Open. Together.

OCP
SUMMIT

Executive Track

Network Services in a Multivendor Enterprise

Saikrishna Kotha
Director of Global Network Engineering and Operations
PayPal

PayPal

Agenda

- PayPal's Core Network Services
- Automation Architecture Pillars
- AZ2.0 - Leaf/Spine Network
- Monitoring fabric
- Infrastructure as a Code (IaC)
- Network Services – a pragmatic approach

Saikrishna M. Kotha

Roles/Responsibility @ PayPal:

- Director, Global Network Engineering & Operations
- PayPal's Global Payments Network is to provide secure, resilient and efficient global connectivity to PayPal customers, merchants partners and business units.

Educational & Overall Industry Experience:

- 15+ Years industry experience; worked for LinkedIn, Xilinx, Dell, Nortel, Ciena, CDOT…
- CAB Member: Cumulus, BigSwitch, Aporeto…
- Web-scale datacenter network architecture, design, delivery & operations
- Systems Strategy for both Datacenter/Enterprise Networks
- Total 25+ patents (issued/pending) focused in cloud networking, SDN, NFV areas.
- B.E (ECE); M.B.A

https://www.linkedin.com/in/saikrishnakotha/

PayPal's Core Network Services (CNS)

Provides a secure, reliable and efficient payments network to enable hybrid cloud deployments.

Current Network fleet:

- 1000's of devices
- Multi-generation, evolved…

Global backbone:

- POP locations, MPLS network
- HybridCloud, Extranet, Secure connectivity

Network Security:

- Least privilege access & regularity policy audits

Operating Systems/ Tech:

- 1G/10G/25G/40G/100G & MACSec encryption

Drivers for Network Strategy:

- Always on & secure: create strong foundation
- Growth/modernization: Network-as-a-Service
- Zero-touch-operations: Autonomous fleet

Network-as-a-Service:

- Business Intent
- LCM automation/APIs
- Operational SLA
- HybridCloud enablement

Autonomous Fleet:

- Programmability
- Anomaly driven telemetry
- Remediation factory
- Self-service enablement

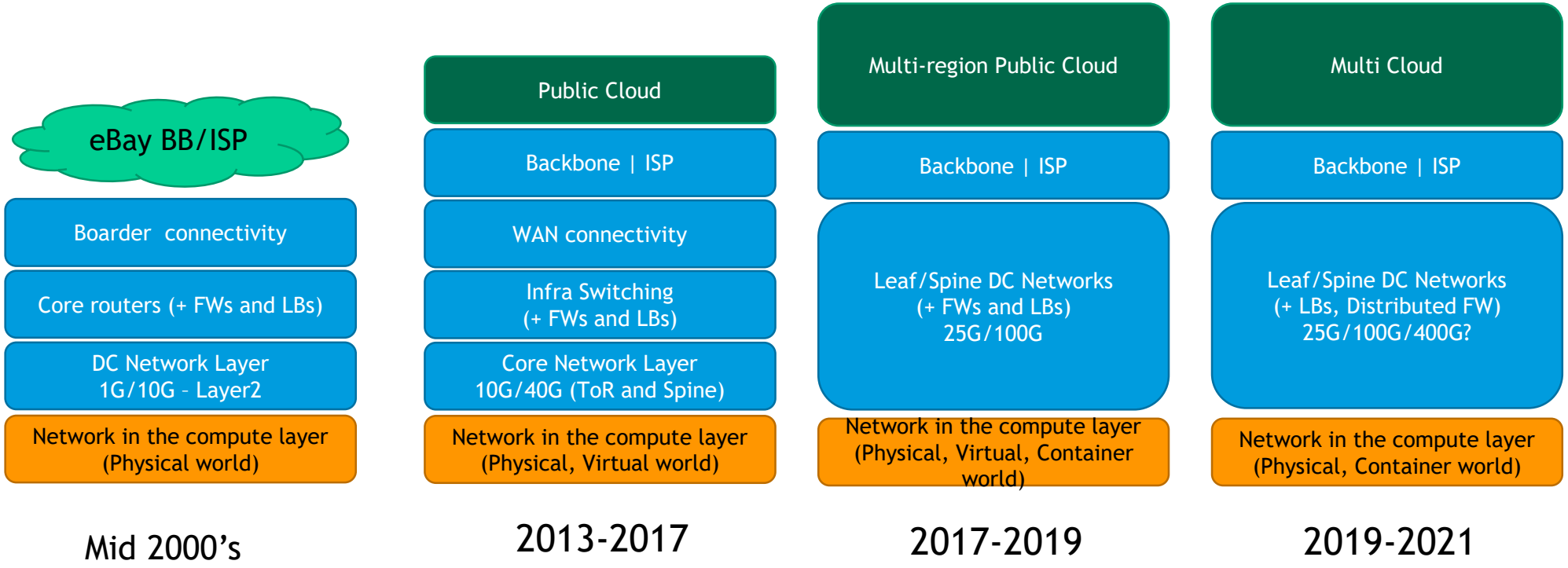
Love all traffic, Serve all Apps

Create Strong Foundation:

- Innovation centered standardization
- Drift avoidance
- Predictable reliability
- Enhanced enterprise tools Integration

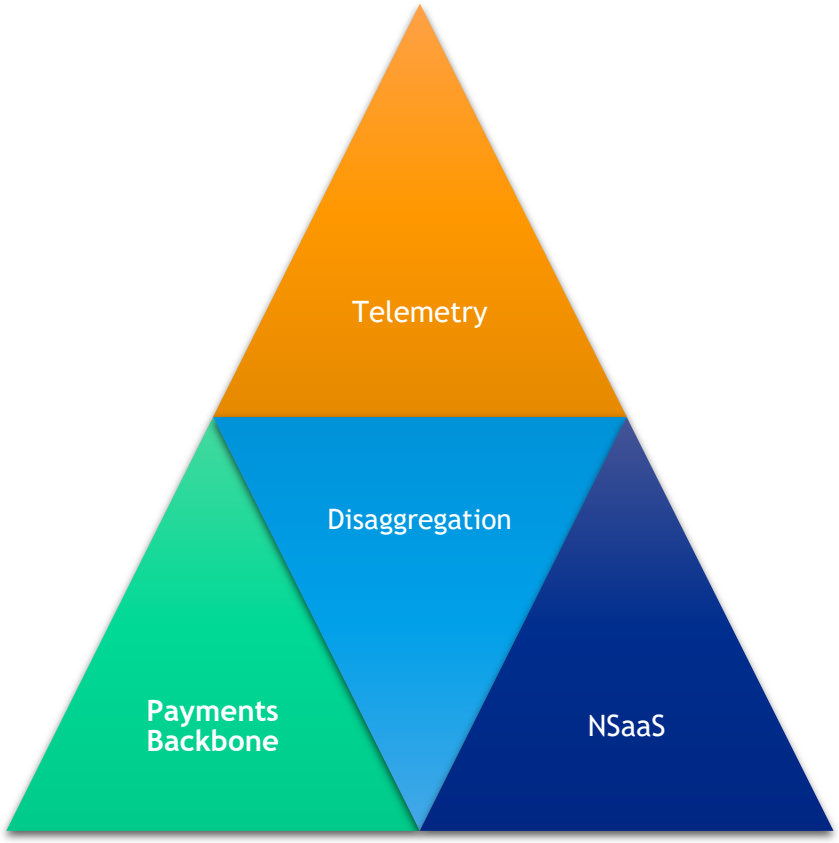
Network Designs Over The Years

It is a journey. Network stack evolved over the years ...



Core Network Services (CNS) –Architecture Pillars

Disaggregation, Secure Global Network, Zero Touch Everything



Powered by: CNS_Shell# programmability & visibility

Disaggregation Centered Networking Fleet:

- Disaggregation of network HW and SW innovation
- Cloud scale economics by leveraging white-box innovation
- Single SKU for DC network : context-based network functions

Network Security as a Service (NSaaS):

- Security as a services through programmability
- Security policy visibility/automation
- Distributed Firewall (DFW) for application level security

Global Payments Backbone as a Service:

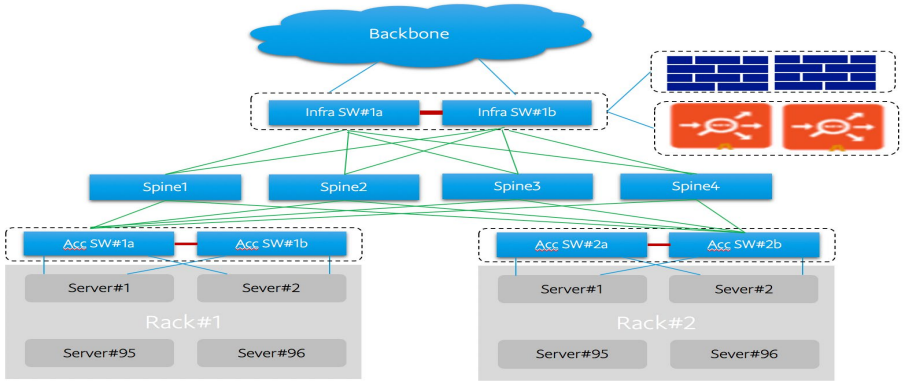
- Template based PoP designs; Extranet-as-a-Service
- Flow level visibility; low-latency global customer connectivity
- Multi-cloud/multi-region enablement

Telemetry Driven Core Network Services (CNS):

- Zero Touch Provisioning (ZTP): deployment agility
- Zero Touch Operations (ZTO): self-healing networks
- Anomaly driven telemetry: HealthChecks & DVR for CNS

PayPal Environment: Transforming DC Networks

Software Defined DC Network



Value Propositions:

- Reduce number of HW device types & spares
- Reduce network designs
- Common HW - leverage SW innovations from various vendors
- Financial Savings

Transformation approach:

- Leverage ASIC evolution through 1RU form factor
- Adopt common HW SKU/network design (leaf/spine)
- Adopt 3rd party optics and cables to work with all vendors
- Build life cycle management (LCM) for entire fleet
- Monitoring fabric comes standard
- Qualify dual vendors for each component:
  - Not to mix vendors in a given environment: for interop/stability reasons
  - Avoid supply chain shortages

AZ2.0 Network requirements

Next generation network build out

32x100G flex port platform

100G CWDM4 3rd party optics

Single mode fiber

40G to 4x10G breakout
100G to 4x25G breakout

HW simplification:

- Single SKU: 32x100G switch device
- Flex port speed: 100G/50G/25G/10G network
- White-box switching OS powered
- Optics & cable consolidation: 3rd party optics/cables

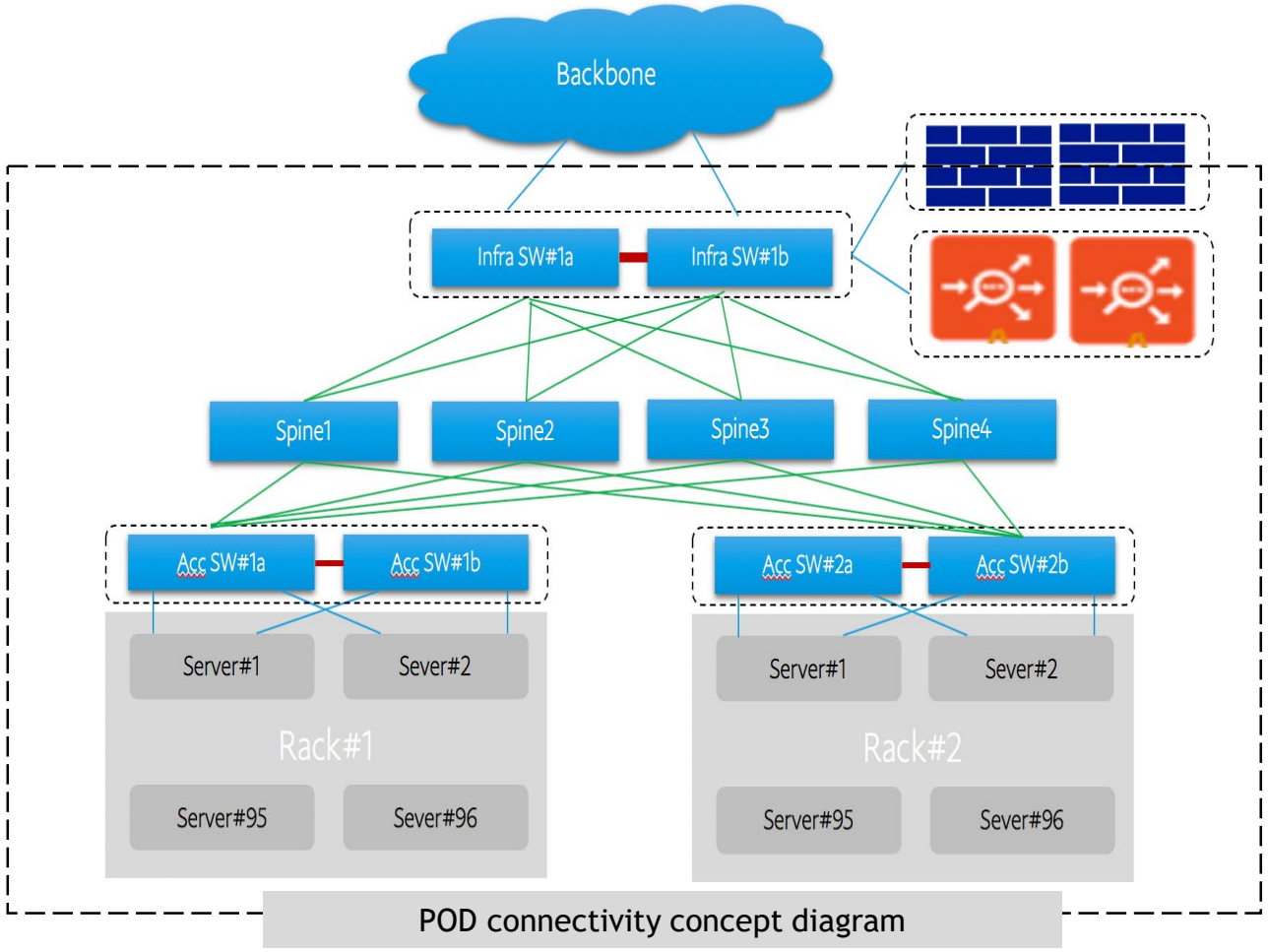
Design goals:

- Extensible leaf/spine architecture: Bubble concept
- Eliminate IP Subnet depletion: Bubble level IP addressing
- Compute morphing: VM Mobility within the bubble
- Container support: Container mobility and address flexibility
- Layer2 adjacencies within the bubble: VxLAN overlay tunnel

Network Automation:

- Day0 automation: Zero Touch Provisioning (ZTP)
  - Automated Network build-out
  - Plug and play Rack-on-boarding
- Day0+ automation & service APIs

AZ2.0 Network Design – Lesson learned



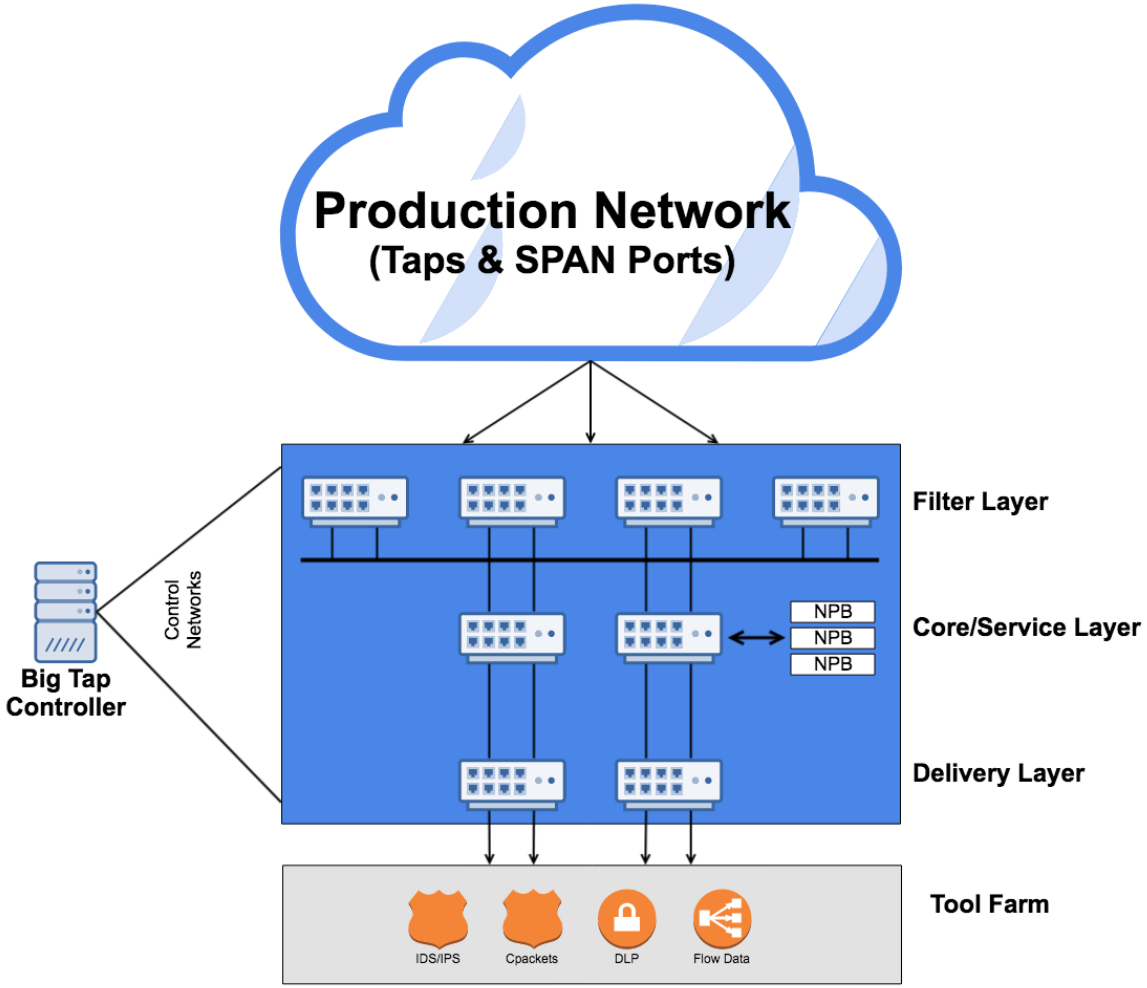
POD connectivity concept diagram

Lessons learned:

- 15 Racks per POD + Infra rack
- IP addressing at POD level – helps with IP deletion issues in the POD
- VxLAN design & Interop tests with FW/LB/ compute nodes
- Tune alerts to catch HW resource utilizations
- Do comprehensive failure & scale tests beforehand. Convergence times vary based on failure scenario.
- Single vendor VxLAN domain

Common Monitoring Fabric

Monitoring Fabric for US-West



Salient points:

- White Box Hardware
- 100gig fabric between Filter/Core/Delivery
- Delivery layer provides 10/25/40/50/100gig
- Firewall's will be tapped
- Switches will use Span
- NPB (Network Packet Broker)
  - Deduplication
  - NetFlow Generation
  - Packet Slicing
  - Header Stripping
  - (and more)
- Plug and play fabric
- Automatic traffic routing on failure
- Additional services
  - Analytics
  - Packet Recorders

100G/White-box Adoption: Roadmap

Path to transformation

Qualified/ Deployed

Qualified/ not-deployed

Not-qualified/ not-deployed

** ODM – Original Device Manufacturer
** OEM – Original Equipment Manufacturer

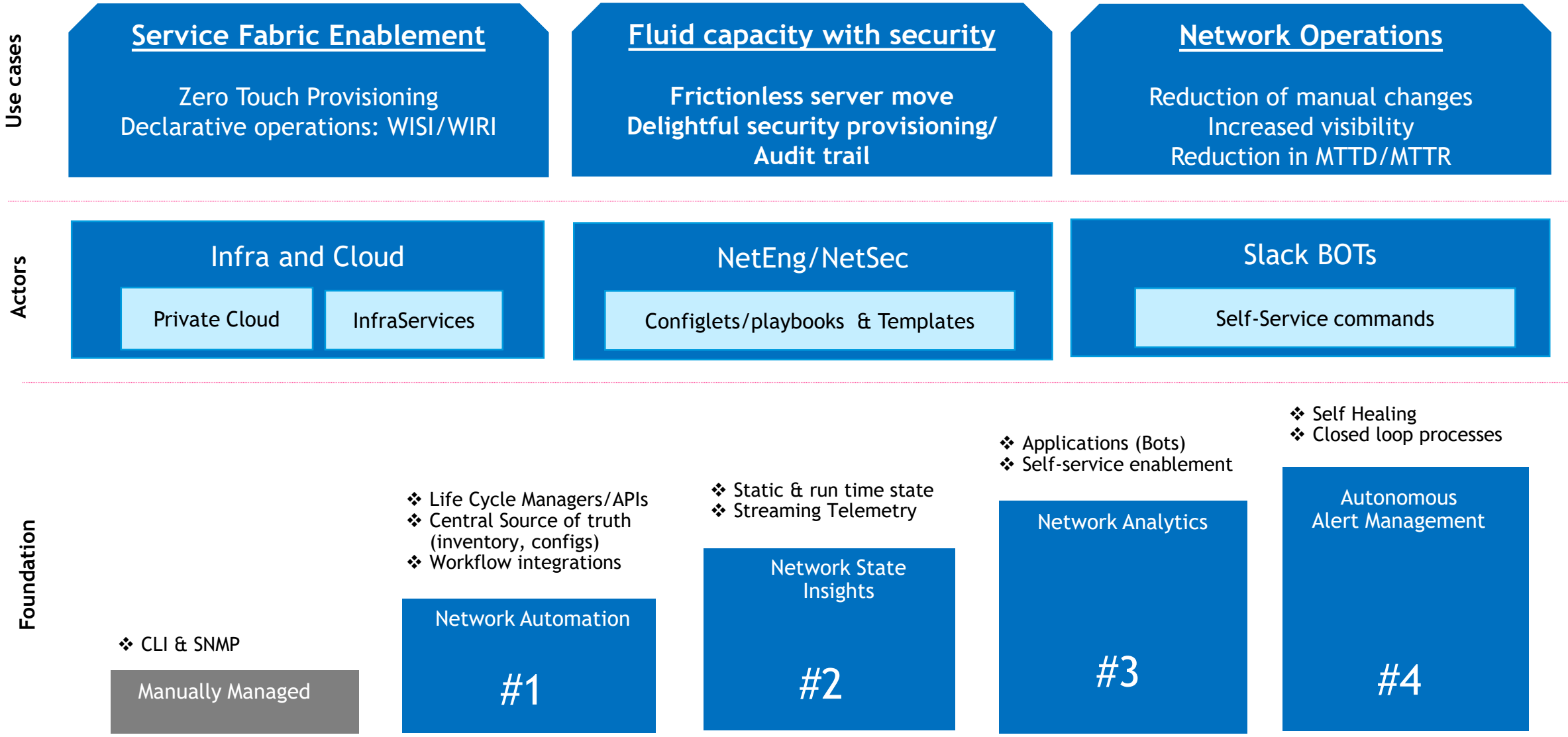
Whitebox OS	Monitoring Fabric	Whitebox OS	OEM1	OEM2	Vendor#1	V#2	Vendor#1	V#2
ODM1 (32x100G device)		ODM2 (32x100G device)			100G CWDM4		100G == (4x25G)	

Common White-box ODM HW

3rd Party Optics and Cables

- White-box HW for both core network as well as for common monitoring fabric
- Leverage common HW and personalize it with specific white-box/OEM SW
  - Helps to avoid mixing vendors in a given environment
- Helps to streamline spare inventory

Multivendor Network Automation Journey

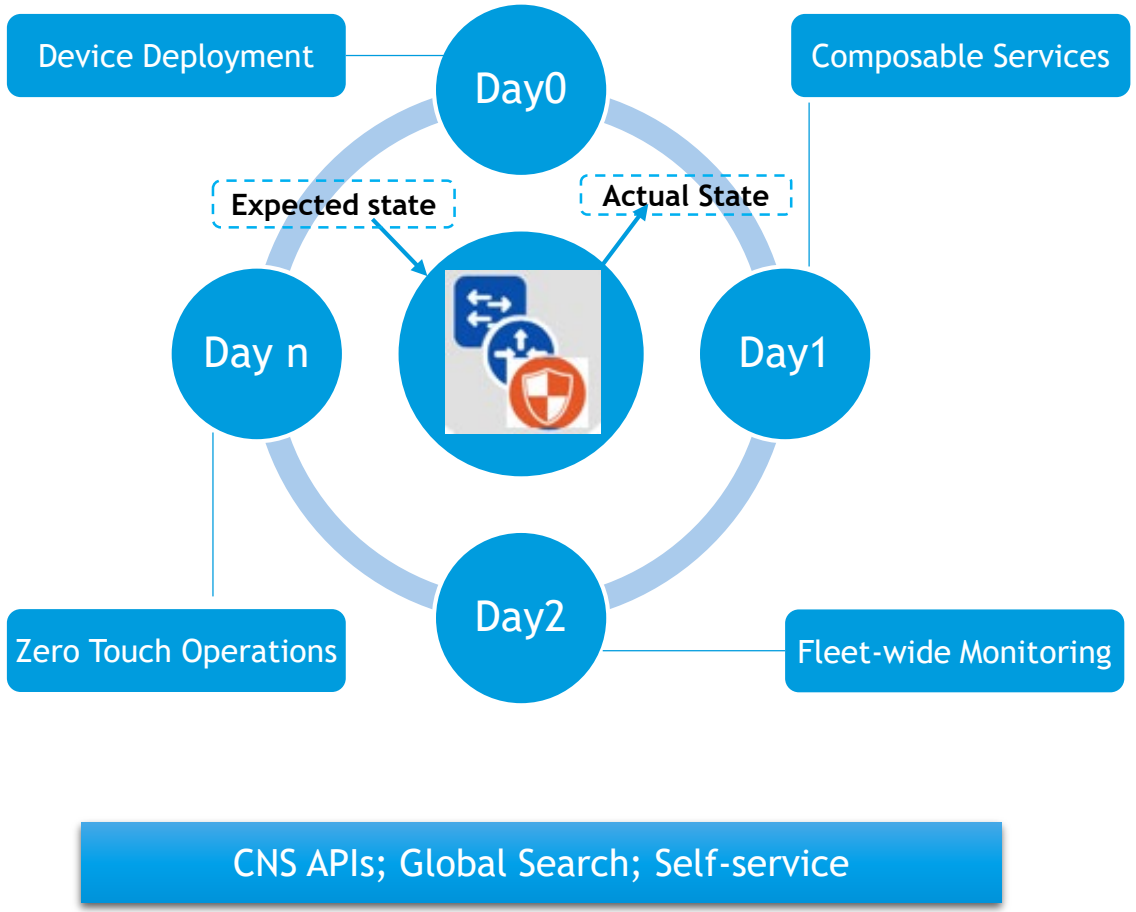


*WISB- What It Should Be
*WIRI - What It Really Is

*MTTD - Mean Time To Detect
*MTTR - Mean Time To Resolution

Infrastructure as Code (IaC)

The Journey: Remove human in-between



Core Benefits:

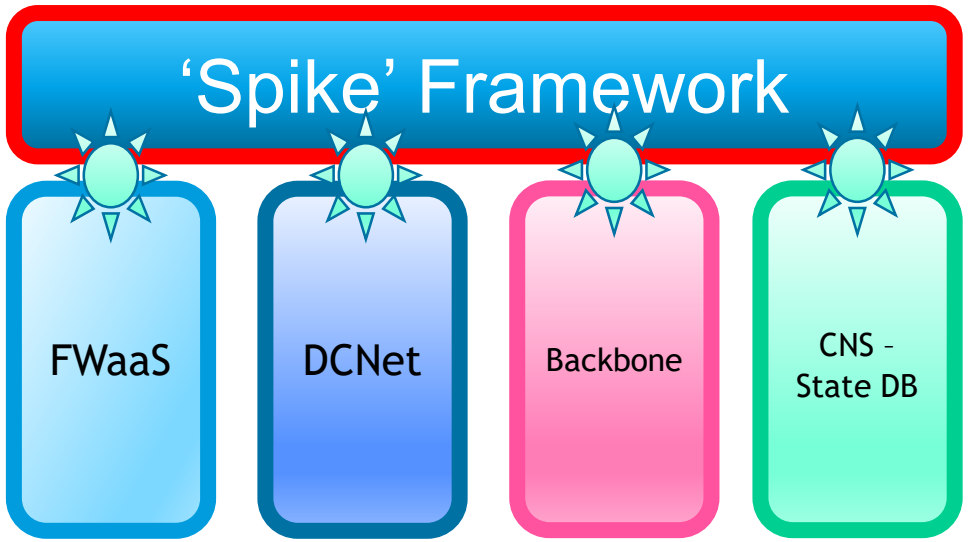
- Determinism and greater network insight
- Increased business agility and productivity
- Lower operation drifts and costs

Projects associated with each phase:

- Day 0: Zero Touch Provisioning (ZTP)
  - Device deployment
  - Day0 config push
  - SOR -Inventory management
- Day 1: Composable services
  - Common framework development
  - Service packs development
  - Orchestration layers integration
- Day 2: Fleet wide monitoring
  - Device static and dynamic state monitoring
  - NetFlow/SNMP based device counter collections
  - Syslog monitoring
- Day n: Zero Touch Operations (ZTO)
  - Device failure handlings/upgrades
  - WISB ← → WIRI : anomaly detection

Spike: Network Services Common Framework

Enablement to develop composable services



CNS composable services enablement

Value Propositions:

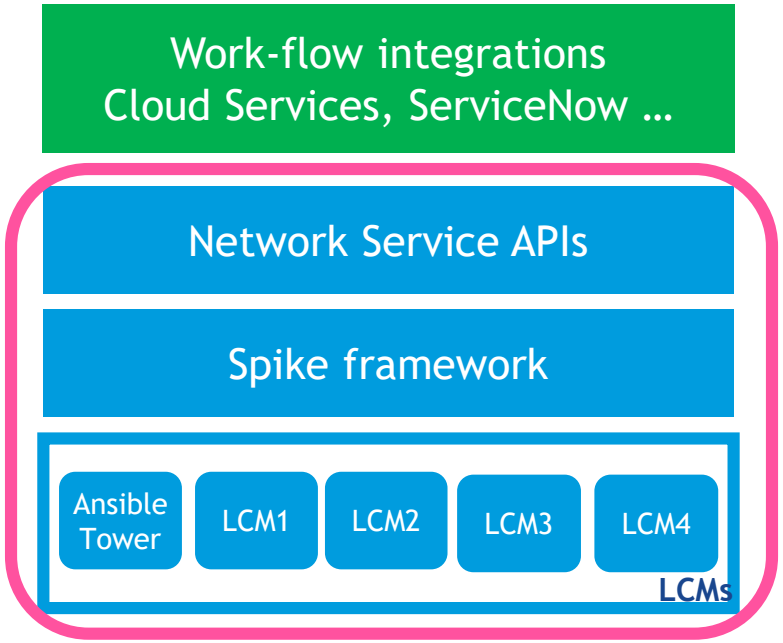
- Uniform service layer interface to all CNS capabilities
- Self service capability enablement
- Integration with PayPal Cloud Services layer for Network APIs

Spike Services:

- LDAP integration
- Key Manager integration
- IPAM integration
- ServiceNow integration
- Workflow engine
- CMDB integration
- Maintain correlation IDs
- Built-in Database
- Device Layer to interact with LCMs
- REST based APIs
- Admin UI

Spike Framework - Architecture

Write once, leverage it for all CNS IaC initiatives



Value propositions:

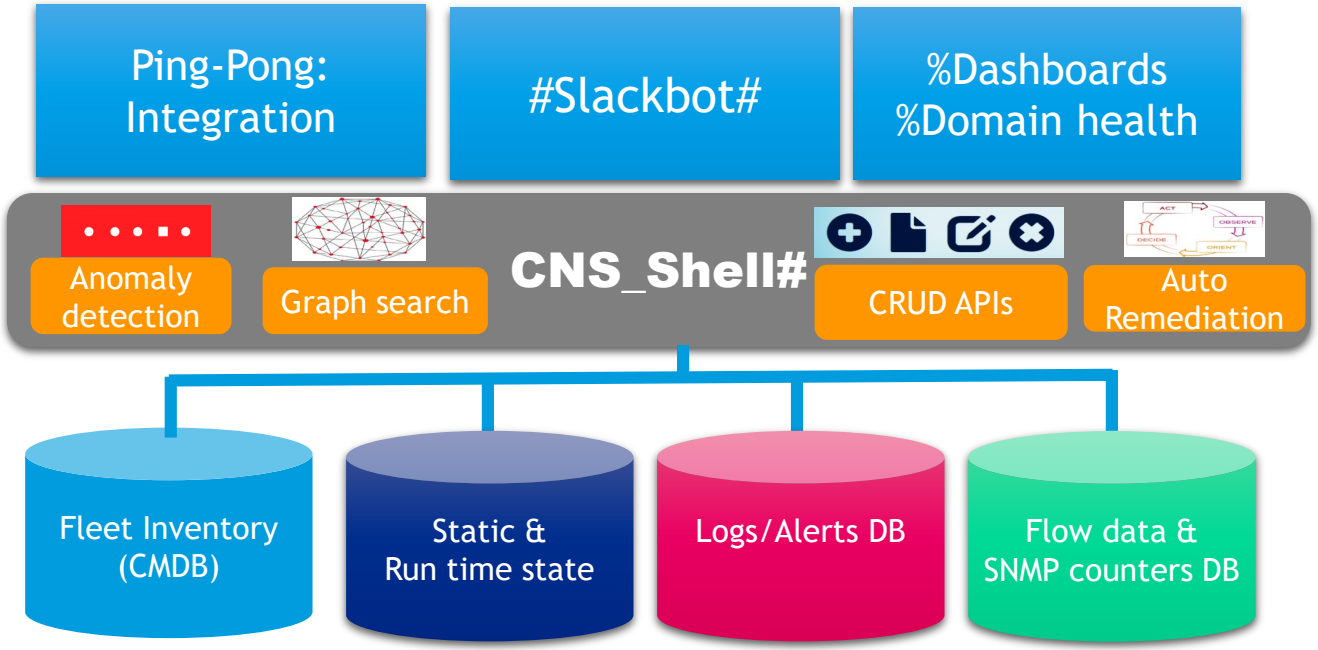
- Repeatable Day0+ task are enabled through CRUD operations
- Eliminate Drift
- Reduce human touch/reduce manual changes
- Network APIs for IaaS orchestration layers
- Brownfield environment: vendor variety & device variety

Design Principles:

- Service layer for heterogenous network environment
- Reduce manual changes and provide APIs for workflow integrations
- Modular design to accommodate plug-n-play sub-components
- Config Consistency and availability
- No operational state persistency in data store
- Asynchronous execution for all APIs
- Auto re-try to handle downstream failures

Network Self-Service Enablement

Network Blackbox to Self-service capabilities



Value propositions:

- Telemetry and visibility at global network level
- Dynamic network map
- Enable self service capabilities
- Drift detection and auto remediation factory

Use Cases:

- Network global ‘path’ search is enabled through ‘Slackbot’
- Network state DB overlaid with SNMP logs
- Integrate with ping-pong service for latency measurements

Final Thoughts

- Build balanced skillset organization with SWdev/NetEng/NetOps
- Designs standardization/Reduce HW SKUs
- Take advantage of leaf/spine network architectures for DC – It works!
- Be pragmatic in your automation journey, leverage vendor tools where available
- Collaborate with like minded industry partners

Happy to share/collaborate:
https://www.linkedin.com/in/saikrishnakotha/

#WeAreHiring


Open. Together.
OCP Global Summit | March 14–15, 2019
OCP
SUMMIT