WHITE PAPER

Service Provider Network Maturity Model

A White Paper from Intel® Corporation

Executive Summary

As a part of a broader strategy to fend off increasing competition from non-product traditional sources and relegation to utility status, telecommunication Service Providers are focused on transforming into software and digital business/services organizations. In order to achieve this lofty goal, the network needs to become more agile, simple, flexible and cost-effective, all while shortening innovation cycles and new service deployment — from months to moments.

Software-defined networking (SDN) and network function virtualization (NFV) promise to revolutionize the industry, but proprietary solutions, legacy business models to protect, and a lack of open interoperability threaten their transformative nature. Key to enabling this transformation are the investments that both Service Providers and ecosystem participants are making to efficiently and effectively accelerate SDN and NFV adoption. In this fast-moving and dynamic environment, some common questions arise:

- Which initiatives or investments should the Service Providers make in the medium term (2015–2020) to realize the promise of SDN and NFV?
- What are the hurdles to adoption that can be planned for?
- How will the Service Providers and supplier ecosystem evolve?
- How does my progress compare to that of my peers?

This paper attempts to answer these questions by proposing a Service Provider Network Maturity Model — a framework by which Service Providers can prioritize activities, measure their progress, and benchmark against best-in-class developments. The Network Maturity Model provides a detailed view of how the Service Providers mature their SDN/NFV capability. The Maturity Model is based on an analysis of key milestones and the precursor dependencies' gating and pacing progress. The unique nature of the telecommunication networks evolution leveraging SDN and NFV technologies takes into consideration the motivations, industry trends, and unique challenges for telecommunication Service Providers.

The driver for NFV is to reduce cost (CapEx/OpEx) and drive new revenue-generating services. Leading Service Providers have devised the basic recipe for success through programs such as AT&T Domain 2.0*, Telefonica UNICA*, Vodafone Spring*, and Deutsche Telekom TeraStream*. While the programs are initially

Table of Contents

Executive Summary 1
Clarification of Scope and Definitions 3
Market Realities for Telecom Service Providers 3
Motivation for Transformation 3
Framework to Create Service Provider Network Maturity Model 3
Choice of Open versus Proprietary Solutions 4
Guiding Principles Utilized in Model Creation 4
Service Provider Network Maturity Model Summary 6
The Five Phases 6
Service Provider Network Maturity Model Phases 7
NMM0: No Virtualization 10
NMM1: Standalone VNFs 10
NMM2: Common Information Models 11
NMM3: Network Function Auto-Scaling 12
NMM4: Federation of SDN 13
NMM5: Full Service Automation 13
Hurdles for Migration to SDN and NFV 15
Technical Hurdles 15
Changes in Culture 15
Recognition of New Business Models 15
Skills Gaps 15
Intel's Vision for SDN/NFV 15
The Role of Open Source in the New Service Delivery Model 16
How Intel Is Helping to Drive Maturity/Openness 16
How Service Providers Can Help Drive Market Maturity 17
Implications for Vendors 17
Conclusion 17
Glossary of Terms 18

focused on CapEx reduction as their primary focus, they need to alter their organizational structure, acquire new skill sets, align executive- level sponsorship, and provide organizational authority to successfully achieve transformation to drive OpEx reduction and ultimately enable new revenue-generating services.

In this context, transformation means bringing network capabilities closer to developers (e.g., DevOps), consumers (e.g., media offerings) and enterprises (e.g., IoT services), while simultaneously increasing service velocity. By transforming its network from a utility to a platform for digitally delivered services, the Service Provider can maintain relevance, capture new revenue streams, and avoid commoditization. By maintaining visibility to the end customer, the Service Provider can facilitate innovation with the network in mind, and ensure it has the power to extract newly created value from the top of the network. Without this, Service Providers can find that their services will become undifferentiated, and cost-competition will ensue.

Service Providers need to find a profitable way to meet increasing demand. The solution recipe, devised by the Service Providers, is made up of four (4) elements:

1. CapEx reduction via common hardware and software ingredients (everything between the applications and hardware);
2. OpEx reduction and OpEx alignment to revenues through virtualization;
3. Adoption of new skills and organizational structure, allowing fast innovation in a service-oriented culture; and
4. Service innovation, development, and service launch similar to those achieved by the OTT provider (such as Google and Amazon).

Table of Figures

Figure 1. Maturation Loops 4
Figure 2. Process in Which "Feedback and Control" Loops are Closed 5
Figure 3. Network Maturity Model Phase 1 11
Figure 4. Network Maturity Model Phase 2 12
Figure 5. Network Maturity Model Phase 3 12
Figure 6. Network Maturity Model Phase 4 13
Figure 7. Network Maturity Model Phase 5 14

Clarification of Scope and Definitions

The title of this paper, “Service Provider Network Maturity Model,” requires definition to ensure that what is ‘in scope’ vs. ‘out of scope’ is clear.

This paper is focused on telecommunication Service Providers, both large and small. Companies such as AT&T, Deutsche Telekom, Vodafone and Telstra are in scope. Enterprises (e.g., Wal-Mart) and Cloud Service Providers (e.g., Amazon), who are also virtualizing their networks, are out of scope. The pain points, opportunities and appetite for risk of Enterprises and Cloud Service Providers differ significantly from those of telecommunication Service Providers, and hence the Maturity Model would be different.

Within telecommunication Service Provider organizations, this paper is targeted at the senior-level decision makers and influencers. For example, CTOs responsible for the network core and who are driving service delivery transformation to enable digital business, CIOs focused on transforming IT, and CMOs interested in shifting the focus from network utility services to digital business services should be considered the primary audiences.

Market Realities for Telecom Service Providers

Motivation for Transformation

Rigid Networks

A Service Provider’s economic value depends on its network’s reliability, scalability and availability to deliver services. Networks are carefully managed and tested, given their requirement to deliver critical services, such as 911 and security. Due to the dependency and importance of the network, Service Providers avoid risk and modifications to the network by demanding a very methodical implementation process. Interfaces, protocols and services require years of standardization before any “innovation” is actually introduced by vendors. As such, integration and introduction of new services may take several months to implement.

Changing Customer Demands on the Network

Networks exist to deliver applications, services and user experiences. Due to the introduction of the smartphone, proliferation of mobile devices, and the near-ubiquity of network access, new innovative applications and services are quickly and substantially increasing demands on the network infrastructure.

Changing Cost Structures

Legacy network cost structures are not favorable to Service Providers, as they are dominated by large capital expenditures (CapEx). Vendor lock-in is reducing the ability of Service Providers to evolve their cost structures. Network transformation brings opportunities to drive innovation and mitigate vendor lock-in — effectively reducing capital and operating costs.

Fighting to Avoid Commoditization

In an environment where new competition is arising from OTT players (such as Google and Amazon), where demand for network capacity is outstripping the revenue generated, where fixed costs are enormous, and where the pace of innovation in the network equipment market is driven by vendors, Service Providers are finding they are in a fight for relevance and a fight to avoid commoditization.

Framework to Create Service Provider Network Maturity Model

Maturity models have been used in a variety of new and evolving markets to help organizations develop a programmatic approach. From cloud adoption[1] to consumer privacy[2], maturity models have provided a framework by which organizations can measure their progress against benchmarks. The organizations undertake the following steps to develop the programmatic approach:

- Assess the current phase of maturity
- Identify the future phase of maturity that aligns with business goals and objectives
- Develop a road map with a list of initiatives to reduce the gap between the current phase of maturity and the future phase of maturity

In markets such as NFV and SDN, maturity models can help telecommunication Service Providers:

- Understand the dimensions that constitute SDN/NFV adoption maturity
- Identify hurdles to market adoption and work with the ecosystem to overcome them
- Focus on initiatives to move selected capabilities to target maturity phases at the appropriate time

The maturity model proposes an approach to broad market adoption of SDN and NFV technologies. To achieve broad market adoption, the solution must have achieved the *Vectors of Maturity*:

Scalability, Reusability, Interchangeability, Reliability, Security and Performance

[1] Open Data Center Alliance Cloud Maturity Model - http://www.opendatacenteralliance.org/docs/Cloud_Maturity_Model_Rev_2.0.pdf

[2] AICPA/CICA Privacy Maturity Model - http://www.kscpa.org/writable/files/AICPADocuments/10-229_aicpa_cica_privacy_maturity_model_finalebook.pdf

Telecommunication Service Providers are conducting trials and limited deployments that incorporate various phases of the maturity model. For example, there have been “end-to-end” proof-of-concepts and/or trials, which incorporate interactions with OSS/BSS, orchestrator, VNFs, and NFVI. While the demonstrations are incredibly important to move the market forward, they are not an indication of maturity. In order to achieve optimal scale, multi-use, and interchangeable deployment infrastructure, we believe that the SDN/NFV adoption initiatives should be in alignment with the phases defined in the model. Unless these demonstrations have achieved *the milestones as defined by the Vectors of Maturity*, they are not mature.

Choice of Open versus Proprietary Solutions

While the maturity model does not distinguish between Open Source and Open Standards vs. proprietary solutions, it is commonly acknowledged that using vendor-specific (lock-in) or proprietary solutions enables portions or all the maturity model milestones to be achieved. While Service Providers are willing to accept proprietary solutions in order to get to market faster, their ultimate desire is to move away from vendor lock-in. In alignment with their objective, our proposed maturity model, phases and milestones take into consideration the Service Provider requirements of open, standard interfaces and interchangeable components.

Guiding Principles Utilized in Model Creation

There are an abundance of “moving parts” across the Service Provider SDN/NFV ecosystem that impact the path to maturation. As guiding principles, it is fundamental to understanding the motivations for the network transformation, the hurdles to adoption of these technologies, and the impact these transformations will have on existing and new innovative services. The last point is particularly important: the network must have high availability and the customer experience cannot be negatively impacted by the adoption of SDN/NFV technologies.

Another guiding principle used within the context of this maturity model is that Service Providers will lead with NFV adoption and will adopt SDN soon after. While Service Providers may choose either SDN or NFV as a starting point, our assessment of the majority of SDN/NFV use cases suggests that Service Providers lead with NFV.

The constituent elements of end- customer service assurance are embodied by the *Vectors of Maturity.*[3] In brief, the network must not only push packets from point A to point B with acceptable throughput and latency, but also do so in a fashion that maintains the reliability and security that customers and applications demand. Achieving the *Vectors of Maturity* is becoming even more complicated in multi-layered virtualized world where elasticity, service chaining, hybrid cloud domains, and virtual SDN network elements permeate the rapidly expanding network.

The hurdles and unknowns described above have a direct influence on network transformation maturity. Scale requires automation. Automation requires programmability. Programmability requires data gathering, analytics, and control interfaces that allow real-time changes to the network. At a high level of abstraction, network reliability/ programmability can be envisioned as several nested “feedback and control” loops.

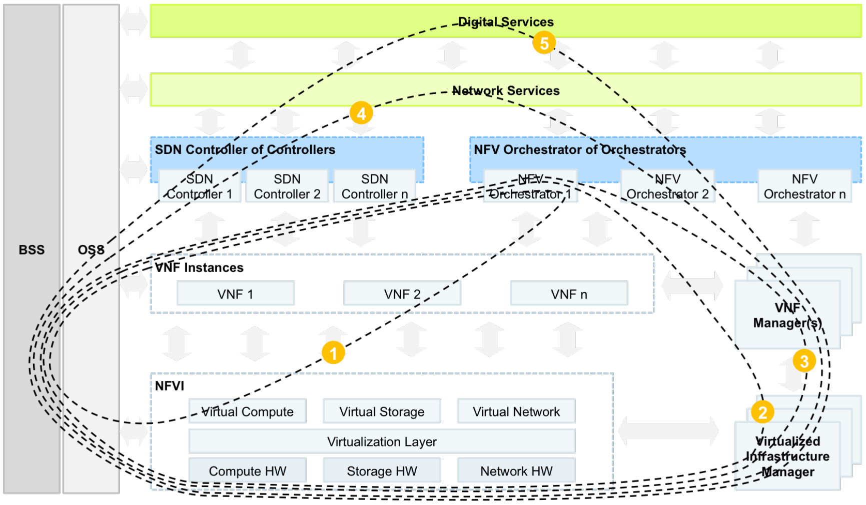

Figure 1: Maturation Loops

In order to achieve the benefits of a virtualized network, a strong base must be built at the innermost control loop and expand outwards to larger and larger loops. This is not to say that as an industry we should not focus on the larger loops. The

[3] The Vectors of Maturity are Scalability, Reusability, Interchangeability, Reliability, Security and Performance

maturation loops depicted in Figure 1 will be explained further in the Network Maturity Model.

When analyzing our model, consider that the overall requirement of service assurance is built on a foundation of monitoring, analysis and manageability. In order to program a network, we must have “intelligence” that is built on a common framework for analytics and telemetry. In order to provide analytics, timely reporting of relevant data must be sent to the analytics engines. Data Reporting → Analytics → Programming. As such, each feedback and control loop will progress as follows:

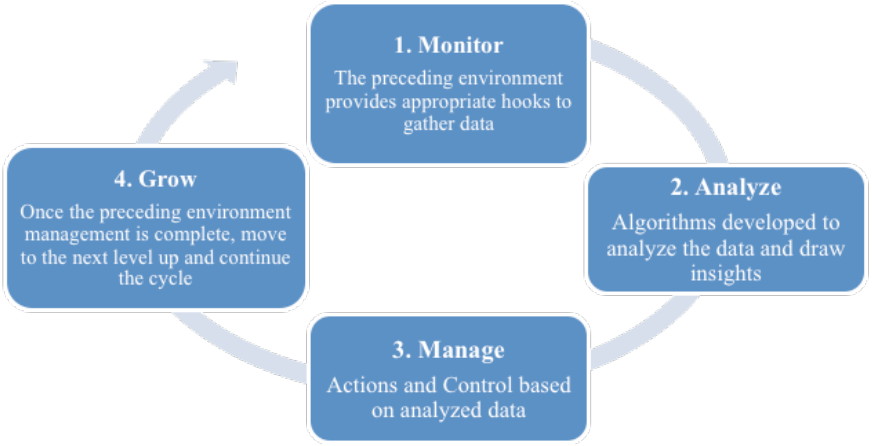
1. Monitor
The preceding environment provides appropriate hooks to gather data
2. Analyze
Algorithms developed to analyze the data and draw insights
3. Manage
Actions and Control based on analyzed data
4. Grow
Once the preceding environment management is complete, move to the next level up and continue the cycle

Figure 2: Process in Which “Feedback and Control” Loops are Closed

As an example, please consider a loop which contains the elements NFVI, VNF, VNFM and VIM. These elements must work together in a closed-loop fashion to provide a foundation for higher orders of abstraction. The steps discussed in Figure 2 will need to be executed in unison to achieve this closed-loop process.

- Step 1: Data from the VNF and NFVI are gathered to provide an indication of how the VNF and NFVI are behaving in a real deployment.
- Step 2: These data will be analyzed to draw insights. How is the infrastructure being utilized? Are the resources required by the VNF consistent with its SLA? Does the infrastructure provide enough capacity to run the VNF as specified by the SLA? Does the traffic require more additional VNFs to support SLA?
- Step 3: Once data have been gathered and analyzed, decisions can be made. Now the network can adjust or notify higher levels of abstraction in the management and orchestration framework.
- Step 4: Now that this loop is closed and behaving appropriately, the industry can focus on maturing the next-order loop, such as a multi- VNF service.

This sort of feedback loop reflects the activities normally found in Service Provider Operational groups, where underlying services may be incorporated and complemented with value additive components to deliver a higher-level service that can ultimately be consumed as a product delivered to end user customers. NFV forms three layers of service, each of which will probably be operated as a distinct entity in the short term. If we were to consider a “Firewall as a Service” capability, that could be decomposed as follows:

- The Firewall VNF will have a “Descriptor” that defines the infrastructure resources required to support a specific service instance. The VNF Descriptor will be used to instruct the VIM over an “IaaS” interface, and the IT/Cloud supplier will then need to ensure that the capacity is actually being delivered as part of the IaaS Assurance.
- Next, if the Firewall VNF was specified as being capable of delivering a specific performance KPI (e.g., throughput of XX Gbit/s) then that is described as a “Network Function as a Service”. It is then the responsibility of the VNF Operations unit to ensure that the service instance is actually delivering the specified capability, which could be affected by either software issues (such as memory “leaks” or configuration errors), or a failure by the underlying IaaS.
- Finally at a “Service Orchestration” layer that delivers the Firewall function as a Network Service, another operational unit may need to consider the required traffic handling capacity at a point in time. That unit could handle capacity delivered from legacy physical appliances, and bring into service additional capacity based on virtualized infrastructure only when needed. This might involve hot-standby working where VNF instances are running prior to production needs and can be made available more quickly than typical IaaS and VNF deployment timeframes.

The example highlights the synergy and mapping between Network Operations and Cloud practices (such as IaaS, PaaS, and NaaS) and the necessary operational evolution to realize a virtualized network function in practice.

Service Provider Network Maturity Model Summary

The SDN/NFV maturity in a service provider environment has been divided into five (5) major levels of maturity. The goal is for each phase to have, qualitatively measured, a significant level of improvement from the previous phase and have surpassed a major hurdle. These phases are called NMM1– 5, that is, Network Maturity Model (NMM) Phase 1, 2, 3, 4 and then 5.

On a larger scale, NMM1–3 can be thought of as "Maturation of VNFs." It is during these phases that VNFs become more manageable, tenant-aware, align with SLA requirements, and can bill appropriately. NMM4–NMM5 can be thought of as "Maturation of Network App/Services." During this phase we see the emergence of applications and services at the network level. For example, Data Center Power Optimization and Network Traffic Engineering will be achieved during these phases.

The maturity model has been broken down into five (5) key areas to help Service Providers address all facets of their business:

- Business and Services — How the business and related services need to evolve to take advantage of the benefits of SDN/NFV
- Technology — How the technology needs to be adopted and deployed in the Service Provider's environment
- Organization — How Service Providers need to think about organizing and sponsoring programs to ensure success
- Governance — How to govern financial and operational components of the new solution
- Customer — How the customer experience is changed by NFV/SDN adoption

The Five Phases

- Phase 1: Standalone VNFs — Commercialization of isolated services. Individual VNFs that make up the service may be from separate vendors, but are orchestrated by a solution from a single vendor.
- Phase 2: Common Information Models — VNF vendors characterize and provide network function SLA via VNF descriptors with a common information model.
- Phase 3: Network Function Auto-Scaling — Network Function Auto-Scaling, or elasticity, is defined as horizontal scalability. As network traffic expands and contracts in real time, Service Providers can re-purpose existing or add hardware or software independently to boost capacity.
- Phase 4: Federation of SDN — An end-to-end network view enables applications/services that take advantage of the entire network, including tasks such as data center power optimization and network traffic engineering.
- Phase 5: Full Service Automation — The analytics loop is closed and able to gather data, analyze data, and program the network appropriately. Applications are able to request services from the network, which will automatically adjust to meet the new service level requested.

Service Provider Network Maturity Model Phases

Area	Capability	Phase 0: No Virtualization	Phase1: Standalone VNFs	Phase 2: Common Information Models	Phase 3: Network Function Auto-Scaling	Phase 4: Federation of SDN	Phase 5: Full Service Automation
Business and Services	Service Provisioning/ Time-to-Marke	• Changes to existing services take place only during scheduled maintenance windows • New services may take weeks or months to bring to market • Plan and provide infrastructure processes for dedicated proprietary appliances including the commissioning for service generally takes 12-18 months, which leads to over procurement to handle unexpected future demands. • IT servers available "Commercially Off The Shelf" – no virtualization	• In service upgrades to standalone VNFs can take place dynamically with no service interruption • Vendors change fees for any new capabilities or enhancements remain high	• Faster onboarding of VNFs with centralized control for rapid service delivery • Improved service monitoring, speeding and hardened solutions to market • More innovative solutions	• Network and Service visibility and analytics enabling dynamic scaling and network elasticity	• New services created and deployed in seconds/days rather than weeks/ months • Coupled with reusable hardware, enables true "Innovation" platform where the majority of new service experiments are expected to fail in the market. As opposed to classic Telco product development that typically waits until the market requirement and opportunity is proven given cost structures	• Optimal resource utilization, network optimization and investment protection through better provisioning and tighter alignment with SLAs
	Digital Services Enablement	• Traditional Telco: Limited digital service offerings	• Initial/ potential use cases are being developed and trialed	• Limited portfolio of digital consumer and enterprise services • Telemetry data is available —enables next generation of digital services	• Demonstrable digital service use case implementations • Revenue benefits are quantified	• Applications/ services to develop that take advantage of service/ network optimization across data center power and network traffic • Underlying VIM/ MANO/ SDN layers are stable enough to allow network-wide applications and services	• New service generation with customer service and customer acquisition focus
	Security	• Minimal end-to-end network security policy framework • Security policies focused on physical infrastructure	• Individual secure VNFs • Minimal scalable policy framework • Minimal scalable forensics or remediation	• VNF system resource isolation/DMZ • VM to VM secure traffic	• Secure VNF(s) environment across network service	• Controller security – secure individual domains and cross-controller domain secure communication	• End-to-end secure and hardened Network applications and service environment • Network traffic awareness and traffic management for filtering and communication with threat management solutions for threat identification and handling

Area	Capability	Phase 0: No Virtualization	Phase1: Standalone VNFs	Phase 2: Common Information Models	Phase 3: Network Function Auto-Scaling	Phase 4: Federation of SDN	Phase 5: Full Service Automation
Technology	**Platform Openness and APIs**	• Network delivered via proprietary vertically integrated "boxes" (both hardware and software) used to support network function	• Common software components (such as a vSwitch, host OS, hypervisor, etc.) that provides sufficient network function performance for KPIs including: throughput, latency, jitter • Software and Service testing/ methodology to ensure network service SLA.	• Common information models that enable onboarding multi-vendor VNFs • Consistent SLA across VNF vendors offered via VNF descriptors based on common information model	•Improved choice offered by interoperability of the linkage between VIM/MANO and SDN controller layers • Support for "complex" virtualized function that is created through chaining of more than one VNFs from multiple vendors • Abstracting services from existing physical appliance infrastructure to achieve automated service orchestration	• End-to-end network view which includes the backhaul • End-to-end network traffic engineering is enabled	• Automated provisioning enabled by the integration of northbound applications with network to offer the ability of network to automatically adjust to changes in service levels
	Data Center Hardware	• No logical or physical separation of Network Hardware and Software (limited ability to support VNF) • No separation of data and control plane (no SDN)	• Abstraction of network hardware from purpose-built boxes to commodity hardware • Virtual machines from the vCPE and vEPC domains do not reside on the same physical infrastructure • VNFs reside on x86 COTS platforms	• Horizontal scalability — hardware has become fully virtualized, allowing for elasticity of physical infrastructure	• Analytics allows for improved capacity planning and automated rightsizing of the network and data center hardware	• East/West bound API enables controller-of-controllers	• All applicable network hardware is fully virtualized, automated, scalable, with self-diagnoses/ self-learning and self-healing capabilities
	Hypervisor, Orchestrator and Controller	• No hypervisor, controller or orchestrator	• Introduction of a Type 2 hypervisor to provision resources for VNF • Isolated deployments, not commonly orchestrated, and confined to a small portion of the network • Virtual network functions orchestrated by a single orchestrator from a single vendor • Control is isolated to specific domains with dedicated intra-domain controllers	• Elasticity of virtual infrastructure by adding software licenses • Vendor-independent orchestration environments for intelligent workload deployment • VNF life-cycle management and service assurance (monitor/ control) across the NFVI • Isolated controllers remain • VNF vendors characterize and provide network function SLA via VNF descriptors with a common information model	• Hypervisor is a Type 2 or more advanced version • Network traffic and KPIs dictate scaling of VNFs • Orchestration has become scalable and elastic, and works across vendors • Domain-specific controllers remain isolated	• Orchestrator-of-orchestrators and controller-of-controllers have visibility and control of the once isolated domains • Scaling has become automated, and virtualization proliferates	• Full scaling, automation, and virtualization across all components • Network elements self-learn and diagnose as needed • Orchestrator is completely agnostic and works across vendor solutions and applications • Controller-of-controllers gathers and analyzes data to program the end-to-end network appropriately

Area	Capability	Phase 0: No Virtualization	Phase1: Standalone VNFs	Phase 2: Common Information Models	Phase 3: Network Function Auto-Scaling	Phase 4: Federation of SDN	Phase 5: Full Service Automation
Organization	Organizational Agility	• No institutional focus on SDN or NFV • Pockets of domain expertise across siloed groups of network operations, IT and vendors • Limited flexibility in engineering and innovation models, resulting in slow service delivery transformation and new service configuration	• Initial developments and advancements are being completed by a small group within technology and functional silos • Medium-term road maps that address the VNF adoption • Identification and acquisition of technology and capabilities to support the road map	• Silos (e.g., product development and operations, network engineering and marketing) begin to break down beginning with a modular approach and simultaneous focus on traditional services while exploring new service delivery capabilities • Isolated expertise helps transform operational KPIs to strategic KPIs	• Further break down of silos and formation of cross-functional collaboration between teams (server, network, and application) • Federation of strategic expertise	• Additional investment in cross-functional teams to move from systems of differentiation to systems of innovation	• Cross-functional teams (network, operations, IT, marketing) working to drive project innovation and digital business priorities • Solutions delivered in accelerated timelines (closer to OTT operators) • Service improvements in accelerated timelines (closer to OTT operators)
	Leadership/ Ownership	• No SDN/NFV sponsorship or dedicated resources	• Establishment of SDN/VNF charter • Emerging skills in network virtualization technologies • Identification of roles and responsibilities with SDN/NFV — emergence of CTIO (or a cross-functional role across CTO and CIO) to set strategy	• Emergence of partnership with CMO in SDN/ NFV strategy decisions	• Broader governance framework that aligns multiple BUs / organizations to expand SDN/NFV adoption	• Broad network-wide strategic, business, operations, and supply chain expertise	• Organizational-wide skills and understanding of the benefits and strategic goals of SDN/ NFV • SDN/NFV initiatives adopted by appropriate lines of business
	Network Operations	• Limited understanding of benefits of SDN/ NFV	• Purchase decisions are ad hoc • Focus on cost optimization to reduce the pricing for network functions • Commercialization of isolated deployments of virtualized network functions • Identification of required changes to existing OSS/BSS to integrate SDN and NFV	• Monitoring of VNF and NFVI performance in deployed environment • Development and integration with OSS/BSS is enabled • Linkage from OSS to 3rd party IaaS supplier	• Cost-based purchasing decisions begin to change to revenue-based purchasing decisions • Clear development of use cases for SDN and NFV • SDN/NFV enabled services tie-in to appropriate billing hooks	• Network-wide KPI monitoring and alerts are available but closed-loop handling is delayed • OSS/BSS integration is dynamic, automatic, and fully scalable	• Seamless interconnectivity with the OSS/ BSS systems

Area	Capability	Phase 0: No Virtualization	Phase1: Standalone VNFs	Phase 2: Common Information Models	Phase 3: Network Function Auto-Scaling	Phase 4: Federation of SDN	Phase 5: Full Service Automation
Governance	**Governance**	• Traditional governance roles and responsibilities	• Network component authorization • No scalable policy framework • No scalable forensics or remediation • Specialized measurement of performance	• Policy framework is socialized and federated • Monitoring and reporting on KPIs and SLAs	• Policy change automation (self-service changes) • Forensics and remediation are enabled	• Policy framework in place for controllers and orchestrators function across environments	• Policy enforcement enabled through the ability to measure, analyze and program each individual feedback/control loop
Customer	**Customer Experience**	• Reactive approach to customer experience	• Service transparency — customers cannot discern between VNF and traditionally delivered services	• Data usage improves customer understanding and ability to develop targeted services	• Elasticity and predictive analytics ensure a consistent user experience	• Data fed into feedback loop from major events helps to improve the customer experience • Improved analytics enables XaaS offerings including pay as you go, pay as you grow models and bundling aligned with customer needs	• Scalability and flexibility ensure SPs outperform traditional competition during major events • Seamless self-service offerings for customers allow for highly customizable service offerings

The first era of maturation is labeled “Maturation of VNFs,” which includes the following maturity phases –

- **NMM0:** No Virtualization
- **NMM1:** Standalone VNFs
- **NMM2:** Common Information Models
- **NMM3:** Network Function Auto-Scaling

The advanced era of maturation is labeled “Maturation of Network Apps and Services,” which includes the following maturity phases –

- **NMM4:** Federation of SDN
- **NMM5:** Full Service Automation

A few highlights regarding the usage of maturity model –

- Service Providers may choose stop at a particular maturity phase as that particular maturity phase aligns with the business objectives. In these situations, while the business objective is achieved, the complete benefits of SDN/NFV adoption may not be realized
- We expect the Service Providers to evolve the maturity of Network VNFs and virtualized network services independently per domain through NMM3 as the evolution happens within specific network domains
- For NMM4 to be realized requires multiple network services (consisting of multiple VNFs) have progressed through the NMM3 to be controlled by a controller-of-controllers across multiple domains

NMM0: No Virtualization

This is the baseline and can be thought of as the network prior to the introduction of SDN and NFV. The network is delivered via proprietary “boxes” of both hardware and software with Command Line Interface (CLI) or dedicated element management systems (EMS) for that node. Predominantly, there is no logical or physical separation of hardware and software (no NFV) and no separation of hardware and software (no NFV) and no separation of data plane and control plane (no SDN).

NMM1: Standalone VNFs

Key outcome of this maturity phase: Single vendor based “service” tenant on a virtualized environment.

Key benefit of this maturity phase: VNF production deployment.
The decoupling of the network functions software from the NFVI requires coordination for VNF and service deployment and life-cycle management. The minimum

dependencies for enabling NMM1 include a commoditized hardware platform, and common software components such as a virtual switch (vSwitch), Type 2 hypervisor, and a host OS that provides sufficient performance (throughput, latency, jitter) to VNFs.

In this phase, Service Providers will implement isolated deployments of virtualized network functions to develop network services. Please note that the term "service" is not used to describe an end-customer service. Rather, it is taken from the VNF point of view. For example, consider a virtualized edge or branch CPE service, which may contain virtualized network functions including vRouter, vFirewall and vLoadBalancer. The three virtual functions in this example may be from varying vendors, but any orchestration required would be by a single entity.

These deployments are isolated from each other, are not commonly orchestrated, and are confined to a small portion of the network. In this phase, control is isolated to specific domains with dedicated intra-domain controllers for that domain. For example, if the Service Provider had a vCPE domain and a vEPC domain, they would not be commonly orchestrated or controlled and they would not communicate with one another.

During NMM1 the ability to measure and guarantee the maximum physical and virtual resource utilization of each "service" will be limited. For example, the Service Provider may not have detailed guarantees of the resource usage by the vCPE functions VNFs in a deployed environment. As such, each service will be placed on dedicated NFVI. Said another way, the virtual machines from the vCPE domain and the vEPC domain described above may not reside on the same physical infrastructure as the physical infrastructure for specific function may need to support specialized functions (for example, high processing capability is required for vEPC versus vCPE).

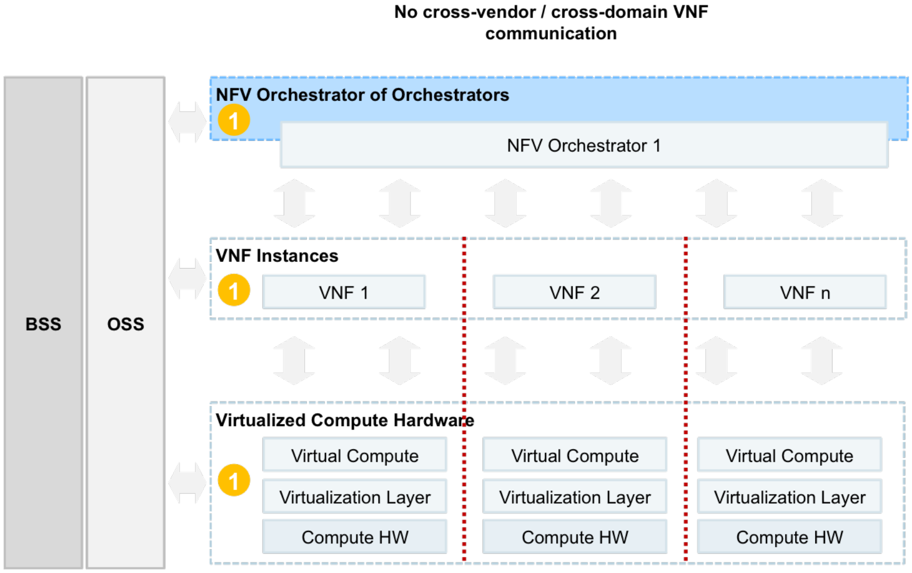

Figure 3: Network Maturity Model Phase 1

NMM2: Common Information Models

Key outcome of this maturity phase: Multi-vendor based NFV environment supported by multi-vendor VNF and multi-vendor NFVI solutions based on common information models across the layers of the stack (VNF, NFVI and Network Service).

Key benefit of this maturity phase: Multi-vendor VNF and multi-vendor NFVI production deployment.

Common information models enable on-boarding VNFs to the vendor-independent orchestration environments for intelligent workload placement, VNF life-cycle management and service assurance (monitor/control) across the NFVI.

VNF vendors characterize and provide network function SLA via VNF descriptors with a common information model. A common resource information model is also used to abstract the capabilities and NFVI characteristics of the underlying infrastructure. Common models from VNF and NFVI layers provide the foundation to enable multi-vendor management and orchestration environment to provide VNF deployment, life-cycle management and service assurance.

Service Providers can then monitor VNF and NFVI independently (essential to bridge the Network/IT interface (IaaS)) in a deployed environment — i.e., telemetry data are available for Service Provider to fine tune the physical infrastructure and virtual infrastructure independently for optimal performance.

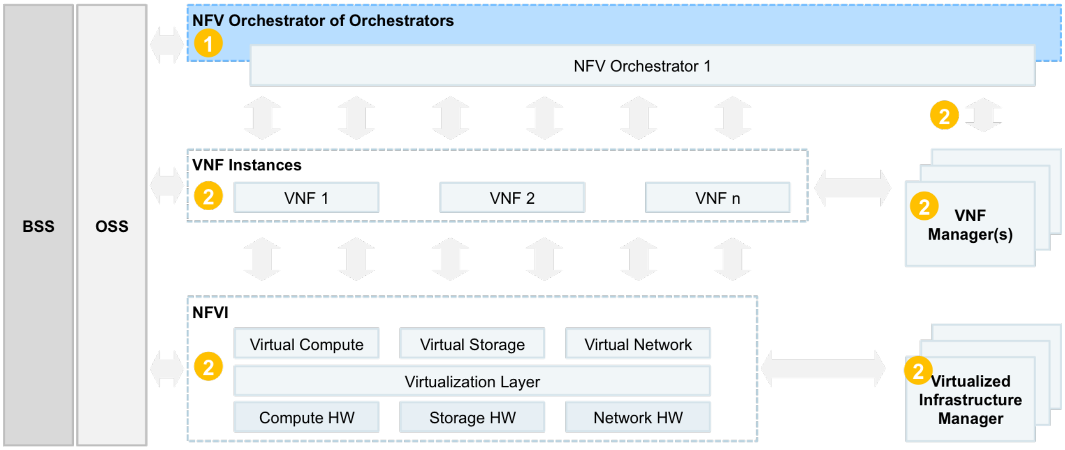

Figure 4: Network Maturity Model Phase 2

NMM3: Network Function Auto-Scaling

Key outcome of this maturity phase: Elastic physical and virtual infrastructure. Closed-loop VNF and NFVI life-cycle management.

Key benefit of this maturity phase: Efficient usage and automated elasticity capability achieve real-time network reconfiguration.

As network traffic expands and contracts in real time, Service Providers can add hardware to boost total network capacity (elasticity of physical infrastructure) and VNF software licenses to support subscribers (elasticity of virtual infrastructure).

In this phase, auto-scaling decisions are made based on network traffic and KPIs. VNFs are automatically created, destroyed and augmented based on capacity and availability. Similarly, the physical infrastructure serving the VNFs must be capable of scaling dynamically to take advantage of available NFVI resources. This dynamic environment will have direct implications for the OSS/BSS and, therefore, require tie-ins to appropriate billing hooks. In order to achieve elasticity, the interoperability across VIM/MANO and SDN controller layers is required. Rapid deployment of the number of VNFs (dynamic addition and deletion) requires real-time network reconfiguration.

In this phase, the metrics and analytics of the prior NMM2 phase have become “predictive,” allowing for capacity planning and automated rightsizing of the network and data center. Service Providers will be able to profile network workloads in order to predict the performance and resource consumption of a function.

The domain-specific controllers (e.g., vCPE, vEPC, Gi-LAN Controller) will remain isolated until NMM4.

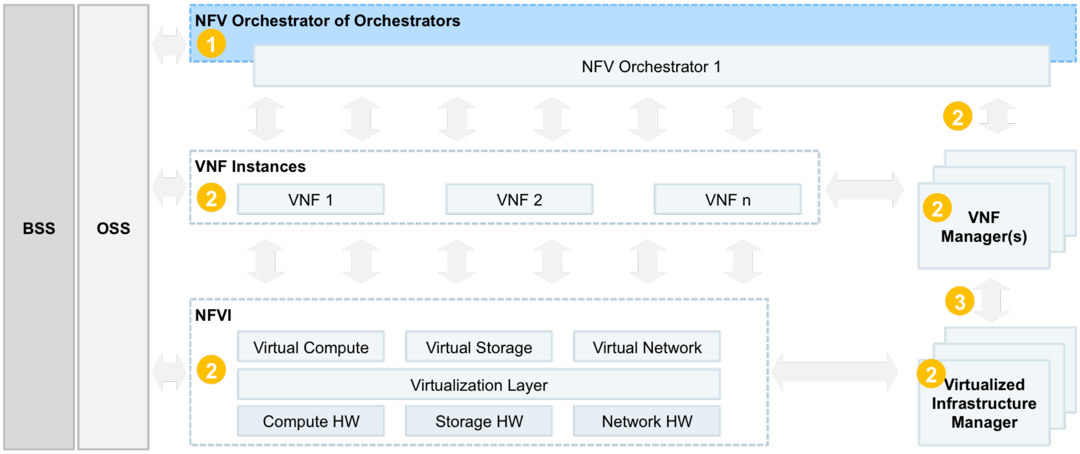

Figure 5: Network Maturity Model Phase 3

NMM4: Federation of SDN

Key outcome of this maturity phase: Federation vertically oriented controllers and orchestrators.

Key benefit of this maturity phase: VNF End-to-end network view that enables network orchestration.

The key in this phase is an end-to-end network view which includes the backhaul. Success in this phase allows applications/services to take advantage of the entire network, including tasks such as data center power optimization and network traffic engineering.

The controller-of-controllers and orchestrator-of-orchestrators (i.e., CMP) will have visibility and control of the once-isolated domain controllers. In previous phases (NMM1–3), the domain controllers were isolated. Due to the isolation of domain controllers, an end-to-end network view or complete control of the entire network was not possible. NMM4 is characterized by the orchestration of any domain to other domains in the entire network.

Network-wide KPI monitoring and alerts are available, but closed-loop handling is delayed until NMM5.

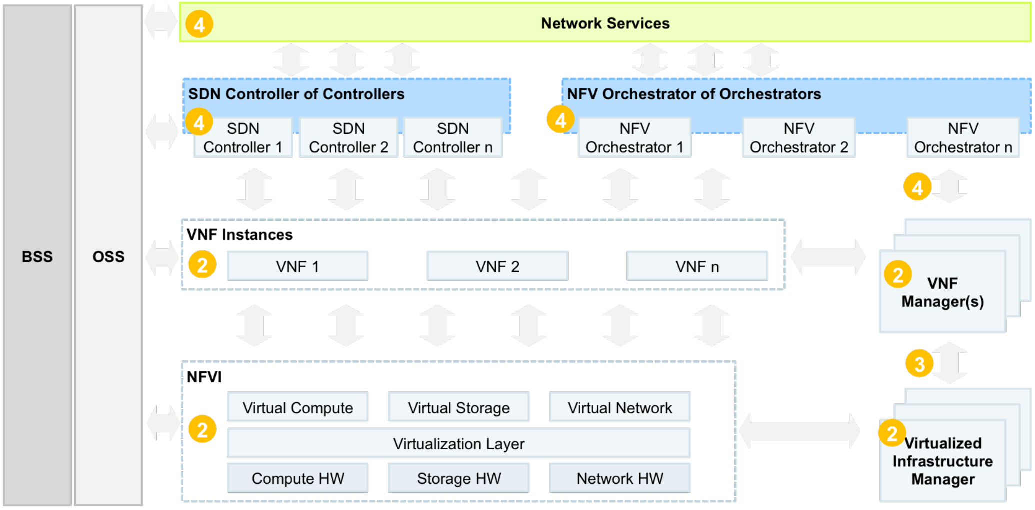

Figure 6: Network Maturity Model Phase 4

NMM5: Full Service Automation

Key outcome of this maturity phase: Closed-loop control at the “controller-of-controllers.” Network can take automatic action to meet KPIs. Service orchestration is possible.

Key benefit of this maturity phase: End-to-end service orchestration.

In this phase, the controller-of-controllers can gather data, analyze data, and program the network appropriately. Standard service descriptors are available, allowing northbound applications to request services from the network, which will automatically adjust to meet the changes in service phases. Network-wide service chaining (within a single operator and cross-operator domains) will be available as algorithms chain together multiple VNFs to achieve the target performance most efficiently.

At this phase, Service Providers are able to develop value added applications that take advantage of interfaces across various tiers of the SDN/NFV architecture that are aligned to customer needs and experiences. For example, a traffic engineering application, which must have detailed knowledge of the network topology and policies of the network operator, will likely reside more on the phase of the controller-of-controllers and will communicate with detailed knowledge of the network. Compare this to a Bandwidth Auction application where customers can temporarily purchase additional bandwidth when needed or when the Service Provider has spare capacity. This application interface will not need detailed knowledge of network topology and can interface to the controller-of-controllers through typical “Service Request” and “Service Acknowledgement” type messages. We expect that there will be multiple integration points to serve both types of applications.

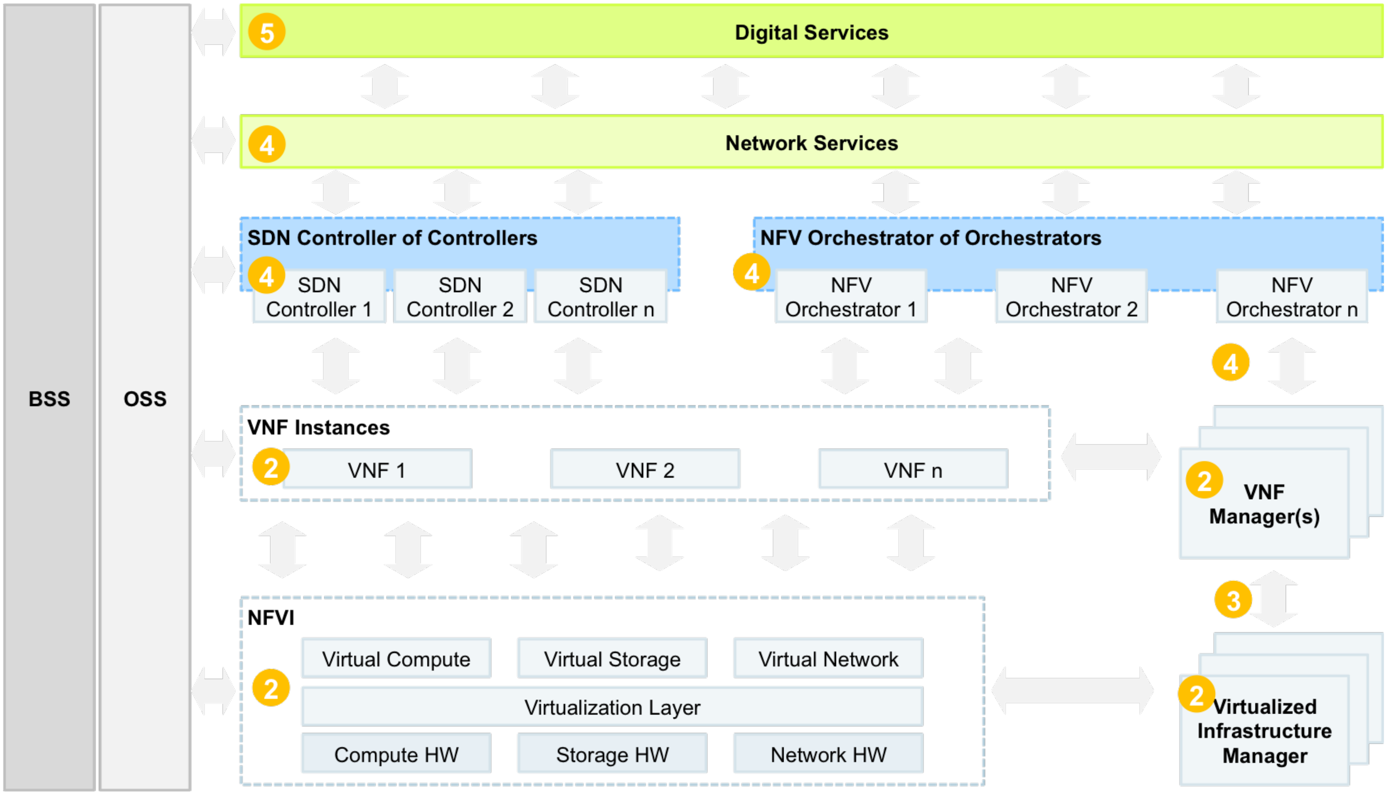

Figure 7: Network Maturity Model Phase 5

In this phase, the emergence of network applications and services will flourish. This will enable Service Providers achieve the full benefits of SDN/NFV technologies — starting with network virtualization overlay applications (available even at NMM1), moving toward domain-specific controllers (more prominent at NMM3), and finally arriving at true network applications and services that assume the network and data centers are programmable through well-known interfaces and can reach the entire network.

The key milestone for this maturity phase is a “closed loop.” The network should be able to provision and correct itself to adhere to SLAs. The key milestone for this maturity phase is not the location of the applications and the communication protocol between the application and the network.

The overall benefit of transformation is furthered by the virtualization of data center resources through Cloud Management Platform. As the VNF in the WAN integrates with software-defined networking, storage, and compute in the data center, Service Providers are able to achieve application/business service focused end-to-end elasticity and programmability driving enormous efficiencies and agility within Service Provider network/business operations.

While the focus of this document is NFV, it is acknowledged there will be instances where fulfillment solely from an NFV orchestrator is not appropriate. The scope of the “orchestrator-of-orchestrators” could be potentially addressed by existing modern service fulfillment tools with appropriate workflow and interfaces to the underlying service capabilities. For example, if the service fulfillment requires the need to supply specific physical infrastructure (such as copper access circuit loops, Customer Premises Equipment as components of a DSL Broadband product, etc.) the service orchestration integrates with workflow engines of service fulfillment tools.

Hurdles for Migration to SDN and NFV

While Service Providers acknowledge the benefits of virtualization technologies, there are impediments to deployment, management, operation and service realization. Given the industry culture and mission critical requirements (FCAPS) of the network, migration to software-based solutions requires changes to the traditional service delivery method. In addition to technology, critical impediments still exist with the required change of culture, recognition of new business models, and development of new skills.

Technical Hurdles

While the past several years have seen significant movement in terms of interest and shipments of NFV solutions, a lack of mature end-to-end solutions both from legacy vendors and nimble start-ups hinders adoption. Some of the technical hurdles to Service Provider NFV adoption include the following:

- Not on par with existing solutions in production (e.g., FCAPS, availability and reliability)
- Lack of interoperability across technology domains (e.g., physical, virtual, legacy)
- Unable to meet commercial needs (e.g., SLAs, licensing, OSS/BSS integration)

Additionally, SDN and NFV will be disruptive to existing OSS/BSS solutions, and may require modernization or upgrade of existing solutions. We expect OSS/BSS to evolve to support network transformation, as the capabilities of the underlying network improve. The integration of OSS/BSS with VNF/SDN elements is arguably the most challenging to achieve, yet this is key to enabling end-to-end service orchestration and automation.

These hurdles, while significant, are being addressed with appropriate focus and participation of SDN/NFV ecosystem.

Changes in Culture

Organizations need to move beyond traditional silos that have been erected in favor of cross-functional (IT, network, and product) teams. While SDN and NFV are primarily focused on the network, they require collaboration across network, compute, and storage teams to achieve an end-to-end business service alignment with infrastructure.

Additionally, new methodologies that leverage the combined strength of these cross-functional teams will be required to improve responsiveness, operational agility (i.e., DevOps approaches), and quality of solutions. These teams will be encouraged to constantly innovate, continually assess the viability of solutions, and manage projects in a more quantitative manner leveraging analytics. This will allow teams to move more quickly, be more innovative, and where necessary to fail fast.

New cultures require new governance models and leadership roles. In order to achieve this cultural shift, organizations with visionary leaders have begun merging traditional roles (e.g., CTO and CIO to CTIO) to eliminate traditional reporting lines, become more agile, and better meet the business' goals.

Recognition of New Business Models

As TEM vendors shift away from traditional delivery methods, Service Providers should be ready to evaluate new and emerging business models that will accompany this transition:

- Separate hardware and software purchasing decisions as vendors shift away from integrated appliances
- Software Pricing/Pay-Per-Use models
- Managed service offerings from traditional vendors who will focus less on products and more on services

It should be noted that while these transitions may take longer than many Service Providers would like, vendors and the larger ecosystem are moving in this direction and Service Providers will need to understand the implications on their business.

Skills Gaps

The transition to NFV requires Service Providers to retrain their workforces with the necessary skill sets. It is a time-consuming and significant endeavor to make this transition. Telecommunication Service Providers who have historically relied on the vendor to be both the domain expert and the functional node expert now must rely on multiple entities for the collective experience, knowledge and expertise to cover all the aspects resulting from the separation of "platform" and network function suppliers. As discussed above, this opens the door to new revenue opportunities for system integrators to provide such domain and functional node expertise.

Intel's Vision for SDN/NFV

In order to achieve the benefits of SDN/NFV, ecosystem participants need to work together. Intel's vision is to help accelerate the transformation of telecommunication Service Providers to meet the needs of a software-defined network (SDN). Intel enables the telecommunication industry to achieve the promise of SDN and NFV by using open platforms to consolidate network workloads. Intel is delivering the building blocks and collaborating with the broader ecosystem to create the infrastructure of the future. Intel's vision is to help telecommunication Service Providers implement their four primary workloads — application processing, control processing, packet processing, and signal processing — with a common architecture, enabling optimal resource utilization.

To achieve this vision, Intel is working in collaboration with the ecosystem to develop open standards that move the entire industry forward. Intel is an active and leading contributor to a number of standards bodies aiming to promulgate and enable open ecosystems. By driving openness in the underlying hardware, Intel is able to support the key tenets of NFV solutions – lower costs, drive interchangeability across the infrastructure through consistent interfaces, and improve performance through hardware acceleration.

The SDN/NFV transformation will enable communication Service Providers with flexible network architectures, service agility and efficient resource utilization to pursue new and unprecedented economic opportunities.

The Role of Open Source in the New Service Delivery Model

Service Providers recognize the need to reduce the costs and complexity of delivering services, in parallel with expediting time to market. The open source communities and consortia provide a vehicle for Service Providers to augment their traditional standards efforts with direct software contributions to the ecosystem. The open source model provides a cost-effective and efficient means to bring new solutions to market, as well as to influence a multifaceted vendor community.

Whether or not open source and the communities that drive these technologies reduce the operator TCO is actively debated. The "horizontal approach" certainly enables ingredients from multiple vendors and allows for competition at each layer. However, Service Providers will often need software warranty, indemnification and support agreements, interoperability compliance, and customization, which drive up the price of commercial open source offerings. The situation is complex because warrantees must guarantee performance and reliability from software ingredients whose authors may not be part of the entity providing the guarantee.

A common challenge or resistance to working with community-led efforts is that the desired outcome and direction of the project is not within the control of only one entity. As a result, open source projects can result in a mesh of contributions that do not account for commercial-level performance, quality, reliability and scale. Similar to the enterprise and cloud markets, this challenge provides an opportunity for new ecosystem players to package open source-based offers to provide the reliability and scale required for telecommunication network providers.

In summary, the open source model enables Service Providers to extend their influence, expedite time to revenue for new services, likely reduce cost for services, avoid vendor lock-in, and provide useable software applicable to their unique environment. New ecosystem players are emerging to harden and commercially monetize the resulting solutions for delivery, deployment, customization and support.

How Intel Is Helping to Drive Maturity/Openness

Intel has been a catalyst of the open source transformation ever since the foundation of Linux* on Intel® architecture in 1991. At the time, open source concepts were just taking shape. Now, they are a driving force for innovation, and Intel architecture remains a vital foundation for open source-based solutions. Together with other members of the open source community, Intel is helping to drive this spirit of innovation forward for NFV/SDN transformation for the communications ecosystem and industry.

Intel is a key contributor and leader in open source projects to optimize software and hardware building blocks used to develop SDN/NFV solutions. Intel has dedicated software teams that make contributions to open source projects and standards, such as Open vSwitch*, DPDK, OpenStack*, OpenDaylight* and Open Platform for NFV (OPNFV)*.Intel's leadership and contributions have played a key role in the maturity of these projects. Intel is a platinum member for OpenStack, Open Daylight and OPNFV.

Intel recognizes that the network transformation requires alignment with Service Providers. A collaborative approach is needed to identify and optimize key open community software ingredients, targeting high-performing SDN and NFV solutions to move the ecosystem forward. The Intel® Network Solutions initiative focuses on alignment with the Service Provider to address the workloads and end-to-end solution aspects to accelerate industry transformation.

For the vendor community, to foster alignment and knowledge-share across the ecosystem, Intel has established the Intel® Network Builders program to accelerate network transformation with the development and deployment of proven SDN and NFV solutions for telecom and data center networks. The program connects Service Providers and end users with the infrastructure, software and technology vendors that are driving new solutions to the market. Intel Network Builders offers technical support, matchmaking and co-marketing opportunities, to help facilitate joint collaboration from the discovery phase to the eventual trial and deployment of NFV and SDN solutions.

How Service Providers Can Help Drive Market Maturity

Participating in open source communities allows Service Providers to have direct influence on the open source initiatives. Open source communities require that participants actively contribute code and give back to the community effort. Service Providers can use this vehicle to augment traditional standards efforts to contribute code to address problems that may be unique to their environment. The collaboration of Service Providers and vendors working as participants in a community project, in parallel to standardization efforts, validates the solution design via "fail fast," agile methodologies. This provides a baseline of usable technology to expedite vendor-provided or Service Provider homegrown solutions. It is important for commercialization of open source technologies to occur in order to create the required ecosystem for innovation and wide-scale adoption of virtualization technologies that leverage open source software and industry standard hardware.

These communities, if properly led, also provide a means to help reduce vendor lock-in. Traditionally, proprietary solutions result in significant cost for new features and are delivered based on the equipment provider's delivery cycle. Neither of these factors supports the transition to a desired rapid service delivery model. Open source initiatives that result in actual code contributions provide a mechanism for Service Providers to reduce dependence on proprietary solutions and expedite new features delivery.

Implications for Vendors

While a difficult transition, virtually all legacy telecommunication equipment suppliers are transitioning from a hardware-based to a software-based model. The new software-based model challenges the ecosystem suppliers to maintain margins while losing the majority of hardware revenue. This transition drives the incumbent suppliers to identify new areas to maintain, if not grow, their revenue from Service Providers. These suppliers will seek to differentiate and grow their offerings with new innovative software and service offerings.

Vendor participation in open source communities enables vendors to help guide the maturation of the standards most Service Providers will rely on. By helping drive these standards and align product offerings with them, vendors can ensure that their solutions meet Service Provider RFP requirements moving forward. The built-in ecosystem effect of these communities will enable both vendors and Service Providers to innovate and bring new products to market faster. As solutions mature, vendors will need to revisit traditional cost structure as hardware and software become increasingly decoupled and abstracted.

The disruptive force of SDN and NFV is leading to significant innovation within the telecommunications equipment market. While traditional vendors will likely be able to effectively transition from legacy markets to SDN and NFV, new markets will emerge, allowing for a new class for vendors and OEMs. To avoid the risk of commoditization, vendors will need to carefully manage their contributions to driving reusability, scalability and interchangeability.

Vendors should be prepared to focus on four key opportunities to take advantage of this shift:

1. Drive differentiation in NVF and SDN technologies by improving solution performance (FCAPS)
2. Improved software and services oriented business models
3. Improve integration with the broader ecosystem to be included in more end-to-end solutions
4. Focus on value added software development through north bound applications

While there are short-term business model challenges to overcome, vendors have an opportunity to transform their businesses in the long term which will generate additional competitive advantage, long-term revenue generation, and higher profit margins.

Conclusion

During the last 20 years, Service Providers have transitioned through several generations of technology that have redefined networks and required new approaches to the core business. As customer needs continue to evolve, new technologies are required. Traditional purchasing models of network appliances with bundled hardware and software packages that provide fixed services are on the decline. SDN and NFV promise to do for the network what virtualization did for the data center, providing flexible, cost-effective solutions, which will empower Service Providers to become digital businesses.

This white paper is one possible approach to SDN and NFV adoption within Service Provider environments. It provides a framework for Service Providers to gauge the progress against the broader market, while achieving their specific business objectives.

Please address any questions or comments on this whitepaper to NMM@intel.com

Glossary of Terms

Acronym	Definition
API	Application Programming Interface
BSS	Business Support System
CLI	Command-Line Interface
DPDK	Data Plane Development Kit
EMS	Element Management Systems
FCAPS	Fault, Configuration, Accounting, Performance, and Security
IoT	Internet of Things
KPI	Key Performance Indicator
MANO	Management and Orchestration
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
ONP	Open Network Platform
OS	Operating System
OSS	Operational Support System
OTT	Over-the-Top
SDDC	Software-Defined Data Center
SDI	Software-Defined Infrastructure
SDN	Software-Defined Network
SLA	Service-Level Agreement
TCO	Total Cost of Ownership
TEM	Telecom Equipment Manufacturer
vCPE	Virtualized Customer Premise Equipment
vEPC	Virtualized Evolved Packet Core
vFW	Virtualized Firewall
VIM	Virtual Infrastructure Manufacturer
VM	Virtual Machine
VNF	Virtual Network Function

333754-001US