addresses, VLANs etc

Role based on context
• AD, LDAP attributes, device type, location, time, access methods, etc...

Use Tagging technology
• To represent logical group (Classification)
• To enforce policy on switches, routers, firewalls

Software Defined
• Policy managed centrally
• Policy provisioned automatically on demand
• Policy invoked anywhere on the network dynamically

Along with authentication, various data is sent to ISE for device profiling

Classification Result:
Device Type: Apple iPad
User: Mary
Group: Employee
Corporate Asset: No

Personal Asset SGT

ISE (Identity Services Engine)
NFV: Why Virtualization for the Enterprise Network?

**Mobility**
Mobile traffic will exceed wired traffic by 2017

**IoT**
IoT Devices will triple by 2020

**Analytics**
76% of companies planning to or investing in Big Data

**Cloud**
80% of organizations will primarily use SaaS by 2018

**Multiple Devices**
Routers, Appliances, Servers

**Difficult to Manage**
Device integration and operation

**Costly to Operate**
Upgrades, refresh cycles, site visits

Mobile traffic will exceed wired traffic by 2017.
IoT Devices will triple by 2020.
76% of companies planning to or investing in Big Data.
80% of organizations will primarily use SaaS by 2018.

Multiple Devices: Routers, Appliances, Servers

Difficult to Manage: Device integration and operation

Costly to Operate: Upgrades, refresh cycles, site visits
Introducing: Cisco Enterprise NFV
Network services in minutes, on any platform

Enterprise Service Automation (ESA) on APIC-EM

Network Functions Virtualization Infrastructure Software (NFVIS)

ISR 4000 + UCS E-Series  UCS C-Series  COTS

Virtual Router (ISRv)  Virtual Firewall (ASA)v  Virtual WAN Optimization (vWAAS)  Virtual Wireless LAN Controller (vWLC)  3rd Party VNFs
Freedom of Choice
Cisco Intelligent Branch

Traditional

Physical Router
ISR 4000 Series

Centralized Services
Fixed Integrated Services
Conservative

Enterprise NFV

Physical Router Virtual Services
ISR 4000 Series + UCS E-Series

Upgradable H/W
Deterministic Routing Performance
Late Adopter

Virtual Router Virtual Services
UCS C-Series/COTS

Elastic Routing and Services
Performance
Early Adopter

Cisco ONE
Access to Ongoing Innovation
License Portability
Investment Protection
Power in Software
NFVIS Software Stack

- Linux
- Interface Drivers
- Platform Drivers
- Virtualization Layer – Hypervisor & vSwitch
- Health Monitor
- CLI
- NETCONF
- REST
- HTTPS
- Orchestration API
- APIC-EM/Prime
- Plug-n-Play Server
- Console /SSH
- YANG
- Device Web Portal
- Plug-n-Play Client

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
Automated Orchestration, Management, Policy

Enterprise Service Automation (ESA)

- Zero-touch deployment
- Automated orchestration of platform and VNFs
- Service chaining and licensing

- Health monitoring
- Dynamic scaling of services
- Operational SLA management

- Create standard profiles for different types of branches
- Cisco tested and validated designs
- Embedded approval process and versioning

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
ESA Intelligent Template Selection & Management

- Goal: create branch architecture profiles based on Business INTENT
- Prescriptive or customized templates
- Intent derived by intelligent template selection based on CVD questions
  - Internet access characteristics
  - Bandwidth
  - Wireless
  - ...
- ESA proposes suitable templates
Branch Profile Design
Enterprise Service Automation

1. Upload Devices to be shipped
2. Upload the Branch locations
3. Custom Design a Profile
4. Select functions
5. Pick validated topologies
6. Associate the templates & attributes
7. Map to Branch(s)
Digital Services: CMX Cloud

Customer Insights and Engagement

Data on Storefront
Conversion
Frictionless
Guest Onboarding

Presence Analytics

Zone-based location analytics

Connect

Drag-and-drop customizable portal on demand

“CMX Cloud has helped us quickly gain business insights, so we can enhance the shopper experience at Santana Row with easy Wi-Fi onboarding, increased customer data, and improved customer engagement.”

Available Now

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public
How CMX Cloud Works – WLC 8.2 (today)

Built on the Cisco Unified Access Platform

Access Points → WLAN Controller → CMX Cloud (10.x)

- Generate Customer Insights
- Increase Mobile Engagement
- Boost Customer Satisfaction

Web auth redirect → nmsp

WLAN Controller

Connector (Proxy)

https

Presence Analytics Data

Connect Captive Portal
How CMX Cloud Works - WLC 8.3 (Summer)
Built on the Cisco Unified Access Platform

Future WLC versions will have native proxy functionality and not require external box.

Generate Customer Insights
Increase Mobile Engagement
Boost Customer Satisfaction
### The Cisco Validated Design (CVD) program Enhanced for DNA!

**Cisco Validated Design Program**

<table>
<thead>
<tr>
<th>Design Guide</th>
<th>Deployment Guides &amp; Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>The “What &amp; Why”</td>
<td>The “How”</td>
</tr>
</tbody>
</table>

**Reference Network Architecture(s)**

- Campus LAN and Wireless LAN Design Guide
- Enterprise Security Baseline for LAN, Wireless LAN, and WAN
- Campus LAN L2 Access with Simplified Distribution Deployment
- Cisco WAN Design Guide
- Intelligent WAN Technology Design Guide
- Internet Edge Design Guide
- User-to-Data-Center Access Control Using TrustSec
- IWAN Application Optimization using Cisco WAAS and Akamai Connect Technology Design Guide
- Easy QoS Design Guide

Training for a Next Generation Network

**Educate**
- Technology Tracks
- Learning Paths
- DevNet Zone
- Roadshows and Pop-up Events

**Enable**
- DevNet membership
  - 350,000+
- Getting Started and API Reference Guides
- Sample Applications
- Community and Pay-for Developer Support

**Integrate**
- 300+ Network Partners and Growing
- 1500+ Solutions
- 250+ Compatible Network Solutions
- Cisco® Professional Services
  - 2500+ Partners Strong

**Structured Training**
- DevNet Express
- Structured Training
  - eLearning
  - Instructor-Led
  - 40+ DevNet Learning Labs

**Certification Program**
- Coming in 2017
- 40+ Developer Sandboxes
- 9800+ Developers
- 4400+ Companies

**Cisco® Professional Services**
- 2500+ Partners Strong

**Sample Applications**
- 1500+

**DevNet Zone**

**Roadshows and Pop-up Events**

**Certification Program**
- Coming in 2017

**DevNet Express**
- Structured Training
  - eLearning
  - Instructor-Led
  - 40+ DevNet Learning Labs

**Certification Program**
- Coming in 2017
- 40+ Developer Sandboxes
- 9800+ Developers
- 4400+ Companies

**Cisco® Professional Services**
- 2500+ Partners Strong

**Sample Applications**
- 1500+

**DevNet Zone**

**Roadshows and Pop-up Events**

**Certification Program**
- Coming in 2017
- 40+ Developer Sandboxes
- 9800+ Developers
- 4400+ Companies

**Cisco® Professional Services**
- 2500+ Partners Strong

**Sample Applications**
- 1500+
Questions