Securing the Evolving Network & Services Virtualized Environment

John Kimmins
CTO
jkimmins@catapultconsultants.com

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

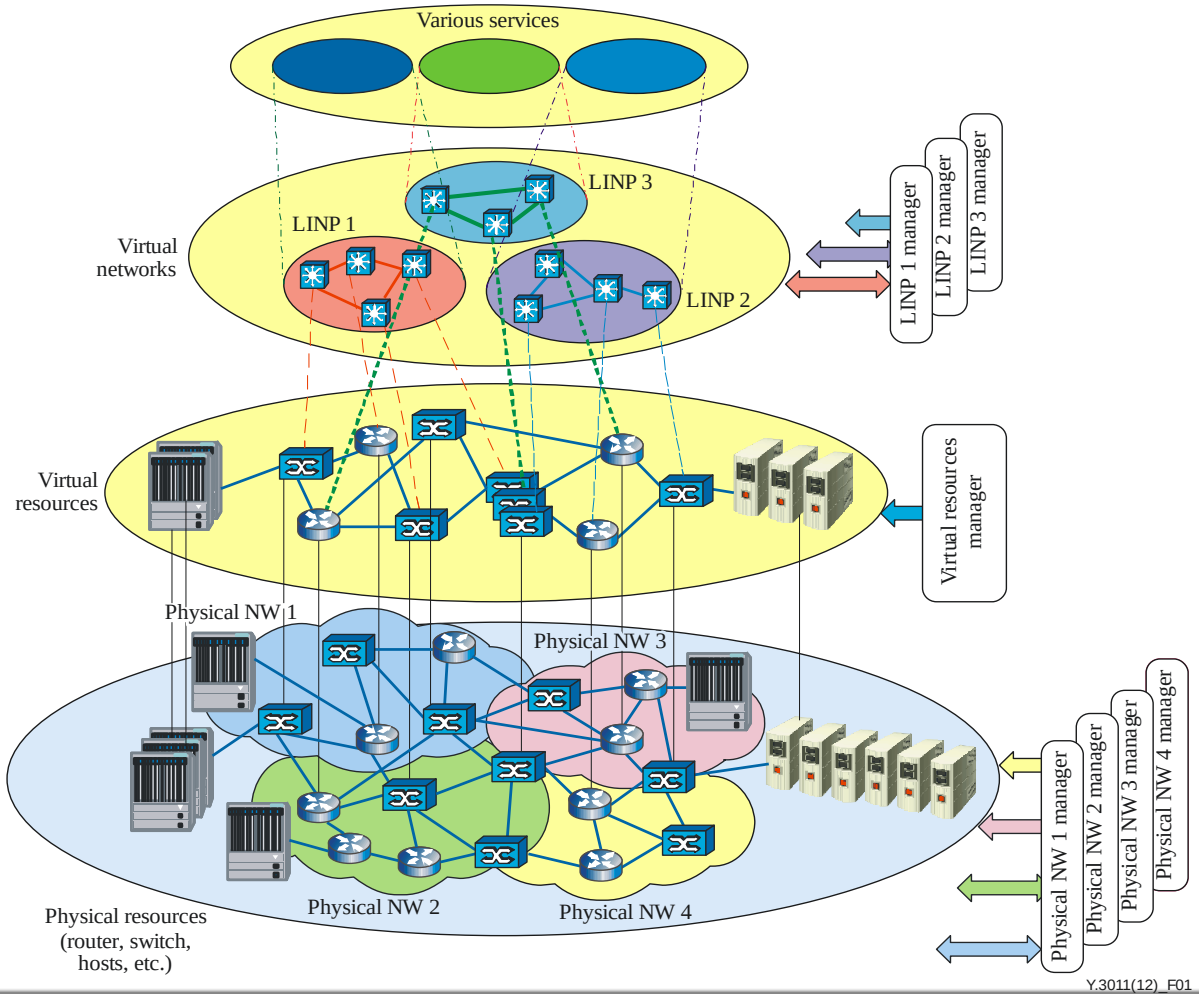
Catapult Consultants, LLC
6700 Alexander Bell Dr., Suite 200
Columbia, MD 21406
301-884-3110

Outline

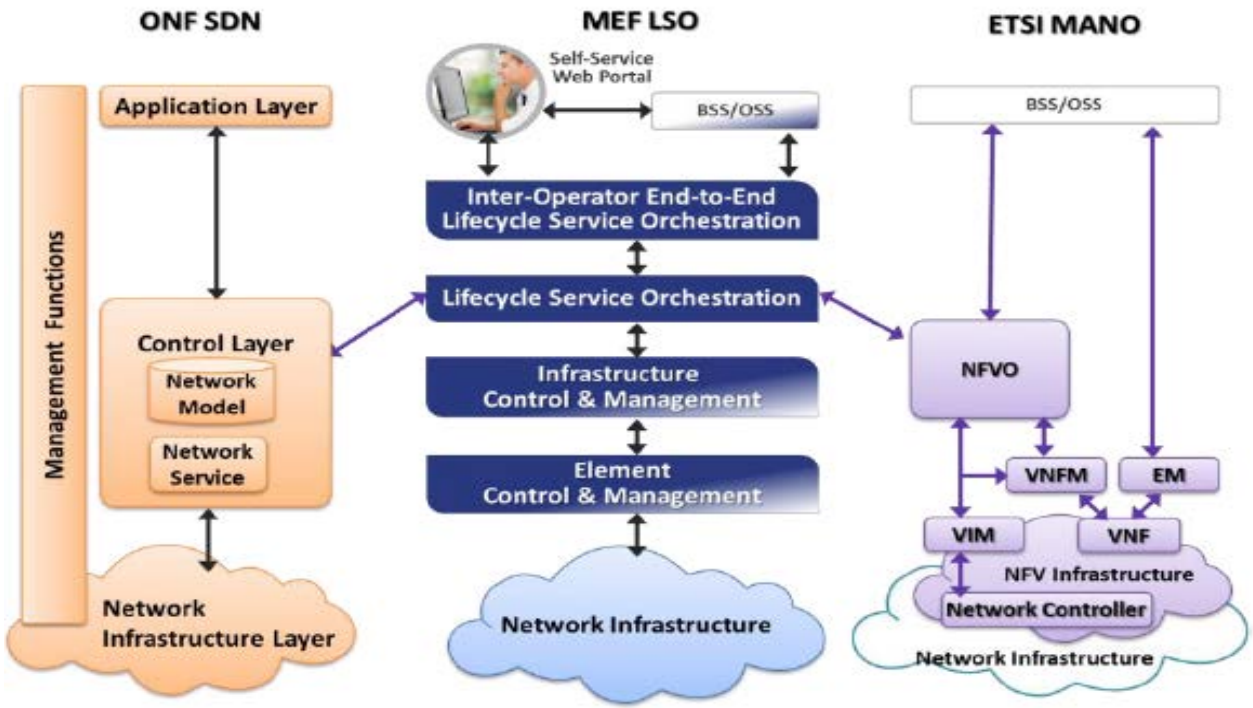
- Network Virtualization Basics
- Service Chaining
- Security Risks
- Evolving Security Model
- Summary

Network Virtualization Basics

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

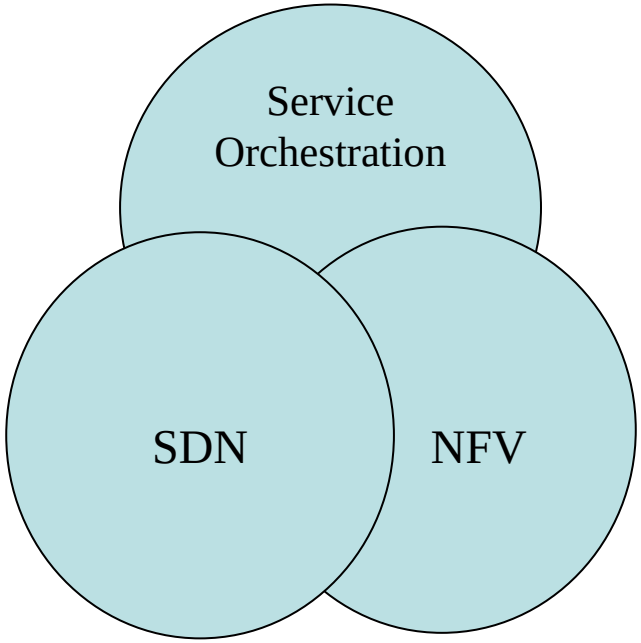


Different Virtualized Infrastructure Views

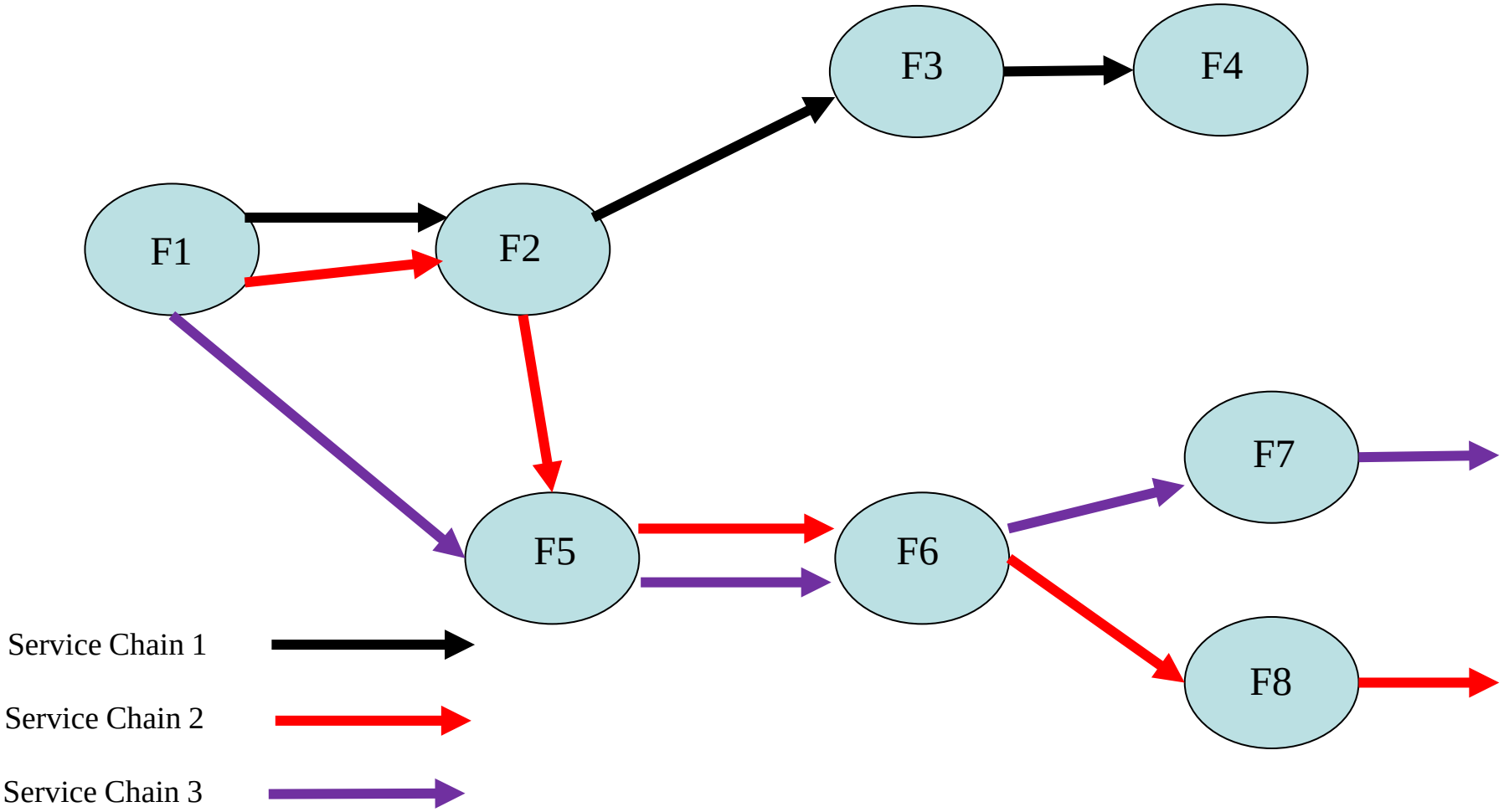


Source: Metro Ethernet Forum - 2014

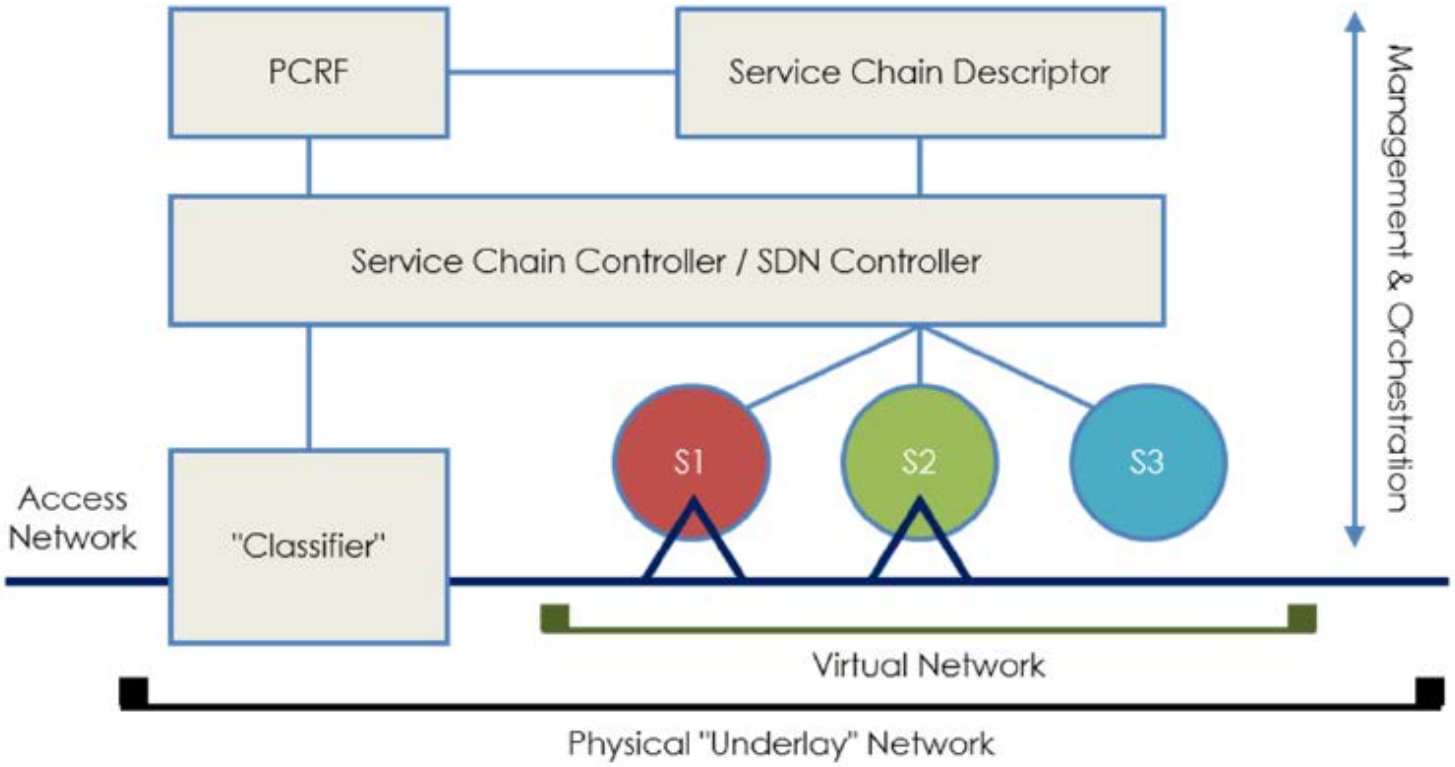
Managing the Virtual Infrastructures



Chaining of Functions to Support Services



Network Service Chaining Model



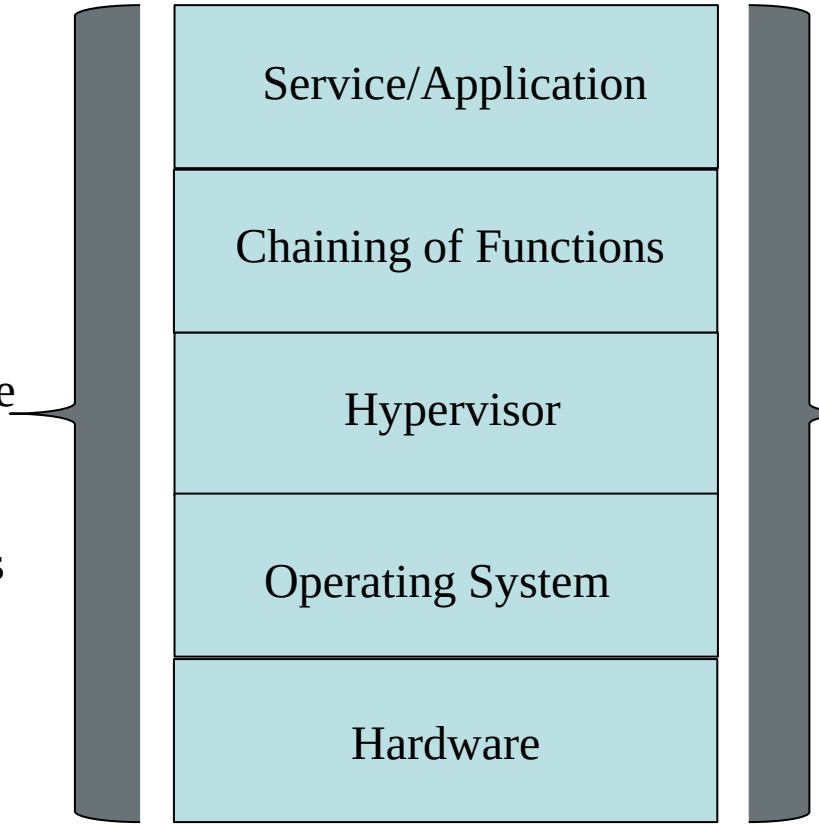
Source: Heavy Reading

Security Risks – Legacy & New Issues

- Denial-of-Service
  - Signaling storms from end devices
  - External network attacks
- User Plane
- Hypervisor
- Security Function Virtualization
  - Application level
- Service Chaining integrity
- Orchestration
  - Platform & interfaces
  - Security policy management robustness
- Amplification attacks enhanced by elasticity functions & Affinity Rules

Evolving Security Model

- Identification of appropriate Security Functions
- Chaining Integrity
- Network Security
- Affinity Rules for reliable & available security functions
- Physical & virtual taps for continuous monitoring
- Lifecycle management of security functions



Security Policy Management

Summary

- New architectures and products are being trialed and deployed
- Security functions are being virtualized and need to be integrated into the application and service flows
- Legacy and new security risks are still being identified
- The robustness, reliability and integrity of Security Policy Management is critical