Introduction to Software-Defined Networking (SDN) and Network Programmability

Jason Davis / Distinguished Engineer (Services)
BRKRST-1014
• What is SDN & Network Programmability
• Use Cases and Problems Solved with SDN
• Cisco’s solutions
• Overview of DNA & ACI
• The Impact to IT Service Management
• How to Get Ready
Cisco Webex Teams

Questions?
Use Cisco Webex Teams (formerly Cisco Spark) 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 Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

Webex Teams will be moderated by the speaker until June 18, 2018.

cs.co/ciscolivebot#BRKRST-1014
Abstract

SDN is an exciting new approach to network IT Service Management. You may have questions about SDN, Controllers, APIs, Overlays, OpenFlow and ACI. You may also be wondering what products and services are SDN-enabled and how you can solve your unique business challenges and enhance your differentiated services by leveraging network programmability.

In this introductory session we will cover the genesis of SDN, what it is, what it is not, and Cisco's involvement in this space. Cisco’s SDN-enabled Products and Services will be explained enabling you to consider your own implementations. Since SDN extends network flexibility and functionality which impacts Network Engineering and Operations teams, we'll also cover the IT Service Management impact.

Network engineers, network operation staff, IT Service Managers, IT personnel managers, and application/compute SMEs will benefit from this session.
What is Software-Defined Networking (SDN)?

- An approach and architecture in networking where control and data planes are decoupled and intelligence and state are logically centralized.
- An enabling technology where underlying network infrastructure is abstracted from the applications [network virtualization].
- A concept that leverages programmatic interfaces to enable external systems to influence network provisioning, control and operations.
SDN is...

...an approach to *network transformation*

...empowering *alternate, non-traditional entities to influence network* design and operations

...impacting the networking industry - *challenging the way we think about engineering, implementing and managing networks*

...providing new methods to interact with equipment/services via *controllers, APIs*

...normalizing the interface with equipment/services

...enabling high-scale, rapid network and service provisioning/management

...providing a catalyst for traditional Route/Switch engineers to branch-out

* [...not the first attempt!]*
SDN is *not*...

...an easy button... [but is intending to make things easier for all!]

...a panacea or end-state

...narrowly defined

...meaning the death of network engineers*

...a mandate for all network engineers to become C and Java programmers*

...a new ISDN service from Apple called iSDN 😊

...a new attempt at network evolution...

* [...but...how do you distinguish yourself and your career?]
Have We Seen This Before?

Overlays / Encapsulations
- MPLS
- VPLS
- VPN
- GRE Tunnels
- LISP

Control Plane / Data Plane Separation - Centralized Control
- SS7
- ATM LANE
- Wireless LAN Controller
- GMPLS

Management and Programmatic Interfaces
- SNMP
- NETCONF
- EEM
Where Did SDN Come From?

Have you tried rebooting the Internet yet?

Clean Slate Program

We created Clean Slate Program more than five years ago with Stanford’s depth and breadth of expertise to explore what kind of Internet we would design if we were to start with a clean slate and 20-30 years of hindsight. Though the mission was well defined, the potential approach was not. We began with a number of small exploratory projects that led to a few flagship projects that show lots of promise.

We are pleased to report that Clean Slate Program led to many small projects and the following four on-going flagship projects that have the potential to transform different parts of the Internet.

- Internet Infrastructure: OpenFlow and Software-Defined Networking
- Mobile Internet: PMIPv6 2010
- Mobile Social Networking: NextSocial
- Data Center: Stanford Experimental Data Center Lab

Clean Slate Program has ceased to exist as of January 2012 and has successfully transformed into these four large projects. We invite you to visit the website of these projects, become familiar and get involved.

http://cleanslate.stanford.edu/
The Traditional Network...

Control and Data Plane resides within Physical Device

Control plane learns/computes forwarding decisions
Data plane acts on the forwarding decisions
The Network As It Could Be…to an SDN ‘Purist’

Control plane becomes centralized
Physical device retains Data plane functions only
The Network As It Could Be…In a ‘Hybrid SDN’

A Controller is centralized and separated from the Physical Device, but devices still retain a localized Control plane intelligence.
Use Cases and Problems Solved with SDN
Use Cases: Network Programmability

**Research/Academia**
Experimental networking algorithms and technologies

**Massively Scalable Data Center**
Customize with Programmatic APIs to provide deep insight into network traffic

**Cloud**
Automated provisioning and programmable overlay

**Service Providers**
Policy-based control and analytics to optimize and monetize service delivery

**Enterprise**
Virtual workloads, Segmentation, Orchestration of security profiles

**Diverse Requirements Across Segments**
(Automation & Programmability)
SDN Addresses Needs for…

- Centralized configuration, management/control, monitoring of network devices (physical or virtual)
- Ability to override traditional forwarding algorithms to suite unique business or technical needs
- Allowing external applications or systems to influence network provisioning and operation
- Rapid and scalable deployment of network services with life-cycle management
Why Change?

• Familiar Manual, CLI-driven, device-by-device approach is inefficient

• Increased need for programmatic interfaces which allow faster and automated execution of processes and workflows with reduced errors

• Need for a ‘central source of truth’ and touch-point
Business Metrics Influencing Routing

- Class Schedule
- Staff Directory
- API
- GUI
- Controller
- WAN1 (MPLS)
- WAN2 (EPL)
- WAN3 (Internet)
- Main Campus
- Remote Classroom
Get Chat Messages From Routers/Switches

NSO bot (@sparkbot.io) | 5/4/17, 10:53 AM
CPO Integration with NSO PROVISIONED the Service named “Jason Test 1” for Job 93 at 5/4/2017 10:53:14 AM with results “Created / 201” in 28.2 seconds
CPO Integration with NSO TESTED the Device "CSS-38" with result
SIGNALING-ENB: Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

You | 5/4/17, 10:54 AM
Hey Team, Chuck went into the DC with a laptop and console adapter, FYI

NSO bot (@sparkbot.io) | 5/4/17, 10:58 AM
**ALERT!** User nso1 made an unauthorized configuration change to device CSS-38 at May 4 20:28:10.970 IST [Review](#)

NSO bot (@sparkbot.io) | 5/4/17, 10:59 AM
Network Administrator “admin” approved the unauthorized config change to device CSS-38. NSO has merged it with the latest archive.
What is OpenFlow?

...a Layer 2 communications protocol that gives access to the forwarding plane of a network device, ...
...a specification for building switches conforming to the protocol
What Makes OpenFlow Different?

### Flow Table

<table>
<thead>
<tr>
<th>Ingress Port</th>
<th>Source MAC</th>
<th>Dest MAC</th>
<th>Ether Type</th>
<th>VLAN ID</th>
<th>VLAN Priority</th>
<th>IP SRC</th>
<th>IP DEST</th>
<th>IP Protocol</th>
<th>IP TOS</th>
<th>TCP/UDP SRC</th>
<th>TCP/UDP DEST</th>
<th>Action</th>
<th>Priority</th>
<th>Counter</th>
</tr>
</thead>
<tbody>
<tr>
<td>3c:07:54:*</td>
<td>*</td>
<td>*</td>
<td>Switching</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Fwd Port 10</td>
<td>100</td>
<td>*</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Routing</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Fwd Port 12</td>
<td>100</td>
<td>*</td>
</tr>
<tr>
<td>Port 1</td>
<td>*</td>
<td>*</td>
<td>Replication/SPAN</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Fwd Port 14...24</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Firewall/Security</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>25</td>
<td>Drop</td>
<td>100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Inspection</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Controller</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>00:01:E7:*</td>
<td>*</td>
<td>*</td>
<td>Vlan10</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Fwd Port 8</td>
<td>200</td>
<td>80</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Combinations</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>0x0800</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>Rewrite 10.1.2.3; Fwd port 9</td>
<td>200</td>
</tr>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>Multi-action ; NAT</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>192.168.1.*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>10.*</td>
<td>Local</td>
</tr>
</tbody>
</table>

---

What Makes OpenFlow Different?

Flow Table

**Ingress Port**
- * (match any)

**Source MAC**
- * (match any)

**Dest MAC**
- * (match any)

**Ether Type**
- * (match any)

**VLAN ID**
- * (match any)

**VLAN Priority**
- * (match any)

**IP SRC**
- * (match any)

**IP DEST**
- * (match any)

**IP Protocol**
- * (match any)

**IP TOS**
- * (match any)

**TCP/UDP SRC**
- * (match any)

**TCP/UDP DEST**
- * (match any)

**Action**
- Fwd Port (port number)
- Drop
- Controller
- Rewrite
- Local handling

**Priority**
- 100

**Counter**
- * (match any)

---

**What Makes OpenFlow Different?**

Flow Table

- **Ingress Port**
- **Source MAC**
- **Dest MAC**
- **Ether Type**
- **VLAN ID**
- **VLAN Priority**
- **IP SRC**
- **IP DEST**
- **IP Protocol**
- **IP TOS**
- **TCP/UDP SRC**
- **TCP/UDP DEST**
- **Action**
- **Priority**
- **Counter**

---

**Example**

- Example: OF v1.0
What Is OpenDaylight?

• ...an open source project formed under the Linux Foundation to further the adoption and innovation of Software Defined Networking (SDN) through the creation of a common vendor supported framework.

• Focus: Customers with some programming resources that desire a free, community-supported SDN controller, especially if focus is on OpenFlow.
OpenDaylight Architectural Model

Releases

Hydrogen - February 2014
- 1.87M+ lines of code
- 28 Projects
- 256 Contributors

Helium - October 2014
- 28 Projects
- 256 Contributors

Lithium - June 2015

Beryllium - Feb 2016

Boron - November 2016

Carbon - May 2017

Nitrogen - Sept 2017

Oxygen - March 2018
OpenDaylight Contributions
ONAP

• ONAP (Open Network Automation Platform) - an open source software platform for the design, creation, orchestration, monitoring, and life cycle management of SDNs and Virtual Network Functions (VNFs)

• SP-initiated from ECOMP and Open-O, provides automatic, policy-driven interaction in cloud environment

• Maintained by the Linux Foundation

• November 2017 – Amsterdam Release

• May 2018 (expected) – Beijing Release

• https://www.onap.org/
ONAP Architecture

Source: https://wiki.onap.org/display/DW/Architecture
Other Aspects of SDN
### SDN Protocols in Networking

#### Application Frameworks, Management Systems, Controllers, ...

<table>
<thead>
<tr>
<th>&quot;Protocols&quot;</th>
<th>OpFlex</th>
<th>OpenFlow</th>
<th>I2RS</th>
<th>PCEP</th>
<th>BGP-LS/FS</th>
<th>Neutron</th>
<th>OMI</th>
<th>Puppet</th>
<th>NETCONF</th>
<th>Ansible</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF</td>
<td>Cisco</td>
<td>IETF</td>
<td>IETF</td>
<td>IETF</td>
<td>IETF</td>
<td>IETF</td>
<td>DMTF</td>
<td>IETF</td>
<td>IETF</td>
<td>IETF</td>
</tr>
</tbody>
</table>

#### Management
- BGP Diameter
- Radius
- SNMP

#### Orchestration
- OpenStack Agent

#### Network Services
- Neutron

#### Control
- PCEP Agent
- BGP-LS/FS Agent

#### Forwarding
- I2RS Agent
- OpenFlow Agent

#### Device
- Cisco API & Agent Infrastructure (YANG)
- Operating Systems – Cisco IOS / NX-OS / IOS-XR
Industry Communities, Projects and Standards Bodies

Technical Advisory Board seat

Technical Advisory Group Chair, Working Groups: Config, Hybrid, Extensibility, Futures/FPMOD/OF2.0

Puppet Agent Modules Puppet Labs investor

Contributor - Technical Committee Management Area Projects

Cisco Innovations: FEX Architecture 802.1 Overlay Networking Project

Founding Platinum member Catalyzed initial Open Source offering

Initiatives: Neutron API Donabe Cisco Innovations: OpenStack API for Nexus OpenStack Extensions

Overlay Working Groups: NVO3, L2VPN, TRILL, L3VPN, LISP, PWE3
Working Groups: NETCONF, ALTO, CDNI, XMPP, SDNP, I2AEX PCE, FORCES I2RS – Interface to Routing System

Open Network Research Center at Stanford University

Contributor - Technical Committee Management Area Projects

Open Daylight

Open Source Cloud Computing project

Technical Advisory Board seat

Technical Advisory Group Chair, Working Groups: Config, Hybrid, Extensibility, Futures/FPMOD/OF2.0

Puppet Agent Modules Puppet Labs investor

Contributor - Technical Committee Management Area Projects

Cisco Innovations: FEX Architecture 802.1 Overlay Networking Project

Founding Platinum member Catalyzed initial Open Source offering

Initiatives: Neutron API Donabe Cisco Innovations: OpenStack API for Nexus OpenStack Extensions

Overlay Working Groups: NVO3, L2VPN, TRILL, L3VPN, LISP, PWE3
Working Groups: NETCONF, ALTO, CDNI, XMPP, SDNP, I2AEX PCE, FORCES I2RS – Interface to Routing System

Open Network Research Center at Stanford University

Contributor - Technical Committee Management Area Projects

Open Daylight

Open Source Cloud Computing project
Overlays

Overlay / Virtual Network
- Mobile
- Scalable
- Supports Segmentation / multi-tenancy
- Programmable & Manageable

Underlay / Fabric
- High Capacity
- Resilient
- Intelligent Traffic Handling
- Programmable & Manageable
Layer-2 Overlays

- Emulate L2 LAN Segment
- Transport Ethernet Frames (IP and non-IP)
- Can emulate physical topologies
  - Single Subnet Mobility (L2 domain)
  - Exposure to L2 Flooding
Layer-3 Overlays

- Abstract IP-based connectivity
- Transport IP Packets
- Can emulate physical topologies
- Full Mobility regardless of subnet
- Contain Network Failures/Flooding
- Useful in abstracting connectivity and policy
The Edges of Overlays

**Network Overlays**
- Physical and virtual end-points
- Protocols for Resiliency & Loops: OTV, VXLAN, VPLS, LISP
- Traditional VPNs: OTV, VXLAN, VPLS, LISP

**Host Overlays**
- Virtual end-points only
- Single administrative domain
- Protocols: VXLAN, NVGRE, STT

**Integrated Overlays**
- Physical and virtual end-points
- Resiliency & Scale; Cross-org & Federation
- Open Standards: ACI
Network Overlay/SDN Humor

This is totally the future. All you folks with drivers licenses – sorry – your jobs are at risk.

Aaaah!! Why can’t I go any faster? I thought I had control?!?

I see smoke but there’s no warning lights on my dashboard! WTH?!?

Credit to Sean McGee
Software-Defined Access (SD-A)

- Design and implementation of Campus LANs using principles of SDN to *selectively forward and segment* without physical constraint, adhering to design intent
- Converged Wired and Wireless Network Architecture addressing Mobile Demand, IoT Growth and Security
- Policy following a user’s profile regardless of location; dynamic policy adjustments based on country/theatre
- Administration via a central controller, reduces provisioning times and eliminates manual configuration of branch routers
- Enabling network programmability through broad availability of APIs
Software-Defined Wide Area Network (SD-WAN)

- Design and implementation of WANs using principles of SDN to *selectively route traffic* (TE)

- Shift Traffic monitoring, service assurance and management from physical devices to (virtualized) applications

- Intelligence abstracted to virtual overlay -- enables private and public connections, automation, centralized network control, and agile, real-time traffic management over multiple links securely

- Enables administration via a central controller, reduces provisioning times and eliminates manual configuration of branch routers

- Enables network programmability through broad availability of APIs
Enabling SD-WAN

Transport-independent design
Intelligent path control
Application optimization
Secure connectivity

Dual MPLS
- Oracle
- Internet
- Public
- Branch
- SAP
- Highest SLA guarantees
  - Tightly coupled to SP
  - Expensive

Hybrid
- Enterprise
- VMware
- Citrix
- SAP
- More bandwidth for key applications
  - Balanced SLA guarantees
  - Moderately priced

Dual Internet
- Enterprise
- VMware
- Citrix
- SAP
- Best price/performance
  - Most SP flexibility
  - Enterprise responsible for SLAs
Network Function Virtualization (NFV)

Network infrastructure Services to run on Virtualized compute platforms

Key Enabler: using cloud technology to support network functions
- Hypervisor and cloud computing technology
- x86 compute hardware
- Network automation / orchestration

Benefits:
- Reduction in CAPEX and OPEX
- Faster service provisioning
- Service agility

SDN is complementary, but not mandatory – APIs, Controllers
Network Function Virtualization (NFV)

- Service provisioning from days to minutes
- From Cabling to Service Chaining
- Simple Logistics & Common Sparing
- Dynamic & Elastic Scale
- Seamless Integration with IP NGN
Virtualizing Network Functions

x86 vs. Custom Network Processing Unit (NPU)

Network Forwarding (L0–3)
- e.g. IPv6/v4, MPLS, VPNs, Optical
- High throughput / BW
- Stateless functions
- Mostly predictable traffic
- Many flows needing isolation, significant traffic management needed
- Interface-specific functions (2-stage forwarding)

Network Services (L4+)
- e.g. DPI, FW, CGN, BNG, Mobility S/PGW, AAA, DNS, DDOS
- Low to Med Throughput
- Stateful functions
- Unpredictable traffic
- # of flows (traffic management) – varies
- No interface-specific functions

Better fit for NPU
- Compute
- Bandwidth

Better fit for x86 (Virtualization)
- Compute
- Bandwidth
NFV – #1 Use-case

Virtual Route Reflector

Primary RR  Secondary RR
IPv4
IPv6
VPNv4
VPLS

Wide Area Network

8 RR chassis

Primary Server
Secondary Server
IPv4
IPv6
VPNv4
IPv6

Wide Area Network

2 Server Chassis 1 RR per VM

Better fit for x86
Cisco's SDN solutions
Cisco SDN: Providing Choice in Automation and Programmability

Application Centric Infrastructure

- Turnkey integrated solution with security, centralized management, compliance and scale
- Automated application centric-policy model with embedded security
- Broad and deep ecosystem

Programmable Fabric
DC / Campus / WAN

- DNA-C, APIC, VTS, Viptela
- 3rd party controller support
- VTS for software overlay provisioning and management across N2K-N9K

Programmable Network

- Modern Controllers with enhanced APIs
- Automation Ecosystem (Puppet, Chef, Ansible, ONAP, etc.)
- Feature-Rich APIs across portfolio

Mass Market
(commercial, enterprises, public sector)

Service Providers / Enterprise

Mega Scale Datacenters
DNA Center

- A purpose-built, easy to use SDN controller for Enterprise Campus Fabrics
- Design your network using intuitive work flows, starting with locations where your network devices will be deployed.
- Define user and device profiles that facilitate highly secure access and network segmentation based on business needs.
- Use policy-based automation to deliver services to the network based on business priority and to simplify device deployment.
- Combine deep insights with rich context to deliver a consistent experience and proactively optimize your network.
SD-Access Software Solutions

- DNA-Center
Cisco DNA Center Architecture

Cisco ISE Appliance

Cisco ISE

Identity Service Engine

Cisco DNA Center

Design | Policy | Provision | Assurance

DNA Center Appliance

SD-Access Fabric

Cisco Switches | Cisco Routers | Cisco Wireless

API / PxGrid

NETCONF
SNMP, SSH

Streaming Telemetry
NetFlow
Syslog
SNMP

AAA
RADIUS
EAPoL
SD-Access Hardware Solutions

- Catalyst 9300, 9400, 9500, 3650, 3850, 4500E, 6500, 6800 switches
- Industrial Ethernet 4000, 5000 switches
- Nexus 7000 Series switches
SD-Access Hardware Solutions

• 1000 & 4000 Series Integrated Services Router (ISR)
SD-Access Hardware Solutions

- Cisco Aironet 3800, 2800, 1850, 1830, and 1815 Series wireless access points
- Cisco 8540, 5520, and 3504 Wireless Controllers.
## SD-WAN / NFV Software Solutions

<table>
<thead>
<tr>
<th>Service Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Integrated Services Virtual Router (ISRv), ASA, vWLC, vWAAS</strong></td>
<td>Virtual Network Functions (VNFs)</td>
</tr>
<tr>
<td><strong>Enterprise Service Automation (ESA)</strong></td>
<td>a module to APIC-EM that automates Virtual Network Functions (VNFs) across multiple sites</td>
</tr>
<tr>
<td><strong>Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS)</strong></td>
<td>provides the Linux-based virtualization layer allowing addition of VNFs to the network with an integrated hypervisor and graphical user interface</td>
</tr>
<tr>
<td><strong>Cisco Virtual Managed Services (VMS)</strong></td>
<td>Automated end-to-end SD-WAN Services managed from the Service Provider Cloud</td>
</tr>
<tr>
<td><strong>WAN Automation Engine (WAE)</strong></td>
<td>Planning and Automation for application engineered routing and analysis</td>
</tr>
<tr>
<td><strong>Viptela</strong></td>
<td>Cloud managed SD-WAN solution for more complex virtualized or physical deployments</td>
</tr>
</tbody>
</table>
Enterprise Service Automation (ESA)
NFV for the Enterprise - Network services in minutes, on any platform

ESA

Virtual Router (ISRv)
Virtual Firewall (ASA v)
Virtual WAN Optimization (vWAAS)
Virtual Wireless LAN Controller (vWLC)
3rd Party VNFs

Network Functions Virtualization Infrastructure Software (NFVIS)

ISR 4000 & UCS E-Series
UCS C-Series
COTS
Enterprise Service Automation

Increase operational efficiency, reduce configuration errors, and improve compliance to standards and best practices.

- **Design**
- **Provision**
- **Manage**

**Devices**
- 117 Devices
  - Assigned 20
  - Unassigned 97
  - Error 0
- View All Devices

**Branches**
- 905 Branches
  - Provisioned 4
  - Unprovisioned 901
  - Error 0
- View All Branches

**Profiles**
- 4 Profiles
  - Approved 4
  - Unapproved 0
  - Error 0
- View All Profiles

**Approvals**
- 0 Approvals
  - Profile Approvals 0
  - Branch Approvals 0
- View All Approvals
Create New Custom Profile

- PHYSICAL
- NETWORK FUNCTIONS
- NF CONTAINERS
- OTHERS

Matching Templates
6 templates found

Topology
Search...

- vBranch-ISrv-FW-
  Relevance: 100%
- Virtual-ISrv-ASAv
- Virtual-ISrv-Only
- Hybrid-Small-VirtualBranch
- Virtual-SmallBranch
- Secured-Virtual-Branch

CiscoLive!

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

#CLUS

BRKRST-1014
Cisco SD-WAN Options
Choose Based on Budget, Expertise, Business Priorities

On Premises DIY
- Purchase, deploy, manage yourself with Cisco® APIC-EM and IWAN App/Prime™
- Maximum control over your network using a single tenant IWAN platform
- Utilize Cisco ONE™ Software for license portability running on Cisco IWAN products

Cloud Managed
- Cloud-based network mgt with Cisco Meraki® for SMB/Enterprises or Viptela for more complex deployments
- Real-time feature and security updates pushed from the cloud
- Subscription-based, using Meraki on-premises switching and security products or Viptela software & HW vEdge offerings

Virtual Managed Services (VMS)
- Deliver Cloud Managed IWAN from your Service Provider using VMS
- Secure multi-tenant platform, simplified NSO orchestration and tenant self-service
- Reduced CapEx, pay-as-you-grow OpEx, using Cisco IWAN and security products (physical and virtual)
Key Capabilities of Cisco’s **VMS Cloud Managed SD-WAN**

Optimized for **Ease of Management**

- Automated end-to-end SD-WAN Services managed from the Service Provider Cloud
- Secure multi-tenant Cloud Managed platform, simplified orchestration and tenant self-service
- SD-WAN created with Zero Touch Provisioning (PnP) and validated IWAN Service Packs (NSO)
- Rapidly create new monetized services, modify existing services instantly from Cloud
- Perfect for distributed customers looking for lower cost and self-managed SD-WAN options
Key Technologies in Cisco’s VMS Cloud Managed SD-WAN

Optimized for **Flexibility and Control**

- Add lower cost Internet and LTE branch links using simple, secure, active-active links
- Integrated compute, storage, voice, caching for branch consolidation and virtualization (x86)
- Scalable, 1000+ sites per IWAN tenant, each tenant can customize their IWAN service
- Customizable Intelligent path control based on PfRv3 for granular path selection
- Application classification using NBARv2, automated link monitoring (jitter, loss, latency)
WAE

Provides a cross-sectional view of traffic, topology, and equipment status.

Provides a predictive model that performs "what if" analyses of failure impacts.

WAE Planning evolved from the Cisco MATE software suite -- used in Service Provider networks for more than 10 years. Cisco WAE Automation combines smart data collection, modeling, and predictive analytics into an extensible API-based configuration platform.

Demand-Admission Requests
Coordinated Maintenance
Load-Balancing Label-Switched Paths
Application Engineered Routing
SD-WAN / NFV Hardware Solutions

- Cisco 4000 Series Integrated Services Router (ISR) with UCS E-series server module
- Cisco 5000 Enterprise Network Compute System (ENCS)
- Cisco ASR 1000 Series Router
- Viptela vEdge
- Meraki MX Appliance
Overview of Application Centric Infrastructure (ACI)
What Is APIC?

• The Data Center-centric SDN controller which is the unifying point of automation and management for the Application Centric Infrastructure (ACI) fabric.

• Offers services for managing System, Tenant(s), Fabric, VM(s), L4-7 Services in the Nexus 9K datacenter fabric

• NBI: REST, Python

• SBI: OpFlex ACI, REST, L4-7 Scripting API/VTY

• Focus: Data Center Customers that desire a Commercially-supported solution that leverages a centralized controller for the Nexus 9k product family
Centralized Automation and Fabric Management

- Unified point of data center network automation and management:
  - Application-centric network policies
  - Data model-based declarative provisioning
  - Application, topology monitoring, and troubleshooting
  - Third-party integration (Layer 4 - 7 services, storage, compute, WAN, etc.)
  - Image management (spine and leaf)
  - Fabric inventory
- Centralized access to all fabric information - GUI, CLI, and RESTful APIs
- Extensible to computing and storage management
Architecture

Network Applications
- Cisco Sourced
- Customers
- 3rd Parties

Cisco APIC-DC Controller
- Python
- RESTful

Northbound APIs
- RESTful

Southbound APIs
- REST
- L4-7 Scripting API / VTY

Controller Applications/Feature
- System Manager
- Tenant Manager
- Fabric Manager
- VM Manager
- L4-7 Services Manager

OpFlex
Cisco’s proposal to IETF to standardize a SBI for policy management

Advanced GUI with Extended Features

OpFlex/ACI Agent

Network Devices
- Cisco Nexus 9k Family
- F5
- Citrix Sourcefire

Web UI
RESTful over HTTP(s)

- JSON + XML
- **Unified**: automatically delegates request to corresponding components
- **Transactional**
- Single Management Entity yet fully independent components

Object Oriented

- **Comprehensive** access to underlying information model
- Consistent object naming directly mapped to URL
- Supports object, sub-tree and class-level queries
### System Health

**Nodes With Health <= 99**

<table>
<thead>
<tr>
<th>Node</th>
<th>Type</th>
<th>Health Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaf1</td>
<td>Leaf</td>
<td>90</td>
</tr>
<tr>
<td>Leaf2</td>
<td>Leaf</td>
<td>99</td>
</tr>
<tr>
<td>Spine1</td>
<td>Spine</td>
<td>90</td>
</tr>
<tr>
<td>Spine2</td>
<td>Spine</td>
<td>90</td>
</tr>
</tbody>
</table>

**Tenants With Health <= 99**

<table>
<thead>
<tr>
<th>Tenant</th>
<th>Health Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
<td>98</td>
</tr>
</tbody>
</table>

### Fault Counts By Domain

- **System Wide**: 0, 1, 7, 37, 216
- **Access**: 0, 0, 0, 182
- **External**: 0, 0, 0
- **Framework**: 0, 3
- **Infra**: 0, 194, 17
- **Management**: 0, 0
- **Security**: 0, 0
- **Tenant**: 0, 10

### Fault Counts By Type

- **Communications**: 0, 0, 182
- **Config**: 0, 135, 16
- **Environmental**: 0, 0, 11
- **Operational**: 0, 3
APIC – Topology/Connectivity
Management Access

GUI
CLI
Web
Object
Browser
Python
SDK
API Tools

Any APIC

https://apic.local/api/mo/uni/tn-common.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalMatch="1">
  <fvTenant childPolicy="" descr="" dn="uni/tn-common" lsId="local" modTs="2014-05-21T18:47:26.886+00:00" namePrio="" monPdDn="uni/tn-common/monepg-default" name="common" ownerKey="" ownerTag="" status="" uid="0"/>
</imdata>
```
API Inspector in GUI
Cisco Virtual Topology System (VTS)

- **Datacenter Overlay Provisioning and Management System**

- **Automates Overlay provisioning across Cisco Datacenter Top of Rack Nexus switches (Nexus 2K-9K), Virtual Switches & DCI routers**

- **Automates fabric provisioning for physical, bare metal, virtual machine and container workloads**

- **For container networking VTS integrates with Cisco Container Networking (CCN) based on Contiv/VPP**

- **Programmable using North Bound REST APIs**

- **Tighter Integration with Orchestration systems such as Openstack, vCenter and Cisco NSO**

**Simplified Management for Ease of Operations**
Network Services Orchestrator (NSO)

• A YANG model-driven software-based controller for configuration management and assurance
• Technology of July 2014 acquisition of Tail-f Systems
• Provides extreme amounts of network programmability
• Reduces network provisioning by normalizing configurations
• Models are focused on Devices and Services
Network Services Orchestrator (NSO)

- Logically centralized network services
- Data models for data structures
- Structured representations of:
  - Service instances
  - Network configuration and state
- Mapping service operations to network configuration changes
- Transactional integrity
- Multiprotocol and multivendor support
In Use at the CiscoLive Network
Impact to ITSM & How to Get Ready
SDN/Network Programmability Impact to ITSM

• External Programs (and App Developers) have access to traditional network devices – You Need to be Good with that!

• Change Control – Must Be More Real-Time – Programs/Apps are participating dynamically!

• You MUST have Focused, Intentional monitoring of the controllers – they are the brains and authoritative sources of truth, config, state

• You MUST have a Robust backup/redundancy plan for controllers

• You MUST implement Good RBAC, security and accounting – lock-down the controllers and APIs!

• The Uncle Ben Principle – “With Great Power Comes Great Responsibility”
What Happens to Element Management Tools?

Management and Orchestration Layer
- CPO
- UCSD
- PRIME INFRASTRUCTURE & NAM
- 3rd Party Apps

Control Layer
- Catalog/Provisioning
- Fault/Events
- User/Data Management
- Performance Monitoring
- Reporting/Analytics

Controller
- APIC
- DNA-C

Device Layer
- Cisco Devices
- Data Center, Enterprise Networks

Operational Intelligence
- Automated Service Provisioning
- Dynamic Service Assurance
- Visualization and Analytics

Network Intelligence
- Device Layer Abstraction
- Network Control
- Policy Enforcement and Network Change

CLI, NETCONF, OpenFlow, OpFlex API

REST API
So...Are All Network Engineers Becoming Programmers?

var myQuestion = { "question":"All Engineers Becoming Programmers?", "answer":true,false };
Remember This Inflection Point?

Telephony then…

And now!

• Approx 1998 IP Telephony struggled until we got ‘hybrid engineers’ to translate between the Circuit Switch ‘Tip & Ring’ and Packet Switch ‘Bits & Bytes’ camps

• Likewise, now, we need the next generation of ‘hybrid engineers’ to translate between traditional network domain engineers and software/application developers
What Skills Are Helpful to a Network Engineer Branching Out?

- Basic Programming constructs – Python (conditionals, loops, data structures)
- REST / Web Services [Postman]
- Regular Expression
- Data encoding – XML / XSLT; JSON
- Basic SQL
- Basic shell scripting – grep
- #1 – *Communicating Effectively with Programmers*
Job Roles: Cisco Network Programmability Evolution

System Engineer/Network Designer

Network Engineer

Support Engineer

Traditional Networking Infrastructure

Development Curriculum

Network Programmability Developer Specialist

Network Programmability Design & Implementation Specialist

Open Infrastructure

http://www.cisco.com/web/learning/certifications/specialist
# Network Programmability Cisco education offerings

<table>
<thead>
<tr>
<th>Course</th>
<th>Description</th>
<th>Cisco Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developing with Cisco Network Programmability (NPDEV)</td>
<td>Provides Application Developers with comprehensive curriculum to develop infrastructure programming skills; Addresses needs of software engineers who automate network infrastructure and/or utilize APIs and toolkits to interface with SDN controllers and individual devices</td>
<td>Cisco Network Programmability Developer (NPDEV) Specialist Certification</td>
</tr>
<tr>
<td>Designing and Implementing Cisco Network Programmability (NPDESI)</td>
<td>Provides network engineers with comprehensive soup-to-nuts curriculum to develop and validate automation and programming skills; Directly addresses the evolving role of network engineers towards more programmability, automation and orchestration</td>
<td>Cisco Network Programmability Design and Implementation (NPDESI) Specialist Certification</td>
</tr>
<tr>
<td>Programming for Network Engineers (PRNE)</td>
<td>Learn the fundamentals of Python programming – within the context of performing functions relevant to network engineers. Use Network Programming to simplify or automate tasks</td>
<td>Recommended pre-requisite for NPDESI and NPDEV Specialist Certifications</td>
</tr>
<tr>
<td>Cisco Digital Network Architecture Implementation Essentials (DNAIE)</td>
<td>This training provides students with the guiding principles and core elements of Cisco’s Digital Network Architecture (DNA) architecture and its solution components including; APIC-EM, NFV, Analytics, Security and Fabric.</td>
<td></td>
</tr>
</tbody>
</table>
Cisco Services

Services from Cisco Together with Cisco Certified Partners

- Cisco Data Center Services for Operations Enablement
- Cisco Readiness Planning
- Cisco Business Strategy
- Cisco Data Center Optimization Service
- Cisco Quick Start Services
- Cisco Accelerated Deployment Services
- Product Support, SMARTNet, Smart Net Total Care
Cisco Business Critical Services: New Capabilities

Analytics
- Trending, anomaly detection, KPI management, and preemptive and predictive recommendations
- Near real-time reporting via online portal

Automation
- Automated fault management: detection, collection, reporting, and notification
- Solution Validation automation and network replication

Compliance and Remediation
- Automated software upgrades and large scale configuration changes
- PCI, HIPAA, SOX. ISO, and other compliance audits

Security
- Threat Management: Incident response, threat hunting, and vulnerability assessments
- Strategy & Planning: Segmentation design, program maturity, and architecture assessments

Outcome: Informed decisions
Outcome: Lower complexity
Outcome: Reduced risk
Outcome: Threat protection
Technical Assistance From Cisco TAC
Resolve Issues Quickly

Direct Access to Cisco Technical Experts

- Highly trained network and application software engineers worldwide
- Expertise and best practices across data center technologies
- Computer science/electrical engineering degrees
- Engineering staff averages 5 years' industry experience
- CCIE professionals
- 24x7 global access by phone, web, or email

24x7
Cisco SDN: Providing Choice in Automation and Programmability

Application Centric Infrastructure

Turnkey integrated solution with security, centralized management, compliance and scale
Automated application centric-policy model with embedded security
Broad and deep ecosystem

Programmable Fabric DC / Campus / WAN

DNA-C, APIC, VTS, Viptela
3rd party controller support
VTS for software overlay provisioning and management across N2K-N9K

Programmable Network

Modern Controllers with enhanced APIs
Automation Ecosystem (Puppet, Chef, Ansible, ONAP, etc.)
Feature-Rich APIs across portfolio

Mass Market (commercial, enterprises, public sector) Service Providers / Enterprise Mega Scale Datacenters
Complete your online session evaluation

Give us your feedback to be entered into a Daily Survey Drawing.

Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Online.
Continue your education

- Demos in the Cisco campus
- Walk-in self-paced labs
- Meet the engineer 1:1 meetings
- Related sessions
Thank you
Acronym Decoder Ring [Aka Glossary]

- SDN -- Software Defined Networking
- BGP-LS – Border Gateway Protocol – Link State
- NFV – Network Functions Virtualization
- SS7 – Signaling System No. 7
- ATM LANE – Asynchronous Transfer Mode LAN Emulation
- GMPLS – Generalized Multi-Protocol Label Switching
- VPLS – Virtual Private LAN Service
- VPN – Virtual Private Network
- GRE – Generic Routing Encapsulation
- LISP – Locator/ID Separation Protocol
- SNMP – Simple Network Management Protocol
- NETCONF – Network Configuration Protocol [IETF Standard]
- EEM – Embedded Event Manager
Acronym Decoder Ring [Aka Glossary]

- CP – Control Plane
- DP – Data Plane
- CLI – Command-Line Interface
- API – Application Programmatic Interface
- GUI – Graphical User Interface
- OF – OpenFlow
- NAT – Network Address Translation
- TLV – Type-Length-Value
- PCEP – Path Computation Element (PCE) Communication Protocol
- I2RS – Interface To Routing System
- OTV – Overlay Transport Virtualization
- VXLAN – Virtual Extensible LAN
- REST – Representational State Transfer
- IDE – Integrated Development Environment
Acronym Decoder Ring [Aka Glossary]

- CA – Controlled Availability
- GA – General Availability
- EFT – Early Field Trial
- NVGRE – Network Virtualization using Generic Routing Encapsulation
- STT – Stateless Transport Tunneling
- ODL – OpenDaylight
- OSGi – Open Service Gateway Initiative
- NBI – North-Bound Interface
- SBI – South-Bound Interface
- iWAN – Intelligent Wide Area Network