A Guide to SDN, SD-WAN, NFV, and VNF

Are you as confused as everyone else with the deluge of new buzzwords in network industry news? The concepts are related but distinct. Understanding the underlying principles illuminates the power achieved by implementing these architectures and technologies in your wide area network (WAN).

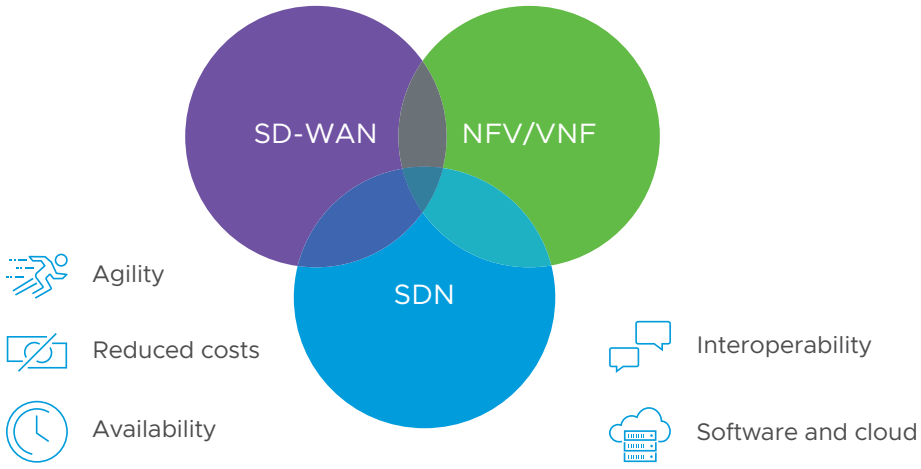

FIGURE 1: SDN, SD-WAN, and NFV/VNF.

Focus on the terms

A good start is a clear definition of each term.

Software-defined networking (SDN) is an architecture where the key principle is the physical separation of the network control plane from the forwarding plane. The control plane software makes decisions about how to handle traffic, while the data plane is the data content flowing between two network nodes. Through this separation, an SDN architecture achieves the key benefits of central management, a global view of the network, redundancy and fault tolerance, agility in the implementation and distribution of policy and routing changes, and hardware independence. It also incorporates open standards and encourages interoperability.

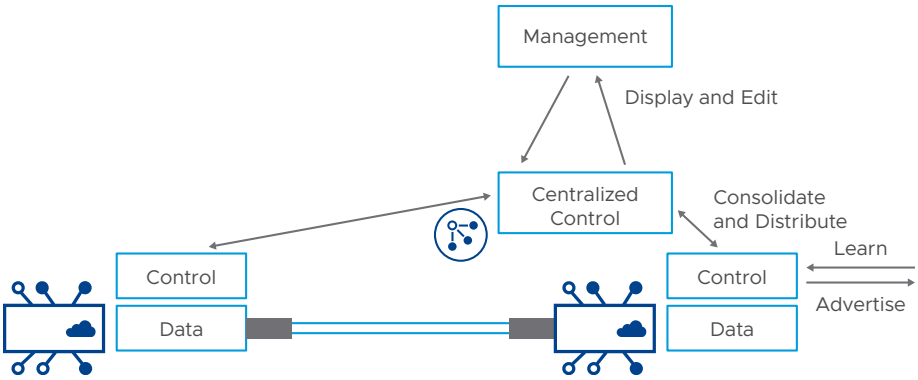

FIGURE 2: An SDN architecture.

Software-defined WAN (SD-WAN) is a technology that applies the key SDN principles to WAN, and then extends them in innovative ways to address the practical realities of WANs, such as minimizing delays over long distances between nodes and providing predictable service quality over often unpredictable links. SD-WAN makes network decisions using both centralized control policies and knowledge of local conditions throughout the distributed network, such as local service quality measurements and the availability of bandwidth on links.

Network functions virtualization (NFV) is an architecture specifying how to run SDN functions independent of any specific hardware platform. NFV is implemented as the infrastructure platform that orchestrates VNFs. Data centers have long used NFV, but the concept has more recently become coupled with SD-WAN to leverage the benefits in individual and remote branches.

Virtual network functions (VNFs) are individual network services (such as routers and firewalls) running as software-only virtual machine (VM) instances on generic hardware. For example, a routing VNF implements all the functions of a router but runs in a software-only form, alone or along with other VNFs, on generic hardware. VNFs are administered and orchestrated within the NFV architecture.

The core goals are the same

These architectures and technologies shift network implementation away from dedicated—and often limiting—single-function hardware distributed through the network to software and virtualization that are significantly more flexible, scalable, and easily upgradable. All four concepts share the same objectives and benefits:

- Future proof – Upgrade software instances (VNFs) by download at any time from a central orchestrator. Instantly adjust scale by assigning appropriate, policy-based server resources and priorities to the VNF.
- Software and cloud focused – Run software functions and services anywhere, and control them from a central orchestrator. That is, the software instances run in the cloud and, simultaneously, they are the cloud.
- Agile – Download, move, upgrade, remove, activate/deactivate, and scale up/down any VNF with a single click from the orchestrator.
- Reduced enterprise costs – Deploy generic hardware to remote locations. Control network services and functions available at the site remotely by downloading VNFs, and scale them by assigning (governed by central policy) processing and storage resources.

- Widespread availability – Maintain network flows despite link failures, node failures, and other network problems by removing the decision-making (control plane) from the forwarding hardware (data plane). If an outage affects the data plane, the control plane can redirect the data flow elsewhere. If an outage affects the control plane, the data plane continues forwarding.
- Vendor agnostic and highly interoperable – Run network functions as programmable (using open standards) entities on generic hardware.

SD-WAN leverages SDN principles

SD-WAN combines the tenets of SDN with those of a distributed WAN, simplifying control and easing the flow of information to the cloud. This evolution makes SD-WAN technology highly scalable, leverages Internet routing to make the network fully redundant without any single point of failure, and obviates the need to wait for information from end devices before taking action.

The primary difference between the tenets of SDN and SD-WAN is where and how decision-making occurs. SDN advocates a central controller to dictate network behaviors. In contrast, SD-WAN generally manages based on central policy control, but decisions may also be made locally while taking into consideration the corporate policies. Or decisions can be made centrally while incorporating knowledge of local conditions reported by remote network nodes.

NFV and VNF: A closer look

The relationship between NFV and VNF is similar to that between SDN and SD-WAN: NFV is an architecture guiding management and orchestration activities, whereas a VNF is the technology providing virtual (that is, hardware-independent) network functions such as routing or firewalling.

The advantages of an NFV architecture allow you to:

- Quickly roll out new locations and services, such as security (in the form of a VNF)
- Distribute services enterprise-wide at low cost
- Reduce dependence on hardware (multiple VNFs can be deployed on the same hardware)
- Flexibly scale services up or down
- Reduce maintenance windows
- Upgrade VNFs independent of the hardware, making the latest version always available

The virtualization part of both NFV and VNF denotes that network functions are implemented in a generalized manner independent of the underlying hardware. VNFs can run in any VM environment (a server or host platform, or infrastructure as a service) in the branch office, cloud, or data center. This architecture allows you to:

- Insert network services in an optimal location to provide appropriate security. For example, insert a VNF firewall in an Internet-connected branch office rather than incur the inefficiency of an MPLS link to hairpin traffic through a distant data center to be firewalled.
- Optimize application performance. Traffic can follow the most direct route between the user and the cloud application using a VNF for security or traffic prioritization.

In a VM environment, several VNFs may run simultaneously—isolated from each other, standards-based—and can be independently changed or upgraded.

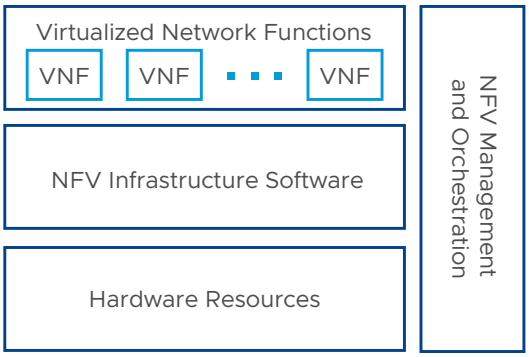

FIGURE 3: VNFs running in an NFV architecture.

Making it all work together

SD-WAN and NFV are complementary and form a powerful combination when used together. Both can easily be deployed in enterprise or cloud data centers with SD-WAN service chaining, or distributed as virtual services (VNFs) all the way to branches. By leveraging NFV services with SD-WAN, service deployments can be made in batches across the enterprise and simplify service insertion at branches. Additionally, while NFV is typically used to deploy services in the cloud, it can be used with SD-WAN to deliver those cloud services across the entire organization to each remote location.

SD-WAN, NFV, and VNF with VMware SD-WAN by VeloCloud

The central orchestrator implements the control plane of a VMware SD-WAN™ by VeloCloud® solution, while the edges and gateways implement the data plane. The separated control and data planes reflect the implementation of both SDN and NFV architectures.

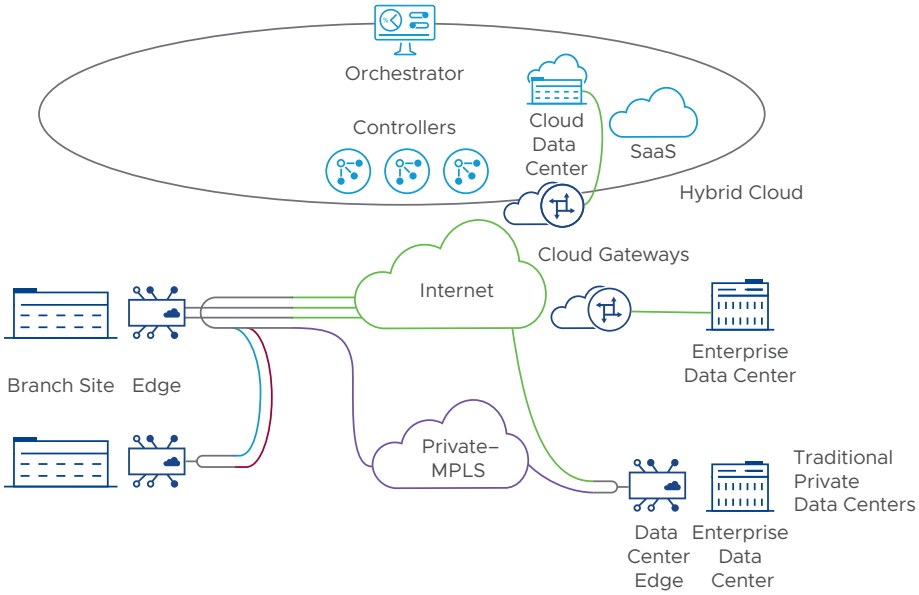

FIGURE 4: Architecture of a VMware SD-WAN solution.

The VMware SD-WAN Orchestrator by VeloCloud maintains a global view of the network and programs the VMware SD-WAN Edges by VeloCloud, which can be either custom (single-function) or generic (VNF) hardware deployed at remote locations. Edges learn routes, which allows central decision-making in conjunction with remote/local execution by the edge. This architecture ensures both survivability when the orchestrator or gateway is out of reach—an edge device makes local decisions based on its last known instructions—as well as optimal performance as no delays are incurred by a distant controller in the middle of the traffic forwarding path.

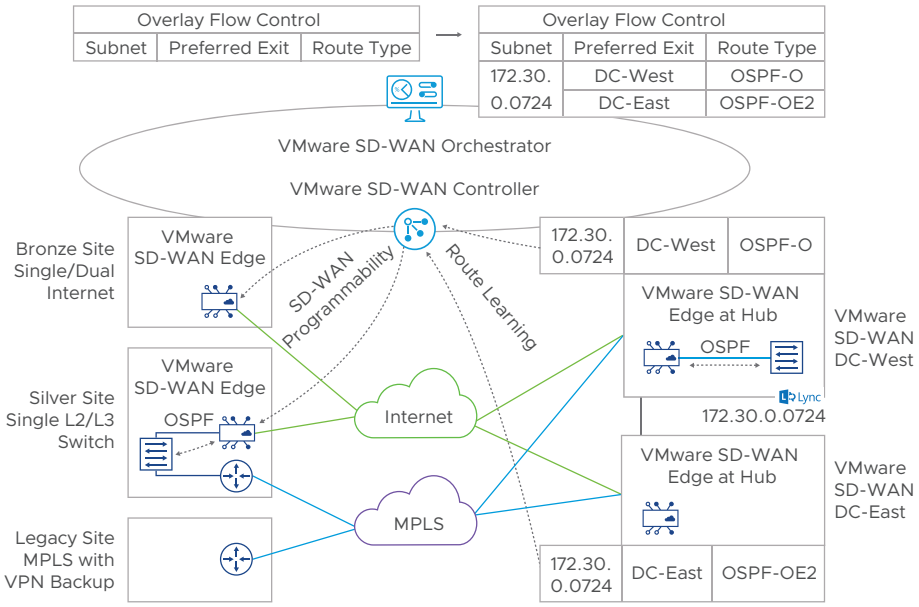

FIGURE 5: VMware SD-WAN solution with multiple, different edge devices.

Edge devices may be implemented in many flavors, such as virtual or hardware. This allows you to optimize the footprint and function of each office, regardless of type or size.

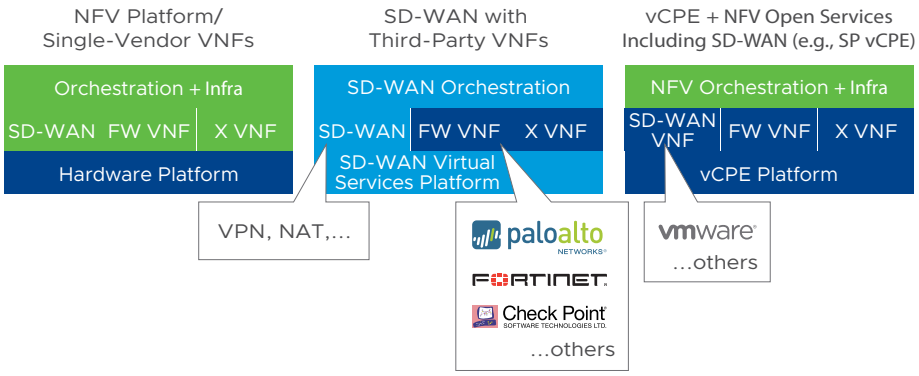

FIGURE 6: Types of VNF services.

It is increasingly important for vendors to offer existing services in VNF form, supporting the trend toward more open, interoperable platforms. VMware recommends either of the following as an open approach:

- An SD-WAN-focused NFV platform – A core SD-WAN platform that additionally runs third-party VNF service choices.
- An open NFV-service platform – A generic virtual CPE (vCPE) platform that allows loading an SD-WAN VNF along with other third-party VNFs. A current example in the marketplace is AT&T's vCPE that supports third-party VNFs and hosts the VMware SD-WAN VNF solution.

In conclusion

SD-WAN, SDN, NFV, and VNFs all share similar principles and goals. Complementary in concept and implementation, these architectures and technologies are extremely powerful when used in combination. There is no reason to choose one technology or architecture over the other. Instead, determine where each can provide maximum benefits to your network.

For the enterprise and channel alike, benefits include:

- Agility
- Reduced cost
- Increased availability
- Interoperability
- Enablement and support for cloud migration

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com