Game Changer for Network Security: Software Driven Networks

John Kimmins
CTO
jkimmins@catapultconsultants.com

Catapult Consultants, LLC
2300 Clarendon Blvd., Suite 600
Arlington, VA 22201
703-849-0960 Ext 182

Catapult Consultants, LLC
6700 Alexander Bell Dr., Suite 200
Columbia, MD 21406
301-884-3110

Outline

- Market Drivers
- Design Tenets
- Architectural View
- Major Players
- Security Challenges
- Summary

Drivers for Software Driven Networks & Applications

- Data Center Virtualization
- Virtualization in RAN, Backhaul and Core Networks
- Cloud services supporting multi-tenant virtual applications, hosts and networks
- Slow and error-prone network management driving higher operations costs
- Changing traffic patterns driven by new higher bandwidth applications and services

Design Tenets of SDN/NFV Environments

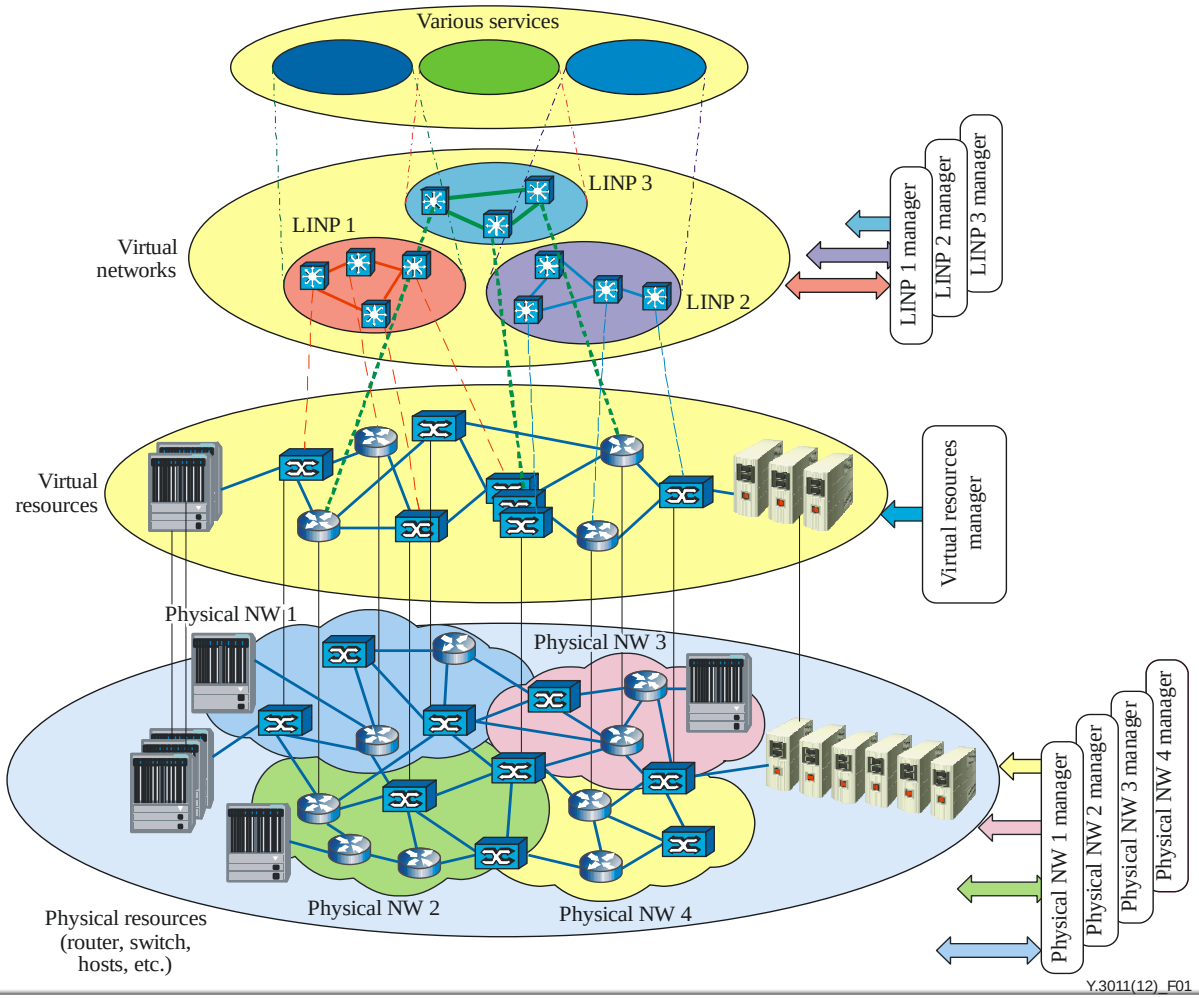
- Network & System Abstraction
- Decoupling of Control Logic
- Service Orchestration: Dynamic Configuration
- Open Programmable Control Interfaces
- Distributed & Centralized Processing & Control
- Open Standards

Network Virtualization

- Customized views may be created using the network view to expose different levels of details and varying scopes.
- E.g., a customer's view focusing on the services of that customer including customer interfaces, service attributes and connectivity, but not exposing the internal details of the network
- In SDN, network virtualization permits clients to define and control slices of the network where each slice or virtualized network appears to be a network dedicated to that client

Network Virtualization

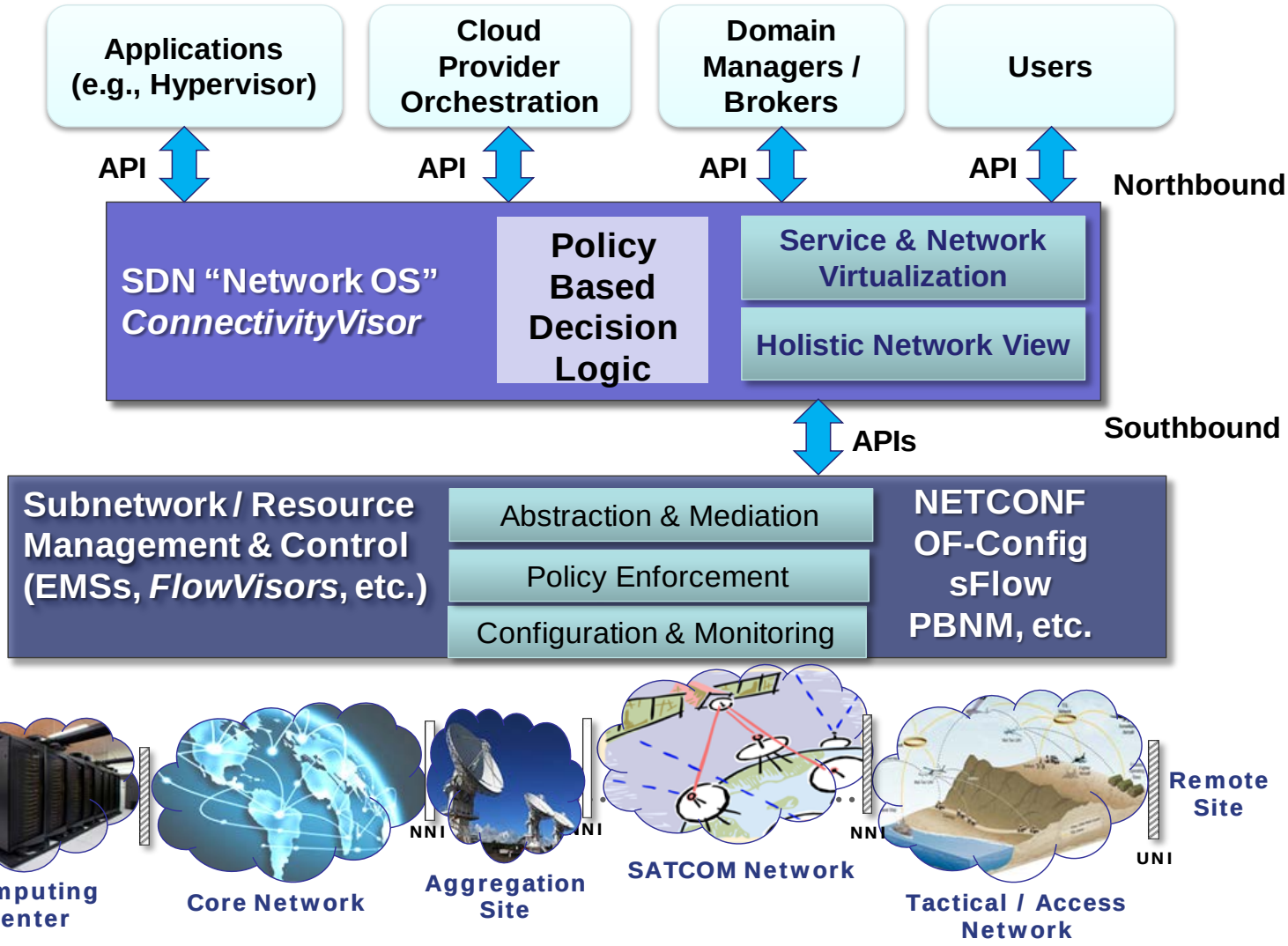
ITU-T Y.3011, network virtualization defines logically isolated network partitions using the same shared physical networks, allowing multiple virtual networks to simultaneously coexist.



Decoupling of Control Logic

- Separated from the network data plane elements
- Responsible for establishing and managing the network services connectivity
- Performed by logically centralized service connectivity control logic functionality (e.g., Network OS)
- Network elements no longer need to process, exchange and store domain-wide control information
- Users interact with the control logic through a programmable interface in order to dynamically manage and control the behavior of their services and related flows to meet their changing functional needs.

Policy Based SDN Functional Architecture



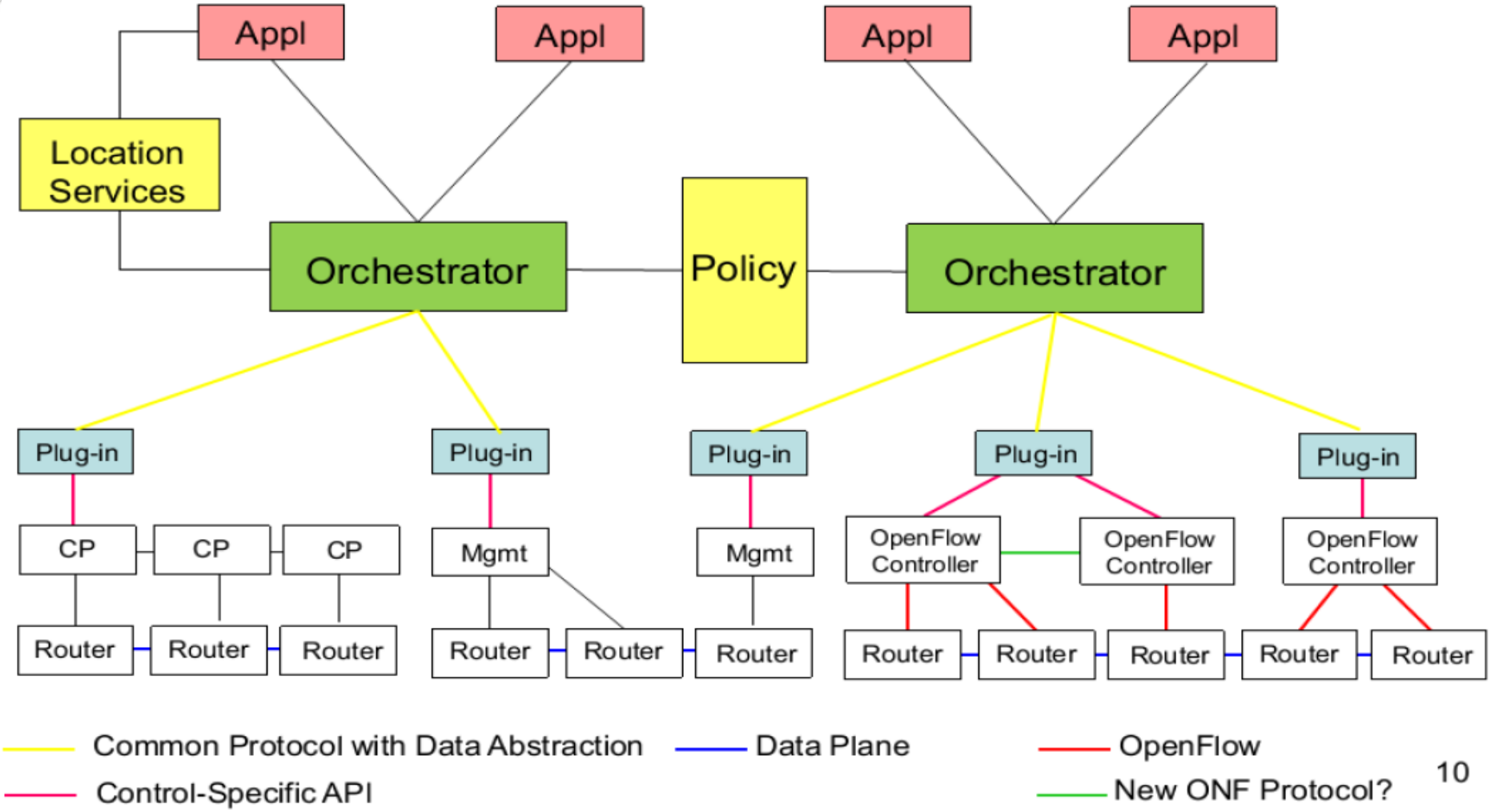
Service Orchestration: Dynamic Configuration

- Balancing the service requirements with the holistic view of the network including current demand, performance, service constraints, and service and resource sharing policies.
- Coordinates traffic engineering capabilities by monitoring the network performance and managing the aggregate flows or virtual trunks within the network in order to support projected service demand while maintaining service quality objectives

Open Programmable Control Interfaces

- Support well-defined service management and control capabilities
- SDN Southbound APIs allow the Network OS to interact with the subtending resource management layer
- SDN Northbound APIs support interactions for controlling services between the Network OS and the controlling applications, users, and orchestrators

SDN Logical Architecture Example



Source: *Software Defined Network, An IETF Update for UKNOF 21, D. King & A. Farrel*

Major Players
All with Different Security Models

- Router & Switch Vendors
- OSS/BSS vendors
- Service Providers
- Third Party Controller Vendors
- Third Party Application Developers
- Networking Integrators
- Security Technology Suppliers
- Standards Forums
- New Entrants
- Academia
- …

Impact to Current Networking & Systems

- Utilizes most existing protocols
  - Inherit existing threats and vulnerabilities
- Virtualized platforms to support network functions & applications
- Routing Protocols run in the Controller
- Big change to management and configuration protocols
  - Centralized vs. distributed
- There are diverse solutions and partnerships being offered with complex features and functionality

Disturbing Trends

33% of victims discovered the breach internally

Down from 37% in 2012

67% of victims were notified by an external entity

229 median number of days that threat groups were present on a victim's network before detection

14 days less than 2012

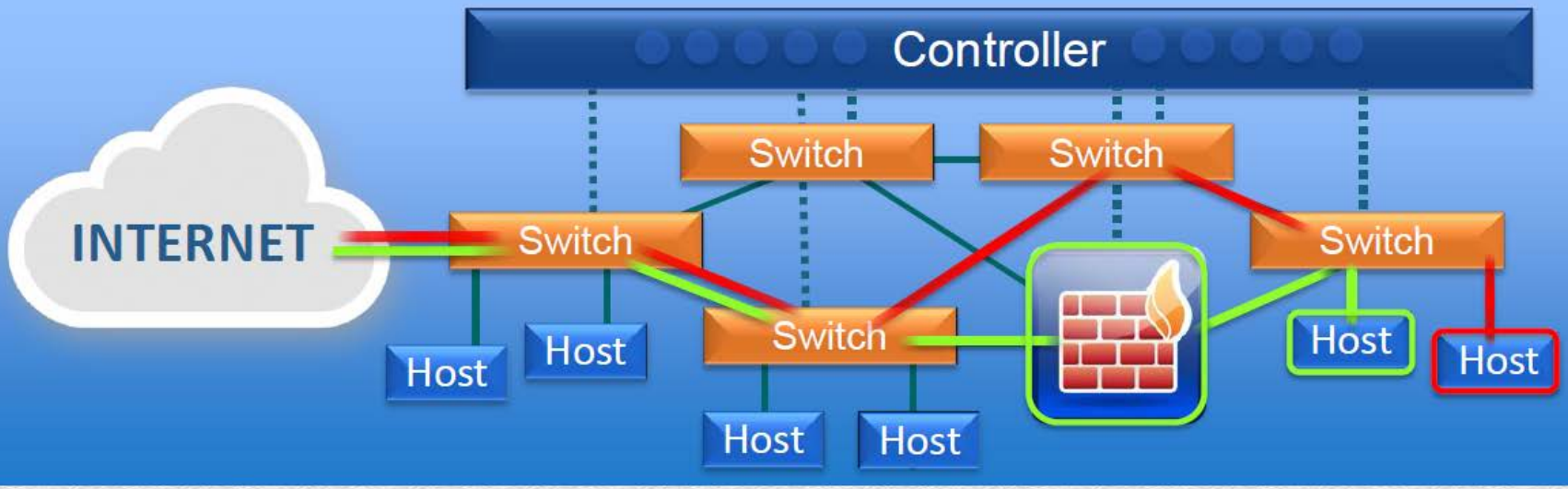
Longest Presence: 2,287 days

Source: 2014 Threat Report, Mandiant

Security Challenges -1

- Security cannot be enforced by physical topology alone
- Many more targets – e.g., EMS, VNF Manager, Service Catalogue, Controller, Orchestrator
- Distributed & Central Control
  - Applications and Controller have complete control of the network – need to be trusted
  - Potentially built on general purpose computing platforms – Is it addressable? Is there diversity?
  - Potential for BIG Impacts if Compromised
    - Route flows around security devices/modules
    - Subverts new flows
    - Send traffic to compromised nodes
    - "Man in the Middle" attacks
    - Modify content
    - Monitor traffic
    - …

SDN Changes the Security Model



- Flow Rules control when or if traffic goes through Security Device
- Network Topology is now virtual

Source: Why Take Over the Hosts When You Can Take Over the Network, R. Hinden, Check Point

Security Challenges - 2

- Physical vs. Logical Security Policy Management
  - Application and service contexts
  - Multiple levels – e.g., platforms, network, virtual middleware, applications, service chains
  - Right Automation level – How is intrusion detection/response handled?
  - New Security KPIs?
- Unprotected APIs
- Third Party Applications – Degree of required security testing?
- Organizational Impacts
  - Network and Security Groups need to work more closely together
- Different Security Approaches Emerging
  - Software Defined Perimeter Architecture from Cloud Security Alliance
  - Various Industry Forums & SDOs

Security Management:
Integrated Continuous Monitoring

Domains	Security Management	Threat Intelligence
• Users • Mobile Devices • Computing Platforms • Access Network • Core Network • IT Systems • Applications • Databases • Interconnections • External Partners	**Asset Inventory**	**Internal Sources** • Users • Applications • Systems • Networks **External Sources** • Informations Sharing & Analysis Center • Malware Analysis • Attack Forensics • Law Enforcement • DHS • Cyber Underground • Global Analysis • Industry Partners • Suppliers
	Configuration Management	
	Software & System Lifecycles	
	Vulnerability Assessments	
	Data Collection & Analytics	
	Patch Management	
	Incident Response	

Summary

- Network, services and application dynamics changes the Security Operations' model
- Different trust model has to be recognized and addressed on component, functional, services and operations' levels
- The threat environment will also evolve
- Legacy network and services still needs to be protected