

Critical success factors for Digital Network Transformations.

Beth Cohen
SD WAN Product Strategist
Verizon Business Group



Table of Contents

Target audience	3
Summary	4
Identifying the problem	5
The network data explosion	5
The pace of change is accelerating	5
Dynamic applications pressure traditional WAN architectures	5
Organizations struggle to support technology change	6
A brief introduction to Digital Network Transformation	7
Standards and Open Source-based architectures mean faster development cycles	8
A mix of technology and business reasons are driving Digital Network Transformations	9
Four critical factors for Digital Network Transformation deployments	9
The unique value proposition for Verizon Virtual Network Services	9
Integrated platform architecture	10
Solutions bundles	11
Purpose-built hardware	12
Premises based uCPE	13
Hosted Network Services	13
Public cloud	13
Why should you care about end-to-end automation?	14
Why choose to migrate to Verizon Virtual Network Services?	16
In closing	16
Appendix	17
A peek behind the scenes... Digital Network Transformation and SDN	17
Basic Network Functions Virtualization	17
Legacy Systems Integration	18
Abstraction, Standardization, and Automation	18
Abstraction	19
Standardization	19
Automation	19
Low Touch Provisioning	20
Integrated Management and Deployment Systems	20
What is dynamic orchestration and assurance?	20
How does Enterprise Orchestration work?	21

Target audience

The document is designed for:

- Enterprise leadership, IT or Operations Managers starting or considering Digital Transformation initiatives which incorporate Software Defined Networking (SDN) and/or Network Function Virtualization (NFV)
- Companies looking for guidance about the best approaches to optimize the effectiveness of their Network Transformation projects

The planning and deployment process typically includes the following stages:

- **Research and assessment** – Determine the level of effort, availability, and best path for undertaking a legacy infrastructure technology refresh and migration to SDN technologies in order to minimize surprises and determine level of effort and organizational technology readiness
- **Managed deployment for risk mitigation** – Manage the deployment by starting with Proof of Concept (POC) lab testing, followed by a field test program or small-scale deployment before undertaking a major deployment. A test or small-scale deployment will allow risks to be identified and mitigated while validating business benefits, operational improvements, and potential cost savings
- **Committed Digital Transformation program** – Have plans in motion targeted at addressing customer demand, improving customer experience, and/or getting products and services to market faster with the understanding that the network is an integral part and enabler of the transformation project

Summary

Wherever a company is on its Digital Network Transformation journey, enterprises can benefit from technical and operational insights. Common formats include reference architectures, adoption challenges, potential barriers and key areas for consideration. Detailed descriptions of technology used, as well as explanations of how Verizon applies and integrates technology and network management platforms, are provided throughout this document. Some of the key takeaways are:

- Digital Network Transformation is all about agility, elasticity and resilience. A hybrid application delivery strategy allows for optimal performance and flexibility
 - Support for multiple Virtual Network Functions (VNF) deployed on a single appliance provides an opportunity for more efficient network infrastructure management and the agility to respond to changing market conditions
 - By employing a cloud and container infrastructure package at the network edge, Verizon has enabled a “Cloud in a box” by combining a Linux-based operating system, hypervisor with open source Application Programming Interfaces (APIs), and accelerators
- Integrated technology and tools, as well as trusted service and management teams, are keys to a successful Digital Network transformation
 - Continued investment in lab-based testing and APIs helps Verizon to benchmark performance metrics which can identify potential pitfalls specific to an organization’s desired outcomes. Benchmarking these metrics can alleviate potential issues with vendor VNF interoperability and enable delivery of automated service chains and solutions bundles which reduce turn up time and speed customers’ ability to generate revenues
 - By maintaining close technology and business relationships with multiple vendors, Verizon is able to ensure end-to-end software and systems integration that is difficult to duplicate for even the largest enterprises due to the scale and the ability to maintain close alignment with the vendors
- Optimal network uptime and performance can only be achieved by deep integration of network connectivity management tools, such as automated self-healing, Closed Loop Assurance, centralized policy management, intelligent networking tools, and other extreme automation techniques

With time, resources and effort, enterprises might be able to do this themselves. However, for a time and resource-constrained IT team, the good news is that a digital network technology refresh need not be complex or time-consuming to deploy or manage. Low-touch provisioning significantly reduces the deployment delays and expense associated with manual turn-ups. Automation and consolidation of policy management means more effective use of limited operational resources, and integrated management tools means optimal uptime and performance in production.

Recognized for innovation, Verizon is not waiting for the future, we are building it! Are you ready to join with us in taking the next steps in your digital network transformation journey?

Identifying the problem.

The network data explosion.

While there are no shortage of signs that delaying an update might potentially lead to detrimental effects on realizing business objectives, enterprises exploring Digital Network Transformation initiatives are finding few common industry standards or best practice models for their projects. A new era of digital business has arrived where organizations must seek ways to apply technology and applications as a means of meeting customers, business partners, and staff expectations. The ability for enterprises to expedite a digital transformation will play a large role in the success of securing a growth position in the new, global, digital marketplace.

The pace of change is accelerating.

The pace of change is only accelerating further with the arrival of 5G, Multi-Access Edge Computing (MEC), SD WAN, virtualized networking services, and other new technologies on the networking side, and Edge Computing, IoT and Artificial Intelligence (to name a few) on the application side. Enterprises are now faced with “always-on, always connected, always performing” application and network expectations from staff and customers. Traditional network deployments are challenged to keep up, making it even more difficult for IT managers to be successful.

The data explosion, combined with increasingly higher user expectations, has been driving technological change at an incredibly fast pace. IT managers are forced to rethink their network strategy – not just the hardware and the software, but the skill sets their staff need to support it. “Digitalization” is possibly an overused term, but this is the environment we are operating in today.

Dynamic applications pressure traditional WAN architectures.

Challenges for traditional WAN architectures also include:

- The proliferation of public and private cloud applications
- The rise in the number of edge computing applications that require a far more sophisticated understanding of application data and compute workflows
- A technology shift from dedicated networking appliances to SD WAN and virtualized CPE (vCPE) platforms
- The rapid evolution of mobile and cloud-based applications underscores the need for an open standards-based, fluid network design
- Accelerating demand for multi-layered security, network resilience requirements, and support for the Internet of Things (IoT) applications

As many enterprises are finding, traditional networks were not designed to optimize (or even be aware of) application performance. They have been complex and cumbersome to manage and maintain, often having been designed for and built on purpose-built proprietary, network equipment such as routers, Ethernet switches, firewalls, and load balancers. Deploying these monolithic network elements has meant long development and installation cycles, overly complex lifecycle management

(adding to operational inefficiency and overhead), and increased need for investment in upgraded equipment, often at a rate that exceeds revenue growth.

Often, existing enterprise networks are composed of “bundled” vendor proprietary network elements where the control, management, and data (including user data traffic) functions are physically tied to the network functions themselves. Deployment of new services or modifications to existing services must be done on an element-by-element basis, requiring tight coordination of internal and external resources. This traditional approach limits the ability to tune network operational flexibility and application awareness and potentially forces IT managers into a risky strategy of reliance on proprietary vendor point solutions. Verizon’s investment in SDN means less reliance on vendor proprietary solutions and more flexibility to incorporate new technologies as they develop.

Organizations struggle to support technology change.

There are significant challenges to be aware of before undertaking a DIY (Do It Yourself) network transformation project. There are many factors that may need to be changed to support a digital network transformation to a SDN network architecture. Following are some common issues that should be considered and addressed:

- Lack of understanding - The implications of applying traditional networking principles to a technology refresh can lead to less than optimal technology choices. Do not assume that a vendor’s black box magically works without thorough testing and field trials. Not all vendor solutions are created equally. Each have strengths and weaknesses that need to be mapped to an organization’s actual requirements
- Traditional infrastructure mindset – Transformation is often thought of as a standalone project rather than part of an integrated infrastructure. While often overlooked, it is essential to consider how new applications, cloud and systems will impact network design and security
- Outdated staff skillsets – For an enterprise to stay current, investments need to be made in training existing staff or hiring new staff with the skills to support SDN architectures. This applies to not only to the network architects but also the network administrators and service delivery staff. These skills are typically not core capabilities for the average enterprise, Attracting and keeping talent is important and becomes a serious challenge
- Poorly integrated tools and management systems – Traditional network architecture tools might not work for a digital network transformation deployment. Organizations need to proactively invest in and build pre-integrated new tools. These systems work better with comprehensive “visibility” tools which may not be included in a given vendor’s solution and are unlikely to work well across multiple vendors

A brief introduction to Digital Network Transformation

Digital Network Transformation offers a better way to deliver and manage networks that support public cloud, IoT, and other exciting applications that are driving modern business in new directions. It really is the time in the networking world to use software-based assets as opposed to physical assets because software based assets have the ability to better integrate the network with digital applications.

The Verizon SDN product portfolio has been designed from the ground up as a business enabler in the digital world. Through a “Network-as-a-service” consumption model working at “cloud speed,” Verizon SDN services leverage many available connectivity types to help organizations maximize network technology investments. Quite simply, Verizon SDN services provide the same type of scalable, consumption-based experience you would expect when provisioning virtual computing resources from a hyper-scale cloud provider.

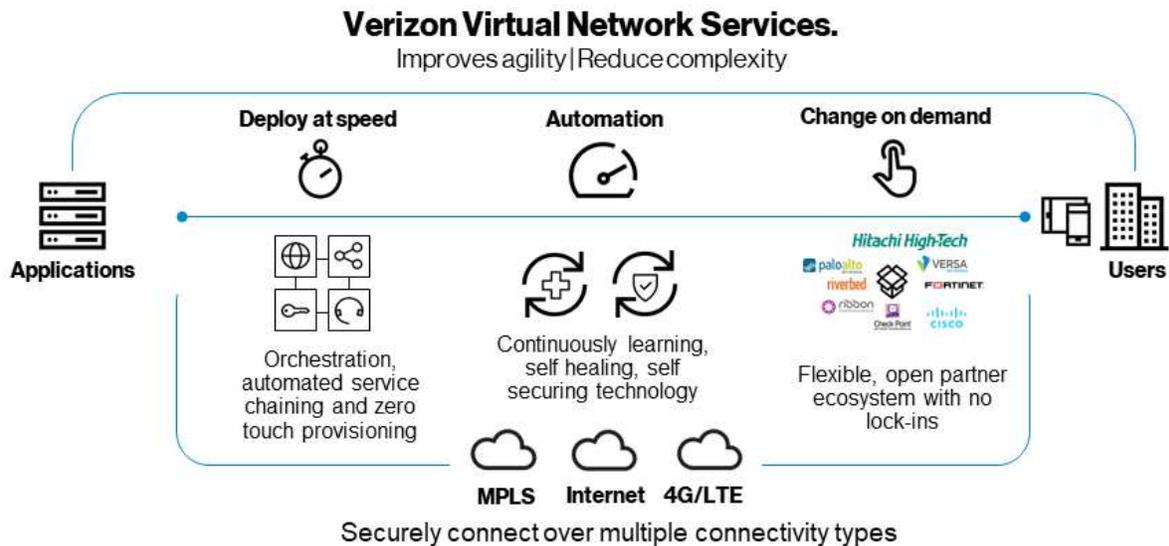


Figure 1: Verizon Virtual Network Services Ties Networks and Applications Together

Through a combination of automated delivery and orchestration of pre-tested and verified solutions bundles, whether on premises, hosted, or any hybrid mixture, Verizon stands by its ability to enable you to realize the most from your existing network resources, create a fluid foundation for the future, and evolve with future technology and business changes.

Standards and Open Source-based architectures mean faster development cycles.

Let's step back for a moment to see how Verizon came to build this powerful portfolio of SDN services. For the enterprise, knowing that Verizon is leveraging and contributing to the development of standard Digital Network Transformation methodologies offers peace of mind because there is consensus across the network service delivery and vendor communities. Verizon is a founding member and a current Board Member of the Open Network Foundation (ONF), the industry organization that develops global standards for Software Defined Networking, as well as the Linux Networking Foundation (LFN) - both pre-eminent bodies focused on the development of standards in support of virtualized networking. Verizon has based its SDN-NFV product suite goals on established Open Source principles:

- Operational efficiencies
 - Elastic, scalable, network-wide capabilities
 - Automated OAM&P (operations, administration, maintenance and provisioning); limit human touch as much as possible
 - Dynamic traffic steering and service chaining
- Business transformation
 - Time-to-market improvements; elimination of point solutions
 - Agile service creation and rapid provisioning
 - Improved customer satisfaction

The following are key features of networks based on SDN and NFV principles:

- Separation of control and data plane
- Virtualization of network functions
- Programmatic control of network
- Programmatic control of computational resources using orchestration
- Standards-based configuration protocols
- A single mechanism for hardware resource management and allocation
- Automation of control, deployment, and business processes
- Automated resource orchestration in response to application/function needs

Combining these principles and concepts facilitates dynamic network adaptations based on application performance requirements, increases operational flexibility, and simplifies service development. Functions may be dynamically scaled to meet fluctuations in demand. Future developments will incorporate autonomous functions with sophisticated analytics and artificial intelligence technologies.

A mix of technology and business reasons are driving Digital Network Transformations.

Digital Network Transformation is still in the early stages of adoption. Many organizations have not yet considered, or are still just starting to consider, undertaking a transformation project. There are great benefits as well as barriers to SDN/NFV adoption. As enterprises learn more about the technology and come to better understand the benefits, the number of field deployments will continue to grow.

The benefits of Digital Network Transformation include:

- Higher network availability and application performance
- Increased agility
- Cost efficiencies

Reasons an IT manager might consider a delay include:

- A perception that Digital Network Transformation may not fully support secure functions against increasingly complex threats
- The total cost of ownership (TCO) balancing new technology investments while maintaining existing infrastructure
- “Rip and replace” may not be seen as a viable option, as the potential for operational disruption might seem devastating for business objectives

An understanding of the financial impact of delaying a digital transformation with newer agile technologies is a commonly ignored variable and critical to keeping ahead of competition. Do It Yourself (DIY) transformations might initially appear to be a cost-effective and efficient option. However, working with a partner (service provider or integrator) who has experience with global digital network implementations, as well as the full breadth of lab and support resources to test, collaborate with disparate technology vendors, and manage a project at scale, can mean the difference between the success or failure of a digital transformation project.

Four critical factors for Digital Network Transformation deployments

The unique value proposition for Verizon Virtual Network Services.

We live in an unpredictable world. With the pace of change accelerating, there is a need to be able to respond quickly to realize short-term opportunities and deliver new services to market ahead of the competition. Whatever the reasons for needing network flexibility, the expectation is that a responsive system should be easy to achieve and that IT should be able to support it. However, while users and applications are dynamic, traditional Wide Area Networks (WAN) were never designed to support such rapid change. They were designed for a world where the enterprise perimeter was fixed. When additional capacity was needed, it had to be planned for in advance. When the instantaneous, elastic nature of cloud collides with the fixed, rigid wide area network, applications potentially suffer performance problems. This, in turn, impacts the user experience and potentially has a negative effect on brand and reputation as well.

Enterprises should understand the need for more flexible and agile networks to be able to adapt quickly in a fast-changing environment. However, the process for enterprises to implement software-defined solutions can often be hindered by budget constraints, a lack of skills, and other business priorities. Lack of skills in particular can be a significant obstacle for enterprises from the very beginning of their network transformation journey.

Four key elements are necessary for a successful transition to an agile, adaptive Digital Network Transformation:

- Integrated platform architecture
 - Integrated architecture across a choice of platforms unifies and simplifies management of all the network functions: virtual, physical or a hybrid of both
 - Centralized service orchestration simplifies and speeds migrations
- Solutions bundles
 - Consumption-based licensing leading to more flexible service delivery; you pay for what you actually use
 - No single network service vendor lock-in provides increased agility
 - Verizon tested and verified solutions mitigate risk
- Low-touch provisioning
 - Ability to spin-up new services and applications faster
 - Less human intervention for fewer errors
- Integrated management and deployment systems
 - Dynamic orchestration and assurance platform for end-to-end operational supportability
 - Automated robust High Availability architectures maximizes uptime and minimizes service disruption
 - Simplified troubleshooting which may lead to better operational management

Integrated platform architecture

Verizon built Virtual Network Services (VNS) on the OpenStack platform, a widely accepted cloud platform used in the Telecom industry for supporting VNFs, using containerization for further efficiencies. Since VNS is available in several options (hosted, public cloud, premise-based or purpose built), you can build the network that is the best fit for your requirements while still being able to take advantage of shortened development times for new features and services. VNS has the ability to rapidly deliver a broad array of best-in-class network technologies from trusted global leaders as well as industry innovators, dramatically reducing sourcing, contracting, and deployment cycle times. In addition, automated solutions bundles accelerate provisioning by delivering multiple services together instead of sequentially, shortening the time to realize value while making digital transformation through SDN simple. The nimble nature of VNS provides the elasticity necessary to meet evolving demands and expectations based on business need.

Solutions bundles

The real value of using Verizon's VNS SDN portfolio is the ability to use pre-defined automated, proven, and tested solutions bundles. For example, each instance can be tailored to different requirements of various types of branch sites or hub sites. For example, some sites may need WAN optimization and others not. By using solutions bundles, Verizon can deploy the services that are needed using our automated deployment and management, while allowing you to retain control of the policies and the ability to make changes as business requirements dictate.

Rest assured that whatever solutions bundle you choose, Verizon has performed extensive lab testing to ensure that what occurs in the lab environment matches what you will experience in a live WAN production environment. Verizon's lab testing creates an exceptional result for customers as it is designed specifically to dig into the performance characteristics of the features of the integrated solution using the typical customer traffic profiles that will occur in the actual user environment. You can have confidence in that we have verified that the solutions bundles you receive from us will perform as they were intended.

In practice this means:

- Dramatically shortened provisioning times (from weeks or months to, in some cases, less than 2 days)
- Network functions delivered as applications. (e.g., Routing, SD WAN, Security, WAN Optimization, Session Border Control as a Service, and Software Defined Secure Branch). No more cabinets stacked with proprietary hardware
- A resilient network with less labor-intensive management enabled by automated healing and security
- Automated configuration and service chaining allowing significant reduction in configuration errors
- Global policy and change management through a centralized console

The Verizon Virtual Network Services portfolio includes network services application solutions that traditionally were provided through multiple, physical appliances. There are a number of different deployment models depending on your requirements, but you will no longer need to purchase many proprietary appliances to run multiple network functions.

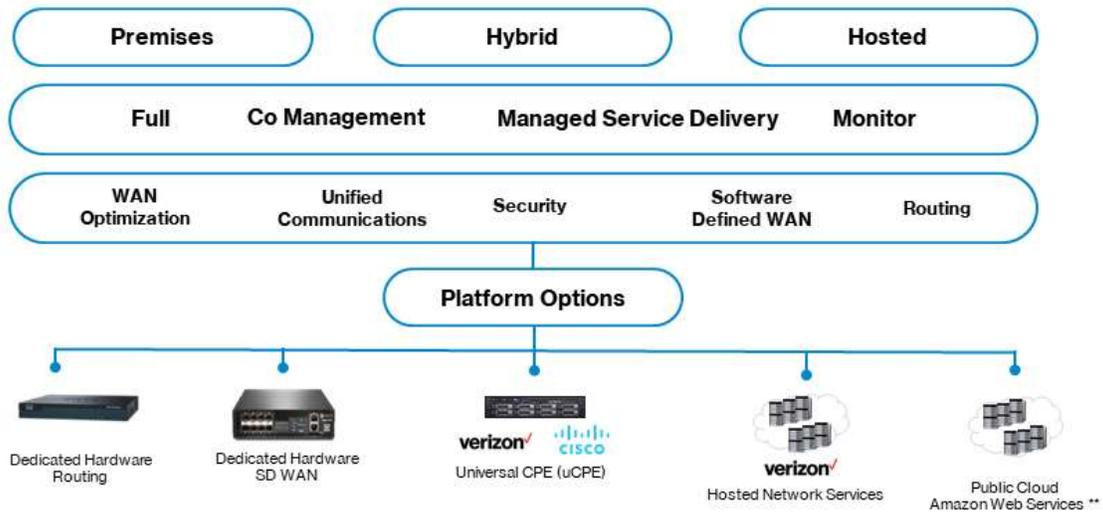


Figure 2: Virtual Network Services platform options

Regardless of the deployment model chosen, you can derive return on investment, not just from the control of capital expenditure on hardware, but also from the reduction of “soft costs” associated with managing vendors, equipment, policies and general administrative overhead.

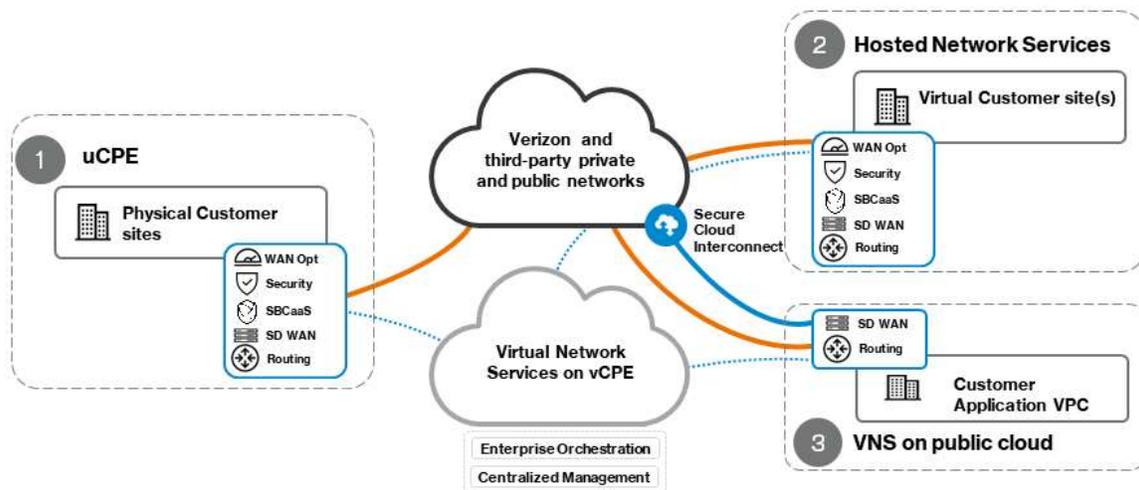


Figure 3: Virtual Network Services deployment options

Purpose-built hardware

Purpose-built hardware is often used for smaller sites that might need only one service – typically SD WAN or Software Defined Secure Branch (SDSB) -- for the foreseeable future (e.g., a retail outlet or a remote office). Whatever the situation, there are times that using a purpose built device is the best

option in terms of cost and efficiency. These purpose built devices are designed to seamlessly work with the same backend orchestration and automation systems in the SDN portfolio.

Premises based uCPE

Often, remote sites need more flexibility to change services as requirements or technology evolve. In this case, a simple x86 “white box” universal CPE (uCPE) can be dispatched. The desired application mix will then be deployed over the network once a basic secure network connection has been established to the device.

A range of uCPE configurations are available to address different performance, high availability, survivability, and size requirements. As with the software technologies, extensive pre-production testing is performed in Verizon labs with each appliance model series and each service chain to ensure proper performance in the field. This eliminates the need to expend time and effort on extensive re-testing the solutions for your digital transformation. Removing the permutations of service-chained configurations and confirming the versions of code for each partner as fully operational has proven to be a challenge for most implementations in our industry. Verizon has conquered this hurdle with an extensive blue-print and design review process to ensure success for your environment.

Hosted Network Services

For the many companies that have migrated their applications to the public cloud, VNS offers a hosted solution that allows cloud-based applications to be connected via co-located hosted nodes, increasing the application performance characteristics. For example, if you want SD WAN routing functionality at each site, but want an advanced firewall to serve multiple sites with the same policy requirements, then it might make sense to centralize the security services rather than having costly security nodes installed at each remote location.

Public cloud

Some VNS services are available on public cloud platforms, such as Amazon Web Services (AWS). Realizing enterprises have assets across many different technology service providers, Verizon made its VNS SD WAN network function available directly from the AWS public cloud.

Why should you care about end-to-end automation?

- **Solutions bundles:** pre-tested and certified VNF service chains and universal automated policy change management
- **Low touch automation:** exceptional provisioning, configuration, and closed loop assurance reduces time to deployment from weeks to just days or hours
- **Visualized services across multiple domains:** views into access, transport and data center (cloud) reducing troubleshooting time and facilitating management
- **Hybrid orchestration:** seamless orchestration across physical and virtual network domains reducing total cost of ownership (TCO)
- **Transition of operations:** Leveraging of orchestration to easily integrate existing systems with other vendor solutions

With VNS, you benefit from an advanced self-service portal that provides a detailed view of security postures, regional and branch level policies, and your micro-services inventory. Think of it as a “shared management” model; you have the ability to manage your sensitive policy changes in near real time, while we manage the automation and complexity behind the scenes. This service offers simplified, centralized, near real-time control of important parameters (security policies, access controls, cost, and performance).

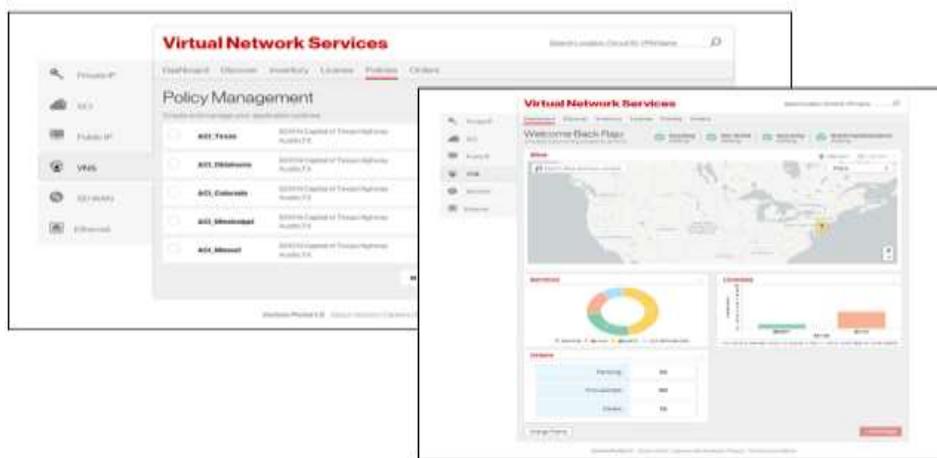


Figure 4: Self-service portal for more transparent service monitoring

Through the portal, you will also have extensive end-to-end visibility of exactly how your sites, applications and network services are performing holistically. This can help you quickly pinpoint and resolve issues, typically without the need to engage expensive senior-level network or application engineering resources.

Administration can be further simplified with a centralized contracting and billing option that will offer a single bill for multiple locations across the globe. The utility-based contracting and billing model means that there is no longer a need to hold separate contracts with multiple vendors, just a single master contract with Verizon. This offers flexibility to change vendors and functionality as your

business needs dictate (e.g., as might be the case with seasonal or cyclical demand spikes). You can also change the features within the services you choose from different vendors. This micro-services approach makes it possible for you to tailor what you need to meet market demands and your business policy requirements on a business segment or down to a site basis.

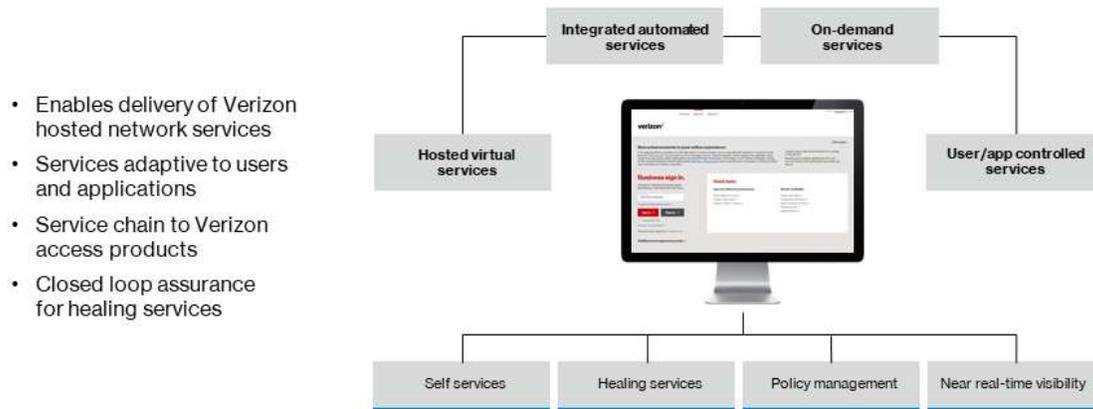


Figure 5: Orchestration helps automate service delivery

Closely coupled to orchestration, deep integration with Verizon’s Network Management and Network Analytics platforms and closed-loop service assurance mechanism helps monitor and heal virtual network services in near real time. Decisions are made based on parameters and service policies defined by us or you. For example, the following set of actions might happen:

1. A “My data center is down” condition is observed by assurance
2. The predefined policy states “move the service to the assigned backup data center”
3. Closed loop actions send instructions to instantiate the service in a new data center and change the routing policies of the on premise devices to map to the new data centers. These actions create a new and complete end-to-end service transparent to the end user

You can think of it almost like spinning-up a new virtual machine to replace one that has stopped, in near-real time. Benefits of closed loop assurance can include improved cost control and simplified and less time-consuming troubleshooting.

Why choose to migrate to Verizon VNS?

Verizon provides the “secret sauce and the management fabric” that helps improve agility, remove complexity, and enable your digital business. Our people, processes, and technology elements manage the life-cycle of the service, meeting your business outcomes. Four levels of service management are available depending upon your needs and the solution bundle(s) selected: Full, Co Management, Managed Security Services (MSS) and Monitor. Through extensive pre-production testing and integration, collaboration, and special licensing agreements with industry-leading technology partners and innovators, VNS helps deliver digital transformation simply, securely, and reliably. Using Verizon’s state-of-the-art orchestration platform, you can change which services you consume, without the requirement for multiple hardware devices or network services vendor lock-ins, giving you the operational flexibility you need in the digital economy of today, with a firm foundation for the future.

In closing

Verizon’s Digital Network Transformation journey has given us the tools and processes to support our customers as we enter this new decade in the 21st century. We hope that this peek behind the scenes has illustrated the depth of our commitment to your success at every stage of the digital transformation journey. Through our investment in state of the industry integrated platforms delivered to you as a packaged service, we are able to provide cross-carrier dynamic network management with end-to-end visibility across your application supply chain.

Now is the time to act. Your successful digital transformation is our priority. Your Verizon account manager is prepared to show you the way. Are you ready to take the next step in your digital transformation journey?

Appendix

A peek behind the scenes... Digital Network Transformation and SDN

As an enterprise leader, it helps to have a basic understanding of what goes into the fundamental concepts of “Software Defined Networking” (SDN) and how it is used to achieve digital network transformation. SDN changes the network design paradigm by introducing network programmability and abstraction integral with the architecture itself. SDN is about separating the network control and data planes in L1-4 devices (Figure 6). This enables independent scaling of control plane resources and data plane resources, maximizing utilization of hardware resources. In addition, control plane centralization reduces the number of managed control plane instances, thus simplifying operations and enabling orchestration automation.

The idea of centralized network control can be generalized, resulting in a broader definition of SDN: standard protocols and data models that enable logically centralized control across multi-vendor and multi-layer networks. SDN Controllers expose abstracted topology and service data models towards northbound (WAN) systems, simplifying orchestration of end-to-end services and enabling the introduction of innovative applications that rely on network programmability. Therefore, network applications perform more as software as opposed to physical assets.

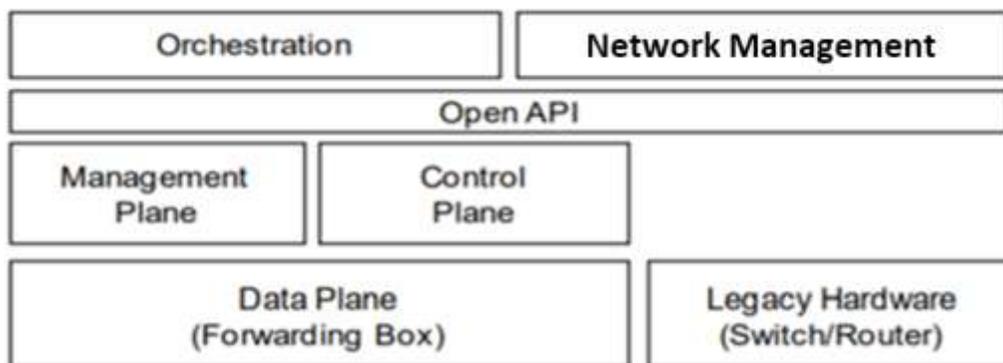


Figure 6: Fundamental SDN concept, the separation of control and data planes

Basic Network Functions Virtualization

The second important concept in understanding SDN is network function virtualization (NFV). This is based on the use of commercial off-the-shelf (COTS) hardware for general purpose compute, storage, and network. Software versions of network functions necessary for running the network are decoupled from the underlying hardware (NFV infrastructure). NFV enables deployment of virtual network functions (VNF’s) and end points within a single operator network or between different operator networks. VNF’s can be deployed in networks that already have corresponding physical network functions (PNFs) or in networks that do not have corresponding PNFs. It is important to note, however, that simple investment in COTS appliances does not negate the need for pre-production deployment testing to ensure that each network function technology performs according to expectations and requirements. This is especially true when service chaining disparate

technologies and distinctly separate IT functions in a single vCPE or hosted platform. Whether deploying small and large scale SDN networks, this need for testing and integration by the operator cannot be over-emphasized; it is crucial for a successful transformation. It is something that is extremely difficult for the enterprise, with its limited resources and divergent business objectives, to achieve.

Legacy Systems Integration

The high-level architecture of fully realized cloud or container based systems shown in Figures 2 and 3 will not immediately replace existing systems and procedures. Rather, the existing systems will be integrated into the new framework, then phased out and replaced by newer systems. For example, WAN SDN Control can be introduced in specific network domains or for specific services, such as Data Center Interconnect. Similarly, EEO can be introduced to orchestrate specific services that rely heavily on virtualized functions, such as SGI-LAN services, while existing services continue to be managed through existing OSS, BSS and EMS systems.

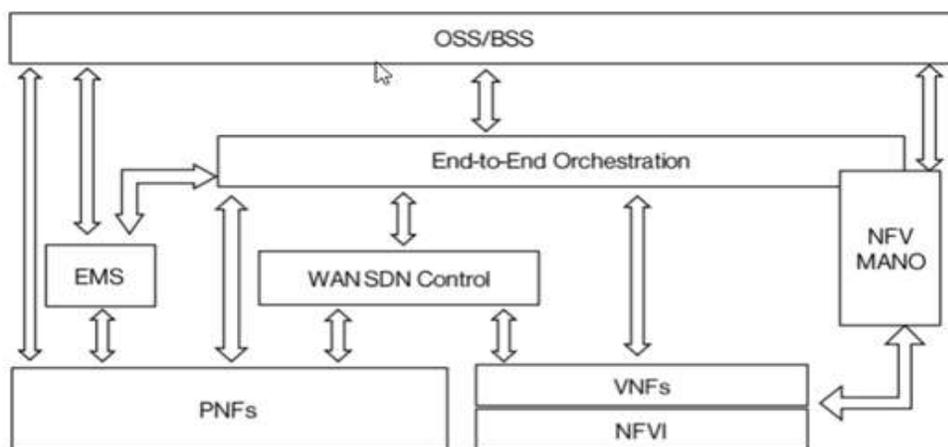


Figure 7: High-Level Management and Control Architecture

Operational disruption in any organization can cause devastating, even catastrophic, effects on business operations. Considering that the potential risk of disruption is one of the main barriers to digital transformation, it's important to mitigate this risk through an integrated underlying architecture. Verizon's approach of using well-tested Open Source systems, such as OpenStack ONAP and MANO, designed to unify the management of both physical and virtual network functions across the global network, can minimize disruption at every stage of service deployment and the ongoing lifecycle of an enterprise's digital network transformation.

Abstraction, standardization, and automation

The desire for service automation is not new, but in the past it was difficult to achieve. Due to a lack of standard interfaces and data models, OSS systems required detailed knowledge of the vendor and technology domains with which they had to integrate. By building on increased abstraction and

emerging standards, Verizon embarked on this journey to enable automation tools built over the existing reactive managed technologies, with the intention to replace legacy components as needed over time.

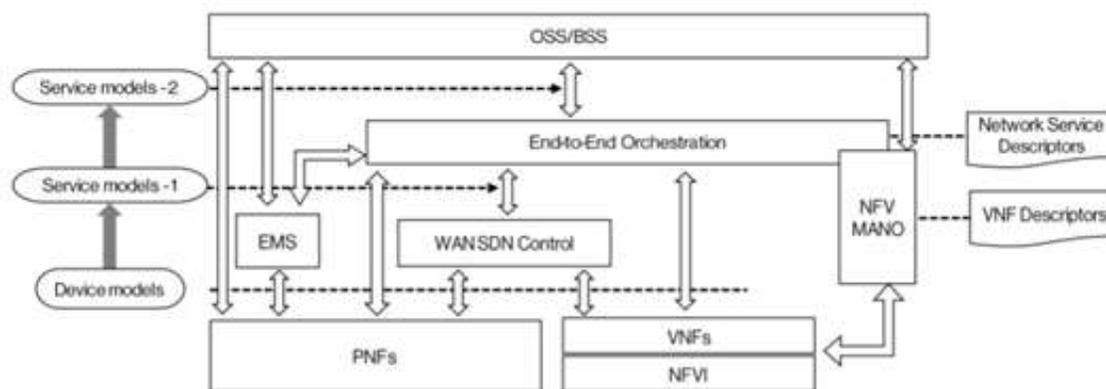


Figure 8 Abstraction, automation and standardization enable service orchestration

Abstraction

Since standardization enables SDN Controllers to manage services across vendor domains, these SDN Controllers can provide abstracted topology and service models to northbound systems, such as EEO. Therefore, EEO does not need the same detailed knowledge about the network as OSS required previously. Similarly, NFV MANO hides the details of the NFV Infrastructure from EEO. With software abstraction, it is easier to create End-to-End Network Service Descriptors that capture end-to-end workflows and implement an orchestration engine that can act on those descriptors and manage end-to-end service instantiation and activation.

Standardization

Work is underway in several standards organizations and open-source communities to create (de-facto) standard data models that describe devices and services. Using new protocols like NETCONF, OpenFlow, OPGCONF and a data model (e.g., YANG), SDN Controllers can provision services across vendor and technology domains because they can use the same data models to provision different network functions in a standard way. This translates into more flexible and responsive systems, and the ability to deliver products with desired feature enhancements to the marketplace faster and more easily.

Automation

Of course, the biggest payoff is using a combination of virtualization, abstraction, and standards to enable automated, template-driven instantiation and management of VNFs, groups of VNFs and the networking connecting them. Today's enterprise networking environment demands a comprehensive, user-friendly solution that supports the transition of purely traditional services to a hybrid of physical and virtual services, with the ultimate goal of transforming to an entirely virtualized network over time. Organizations should be looking for a solution that can support delivery of all

types of services and applications - those available today as well as those envisioned for the future – while simultaneously reducing the time and cost to deliver them.

Low-touch provisioning

Traditional network provisioning is a multi-step, labor intensive process for CPE deployments. The design phase, sourcing, and on site provisioning can typically take several weeks, delaying growth and return on investment. Manual provisioning performed by skilled technical staff is time consuming and vulnerable to human error. Since low-touch provisioning has less human intervention, there is less chance of manual errors and increased reliability.

Low-touch provisioning is an automated service delivery model which reduces the need for high-value technical personnel to be dispatched to remote site locations to install new services. Instead, once the universal CPE (uCPE) is delivered to the location and powered-up, a secure connection will be made to back-end orchestration servers at initial power up and registration activated on the network. Configurations that have been ordered will automatically be received. Verizon has the ability to deliver services through low-touch provisioning over broadband, internet dedicated circuits, and MPLS as well as Wireless 4G LTE. In the case of a Hosted Network Services model, provisioning can be done quickly --- in some cases within a matter of days after the time the order is sent to service delivery.

Integrated management and deployment systems

Organizations are moving away from traditional OSS stacks to a simplified, pre-integrated horizontal architecture that can be readily configured to support specific service offerings including those that leverage Virtual Network Functions (VNF) such as SD WAN, mobile Virtual Private Networks (VPN), and 5G network slicing.

What is dynamic orchestration and assurance?

The right orchestration platform brings together a comprehensive and flexible end-to-end solution to manage the rapid deployments needed to manage, monitor, and maintain the needs of your applications-based services in hybrid environments.

Verizon's VNS solution is driven by the Verizon Network Service provisioning and orchestration platform which allows us to automate complex service provisioning, delivery, and assurance. Verizon Network Service provisioning enables:

- Rigorous design and validation of template Blueprints, prior to release
- Standardized Network Service templates (referred to as Blueprints in Verizon) that are the hallmark of service provisioning automation
- Catalog and inventory-driven service order management
- Central repository for inventory management with all service configurations
- NFV Orchestration with VNF and network service resource orchestration and networking based on Open Source OVF, HEAT, and Tosca models and to eventually incorporating container-based deployments.

- Service configuration management with model-driven provisioning based on Open Source YANG and REST models and agnostic of the protocol leveraged by the VNFs for the configuration interface
- VNF Management with VNF and virtual network service modeling and lifecycle management
- Dynamic network topology discovery and automated VNF snapshot management ensuring continuous monitoring and quick recovery in the event of service faults
- Closed-loop policy-based service assurance supporting customer Service Level Agreements (SLA) using policies based on potential VM fault alarms

How does Enterprise Orchestration work?



Figure 9: Verizon Enterprise Orchestration value and benefits

Verizon’s Enterprise Orchestration platform fully automates multiple layers of complex processes across the service lifecycle allowing rapid onboarding and validation of VNFs and service chains to create new solutions, including automated resource management, service design and configuration, and policy-based service assurance. Significant investment has been made to integrate Verizon’s state of the industry Multi-vendor Event Translation Layer (METAL) system to communicate with our Integrated Management Platform for Advanced Communications (IMPACT) and SMARTs service assurance platforms. The Enterprise Orchestration system interfaces with IMPACT to provide durable alarms and notifications for service impacting events. This is used to facilitate effective and efficient event management and customer notifications. Verizon uses dynamic topology discovery of the VNF’s and Network Services to ensure the monitoring is based on the true topology of the network. Closed Loop Assurance uses the alarms generated by VNF’s and reported to the monitoring systems to perform appropriate corrective actions. For example, if a VNF goes down due to a software failure, the event will be immediately identified by the monitoring tools which will determine how to best re-start the VNF (providing resiliency to the given VNF).

© 2020 Verizon. All Rights Reserved. The Verizon names and logos and all other names, logos and slogans identifying Verizon’s products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.