WHITE PAPER

SOFTWARE-DEFINED NETWORKING IN THE DATA CENTER

The changing roles of software and hardware network infrastructure

vmware®

Table of Contents

Executive Summary: Software-Defined Networking in the Data Center

All IT organizations deal with complexity. Having complexity itself is not the result of mediocracy. In fact, it's the opposite. Complexity is a byproduct of success. Complexity can be an artifact of rapid growth or the result of mergers and acquisitions. Yet regardless of its origins, complexity is a problem. It's the enemy of efficiency, security, and innovation.

"Traditional network offerings are not well-suited to fulfill enterprise expectations for rapid delivery of new services, more flexible business models, real-time response and massive scalability."[1]

—GARTNER

This paper proposes a set of design principles that lay a foundation for alleviating IT complexity and achieving new levels of efficiency and security. These design principles begin with a software-first strategy that enables your IT professionals to manage the complexity of the past with the consistent networking and security model of the future. This future state of the network gives your IT organization the ability to create dynamic, software-defined networks that build upon static, stable, reliable physical network infrastructure. Among other business and IT benefits, this strategy of integrating software helps networking and security functions attain the characteristics of cloud: agility, speed, manageability, and portability.

At the highest level, this paper makes the case that the problems that exist in today's networks can't be solved with yesterday's approaches. To solve today's problems, while creating a platform for future growth, IT organizations need to think in new ways. The mindset in networking and security must evolve to one that breaks away from the hardware-centric models of the past and embraces the integration of software for the network strategies of the future.

Software Has Eaten the World

It's been seven years since Marc Andreesen's Why Software Is Eating the World was published in *The Wall Street Journal*. Today, the points made in that article have been proven at enterprises around the world. A survey conducted by Dell Technologies and the Institute for the Future found the mantra that "every business is now a software business" has become a reality, with 82 percent of respondents planning to be a software-defined business within five years.

The network is next. Not because physical networking is going away. There will always be physical networking infrastructure to move bits and bytes from A to B, deal with latency, manage flows, and more. Physical network infrastructure continues to evolve and become rock solid based on the specific needs of data center fabrics, campus networks, and routed WANs. Hardware forms a web of highly reliable connections, which by itself is a complex task to refine to a highly efficient operational model. But history has taught us that when we rely on hardware to do more complicated things, like defining policies that automatically follow dynamic ephemeral workloads, hardware starts to buckle under the pressure. Further, the cloud has no hardware boundaries and extends transparently through private data centers and on to users.

When you virtualize the network and move to a software-first strategy, two things happen:

- You simplify and make your infrastructure fundamentally more efficient.
- You make your infrastructure more secure, because there are fewer "seams" to exploit.

[1] Gartner 2018 Strategic Roadmap for Networking, May 3, 2018 - ID G00351455

The Changing State of the Network and Software-Defined Networking

The age-old mantra of "You can't know where you're going until you know where you've been" holds true for today's modern data center networking. As we delve into why the world is changing, and how leading with software is becoming more and more critical, it is important to know the recent history of networking to understand how we got to the current state we are in.

"After decades of focusing on speed, network performance and features, future network innovation will target operational simplicity and business models that closely align with elastic cloud-based services."[2]

—GARTNER

With that thought in mind, we have included an appendix to this paper that presents a brief history of time for networking in the data center. This history creates context for the distinct goals networking is trying to address, either with new software technologies or ones that will remain rooted in hardware.

The Evolution of Software-Defined Networking

The Open Networking Foundation (ONF) defines software-defined networking (SDN) as "the physical separation of the network control plane from the forwarding plane, and where a control plane controls several devices." This is a design principle being widely used now but is not an actual solution to specific use cases. While different use cases still use this basic design principle, the problems they address are very different. The following diagram shows the high-level use cases and the market adoption that drove them.

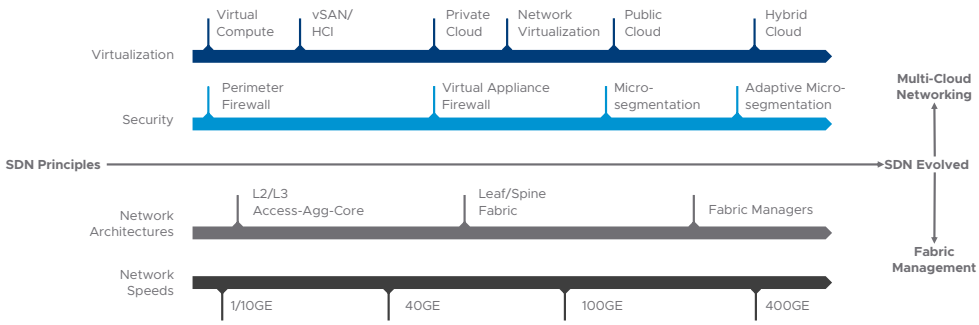

Figure 1. High-Level Use Cases for Software-Defined Networking

Multi-Cloud Networking: Virtualization paved the way to the private cloud, which demanded the same agility from the network as from the rest of the data center, leading to the first use case of network virtualization to complete the automation needed for the software-defined data center (SDDC). Network virtualization abstracted the networking done for virtual machines (VMs) from that of the physical network. The new network edge had moved into the virtual with an estimated 80M virtual ports and counting.[3] At the same time, public clouds started to become a reality, making it even more critical for a software abstracted network enabling the same operational practices across disparate environments. Further, applications began moving to new micro-service architectures based on containers, leading the movement to cloud-native applications. This shift proved that virtual networking could extend beyond the virtual machine to new future workloads.

[2] Gartner 2018 Strategic Roadmap for Networking, May 3, 2018 - ID G00351455

[3] VMware internal calculation.

Network Security: The move to the private cloud and SDDC inherently created a vast pool of resources that placed applications from very different parts of the organization right next to one another. For example, a human resources (HR) app could be running on the same physical server as an app from finance. Perimeter firewalling along with DMZs separation was not enough to stop attackers from hopping from one app to another. Network security needed a new way to segment. The same principles for SDN provided the next use case of micro-segmentation. The central control point, which was also building the virtual networks, could segment by creating unique networks for each application and deploy internal firewalling to protect traffic among apps. This also enabled a shift to zero-trust security models.

Physical Fabric Management: The need for physical networking does not go away with SDN. Physical network architectures evolved in both design and speed. Data movement within the data center, often referred to as east-west traffic, began to far outpace that of the data coming and going. Legacy tiered architectures could not keep up, so a new spine-leaf design was adopted. This design led to the third evolution of SDN as a physical fabric manager. The same SDN design principle could abstract the complexities of managing and operating the physical fabric by controlling the interconnection and physical networking protocols and providing advanced visibility.

Software-First Requirements for Network Upgrades

As your organization approaches network upgrades and the shift to software-defined solutions, it's important to remember that business drivers should guide infrastructure decisions. The drivers can take the form of higher-level goals to modernize the data center, cloud-first strategies, or something more tactical, such as an in-progress data center consolidation. Either way, the conversation should begin at a strategic level that considers the business and its priorities.

After that, IT practitioners build an environment that supports the new initiative using a software-defined networking strategy aligned with business priorities. For the infrastructure, the high-level requirement of multi-cloud networking takes the form of network virtualization, automation, multi-cloud extensions, and cloud-native approaches. Network security becomes intrinsic to the workload and applications. Fabric management moves to operational efficiency initiatives.

NETWORK VIRTUALIZATION CAN HELP YOU:

- Reduce network provisioning time from weeks to minutes
- Achieve greater operational efficiency by automating manual change processes
- Place and move workloads independently of physical topology
- Improve network security within the data center
- Enable agility while meeting uptime requirements by reducing fault domains

Network Virtualization

The foundation in any network upgrade with a software-first approach is network virtualization. Starting with network virtualization establishes a base platform that is agnostic to future hardware cycles, enables data center migrations, and flows seamlessly from the edge/branch, the data center, and into the cloud. Just as server virtualization re-creates the traits of a physical server within software, network virtualization replicates the components of network and security services in software. Consequently, the virtualized network is provisioned and managed independently of your hardware, and the physical networking devices simply become vehicles for forwarding packets.

Changes to networks have traditionally been viewed in a very risk-averse way. The fault domain of the network can be the entire data center. The network is just supposed to work, with key success criteria measured as uptime. Network virtualization still keeps the same goal of uptime and having the network just work, but it also adds agility as a top priority. Since networks are now built for each app or even workload, the fault domains are now small, and quick changes providing agility can now be realized.

With network virtualization, your network administrators can provision and change virtual networks—including logical switches, routers, firewalls, load balancers, and VPNs—in minutes rather than days or weeks. With these capabilities, network virtualization helps your enterprise achieve major advances in simplicity, speed, agility, and security by automating and simplifying many of the processes that go into running a data center network.

With benefits like these, many enterprises are realizing the power of network virtualization to transform their IT from hardware-based infrastructures to agile, software-based architectures. By looking at software first, they can deliver services faster, strengthen security, keep applications up and running, and save substantially on CapEx and OpEx costs.

A QUICK NOTE ON TROUBLESHOOTING

As with any abstractions, a meaningful level of operational integration offers the most visibility. Fortunately, since these abstractions are not net new themselves, a common operational scheme can take place. In fact, bringing the network abstraction layer into software increases the level of visibility by increasing the intersection of network and compute tools. For example, a traditional networking tool is traceroute, which shows hop-by-hop through the network. This same tool is available, but now starts within the host and can include all the virtual infrastructure as well with application context built in.

Automation

Automation is not a goal, it is a necessity. Automation in a virtual network leverages the application-level constructs to become part of the solution, rather than a bolt-on afterthought. "Integration" can mean very different things, which are discussed in detail in the following design criteria section. Automation that is part of the application-layer constructs is native to the hypervisor for virtual machines, into container orchestrators like Kubernetes, and extends to the cloud. To know automation is to know the goals of the users whom automation targets.

TOP-LEVEL DESIGN CONSIDERATIONS FOR AUTOMATION

1. Automation should start with built-in constructs, not bolted-on, after-the-fact approaches.
2. Software can remove constraints to automation by leveraging the workload constructs.
3. Platforms rooted in software can then extend the native integrations past the data center to the cloud and to the branch.

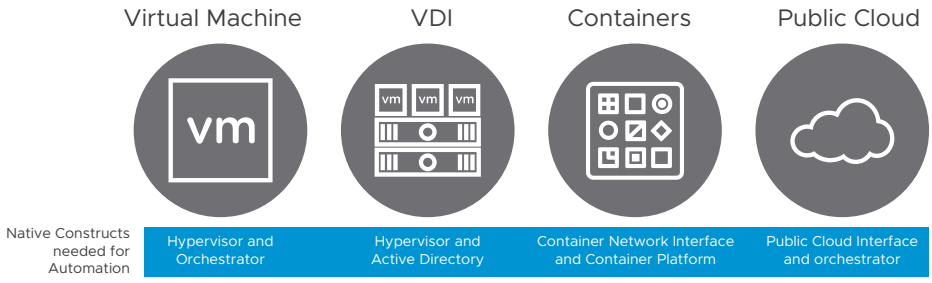

Figure 2. Application Layer Constructs

The terminology of software-defined networking started with projects that had their conception in the fact that networking constructs, such as routing, IPs, VLANs, and switches, were all a bottleneck in an otherwise fully automated process. These same bottlenecks drove the rise of the cloud and shadow IT. Completely separated environments were being created that were run by developers, for developers, like developer clouds.

End-to-end automation, from branch to data center to cloud, removes networking bottlenecks. But while the vision of ubiquitous automation is important, it can be difficult to implement and run such a structure. There are constraints to consider.

THEORY OF CONSTRAINTS

The theory of constraints is a management paradigm that views any manageable system as being limited in achieving more of its goals by a very small number of constraints.

Network and security automation are often constrained by the disjointed nature of the infrastructure that runs workloads. Software can remove this constraint by including networking and security into the workload constructs, such as within VMware vSphere® itself. This virtual networking security automation unlocks 80 percent of the benefit. The remaining 20 percent is unlocked by taking the initial steps toward a software-first strategy—network virtualization and automation. Once the platform is in place and the first use case has been implemented, the remaining pieces quickly fall in line as the initial constraint has been lifted.

Multi-Cloud Extensions

Today, multi-cloud is a very common reality. Already, 86 percent of enterprises have adopted a multi-cloud strategy, according to a study conducted by Forrester Consulting on behalf of Virtustream.[4] A software-first platform choice extends a common platform to multi-cloud environments with common policy, components, and enforcement.

The use of diverse, purpose-built platforms, such as AWS and Azure, has led to a breakdown in the IT flexibility these platforms seek to provide. These bespoke systems either force a slowdown in development or cause development to go around IT. The virtual cloud network alleviates these challenges. It uses network virtualization and automation with intrinsic security to create a broader holistic architecture.

This architecture enables developers to develop anywhere, without bypassing IT. Each public cloud environment has built its own IaaS environment that acts as the foundation for other PaaS and unique differentiated offerings like machine learning, database services, storage options, and much more. In the same way network virtualization runs across physical fabrics within an SDDC, these services can also run across public cloud infrastructure. This enables IT to maintain common control and operations for networking and security, while enabling developers to use the unique benefits of each without worrying about how each cloud environment has implemented the IaaS.

Cloud-Native

Multi-cloud networking has created a new model that serves as a platform that developer-ready infrastructure fits right in. It is an environment that "just works" for the developers and allows IT to maintain control without impeding the work of the development team. Containers as a Service (CaaS) is exactly this: IT infrastructure deployed and managed by IT. In this use case, the microservices components are individually configured, secured, optimized, and hardened to meet IT requirements.

Cloud-native developers typically have a few primary concerns (such as continuous delivery, a microservices-based application architecture, and mobile-first development), and they typically are looking for support with multiple languages and frameworks. It is often easy to discuss cloud-native in the bubble of containers or the bubble of one particular public cloud. But it's important to remember that cloud-native has its roots in software, not hardware. Cloud-native as advocated by the Cloud-Native Computing Foundation is an approach that uses an open-source software stack to deploy applications as microservices.

[4] Virtustream news release, "New Study: Shifting Business Priorities Herald the Era of Multi-Cloud," July 12, 2018.

BENEFITS OF HAVING SECURITY CLOSER TO THE APPLICATION INCLUDE:

- Minimize gaps in security posture to prevent data breaches
- Secure applications without hindering development and increasing time to market
- Simplify audits

Network Security

The evolution from virtualization to private clouds and SDDC brought the rise of micro-segmentation. It took the notion of general network segmentation, done by networking constructs like VLANs, ACLs, and even physical firewalling, and moved it closer to the application. This change was necessary because network constructs did not provide enough security, while physical firewalling proved not operationally feasible to segment all east-west traffic in the data center due to cost and complexity. To first solve the need of agility, micro-segmentation first must move closer to the workload to be close enough to the "application to know" context, yet remain far enough away that it is not exposed to the guest leaving it open to attacks.

The next step is to distribute the firewalling function to provide deep and broad policy enforcement. The control remains centralized and collocated with network virtualization control to provide the same automation benefits. Micro-segmentation that is based on the principles of SDN through the use of a distributed firewall can handle broad policy along with a deep level of inspection all the way to Layer 7. Creating security policies can then be automated through tooling based on application context along with identity such as Active Directory.

With the foundation of intrinsic security and micro-segmentation applied to virtual machines, the same principles extend to cloud-native and public cloud workloads. Having the control and enforcement in software allows for it to move seamlessly to other workloads. This provides consistency not only in policy but also in enforcement. This serves as a foundation of the concept of intrinsic security that will be examined in more detail in the design guidelines.

Fabric Management

The physical fabric management requirements are inherently partitioned from that of the rest of the virtual network. The two should still be considered together from an operational standpoint, but not as part of the same end use case. The physical fabric can be designed in many ways from standards-based protocols to full proprietary fabric managers or somewhere in the middle. Requirements of the physical fabric are designed to meet the needs of specific infrastructure environments (data center, campus, branch) and optimized for price, throughput, and latency. The original requirements of uptime and minimal change remain.

RESOURCES

Certain best practices follow separation of duty and goals while maintaining operational simplicity. Examples of these best practices can be found in the "Deploying NSX Data Center with Cisco ACI Underlay Design Guide 2.0."

Further tools like VMware vRealize Network Insight can provide visibility across virtual and physical infrastructure.

For more detailed reference design guides, see:

- VMware NSX-T Reference Design
- Reference Design Guide for PAS and PKS with VMware NSX-T Data Center

Software-First Design Guidelines

To this point, we have reviewed the requirements and seen the different approaches to SDN. As outlined in the "Software-First Requirements for Network Upgrades" section of this document, not all solutions that follow the principles of SDN are accomplishing the same task. Some solutions may even be provided by different vendors. This section includes a set of design guidelines for upgrading from a traditional networking architecture to an architecture that is automated, works with developers, and contains intrinsic security and cloud. These are all among the benefits of VMware NSX® solutions, which provide a network virtualization platform for the software-defined data center (SDDC).

VMware NSX solutions deliver networking and security entirely in software, abstracted from the underlying physical infrastructure and agnostic to any underlay network. NSX lends itself perfectly to a software-first strategy and the virtual cloud network. It provides pervasive, end-to-end connectivity for your apps and data, wherever they are.

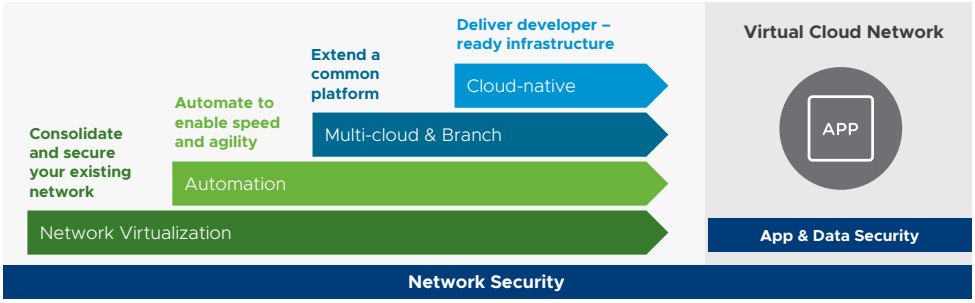

Figure 3. Multiple Paths to Transforming Networking and Security

Design for Solutions

Intrinsic Security

While once a pure technology conversation around the role the hypervisor plays in security, micro-segmentation is now a marketing term used by many companies to provide a bolt-on solution in their own specific way. The original goals of micro-segmentation are still valid, but they have now evolved to be an intrinsic part of the virtual cloud network.

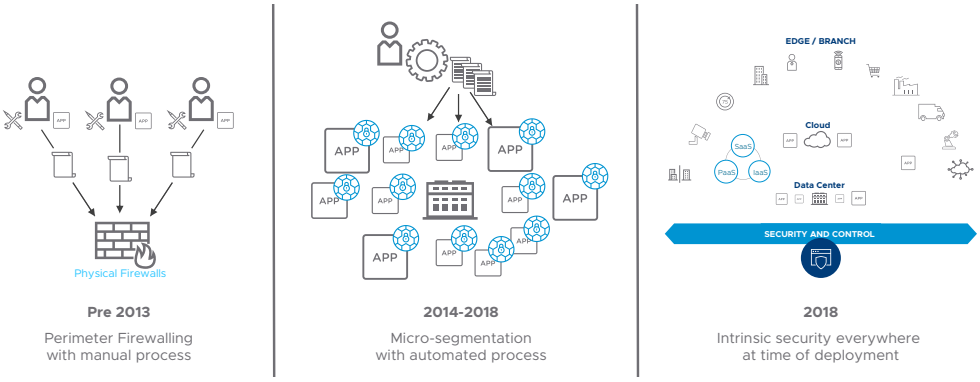

Figure 4. From Micro-Segmentation to Intrinsic Security

Intrinsic security:

- **Grows with the workload**—the security constructs scale along with the software it runs on.
- **Evolves naturally to new workloads**—the constructs are flexible to new types that match the pace of the software itself.
- **Is agnostic to domains**—workloads can be placed seamlessly at the DMZ, on-premises, in the cloud, in hosted environments, or in the edge or branch.
- **Is broad and deep**—it must be simple to start broadly while having the context, automation, and scale to cover depth.
- **Is extensible**—the limitations are clearly defined and partner constructs are built in.

The fundamental characteristic of intrinsic security is that it inherits the properties of the workload.

Coverage of Both Virtual and Physical Assets

This all begs the question: What about the physical workload? The virtual cloud network software-first approach surrounds native hardware workloads with software.

The first point of entry is the DMZ. The virtual cloud network enables a "DMZ anywhere" approach that takes DMZ security principles and decouples them from traditional physical network and compute infrastructure to maximize security and visibility in a manner that is more scalable and efficient. The challenge with traditional methods of securing the borders is that the firewall or sentry typically protects a single location along the frontier. To successfully monitor all activities, both at the border and inside the DMZ, the security solution must be able to scale to provide boundary protections for every individual device in the DMZ, as well as a secure network. This was a challenge using traditional hardware-based approaches. With the virtual cloud network, a DMZ can be anywhere.

Next is the set of workloads waiting to be migrated to a virtual environment. The virtual cloud network realizes this migration by easing the network and security impact through software abstraction. Often these workloads are abandoned to physical as the time or energy for the project has moved on, but with the ease of migration offered by the virtual cloud network, these resources can be reclaimed to the virtual.

Then there is a set of legacy systems that cannot be virtualized (for example, AIX) or systems that are inherently non-virtual (for example, hospital equipment). These systems are inherently averse to software integration solutions; otherwise they would likely already be virtualized or would eventually be virtualized as part of Internet of Things initiatives. These systems often have either legacy or bespoke operating systems that agent-based or native OS endpoint security approaches cannot handle. For these systems, the virtual cloud network takes a hardware-surround approach.

The first flow of traffic from these systems is to and from workloads already natively integrated into the virtual cloud network. This had traditionally been the most difficult scenario to cover, because the virtual domain is filled with changes in real time, but the mechanisms for securing the physical, such as Access Control Lists (ACLs) or physical firewalling, involved a manual process. Now, with security to and from this virtual domain built in, these flows are among the simplest. They are an intrinsic part of the virtual cloud network.

Finally, there are the flows from physical to physical and, unlike physical to virtual, they are some of the simplest to lock down with traditional methods. These flows can now be brought into the single pane of glass through visibility tools and firewall integrations built into the virtual cloud network.

If the workload is already cloud-native, as in the case of containers on bare metal, then the intrinsic security is already in place. With the container network plug-in on bare metal, container workloads already have the virtual cloud network extended.

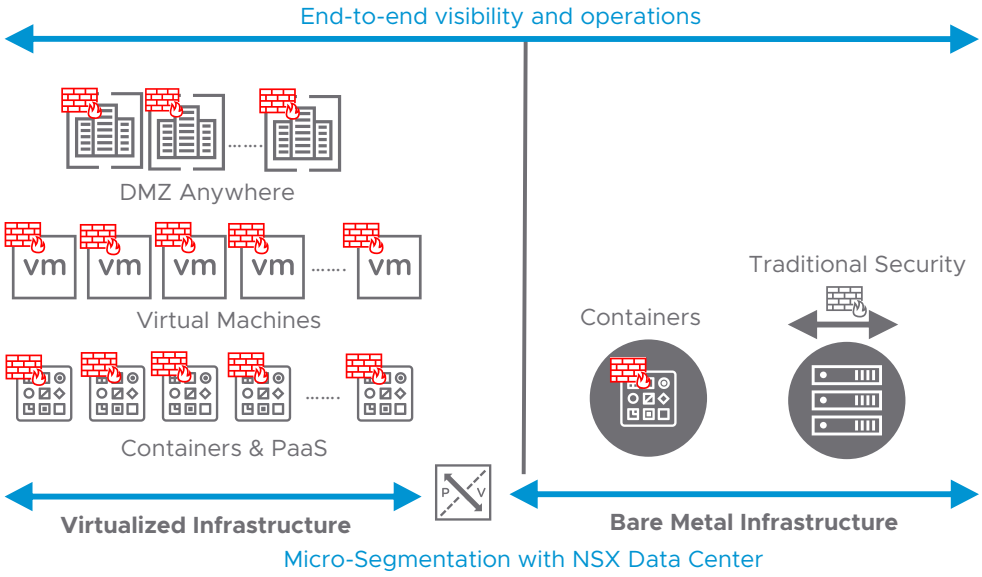

Figure 5. Virtual and Physical Security

Then, the virtual cloud network extends to the remote office/branch office (ROBO) and to the end users themselves. With SD-WAN moving the WAN to software, the digital workspaces and virtual desktops are all already baked in.

The Mixed State Is the New Norm

The goal of complete consistency at the end of network hardware upgrades is no longer valid. Once one cycle has finished, the next has already started. Domains outside of the physical network now exist in the cloud and in hosted environments. It is safe to say that any solution must support a variety of old hardware, new hardware, and no hardware at all. Almost all enterprises have a mix of legacy networking hardware, new networking hardware, and workloads in areas where networking hardware is out of IT's control (for example, public clouds, service providers, and more).

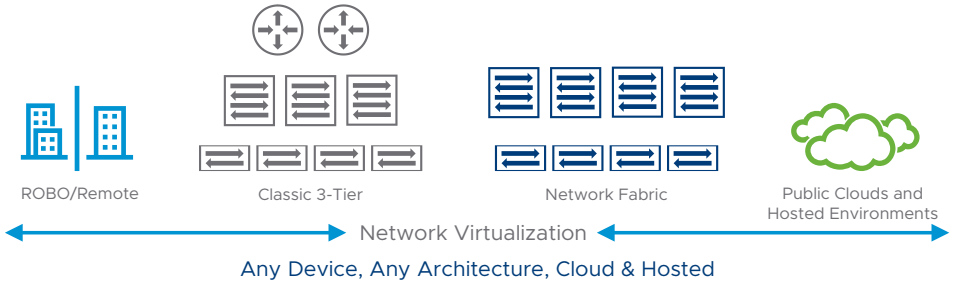

Figure 6. Designing for the Mixed State of Networking

Providing a simplified network overlay in software allows the physical network upgrade to be completed based on considerations to the physical network, and it simplifies the migration to new network hardware and fabric managers. The overlay takes care of the logical networking, allowing physical infrastructure upgrades to be done without interrupting the automation or development of applications.

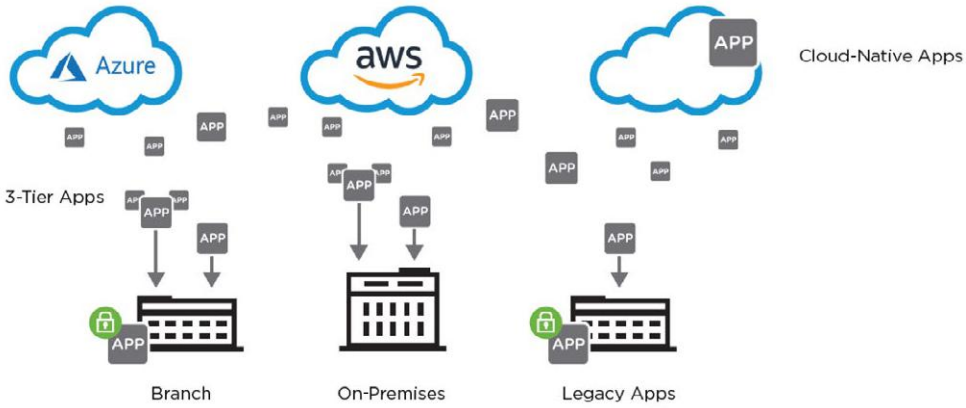

Figure 7. Designing for the Mixed State of Applications

The Greenfield Data Center

If you're designing a new data center, the network discussion should begin with software that can enable the entire organization. Yet in many cases, organizations make the mistake of keeping the networking decision siloed and defaulting to the next generation of networking gear from the current networking vendor.

This planning mistake puts an organization on a path that further ingrains solutions into future hardware purchases. Decisions on bringing in all the latest and greatest kit along with converged, hyper-converged, and software stacks can overshadow the end goals these solutions are looking to provide. To operationalize the new data center—from migration of workloads to seamless operational models—the network should enable a solution for use not only in the new data center but also across the current environment, while embracing the path to the cloud.

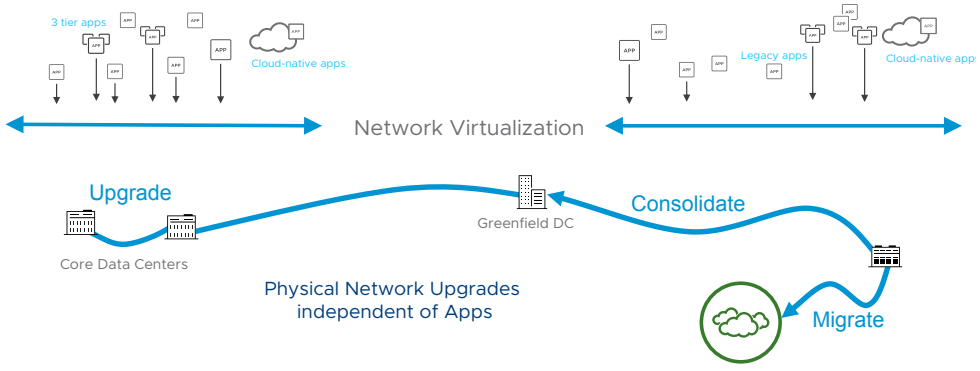

Figure 8. Seamless Migration and Upgrades

The Path to Cloud

Finally, whether you're choosing your next generation of switches or a fabric management technology, thinking software-first fundamentally embraces cloud strategies. The network upgrade is a perfect opportunity to envision a solution that starts with software and can simplify that upgrade.

Figure 9. End-to-End Consistency from Data Center to Branch to Cloud

Key Considerations and New Design Criteria

In this section, we outline key considerations and new design criteria that will help your organization create a foundation for a software-first strategy, one that alleviates IT complexity and enables new levels of efficiency and security.

Interactions Between Software and Hardware

Often the interaction between software and hardware are thought about too late in a project. Having these conversations early can lead to a more comprehensive approach to networking that breaks down silos and helps reduce risk. Here are some issues to consider in these conversations.

Codependency

Do the hardware and software services blend to form one cohesive management layer, control, and data plane layer? Is blending a good or bad approach? Hardware device capacity and service ability, together with its management software, will refresh in a codependent fashion. This codependency can lead to upgrades of some components held hostage to other components, negating the benefits of speed and agility that software brings.

Even networking hardware is being abstracted from the hardware it runs. Cumulus Networks was founded on this ideal in 2010, and Cisco also began offering this separation of data center networking operating systems and hardware in 2018.[5]

Independence

If hardware and software services are disaggregated, then independent cycles of either service allow for longer utilization of the hardware with less concern about the software lifecycle timeframes. This allows your software abilities to continuously increase with the latest updates, with little to no concern about the underlay. One area of innovation should not hold up another area's ability to innovate.

[5] https://blogs.cisco.com/datacenter/new-portability-options-for-ciscos-data-center-networking

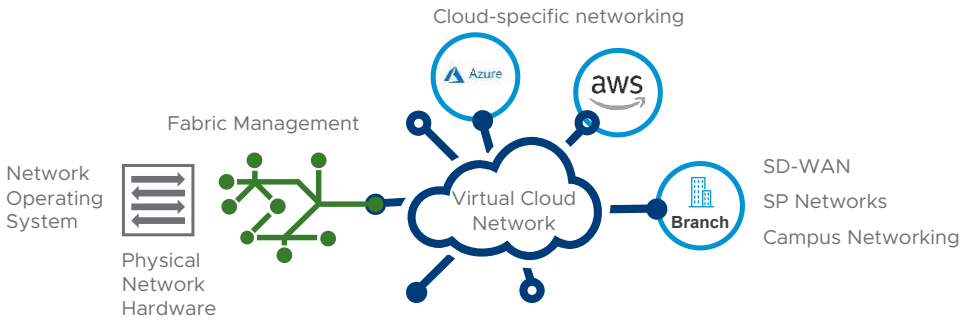

Figure 10. Network Abstraction Points

With these two thoughts in mind, what does the lifecycle of the application look like? Is it tightly coupled with hardware or with clear delineations? Should virtual networking constructs be tied to hardware-based management solutions? Software will overcome hardware-bound solution paradigms in terms of speed of innovation, service function, scale, and agility.

Hardware Remains Important

While we talk about putting software first, hardware remains relevant. All on-premises data center environments require a hardware fabric to provide packet movement. Similarly, all environments require software services to run the hardware fabric and software services to drive application deployment, management, and various operations.

Division of Labor

Where does the division of labor rest for these two goals: managing a hardware switch fabric and managing a virtualized stack for the application and related service dependencies? Finding that intersection point should help your organization provide the highest level of operational productivity. This is the point at which management, application agility, and, most important, the highest level of operational availability can be attained. The virtual platform for the application should ride on top of this intersection point.

Intersections

Designing intersections is nothing new for software. Interactions through application programming interfaces (APIs) are well defined and used. Applications themselves are disaggregating and interacting through APIs. Now the same level of disaggregation is happening for software running the data center infrastructure, but in a slightly nuanced way. Platforms don't just expose APIs but develop interfaces or plugins.

Take, for example, the container network interface for containers or the Neutron plugin for OpenStack. This interface and plugin map a complete flow along with a set of APIs to support a level of "integration" and service-level agreements (SLAs). These APIs create the building blocks of the software-defined data center—if they are well defined. A gray area of the data center is the Wild West of open APIs without well-defined interfaces or plugins. Open APIs do not make an "integration."

A NOTE OF CAUTION:

If you are researching solutions, remember that "integration" is now a marketing term that should be treated with a high degree of skepticism. Always do your due diligence.

Current and Future Infrastructure

Where is the intersection between current and future infrastructure? Today, your organization maintains a large mixture of not only different workload types but different physical infrastructure or no physical infrastructure at all (as in the case of cloud, hosted, SaaS, and more). Any solution should examine the intersection between solutions that are under hardware control with those that are controlled by software.

Data center operations are evolving in the same way that applications are being disaggregated and serviced through a set of APIs. The physical network fabric has been abstracted into a simple set of fabric functionality. Various hardware components can plug-and-play into this fabric, and various fabric techniques can be used, both new and old. The abstraction platform is disaggregated from that underlay, allowing independence.

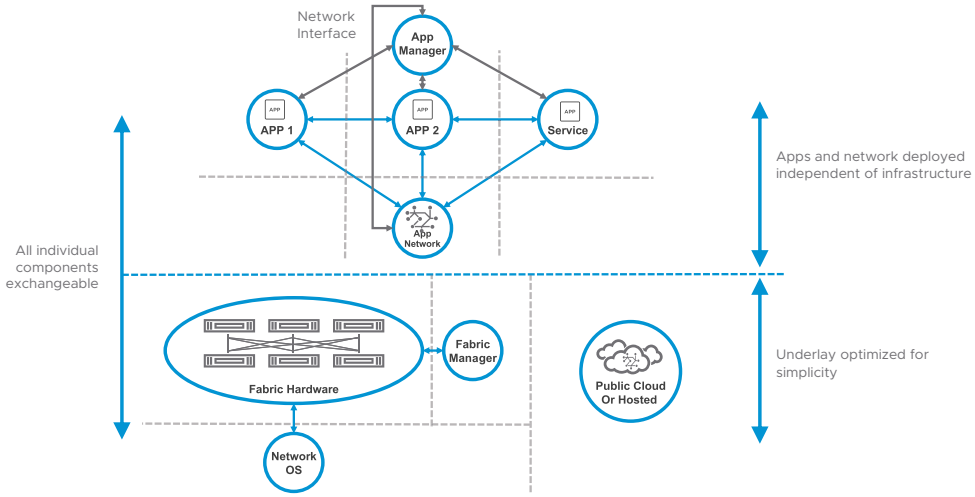

Figure 11. The API-Driven Infrastructure

It would be easy to assume that one solution set should handle it all: software that runs everything from the hardware fabric to the application solutions deployed upon it. Yet reality gets in the way. Software can change quickly in terms of capability, capacity, serviceability, functionality, and scalability. Hardware's limitations are defined at a specific moment in a chipset's initial engineering stages; the hardware is now "hardware bound," for lack of a better term for its limits. This is something that all IT shops experience when looking at their "legacy" networks and deciding what needs are lacking to support the vision of the next generation of data center.

Software tied to a hardware system is by its very definition tied to that fabric's past. The software must continually support the legacy needs while attempting to deliver new capabilities. This tie to the past slows innovation in the software, and thus causes a faster hardware churn for new service needs. This is happening all too frequently in today's data centers.

A NOTE ON HYPER-CONVERGED INFRASTRUCTURE (HCI)

It may seem that the goals of HCI break with the software-first methodology. Instead, software-first actually builds upon these fundamental values to create turnkey solutions. There isn't a need to tie software to hardware to get these same benefits. These solutions are also being offered as validated designs.

Overlays for Network Virtualization

At its core, network virtualization creates a set of overlay networks between workloads. The workloads could be VMs, containers, or even bare metal. The considerations for overlays can be broken down into two sets: goals and implementation.

Goals of the overlay—connecting tenants, workloads, or as a fabric manager technique

There are many separate goals for overlays that may all be used at the same time. On first look, this might appear as "death by overlay." But the fact is that overlays have been stacked for decades. A typical packet in the data center has been encapsulated several times already: Layer 2 with MAC, Layer 3 with IP, Control with TCP/UDP, and finally the workload's native overlay, VLAN. Anything beyond this will be abstractions that can serve various purposes.

The first use case has been used for decades to transport multiple tenants over service provider networks: MPLS. The concept is the same for network virtualization use cases, to provide isolated network domains for applications, tenants, or other bespoke frameworks. VXLAN and now GENEVE provide the encapsulation of the application or tenant traffic across any IP fabric. But these encapsulations can be used to simplify the physical fabric connectivity, as well as to enable fabric management.

Implementation of the overlay—co-located with the hypervisor or native workload environment, or split with network hardware

Implementation details may seem to concern only the vendors providing the solutions, but in the world of convoluted interactions between hardware and software, the concern is now being brought to the end user of the technology. Two outlines published by the Network Virtualization Overlay (NVO3) working group (RFC 8014 – An Architecture for Data-Center Network Virtualization and RFC 8394 – Split Network Virtualization Edge (Split-NVE) Control-Plane Requirements) illustrate that there are different mechanisms to implement an overlay. These outlines should be considered informational only and not implementation guides.

RFC 8014 describes the concept of "NVE Co-located with Hypervisor." For this mode, the only solution for VMware ESXi™ is NSX, because it is the only native network virtualization technique in the ESXi hypervisor. Any other solutions would fall under the "Split-NVE" mode, which introduces several complex considerations as outlined in RFC 8394. In the Split-NVE mode, the actual entry point to the overlay is external to the hypervisor, so substantial control considerations must be understood. The RFC calls for part of this intelligence to be implemented on the hypervisor for what it calls the tNVE, but in practice the tNVE is not something implemented by the hypervisor. For ESXi some solutions that are not native, try to replicate this functionality through a mix of APIs, but these solutions generally fall into the use case of fabric management and not application, workload, or tenant network virtualization. The Split-NVE also causes a hook to hardware and goes against the software-first approach outlined throughout this document.

What about other hypervisors, containers, or cloud? The RFCs don't implicitly address these elements, but the concepts remain the same. Take, for example, KVM, which has OVS to provide a co-located interaction. Containers have the container network interface (CNI) to provide a co-located interaction. A third type of design, not outlined by the RFC, is co-located with guest. The reason being, in the data center the co-located with hypervisor is the preferred method. For cloud, the option would be a guest co-location through an agent.

The Cloud

Cloud-first is not just an application strategy. Cloud networking has no hardware bounds. Cloud services are bound only by the software services and have an inherent ability to be modified on a continual basis with no consideration for the underlying hardware systems or the impending disruption a hardware cycle imposes. Cloud services have already shown the advantages of a complete disaggregation of the application platform from its underlying hardware devices. Therefore, virtual networking should not require consideration of the hardware fabric.

Separate the Fabric

Cloud services and network virtualization platforms do not tie containers, microservices, and virtual machines to heavy-handed management structures that invite complexity. Fabric management built on a maze of leaf-and-switch policies and profiles tied to physical fabric domains by other attachable policy abstractions creates unstable underpinnings for network virtualization management.

Simplicity with Virtualization

Simple compute virtualization has already shown that disaggregating compute dependencies from the underlying server systems provides an incredible level of operational productivity. Network virtualization should do the same. The network virtualization platform provides the application platform with the same level of disaggregation from the switching fabric. It also allows for an independent lifecycle from the physical fabric, which can lead to better operational costs. The network constructs for this virtualized network—using the same simple paradigm of logical switching, routing, and application service features—build a firm foundation for an application platform over an independently managed switch fabric. This foundation allows the application platform to deliver an independent virtual cloud platform, anywhere.

Remember, all IT environments require a switch fabric for high-performance packet movement. But an application platform does not require the hardware switch fabric to provide anything above high-speed packet movement in the right direction.

A Changing Mindset

Ultimately, networking and security must attain the characteristics of cloud: agility, speed, manageability, and portability. Networking is no longer about brand loyalty for the sake of history. Network teams are now in a key position to get off the hardware-centric solution treadmill and to promote change. Don't mistake this for bias toward a virtualization-only solution. The only bias should be toward the solution that best solves business problems.

To solve the problems that exist today while creating a platform for future growth, IT organizations need to think in new ways. The mindset in networking and security must evolve to one that expects and embraces growth. This shift includes embracing new challenges, being willing to overcome obstacles, not being afraid of failure, and finding value in the success of new ideas (for example, virtual cloud network). A growth mindset resonates at both the corporate and personal level. In a time of significant (digital) transformation, where software is a dominant force, both companies and individuals alike must be open to evolving processes, tools, and, most of all, people.

"To deliver the significant network changes that digital business requires, incremental technology and organizational changes will not suffice; significant cultural shifts must also occur."[6]

—GARTNER

For any architectural design, there is going to be a give and take between availability, manageability, performance, recoverability, and security. A solutions architecture should provide for these characteristics based upon an organization's business and technical requirements within the confines of their constraints and risk acceptance. Gone are the days of VLAN trunks and spans and complex tie-ins to the hardware fabric. The future lies in the ability to build static, stable, reliable physical networks upon which a more dynamic software-defined network can run. Gone are the days of relying on physical firewalls to protect information. The future lies in a multi-part defense-in-depth strategy that addresses all aspects of data security. To succeed in this new future requires a change in the mindset of networking and security.

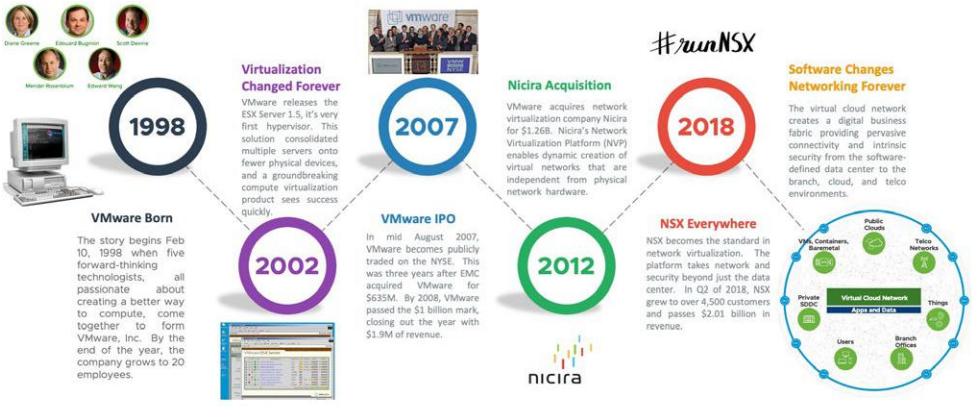

Figure 12. The Evolution of the Modern Network

Why VMware and NSX, you might ask? As previously mentioned, software is eating the world, and VMware has been a part of that process from the beginning. Since the company's inception, there have been tremendous milestones achieved in server virtualization with the VMware ESX® and vSphere product lines. In the past five years, we've seen similar growth and success in the network virtualization space with NSX. Now is the time to think slightly differently about your next network refresh and upgrade, looking beyond just the "packet plumbing" into how your business wants to evolve. A network fabric delivered in software can help you get there and deliver those experiences for your customers.

GET STARTED

Learn more about VMware NSX Solutions and a new approach to modernizing your network >

Join Us Online:

[6] Gartner 2018 Strategic Roadmap for Networking, May 3, 2018 - ID G00351455

Appendix A: The Historical View

In this reference section, we offer a look at the evolution of networking in the data center, from the race of speeds and feeds, to the rise (and in some cases, reversal) of merchant silicon, to fabrics and fabric management, and finally to software-defined networking. This brief history creates context for the distinct goals networking is trying to address, either with new software technologies or ones that will remain rooted in hardware.

Speeds, Feeds, and the Rise of Merchant Silicon

When Google introduced its infamous networking RFP in 2004—an RFP that no one could answer because of their current scale—a titanic shift in the networking world was already well under way. Central packet processing was being replaced by distributed control and forwarding planes. The rise of 10 Gigabit Ethernet (10GbE) was taking place, sparking a war over the next network upgrade cycle and hoping to put new bandwidth requirements on the traditional core and aggregation layers to support higher speeds at the access edge.

At the time, companies like Force10 (pre-Dell acquisition) were already building custom-designed ASICs in this new model and supplying them to some of the larger web scale and web services customers. Meanwhile, the likes of Arista Networks were just being founded in 2004 as "Arastra," looking to leverage a strategy using off-the-shelf chips, in what would become widely known as merchant silicon. This was the spark that started the fire to use chips provided in mass by companies such as Broadcom, Intel, Dune, and Fulcrum. This movement to leverage silicon built by companies whose main focus is building networking silicon would eventually lead to what is known today as "white-box" switches, and eventually to various disaggregated network operating system models.

So, what about Cisco? Around 2006, Cisco spun out Nuova Systems to build and deliver access switches purpose-built for the data center, leading to their expansion into the server business as well. During this time, Cisco was also busy building the first generation of purpose-built data center switching with the Nexus 7000 Series, which first came out in 2008. All the while, Cisco was sticking to its original hardware strategy, which had been in place since the company was founded in the 1980s: building networking telco equipment based on "custom" or in-house silicon.

This strategy is based on the belief that specialist engineers can develop a chip with advanced features and functionality at a pace faster than that of the companies providing merchant silicon. Typically speaking, this strategy also led to a higher price justification, because the feature innovation, speed of delivery, and faster and larger table sizes meant the hardware could be sold at a premium.

Fast forward to more recent times: Cisco's most up-to-date, purpose-built data center switch is the Nexus 9000 series. The family of switches started out with an interesting approach. As HP, Arista, Brocade, and others eroded the networking giant's data center switching market share, Cisco launched the Nexus 9000 in 2014 with a "merchant plus" development, marketing, and sales campaign. Essentially, Cisco was saying that the path forward and the future of switching in the data center was a hybrid approach. This design principle would technically combine Broadcom's Trident 2 ASIC with a second chip, Cisco's own custom silicon.

"Many of the largest data centers in the world look very much like an overlay solution. The underlay is a simple Layer 3 fabric, and the overlay is normally application specific. For companies like Yahoo, Google, or Facebook, it's going to be an HTTP overlay. But at this level, all of the technology looks effectively the same—almost exactly like a virtual overlay solution, where software on the edges is doing something, and a very simple physical network isn't doing much."

MARTIN CASADO, MANAGING THE PHYSICAL AND VIRTUAL WORLDS IN PARALLEL

Finally, let's jump ahead to 2018. For the Nexus 9000 family, in fewer than four short years, Cisco has jumped back to focus on homegrown, in-house silicon development. At the end of 2018, almost all of the first- and second-generation merchant plus Nexus 9000 models will be officially EOS or EOL. The hardware churn for networking devices is no longer in the multiples of years.

We will examine why this churn is increasing, but for now it is enough to highlight the ever-growing change in the data center hardware landscape that should be taken into consideration. The market research firm Dell'Oro Group started tracking these new switching architectures in the data center switching category in 2010.

Networking Software in the Data Center

Concurrent with the rise of merchant silicon was the beginning of a shift to networking software purpose-built for driving larger distributed systems specifically engineered for data center networking. This shift will eventually lead to the disaggregated hardware and switching models discussed later in this document. This shift is important to note, as data center networking software is still run this way today, but this is very different from the software-first decision.

The data center switch operating system was on the rise with the likes of FTOS (Force10), EOS (Arista), and NX-OS (Cisco). These new systems were not only hardening the operating systems to support the demand of the data center environment, but they were also starting to tie systems together in groups using protocols like Multi-Chassis Link Aggregation (mLAG) or Virtual Port-Channel (vPC), creating larger and larger points of control. While this remains an important decision criterion for the physical network infrastructure, it is a piece of the puzzle and not the end or beginning of designing data center networking with a software-first approach.

The Rise of the Fabric

Going back to 2004, the larger web-scale companies started to move to a new design for data center networks altogether, which kicked off the idea of data center fabrics.

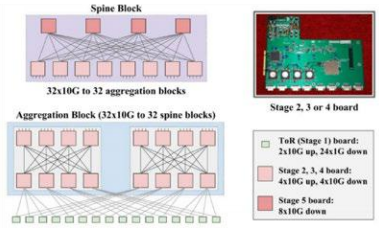

Figure 5: Firehose 1.0 topology. Top right shows a sample 8x10G port fabric board in Firehose 1.0, which formed Stages 2, 3 or 4 of the topology.

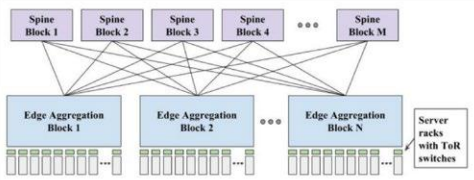

Figure 4: A generic 3 tier Clos architecture with edge switches (ToRs), aggregation blocks and spine blocks. All generations of Clos fabrics deployed in our datacenters follow variants of this architecture.

Datacenter Generation	First Deployed	Merchant Silicon	ToR Config	Aggregation Block Config	Spine Block Config	Fabric Speed	Host Speed	Bisection BW
Four-Post CRs	2004	vendor	48x1G	-	-	10G	1G	2T
Firehose 1.0	2005	8x10G 4x10G (ToR)	2x10G up 24x1G down	2x32x10G (B)	32x10G (NB)	10G	1G	10T
Firehose 1.1	2006	8x10G	4x10G up 48x1G down	64x10G (B)	32x10G (NB)	10G	1G	10T
Watchtower	2008	16x10G	4x10G up 48x1G down	4x128x10G (NB)	128x10G (NB)	10G	nx1G	82T
Saturn	2009	24x10G	24x10G	4x288x10G (NB)	288x10G (NB)	10G	nx10G	207T
Jupiter	2012	16x40G	16x40G	8x128x40G (B)	128x40G (NB)	10/40G	nx10G/ nx40G	1.3P

Table 2: Multiple generations of datacenter networks. (B) indicates blocking, (NB) indicates Nonblocking.

Figure 13. The Evolution of Network Fabrics at Google, Jupiter Rising: A Decade of Clos Topologies and Centralized Control in Google's Data Center Network

The race had begun to make switch fabrics more consumable to the enterprise. Cisco kicked off its own custom fabric technologies, such as Fabric Path and Dynamic Fabric Automation. While Juniper came out with QFabric and Arista, Force10, and others were taking more of a "standards" approach to fabrics, using the leaf-and-spine concept with standard protocols like BGP now moving into the data center and Layer 3 moving to the top of rack. Fabrics are still being built this way today and fall under the common terminology of leaf-spine designs. The key to these designs is to create very simplified building blocks for the network. Simplification of the network has now started to become a large theme across all the major networking vendors.

Software Is Eating the World

As networks evolve, software is changing the way the data center operates and public clouds are rising. Virtualization, pioneered by VMware, is leading a fundamental shift in IT operations and how developers interact with infrastructure. Along the way, the networking edge is shifting into the virtualization layer.

From Fabrics to Fabric Manager and SDN

Fabrics that were being built were still lacking the fundamental tools to automate and troubleshoot the physical networking fabric, leading to the development of Cisco ACI, Arista CloudVision, Big Switch Networks, and others. Initial goals focused mainly on the issues of the operation and automation of the physical networking fabric but started to dive into the virtual edge as well.

During this time, as virtualization and cloud were shifting the new edge of the network into the virtualization tier, the term software-defined networking started to become common. Projects like OpenFlow kicked off, and others looked to create a more programmable software-driven network. Unfortunately, SDN the term started to span the mix of physical fabric management, programmable fabrics, and what VMware pioneered through Nicira: network virtualization. This confusion remains today and is another reason why it is important to establish the key goals of a network upgrade.

Virtualization and cloud fundamentally changed the edge of networking, convoluting the choices IT organizations have when performing a network upgrade. When network upgrades are discussed, fabrics, fabric managers, white boxes, and data center operating systems all compete for networking teams' time. Networking professionals are challenged to clearly define the problems they need to solve and to identify where to begin building the solutions to those problems.

GET STARTED

Learn more about VMware NSX Solutions and a new approach to modernizing your network >

Join Us Online:

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