Software Defined Networking Demystified

David Gierke and Lee Glenn
System Architects with Cisco

Thursday, October 3, 2019
DIR Technology Forum

Contact Info

David Gierke

dagierke@cisco.com

Tel: 210-787-9852

Lee Glenn

leglenn@cisco.com

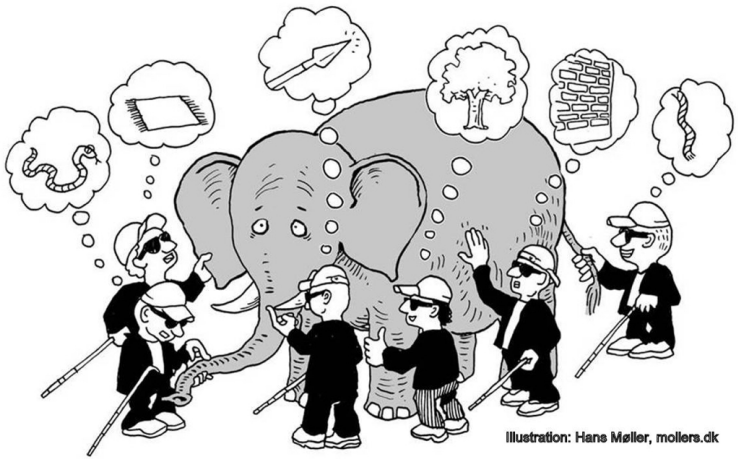
Tel: 734-658-0999

Abstract

SDN is an exciting new approach to network IT Service Management. You may have questions about SDN, Controllers, APIs, Overlays, and OpenFlow. 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. SDN-enabled solutions 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 *alternative, 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!]

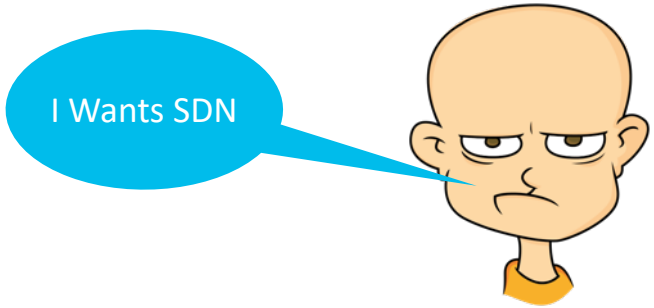
…a panacea or end-state

…narrowly defined

…meaning the death of network engineers*

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

…a new 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

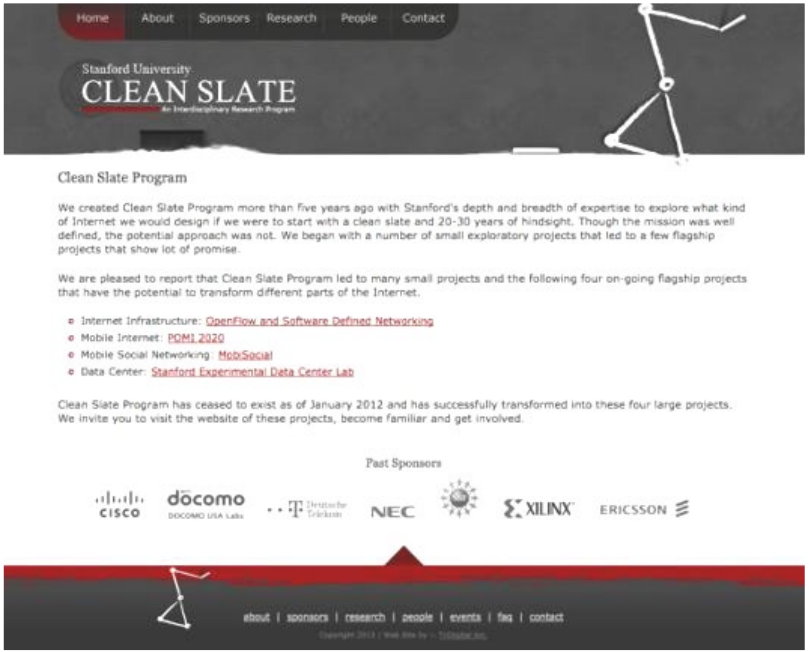
Management and Programmatic Interfaces

SNMP
NETCONF
EEM

Where Did SDN Come From?

Have you tried rebooting the Internet yet?

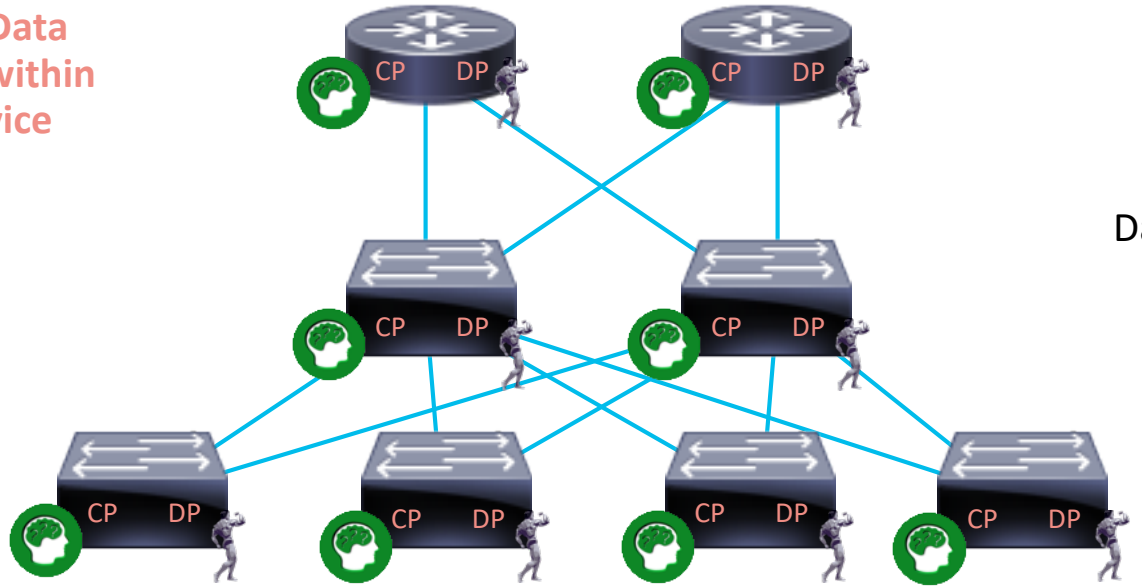
2008



http://cleanslate.stanford.edu/

The Traditional Network…

Control and Data Plane resides within Physical Device

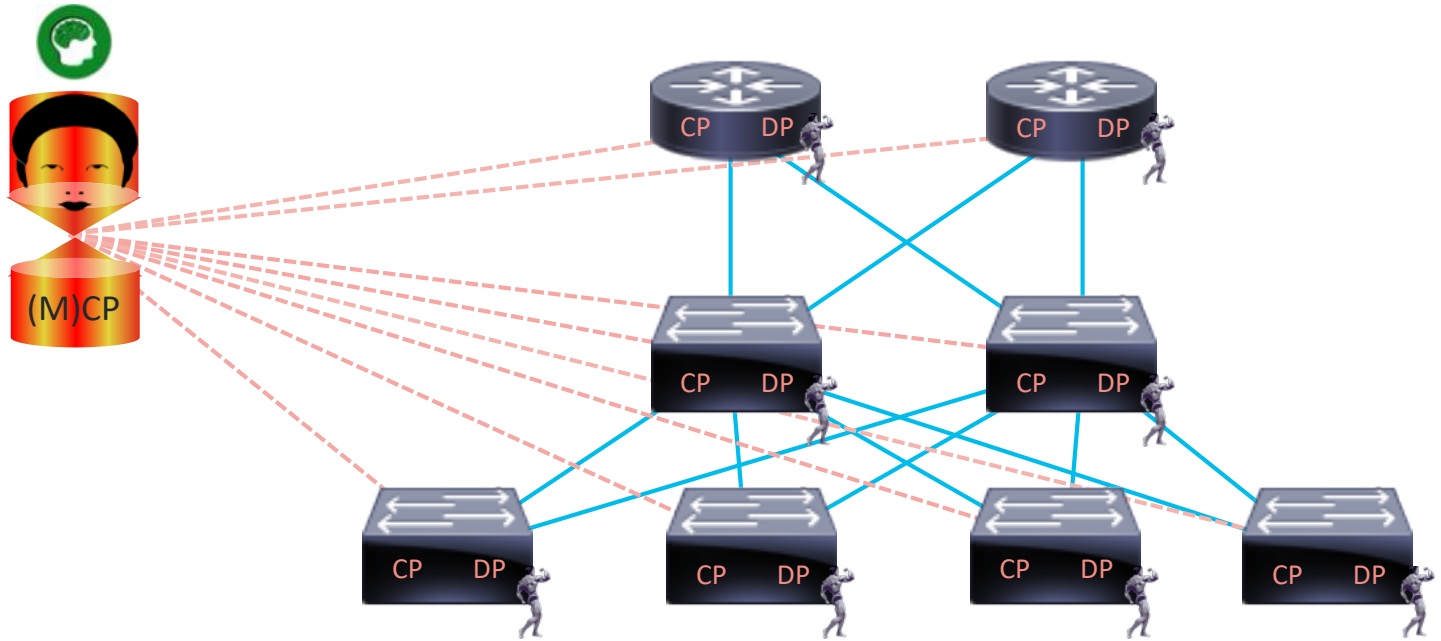


Control Plane (CP)

Data Plane (DP)

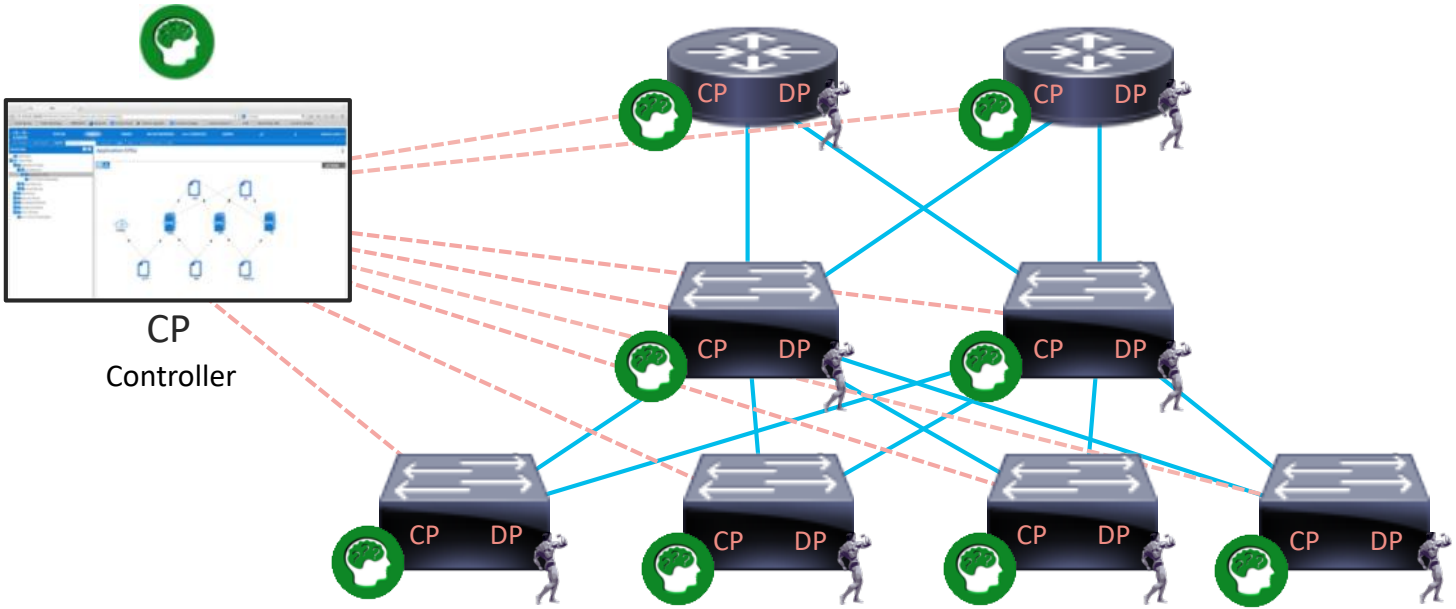
Control plane learns/computes forwarding decisions
Data plane acts on the forwarding decisions

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’



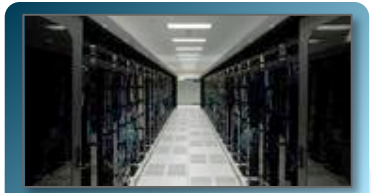
A Controller is centralized and separated from the Physical Device, but devices still retain a localized Control plane intelligence

Use Cases and Problems Solved with SDN

Use Cases: Network Programmability

Gov. Research/ Academia

Experimental networking algorithms and technologies

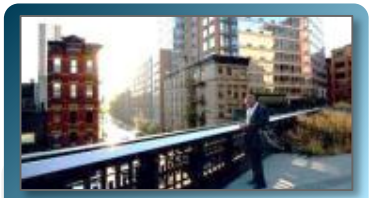


Massively Scalable Data Center

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

State Agencies

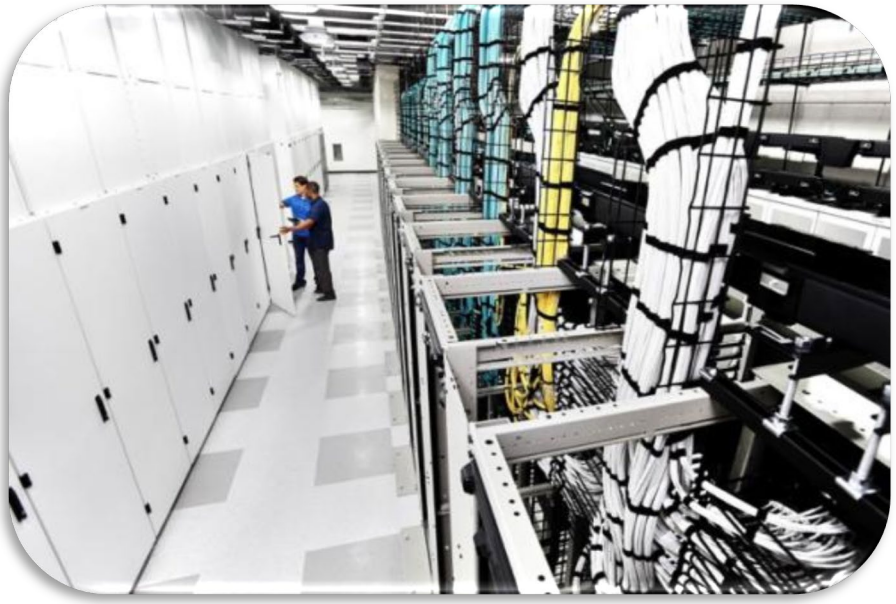
Virtual workloads, Segmentation, Orchestration of security profiles

Network Segmentation | **Network Flow Management** | **Scalable Multi-Tenancy** | **Agile Service Delivery** | **Private Cloud Automation**

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?

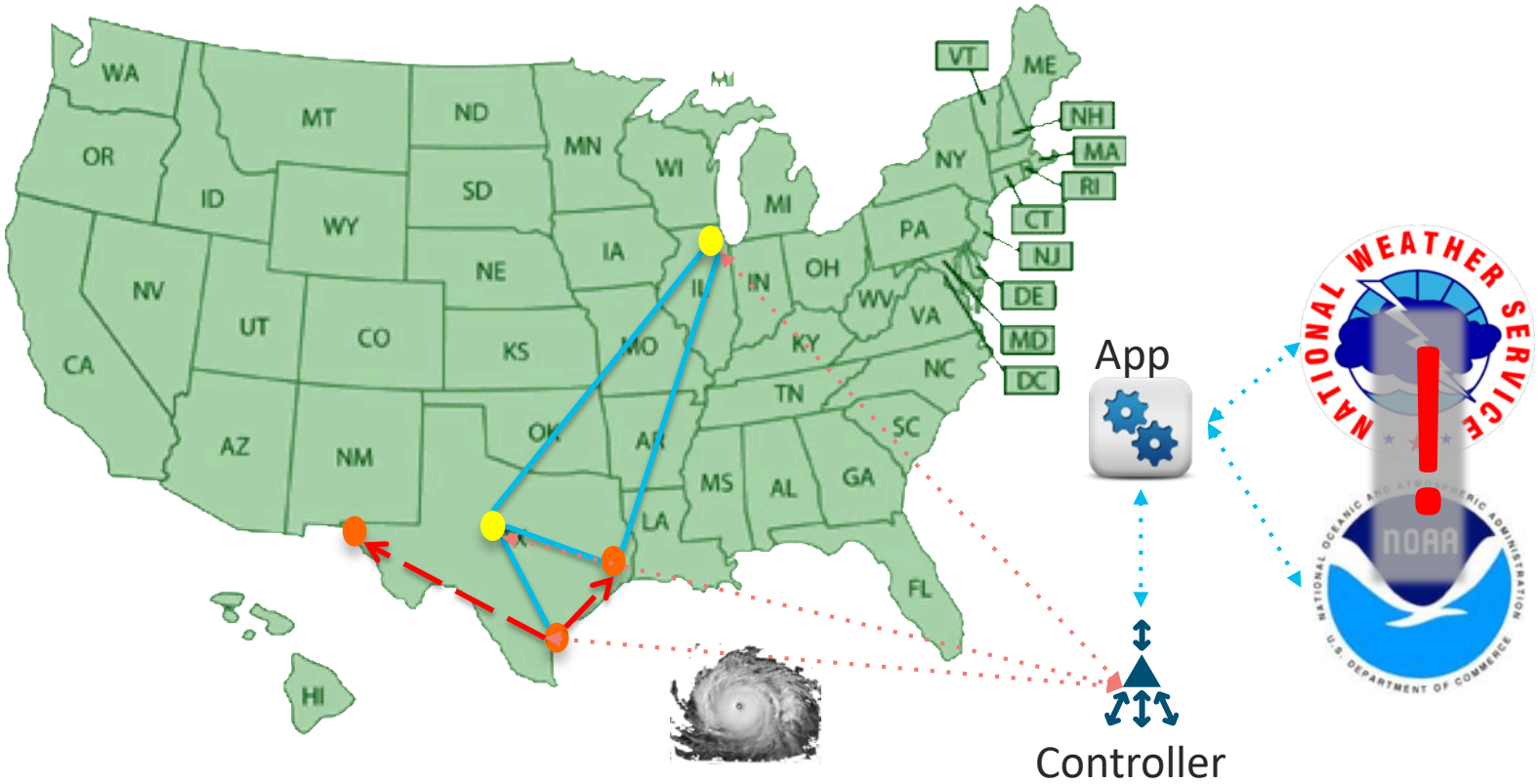
- Familiar Manual, CLI-driven, device-by-device approach is inefficient
- Increased need for programmatic interfaces which allow faster and automated execution of processes and workflows with reduced errors
- Need for a ‘central source of truth’ and touch-point

```
RP/0/RSP0/CPU0:CLNOC-ASR-1#show int Te0/0/0/0
Thu May  3 13:01:36.069 EDT
TenGigE0/0/0/0 is up, line protocol is up
  Interface state transitions: 1
  Hardware is TenGigE, address is 0042.5          (bia 0042.          )
  Layer 1 Transport Mode is LAN
  Description: Temp Lab Link to Colo
  Internet address is 128.107
  MTU 1514 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
     reliability 255/255, txload 0/255, rxload 0/255
  Encapsulation ARPA,
  Full-duplex, 10000Mb/s, LR, link type is force-up
  output flow control is off, input flow control is off
  Carrier delay (up) is 10 msec
  loopback not set,
  Last link flapped 6d01h
  ARP type ARPA, ARP timeout 04:00:00
  Last input 00:00:00, output 00:00:00
  Last clearing of "show interface" counters never
  5 minute input rate 69000 bits/sec, 70 packets/sec
  5 minute output rate 505000 bits/sec, 115 packets/sec
     35023394 packets input, 4688701110 bytes, 19 total input drops
     34982 drops for unrecognized upper-level protocol
     Received 18137 broadcast packets, 307061 multicast packets
              0 runts, 0 giants, 0 throttles, 0 parity
     304 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     47770857 packets output, 21895875641 bytes, 0 total output drops
     Output 17 broadcast packets, 0 multicast packets
     0 output errors, 0 underruns, 0 applique, 0 resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
```

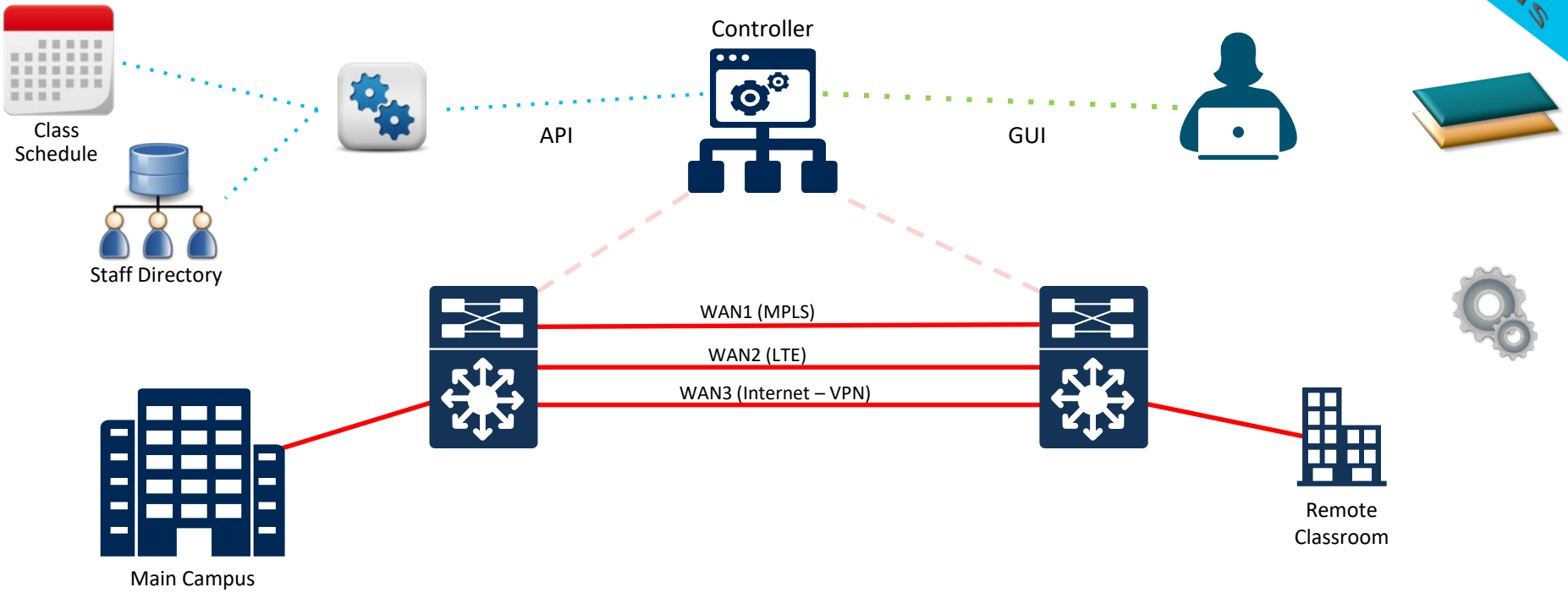
```
<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply message-id="4" xmlns="urn:ietf:params:netconf:base:1.0">
    <data>
        <xml-config-data> Building configuration...
            <Device-Configuration>
                <interface>
                    <Param>GigabitEthernet0/0</Param>
                    <ConfigIf-Configuration>
                        <ip>
                            <address><dhcp/></address>
                        </ip>
                        <duplex><auto/></duplex>
                        <speed><auto/></speed>
                    </ConfigIf-Configuration>
                </interface>
                <end></end>
            </Device-Configuration>
        </xml-config-data>
    </data>
</rpc-reply>]]>]]>
```

Weather-Based Routing

Innovation



Business Metrics Influencing Routing



Extending Functionality

Get Chat Messages From Routers/Switches

NSO bot (@teamsbot.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

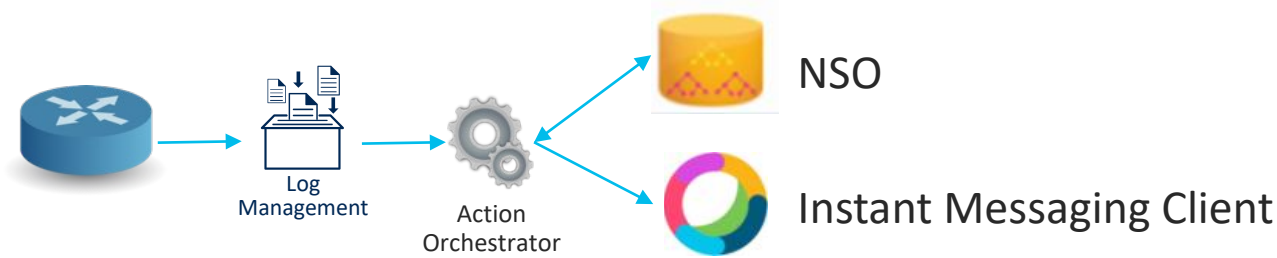
Hey Team, Chuck went into the DC with a laptop and console adapter, FYI

NSO bot (@teamsbot.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 (@teamsbot.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.



SD this, SD that

Overlays, NFV, SD-LAN, SD-WAN, SD-Datacenter

Industry Communities, Projects and Standards Bodies

Technical Advisory Board seat

802.1 Overlay Networking Project

Open Network Research Center at Stanford University

Puppet Agent Modules
Puppet Labs investor

Contributor - Technical Committee
Management Area Projects

Initiatives:
Neutron API
Donabe

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

Founding Platinum member
Catalyzed initial Open Source offering

Open Source Cloud Computing project

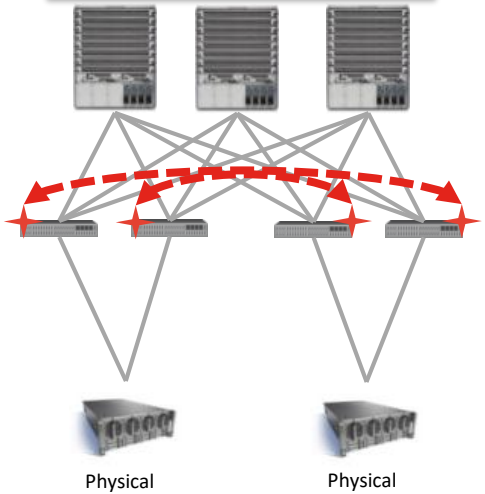
Overlay Working Groups:
NVO3, L2VPN, TRILL, L3VPN, LISP, PWE3
Working Groups:
NETCONF, ALTO, CDNI, XMPP, SDNP, I2AEX
PCE, FORCES
I2RS – Interface to Routing System

What is an Overlay?

Examples of Overlays

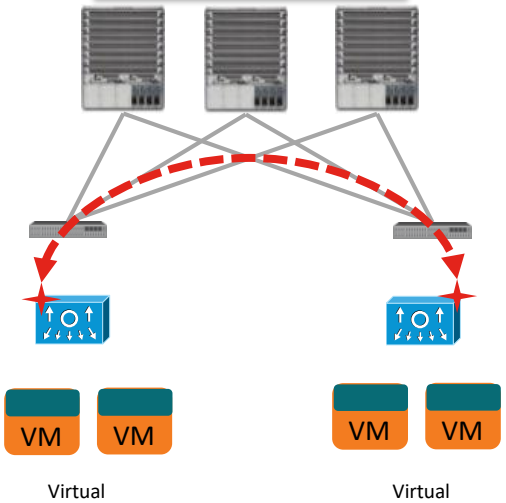
Tunnel End-Point

Network Overlays



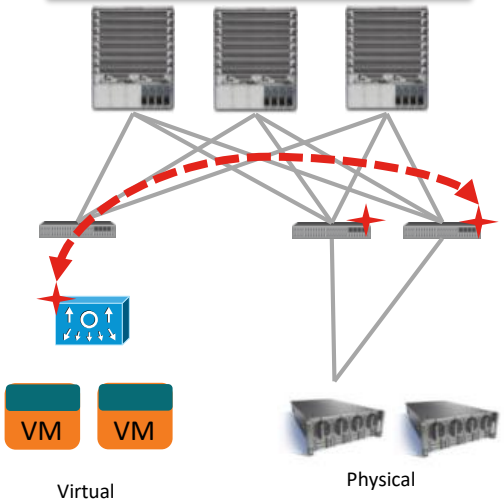
- Router/Switch end-points
- Protocols for Resiliency & Loops
- Traditional VPNs
- OTV, VXLAN, VPLS, LISP

Host Overlays



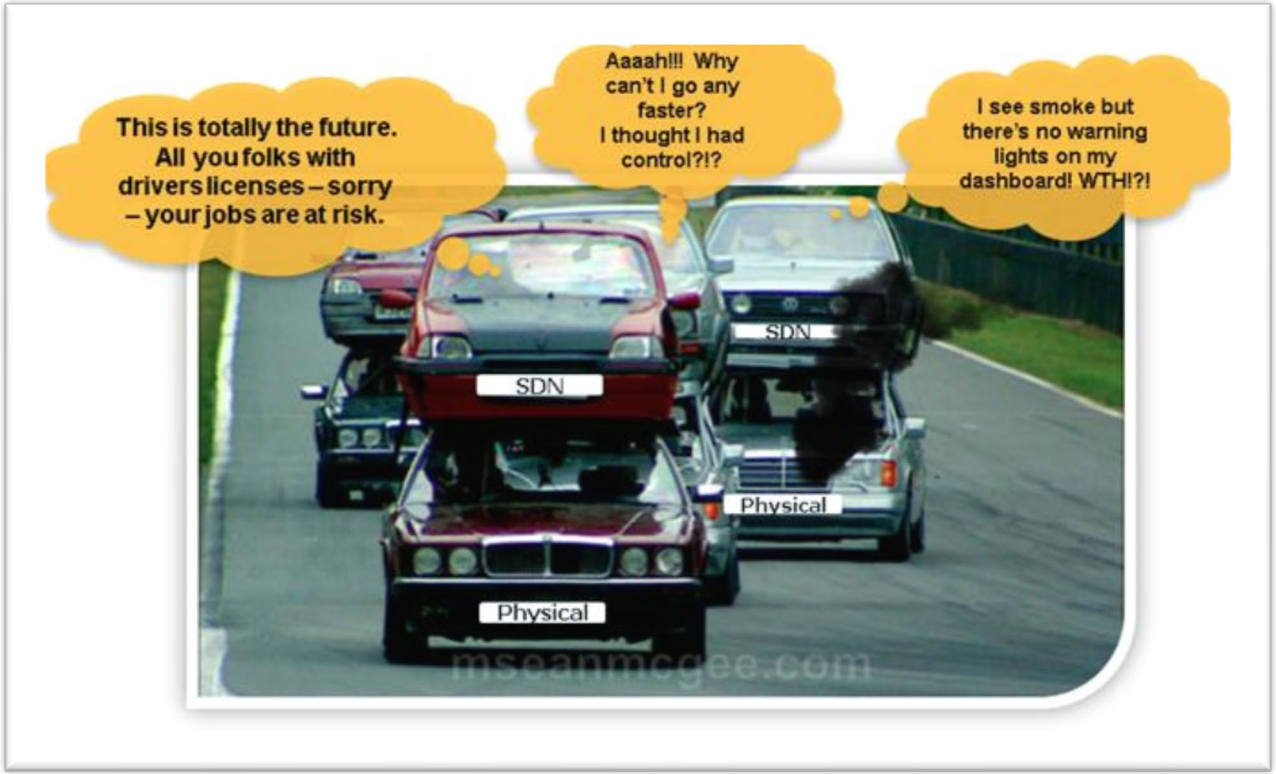
- Virtual end-points only
- Single administrative domain
- VXLAN, NVGRE, STT

Integrated Overlays



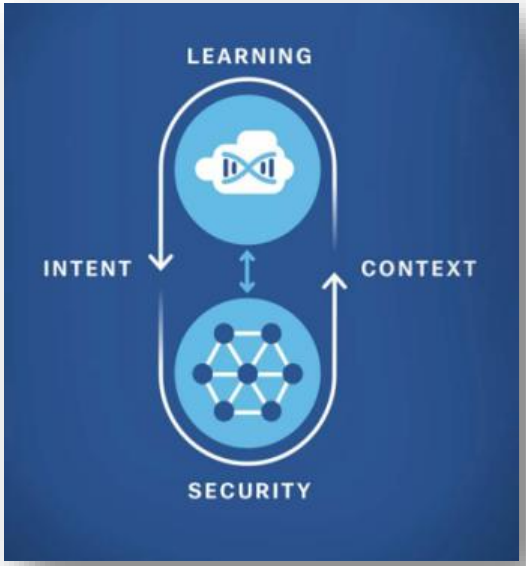
- Physical and virtual end-points
- Resiliency & Scale; Cross-org & Federation
- Open Standards
- ACI

Network Overlay/SDN Humor



SD-LAN
SD-WAN
SD-Data Center

Software-Defined LAN (SD-LAN)



- Design and implementation of Campus LANs using security policy to ***selectively forward and segment*** without physical constraint
- **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)

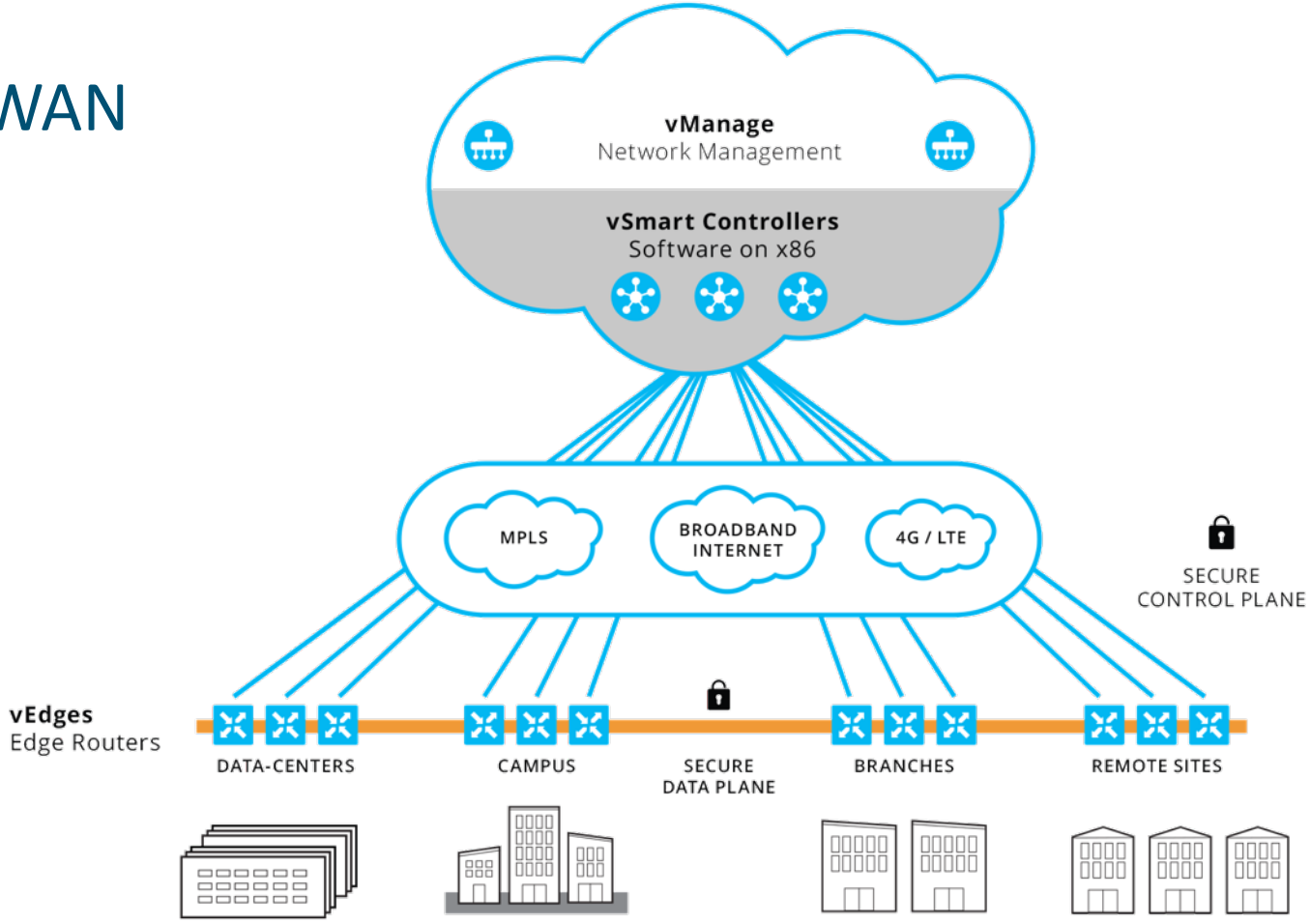
- Design and implementation of WANs using principles of SDN to ***selectively route traffic***

- 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

SD-WAN


vManage
Network Management
vSmart Controllers
Software on x86
MPLS
BROADBAND INTERNET
4G / LTE
SECURE CONTROL PLANE
vEdges
Edge Routers
DATA-CENTERS
CAMPUS
SECURE DATA PLANE
BRANCHES
REMOTE SITES

Enabling SD-WAN

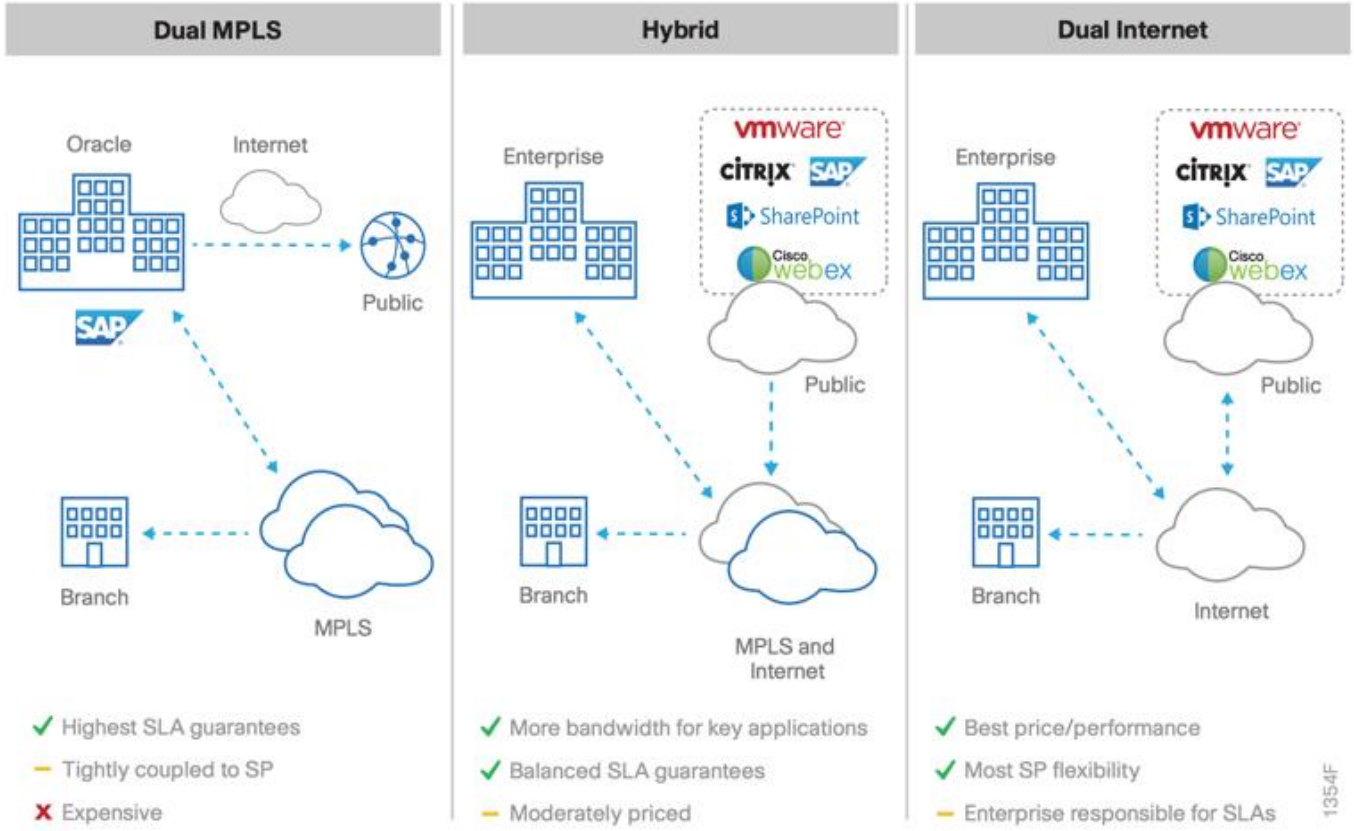
SECURE

Transport-independent design

Intelligent path control

Application optimization

SECURE!

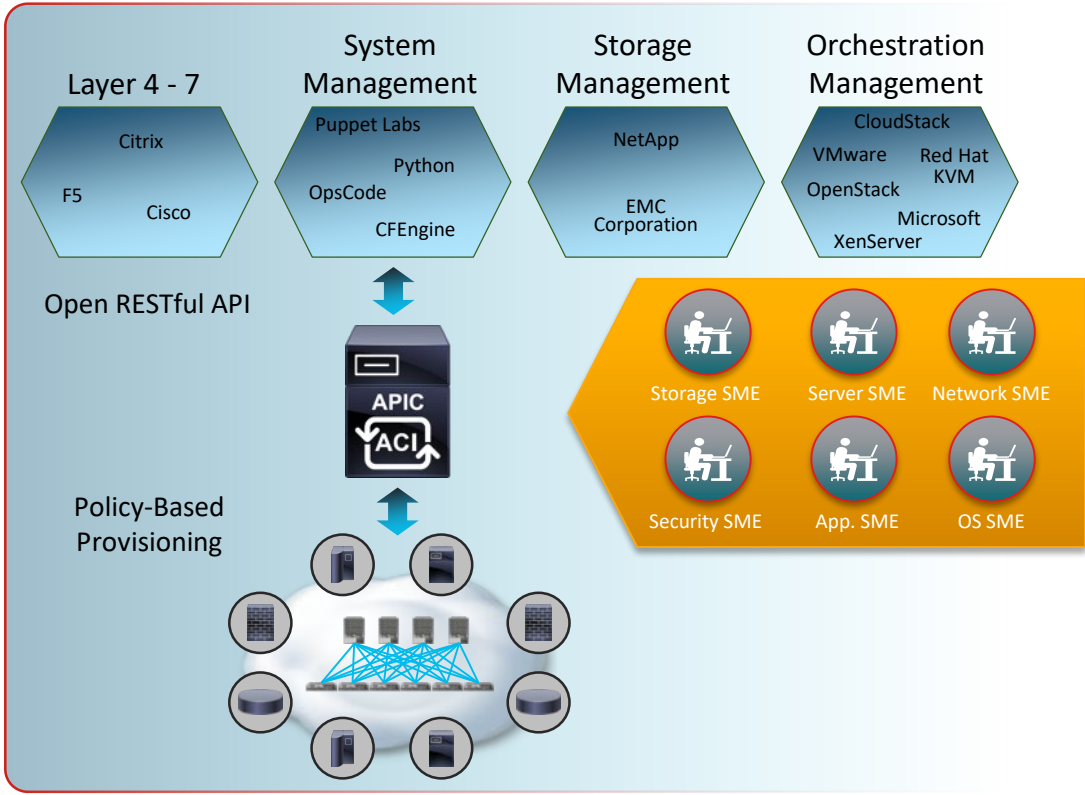


What Is SD-Data Center?

- Offers **services for managing** System, Tenants, Fabric, overlays, Virtual Machines, Containers, etc.
- **L4-7 Services** in the datacenter fabric
- **Extending datacenter policy** and fabric to Cloud providers (SaaS, IaaS, PaaS, etc.)
- North Bound Interface (**NBI**): REST, Python
- South Bound Interface (**SBI**): OpFlex ACI, REST, L4-7 Scripting API/VTY

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.)
- Centralized access to all fabric information - GUI, CLI, and RESTful APIs
- Extensible to computing and storage management



NFV

Network Function Virtualization (NFV)

Network infrastructure Services to run on Virtualized compute platforms

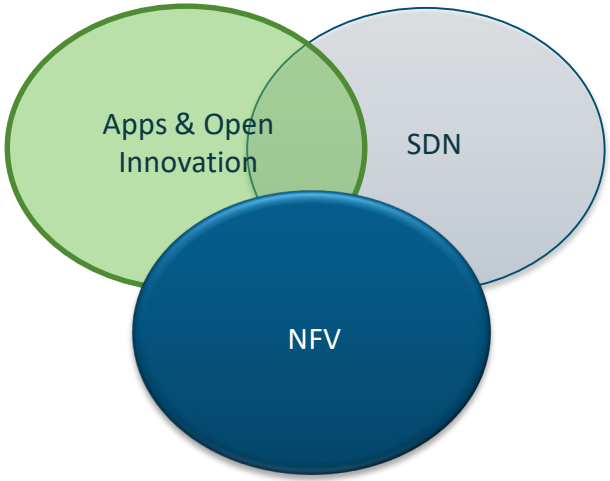
Key Enabler: using cloud technology to support network functions

- 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 Next Gen Network

SDN is Here –
Are You Ready?

SDN/Network Programmability Impact to Traditional Network

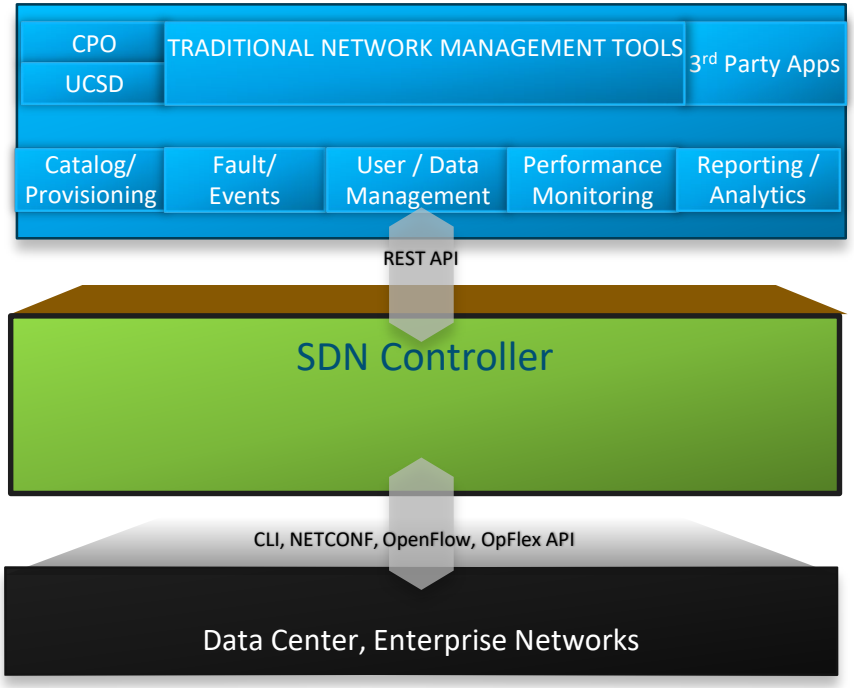
- External Programs (**and App Developers**) have access to traditional network devices – You Need to be Good with that!
- Change Control – **Must Be More Real-Time** – Programs/Apps are participating dynamically!
- You MUST have Focused, Intentional monitoring of the controllers – **they are the brains** and authoritative sources of truth, config, state
- You MUST have a **Robust backup/redundancy** plan for controllers
- You MUST implement good Roles Based Access Controls (RBAC), security and accounting – **lock-down the controllers and APIs**!
- Spiderman's Uncle Ben Principle - "With Great Power Comes Great Responsibility"

What Happens to the Tools I Already Have?

Management and Orchestration Layer

Control Layer

Device Layer



Operational Intelligence

Automated Service Provisioning

Dynamic Service Assurance

Visualization and Analytics

Network Intelligence

Device Layer Abstraction

Network Control

Policy Enforcement and Network Change

So…Are All Network Engineers Becoming Programmers?

var myQuestion = { ”question":”All Engineers Becoming Programmers?", ”answer":[true,false] };

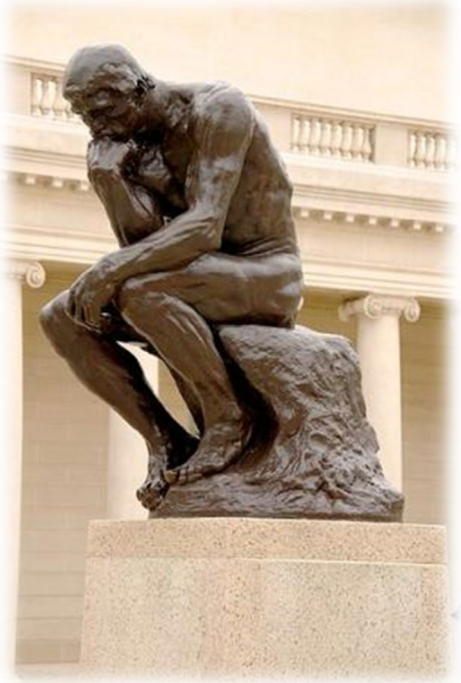
Remember This Inflection Point?

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: 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

Questions?

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