Vulnerabilities and Opportunities in SDN, NFV, and NGSON

IEEE CQR 2014 International Workshop

Emerging Technology Reliability Roundtable

Tucson, Arizona, USA

May 12, 2014

Mehmet Ulema

Manhattan College, New York, USA

Outline

- Overview of emerging technologies and trends in networking and services
  - SDN, NFV, NGSON
- RAS related issues in SDN and OpenFlow
- Designing and building secure platforms with automatic failure recovery and fault tolerant features, self organizing capabilities
- Vulnerabilities observed in the design and implementation of NFV
- NGSONs built in RAS features
- Conclusion

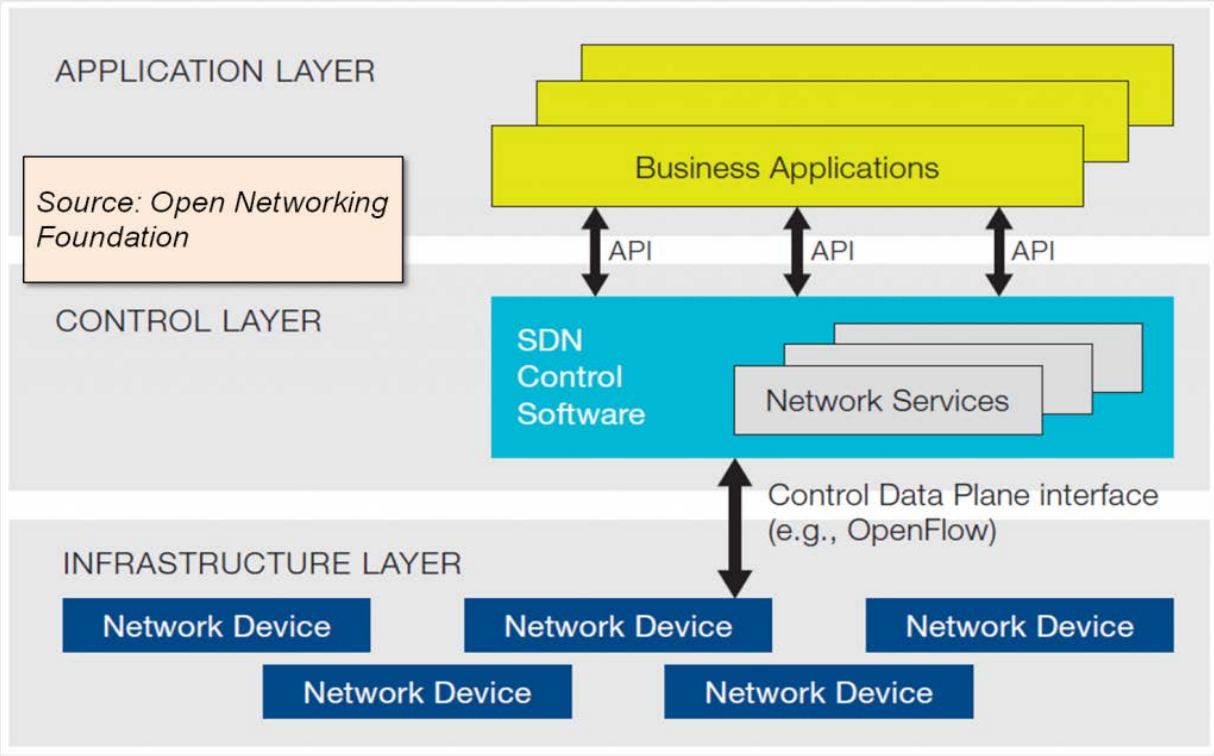
Emerging Trends and Technologies in Networking and Services

- Virtualization
- “Softwarization”
- Commoditization
- Service Chaining
- Dynamic Adaptation
- Context Awareness
- Self Organization
- ….

- SDN
- NFV
- NGSON
- …….

Software Defined Networks / Networking

- Network control plane is decoupled from forwarding and is directly programmable
  - Programmability: enabled through **Controller**, executed through **Forwarding** elements
  - Allows network operators to customize and optimize
    - delivery of new types of network services, new business models, products & services
    - reduce CAPEX and OPEX



Focus on network paths and flows for Big Data, Composed Services, etc.

SDN Controller

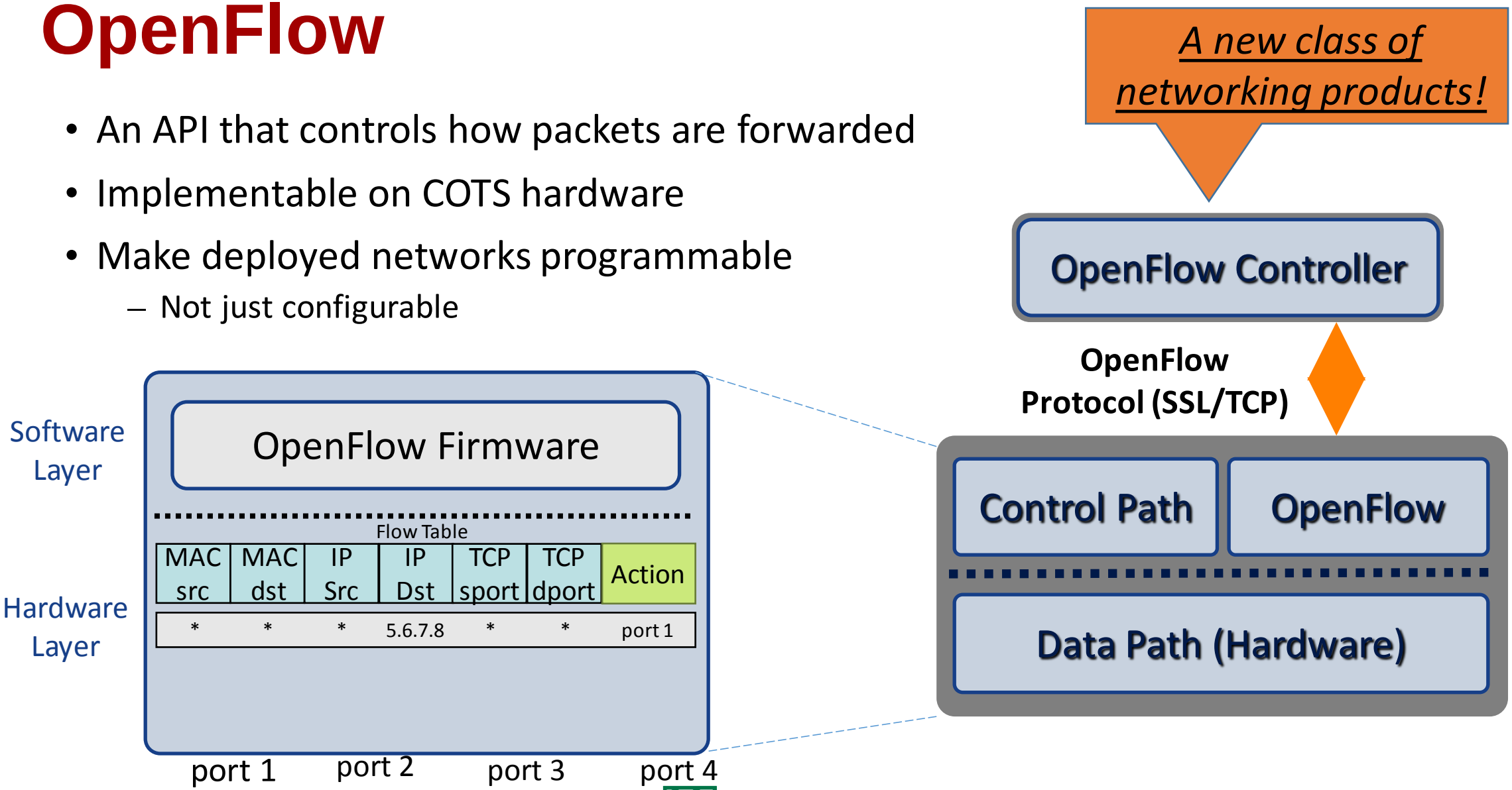
(Programming FlowTables)

SDN Forwarding Elements

https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

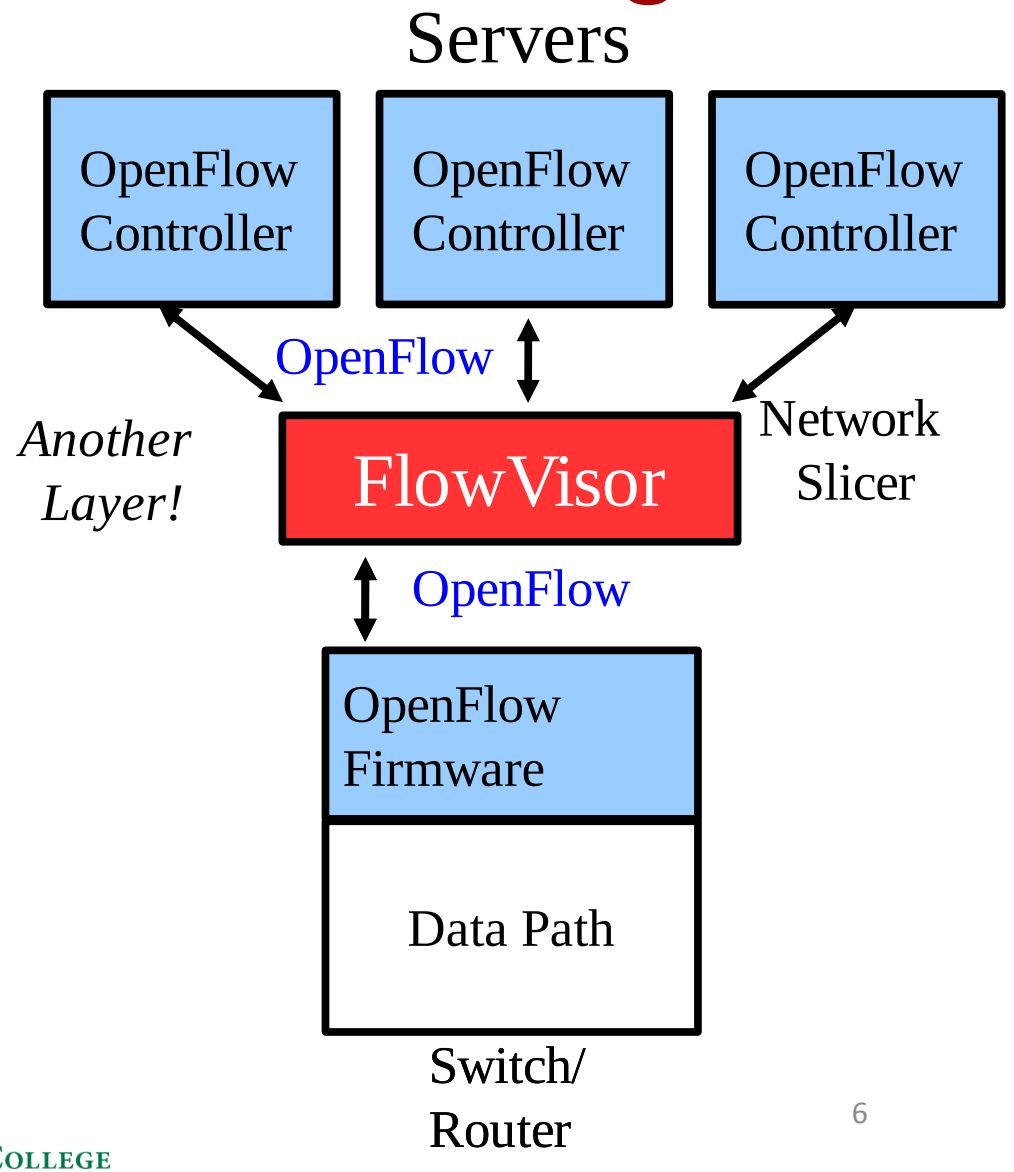
OpenFlow

- An API that controls how packets are forwarded
- Implementable on COTS hardware
- Make deployed networks programmable
  - Not just configurable



OpenFlow Application: Network Slicing

- Divide the network into logical slices
  - A slice: a collection of switches/routers
  - Each slice/service controls its own packet forwarding
    - Existing services run in their own slice
      - E.g., Spanning tree, OSPF/BGP
- Data plane is unmodified
  - Packets forwarded with no performance penalty
  - Slicing with existing ASIC
- Transparent slicing layer
  - Enforce strong isolation between slices
    - Actions in one slice do not affect another
- Prototype implementation: FlowVisor



Broader Vision

Commonly Known View

A "Networking" technology with separate control and data planes resulting in inexpensive hardware controlled by software creating new opportunities (Network OS, programmability, virtualization, abstraction, etc.)

A Broader Vision: Software Defined Ecosystem

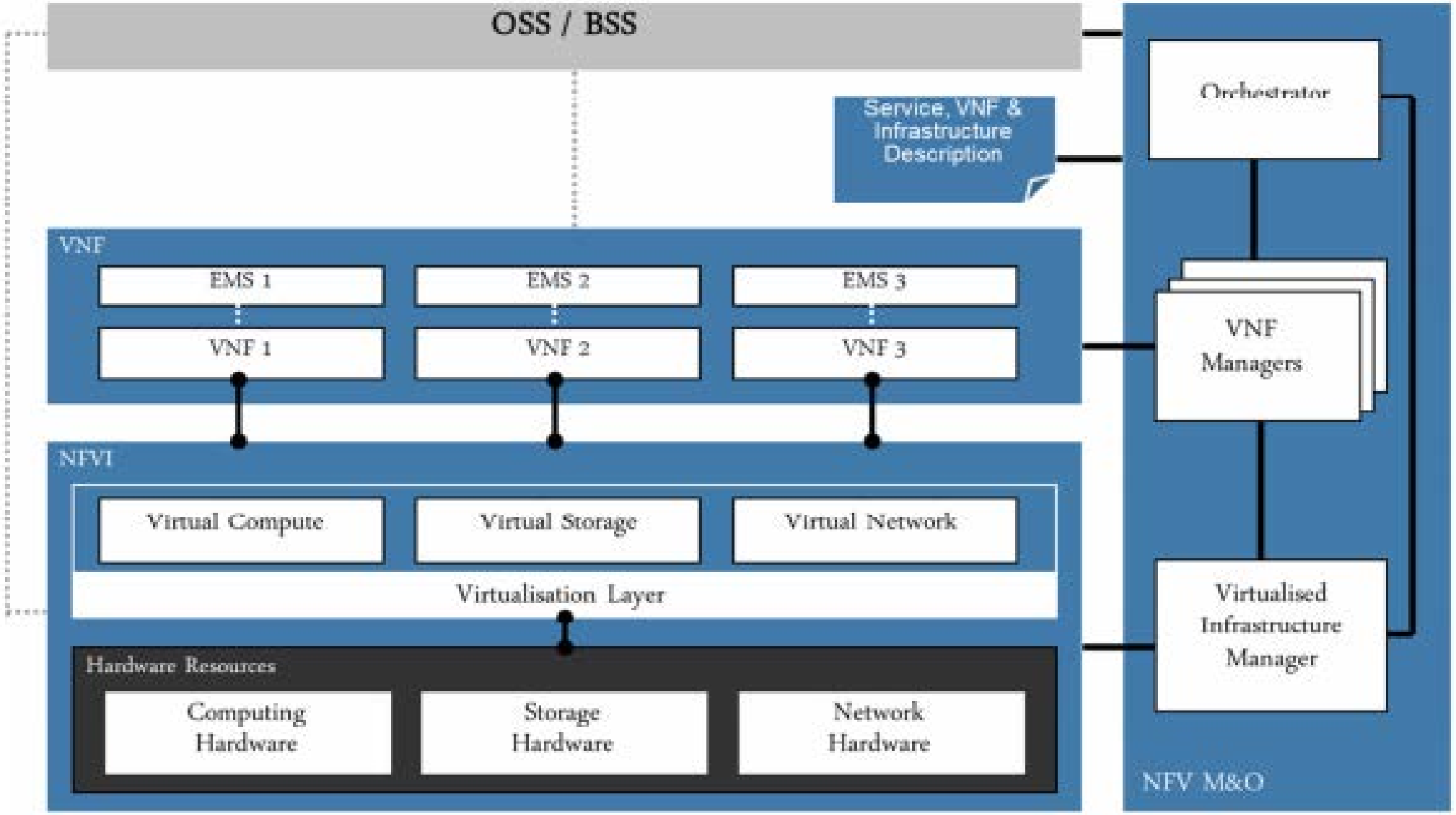
SDN concept generalized and applied to all segments of networking with modularity (e.g., User Equipment, Radio, Transport, Operations, Applications), all areas of technology (e.g., wireless, optical), and abstractions that allow management, cloud, cognitive, smart grid, etc.

Network Functions Virtualization (NFV) or Profit Realization (PR)?

- Use standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage,
- Implement network functions in software that can run on industry standard servers,
  - that can be moved to various locations, without the installation of new equipment
- Five basic principles of NFV:
  - Orchestrate distributed data centers, manage application lifecycles, leverage the network, automate cloud "nodes," and be open and multi-vendor

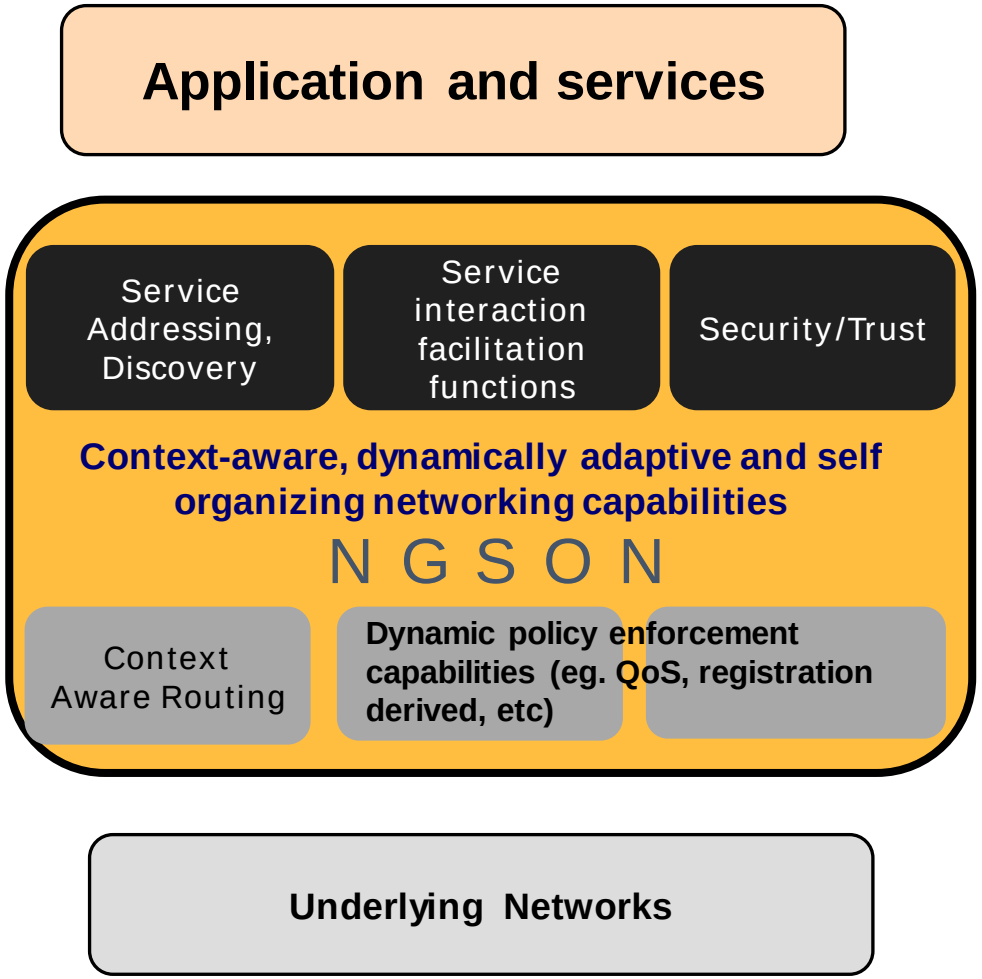
Source: ETSI NFV ISG's – Introduction White Paper, October 2012
http://portal.etsi.org/NFV/NFV_White_Paper2.pdf

NFV: Reference Architectures



What about Service Functions Virtualization? Next Generation Service Overlay Network (NGSON)

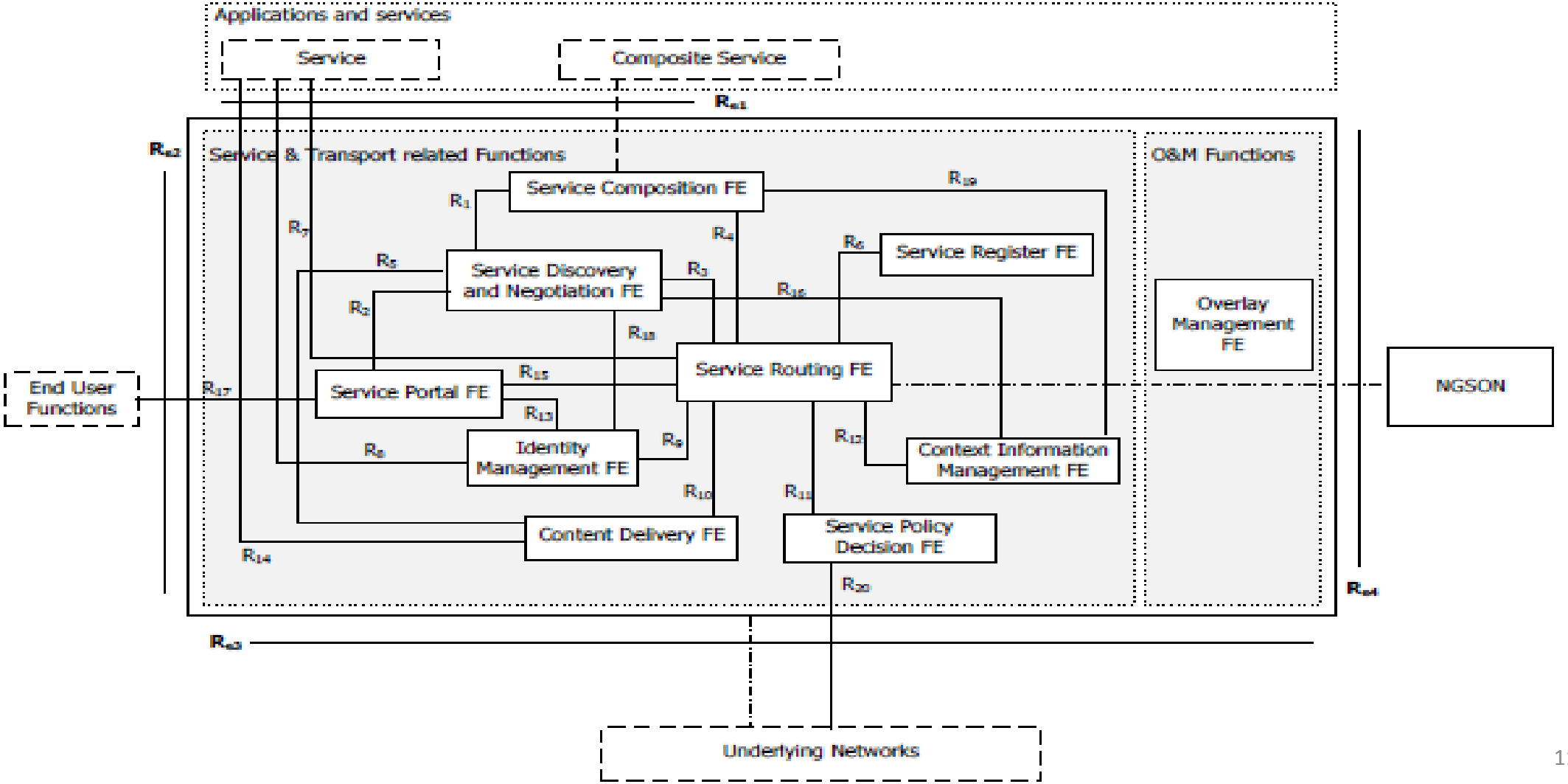
- An IEEE standard for a framework of IP-based service overlay networks
- A set of context-aware, dynamically adaptive, and self-organizing networking capabilities, including advanced routing and forwarding schemes to support applications



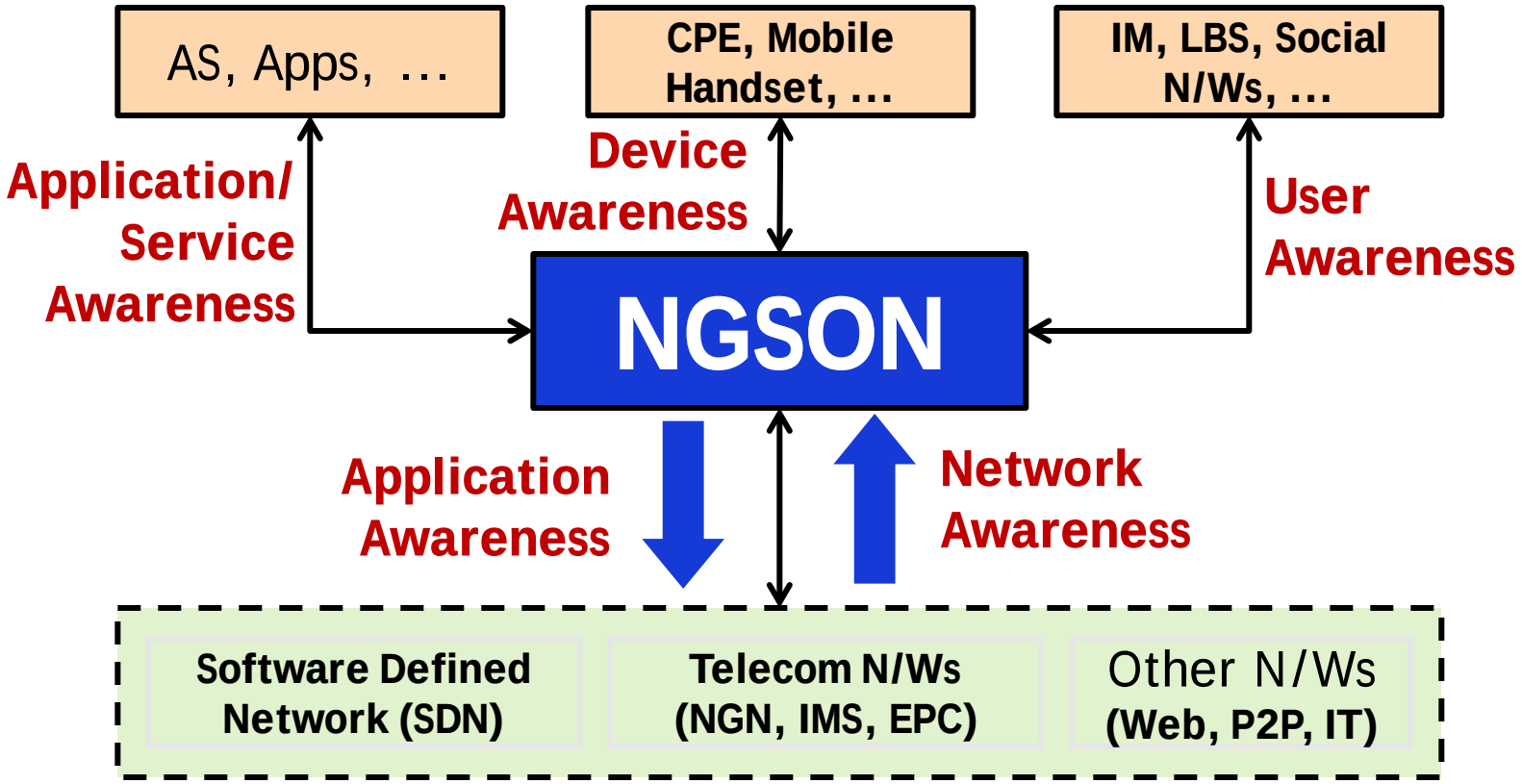
P1903-2011 IEEE Standard for Functional Architecture of Next Generation Service Overlay Networks

NGSON: Reference Architecture

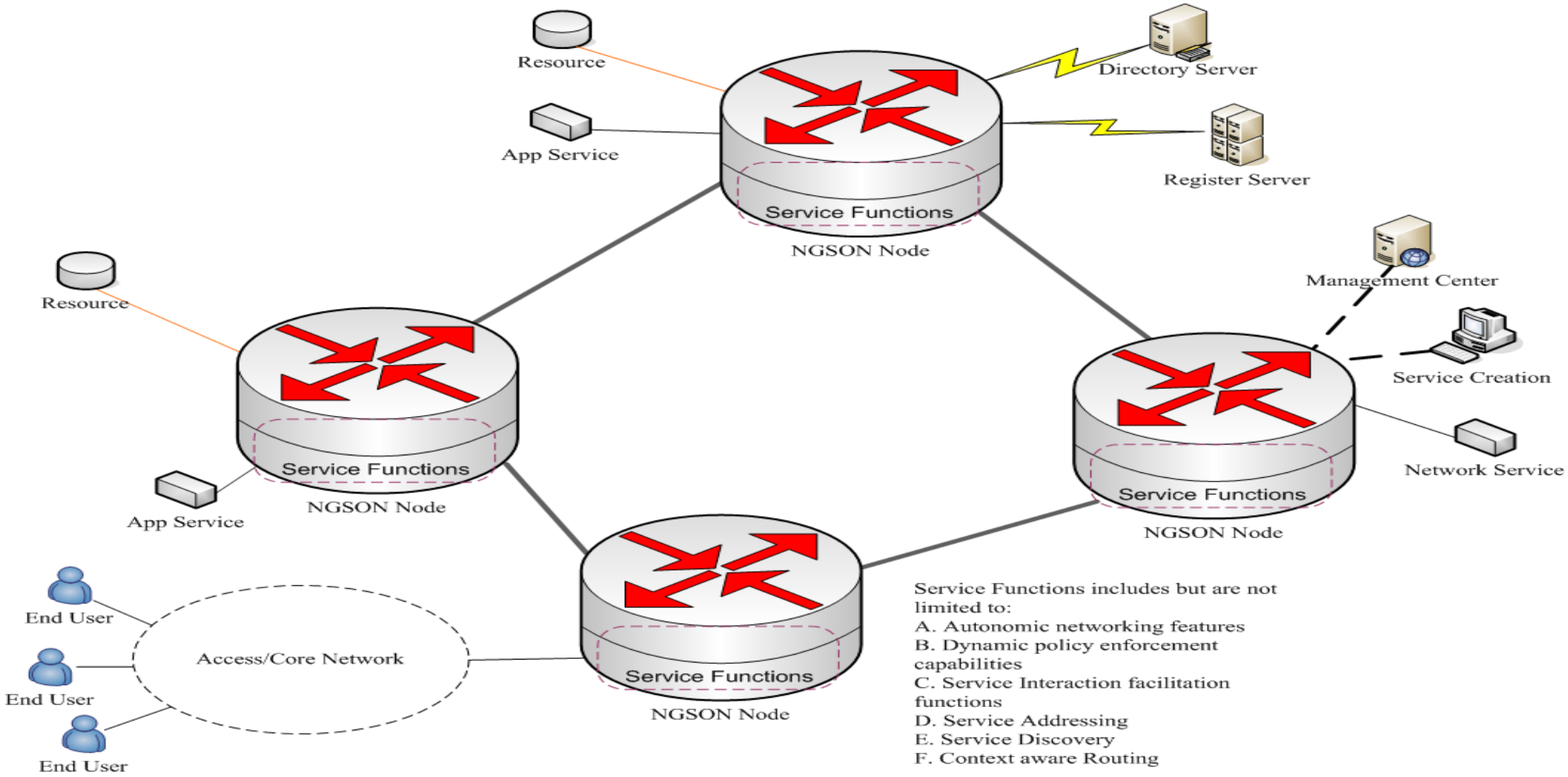
NGSON focuses on the services, service chains, collaboration of services by networking servers/systems used for providing/supporting services



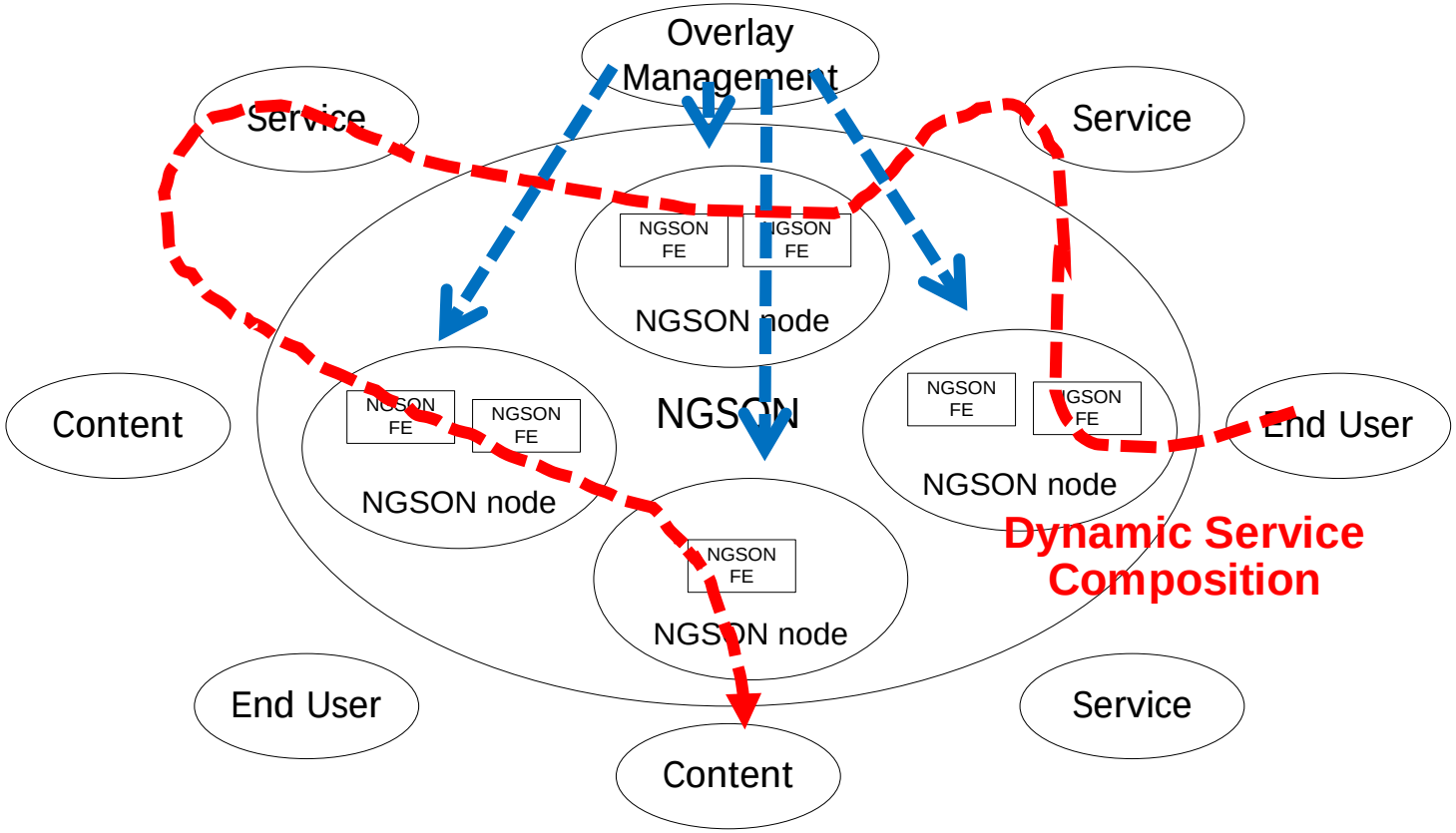
X-Aware Service Ecosystem



A Deployment View of NGSON



P1903.3: Self-Organizing Management

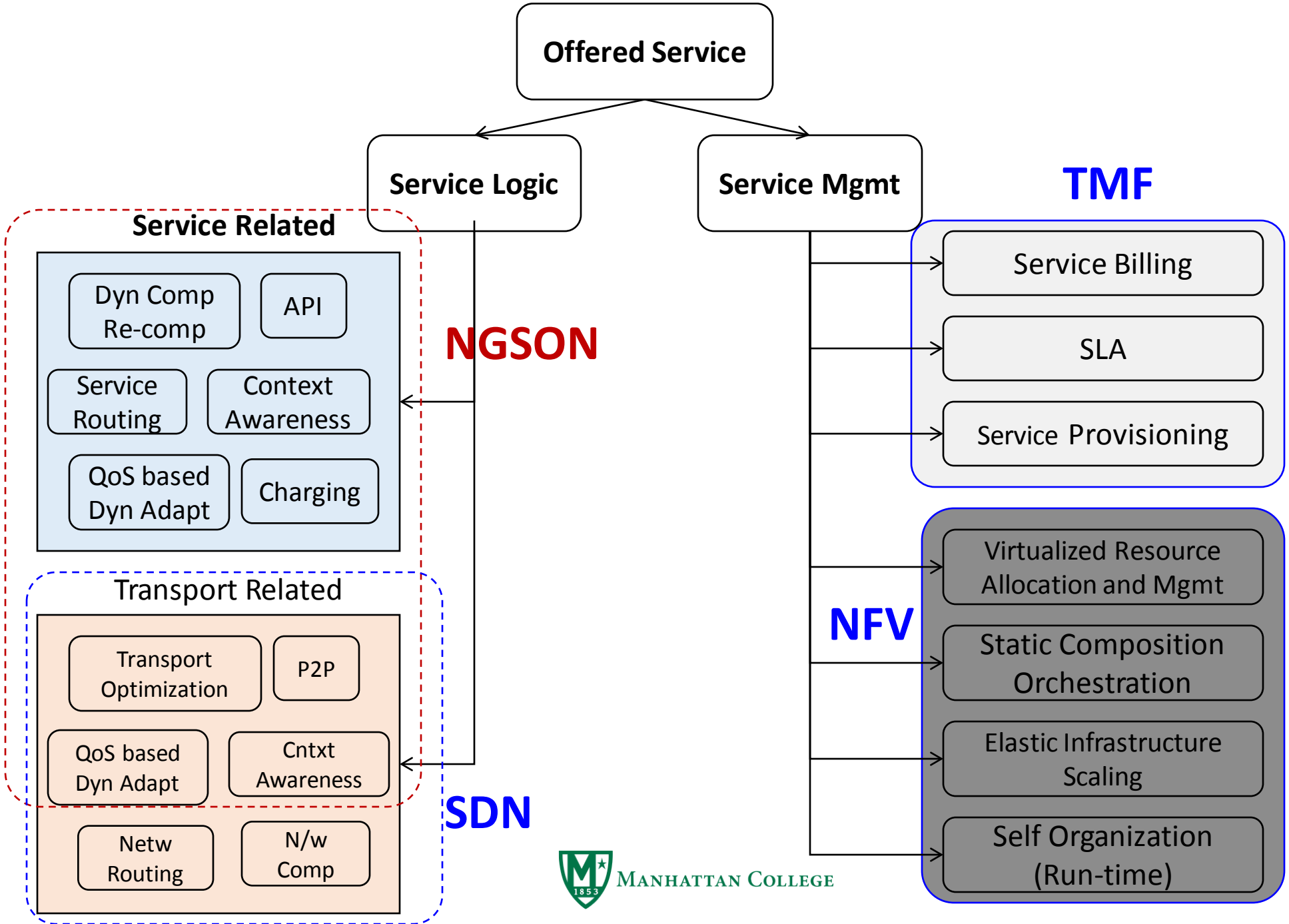


- NGSON network operators to reduce OPEX of NGSON networks based on self-organizing management capabilities of NGSON including self-configuration, self-recovery and self-optimization of NGSON nodes and functional entities

Self-Organization Aspects - Built-in

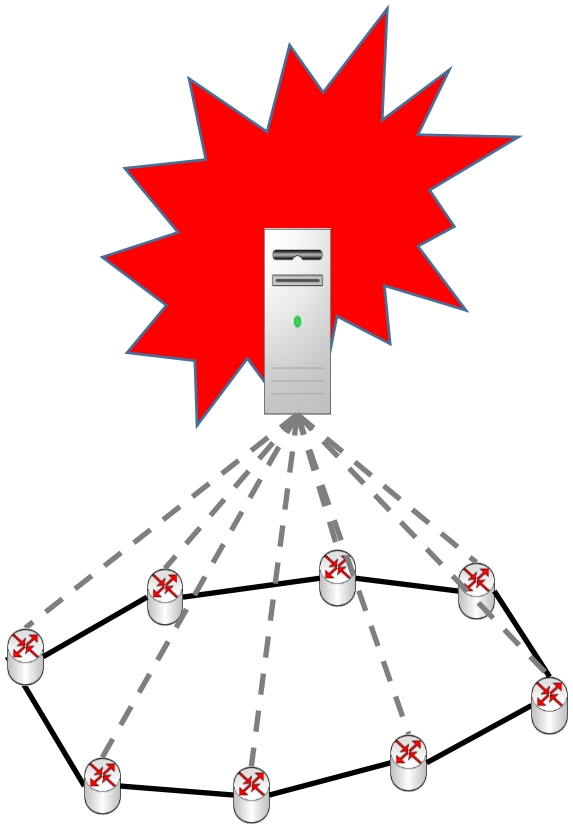
- Self Organization
  - Self Healing (a.k.a., Self Recovery)
  - Self Optimization for performance reasons
  - Self Configuration – typically triggered by self healing or self optimization such as load balancing
- "Self-Configuration" Operations Examples
  - ADD NGSON FE
  - DELETE NGSON FE
  - MOVE NGSON FE
  - COPY NGSON FE
  - ACTIVATE NGSON NODE
  - DEACTIVATE NGSON NODE

Large Scale Deployment (Cloud)
Automated Management
Virtualized NGSON Functions
Decoupling Hardware and Software


Offered Service
Service Logic
Service Mgmt
TMF
Service Related
Dyn Comp Re-comp
API
Service Routing
Context Awareness
QoS based Dyn Adapt
Charging
NGSON
Service Billing
SLA
Service Provisioning
Transport Related
Transport Optimization
P2P
QoS based Dyn Adapt
Cntxt Awareness
Netw Routing
N/w Comp
SDN
NFV
Virtualized Resource Allocation and Mgmt
Static Composition Orchestration
Elastic Infrastructure Scaling
Self Organization (Run-time)

RAS Concerns in SDN and OpenFlow

- SDN raises serious performance, scalability, reliability, and security concerns
- Centralized or distribute, the control plane is troublesome:
  - Reliability - bottleneck
  - Performance - bottleneck
  - Scalability - placement, connections, etc.
- Secure in OpenFlow based networks is an active research area:
  - Control channel between the controller and switches: TLS optional
  - This leads to a number of vulnerabilities (e.g., Listener Mode)
  - Even with TLS implemented, there are still several concerns



SDN Control Plane: Distributed Physically, but …

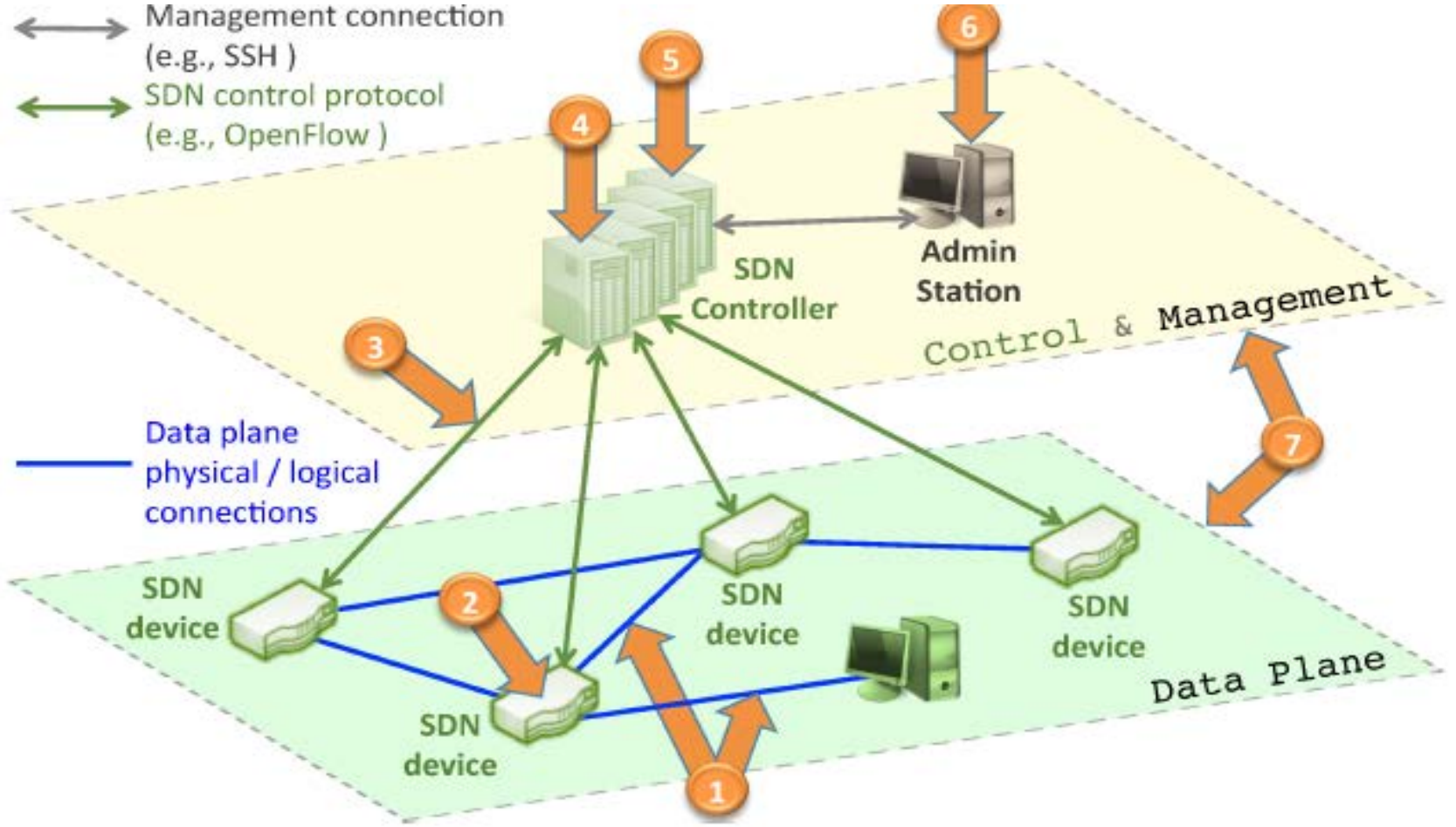
- Logically-centralized controller must be physically distributed
  - This will help to increase scalability, reliability and availability
  - But, it raises new challenges:
    - Staleness versus optimality; application logic complexity versus robustness to inconsistency
    - Controller placement problem
      - How many and where?
      - How to assign switches dynamically to controllers: based on controllers' load estimates ?
      - How to handover switches from one controller to another dynamically (when needed)?

B. Astuto, et. Al. "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," hal.inria.fr/hal-00825087/PDF/hal_final.pdf

Performance of OpenFlow Networks

- Hard to predict because:
  - OpenFlow is different:
    - Control plane performance + data plane performance
    - Performance variations of equipment used in different vendor equipment
  - Each vendor has a different OpenFlow switch:
    - Flow table size, flow management policies, switching hardware resources
- Key performance metrics associated with an SDN controller:
  - Flow set-up time, and
  - Number of flows per second that the controller can setup
- Factors that play key role:
  - Processing power of the switch
  - Processing and I/O performance of the controller
  - Reactive vs proactive setting up the flows
- Need new tools, new emulation software to predict SDN performance

Threat Vectors of SDNs



D. Kreutz, et. Al. "Towards Secure and Dependable Software-Defined Networks," HotSDN '13, Aug 2013

Vulnerabilities Observed in OpenFlow

- Control channel between the controller and switches:
  - OpenFlow protocol runs over TPC with TLS being optional!!!
    - TLS requires multiple certifications → difficult, thus ignored by many vendors
    - → an avenue for adversaries to infiltrate OpenFlow networks and remain largely undetected
- Even with TLS implemented, there are still several concerns:
  - Switch authentication - if ignored, attacker can observe controller response
  - Flow Table Verification - detect switches that erroneously alter rule
  - Denial of Service Risks, - higher with the centralized control
  - Controller Vulnerability - OpenFlow apps performing deep packet inspection on the host responsible for the control of the whole network

"K. Benton, et. Al., OpenFlow Vulnerability Assessment," HotSDN '13, Aug 2013

Vulnerabilities Observed for OpenFlow Apps

- The open interface between the controller and applications and the involvement of multiple parties is another big concern (control layer attack)
  - A survey suggest that all state-of-the-art OpenFlow platforms expose the full privilege of OpenFlow indiscriminately to every app without protection
- A possible solution
  - Use a permission system that incorporates a customized permission set and a thread-based isolation mechanism to enforce least privilege on the level of OpenFlow apps
- Creating secure networks using OpenFlow is an active research area
  - Some examples: FRESCO, FortNOX, FlowVisor

X. Wen, et. Al. "Towards a Secure Controller Platform for OpenFlow Applications," HotSDN '13, Aug 2013

Other Security Concerns for SDN Networks

- Ability to support enterprise class authentication and authorization of the administrators of the network
- Ability to lock down access to SDN control traffic
- Ability to apply sophisticated filters to packets
- Ability to ensure that each tenant that is sharing the infrastructure has complete isolation from all of the other tenants
- Ability to both rate-limit the control communications, and to be able to alert the network administrators when the network is experiencing a suspected attack

Reliability-aware Controller Placement for SDNs

- SDN decouples control and forwarding planes
  - Such separation introduces reliability design issues of the SDN control network, since disconnection between the control and forwarding planes may lead to severe packet loss and performance degradation
- A solution lies in placing controllers in SDNs in such a way, so as to maximize the reliability of control networks
  - Placement algorithms?
- Need a metric to characterize the reliability of SDN control networks

Y. Hu, et. Al. "Reliability-aware controller placement for Software-Defined Networks," IEEE IM'13, May 2013

Increasing the Network Reliability by Controller

- Alternative 1: A single path from source to destination,
  - When a link fails, the controller must be capable of rerouting the traffic onto on of the other operational links
    - Controller must monitor the network topology in real time
    - Computation of the new forwarding state (in response to a failure) takes place at the controller
      - Requires an extra SW logic at the controller; if modular architecture, then each module needs its own logic → difficult to develop, error prone
- Alternative 2: Incorporate into the controller the ability to discover and sets multiple paths from source to the destination.
  - If a single link on a path fails, there are other paths that can be used to route the packet

Increasing the Availability of the Controller

- Redundancy
  - With both hardware and software redundancy features
- Clustering
  - 2 SDN controllers increases reliability (one active, another in hot standby)
  - 3 or more SDN controllers increases the availability, performance and scalability (one in hot standby)
    - Important: maintaining the synchronization of the memory between the active and standby controllers

NFV Requires Redefined Telecom Resiliency

- The traditional telecom reliability:
  - 99.999 % reliable → Hardware fails an average of 3-5 minutes per year
  - Traditional, purpose-built telecom hardware to meet this standard
- The shift to SDN and NFV → use of commercial off-the-shelf (COTS), commodity hardware
  - Expect failures all the time at the hardware layer
  - Are service providers willing to accept the reduction in reliability?
- Need to design services differently and measure service uptime, instead
  - Service downtime vs hardware downtime – need to build resilient software
- Virtualization will require different tools to address trouble alerts, root cause analysis, and recovery
  - It is a virtual network, the elements that make up a service will in many different places
  - Detecting trouble won't be as simple as observing a red light

Recent Standardization Activities

- IEEE ComSoc Study Group
  - On April 25, 2014, IEEE ComSoc Standardization Activities Council, after a one-day working meeting of experts, concluded to form a Study Group on the Reliability and Security of the Software Defined Ecosystem
  - The group will perform a gap analysis and recommend an action toward formation of IEEE project Working Group to work on and produce IEEE standards in this area
  - Ultimate objective is to create standardized reliability and security related specifications for a broad vision of software defined ecosystem
- "Reliability and Availability" WG of ETSI ISG NFV chartered
  - On January 17, 2014, the "Reliability and Availability" WG within ETSI's Industry Specification Group on "Network Function Virtualization" was chartered
  - The group will provide resilience guidelines for the general NFV architecture and the software functions
  - Moreover, the WG will provide engineering guidelines and methodology for high-resilience systems built from low-reliable components

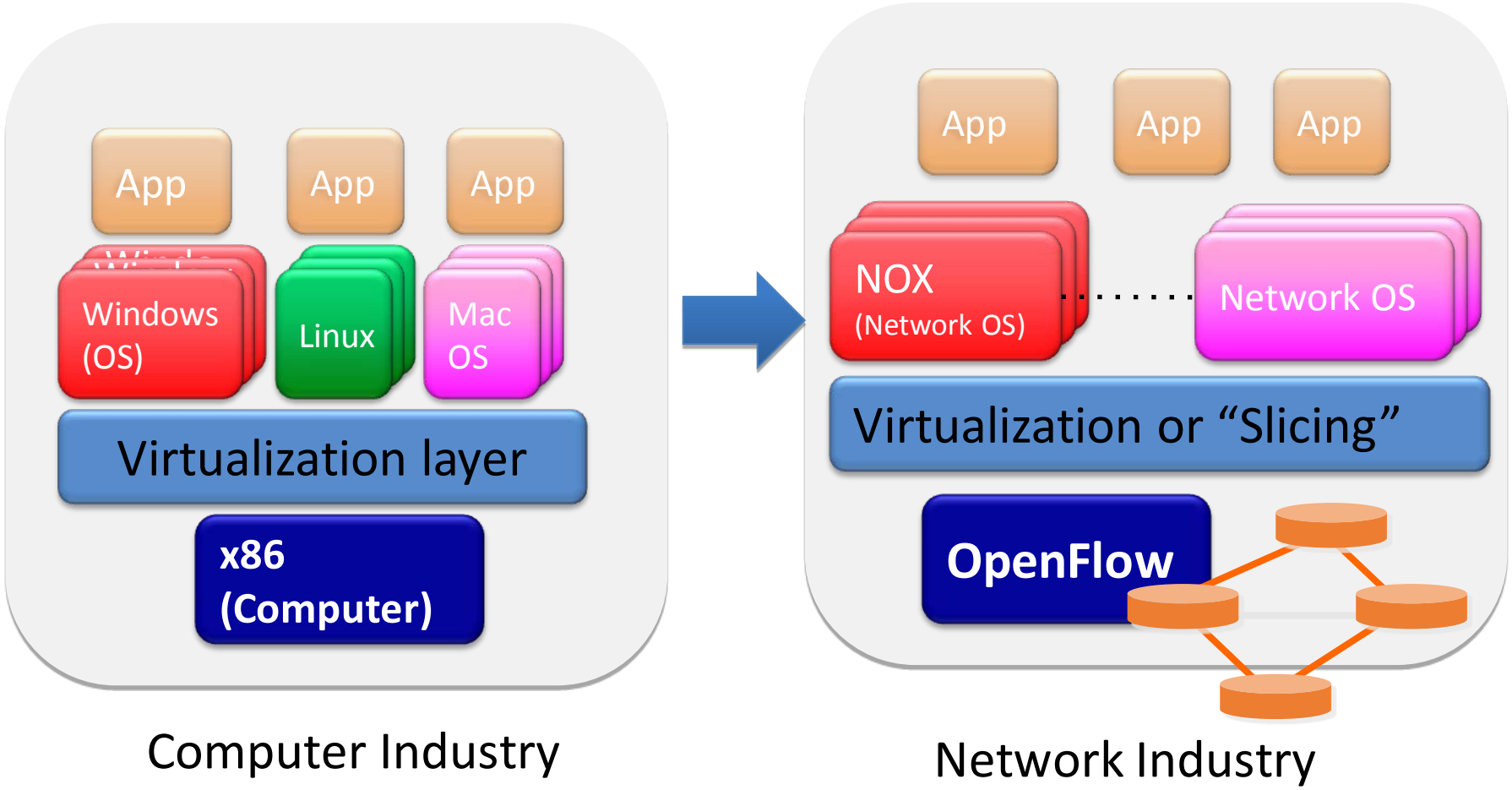
Conclusion

To Fulfill the Promise of Service Convergence in Emerging Technology based Networks

The industry needs, immediately, a set of reliability metrics and terminology that are common across the network for which individual service availability requirements can be specified.

Backup Slides

Toward Commoditization

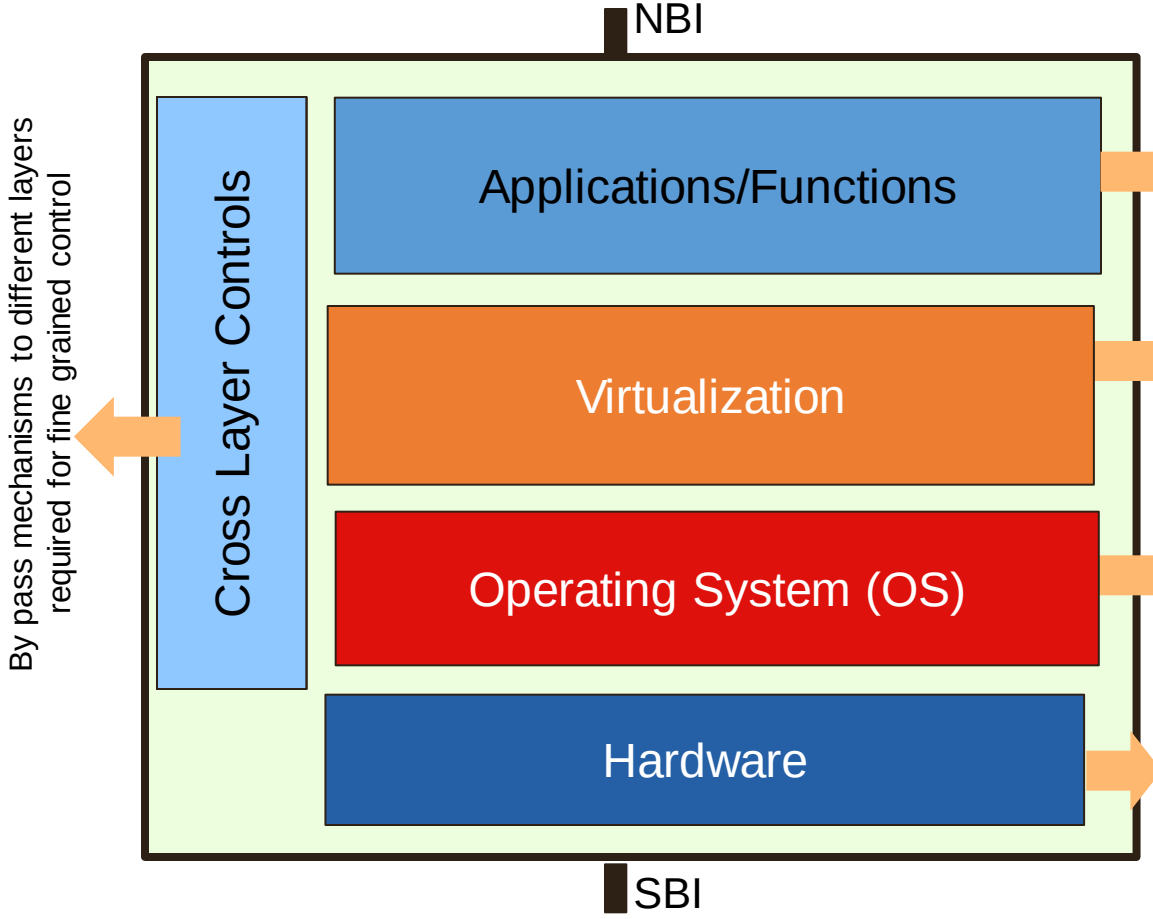


Computer Industry

Network Industry

A General Framework for the Broad Vision of SDN

Can be instantiated and used recursively for a variety of environments including SD-A, SD-RAN, SDN, SDN-SP, NFV, NGSON, Cloud, etc.



Applications, Orchestration functions, or Algorithms for a scenario to be controlled. Initiates the control signals to the Programmable functions (e.g. Congestion Control, Service Routing, Self Organization). Specification of Controls for programmable functions (e.g., Rules, Program Languages). Exposed as APIs for Apps to code

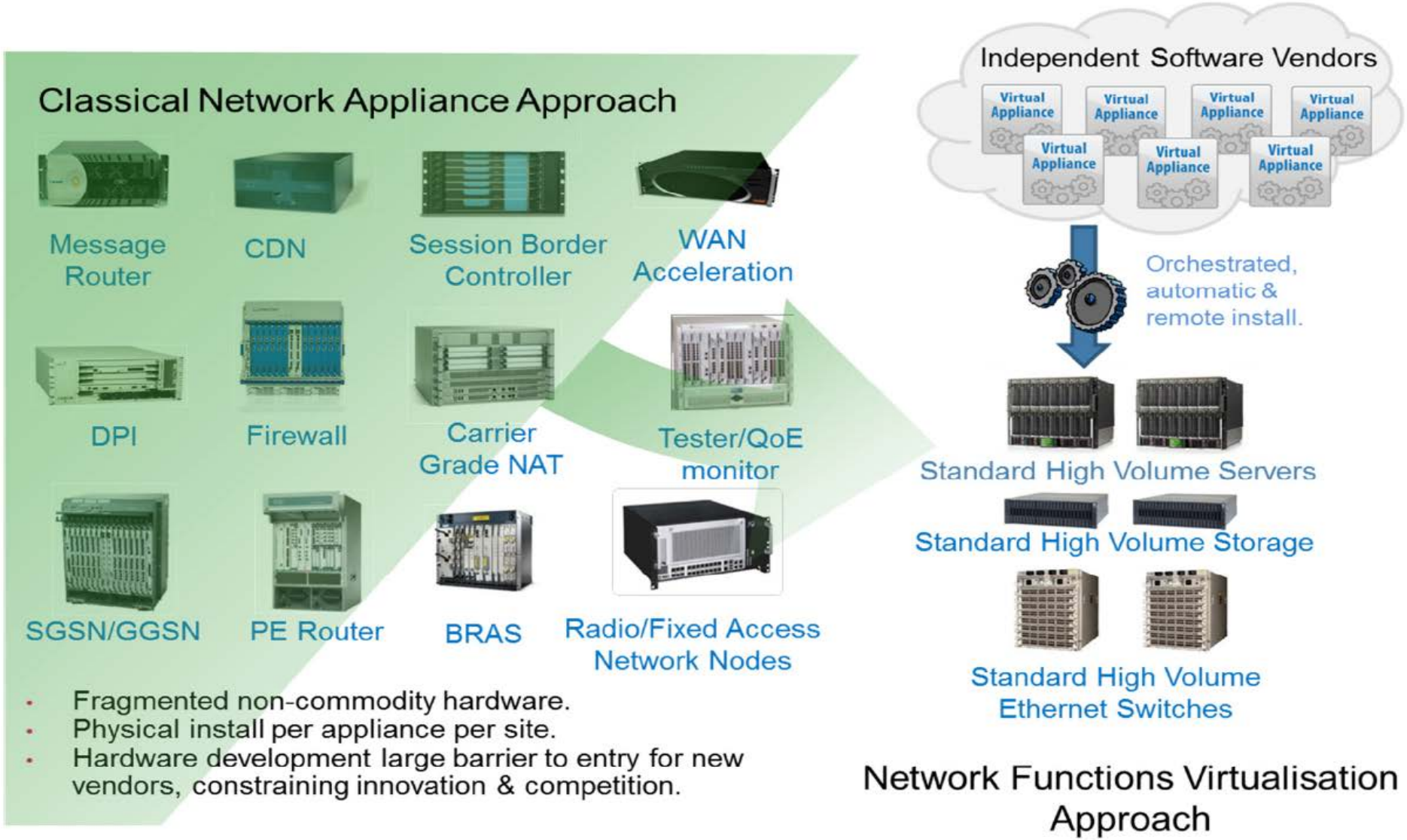
Virtualization of the functions for business policy control (e.g., Choose controller, allow control execution, single point access). Critical functions execution designed for programmability (e.g., Flow Table, VM Configuration, Service Routing table)

Operating system should support programmable control functions with real time characteristics. Provide Services abstraction and support Northbound/Southbound APIs

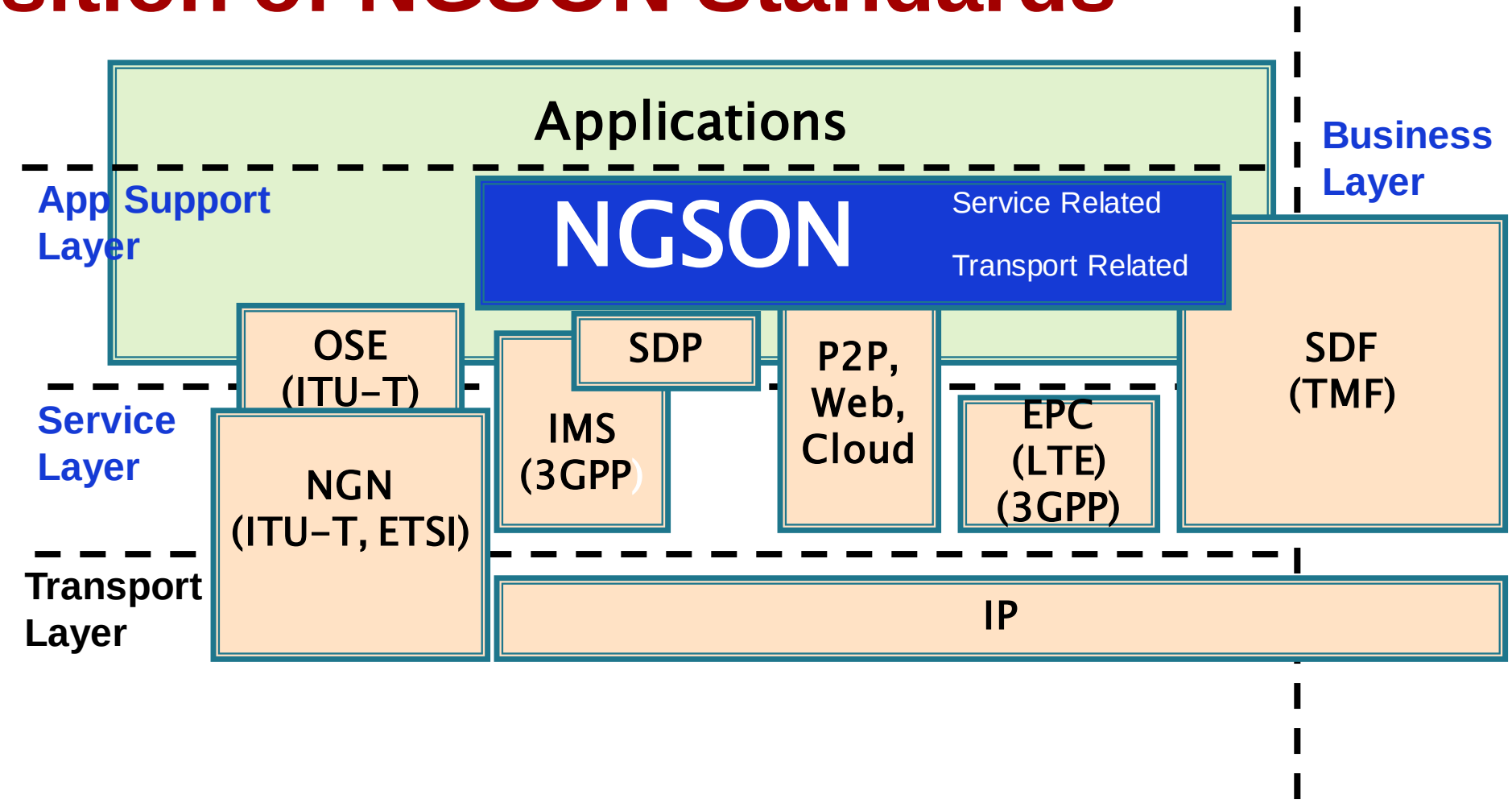
Commodity Hardware capable of operating on any layer like Radio, Network, Services, etc., which can provide real time characteristics

North Bound Interface/South Bound Interface: Business applications, Interworking with other SDNs like Controller – Controller, OS-OS, Orchestration, Cross Layer

ETSI NFV Industry Specification Group's Vision



Position of NGSON Standards



- IMS/NGN: focus on the underlying infrastructure and networking technologies to facilitate services
- Others: focus on different aspects (e.g., SDP has service delivery oriented purpose, centralized architecture)