The Five Pillars of Federal Data Centers

TABLE OF CONTENTS

Brocade is at the forefront of a radical shift in data center networking. The architectural pillars of these emerging technologies will more closely align network capabilities with server virtualization and cloud computing, while reducing administration costs and supporting open, best-of-breed solutions.

This paper describes how Brocade delivers increased application effectiveness, programmatic control with orchestration, security and data integrity, elasticity and scalability, and automation with simplified management to the federal data center.

Introduction

In the last twenty years, data centers have been the focus of tremendous investment and innovation, with the goal of improving application service delivery to both internal organizational and external paying customers. The first major change during this period was the disaggregation of monolithic mainframe systems into modern server architectures, enabling best-of-breed competition for each sub-element, including CPUs, servers, operating systems, and applications. Server virtualization and cloud computing have dominated data center architectures more recently, both of which have driven east-west (server-to-server) communications to constitute 80 percent of all traffic. These trends are exposing serious shortfalls in traditional data center networking, including great complexity in large-scale environments, error-prone manual configuration, and a reliance on special-purpose appliances. Additionally, most networking equipment today very much mirrors the mainframe systems of yesterday, where processors, hardware (HW) systems, operating system software, and applications are often integrated, closed, proprietary, and managed with closed toolsets.

As a market leader in data center networking and the leader in the emerging field of software networking, Brocade is at the forefront of a radical shift within the networking industry to address these shortfalls. Brocade is delivering agile networking capabilities that increase the velocity of application service delivery in ways that enhance and complement compute and storage innovations like no other vendor in the sector. As the provider

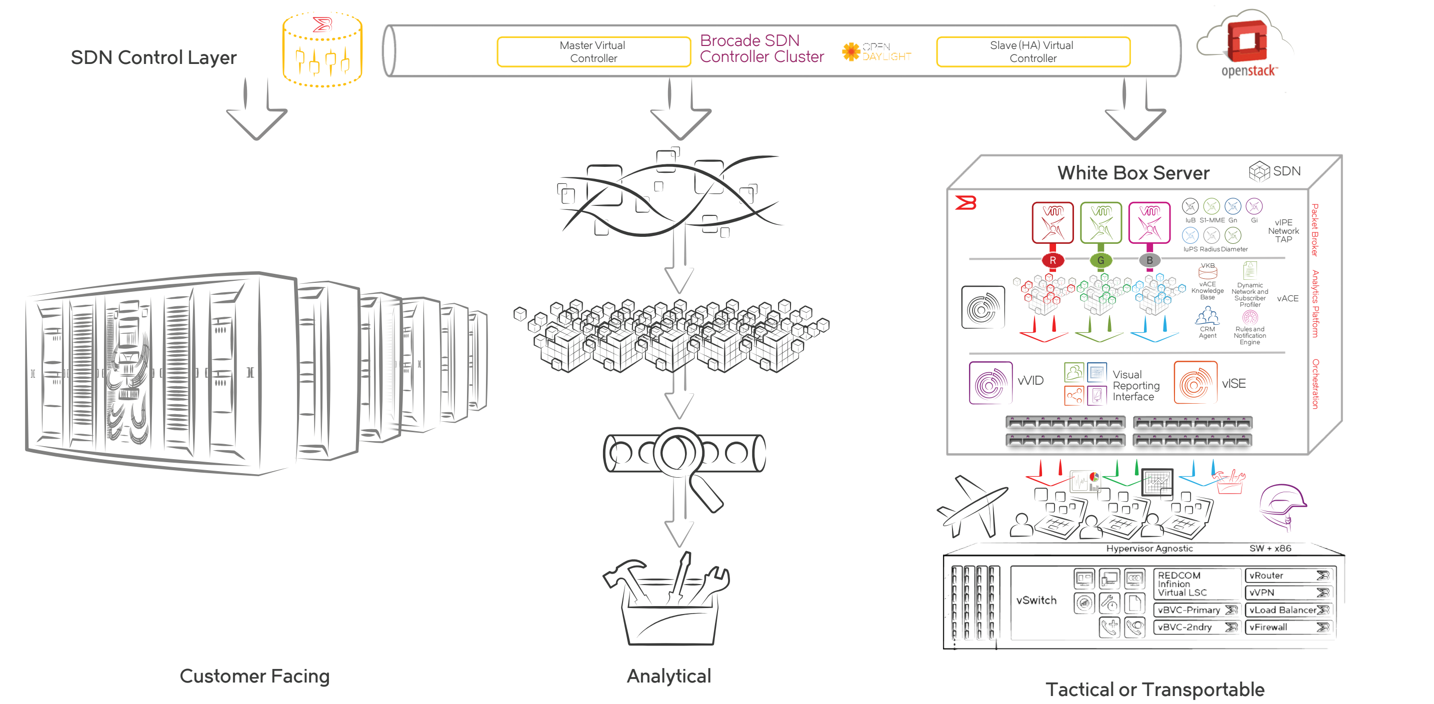


Figure 1: The Customer-Facing, Analytical, and Tactical Transportable Data Centers each play a role in the mission of the federal government, be it through enterprise-wide services, Big Data analytics, or virtualized mobile in-theater tactical and first-responder solutions for in-the-air and on-the-ground data center services.

of data center networking equipment to 90 of the Fortune 100 companies, it is the view of Brocade that data centers fall broadly into one of three categories, based on their purpose. These categories are: customer-facing data centers, analytic data centers, and tactical or transportable data centers. Additionally, while each of these types consists of compute, storage, and networking resources, each has different priorities and constraints on how these resources are deployed, managed, or optimized.

Customer-Facing Data Centers

Customer-facing data centers support revenue-generating, organizational mission, or public information access services. Examples include cloud hosting, e-commerce portals, and information access web sites such as IRS.gov or Wikipedia. As profit centers, the availability of the offered services (Application Effectiveness – Pillar I) is the driving priority for these data centers: downtime equates to lost revenue and customer dissatisfaction. Automation and Simplified Management (Pillar V) leads to greater stability and increased flexibility of the infrastructure while reducing administrative costs and the potential for configuration mistakes. Finally, an infrastructure that provides Programmatic Control and Orchestration (Pillar II) for delivering new service offerings adds new service offerings and simplified provisioning of server, storage, and network assets accelerates application deployment, adds new revenue sources, and provides a competitive advantage. This type of data center requires the flexibility to effectively and efficiently react to customer demand while maintaining the requisite security profile.

Analytic Data Centers

Analytic data centers support internal efforts to utilize data sets to make business decisions, create differentiated offerings to customers, further scientific research, and potentially find patterns in the data through the application of analytics tools. These data centers have a high volume of machine-to-machine traffic, supporting distributed or parallel processing applications and analytics tools. Legacy protocols such as Spanning Tree can block up to half of these east-west ports, requiring operators to overbuy to get the capacity they need. Low Latency (Application Effectiveness – Pillar I) is important to all applications, but the analytics data center requires network assets with a combination of high bandwidth and ultra-low latency for distributed applications such as Hadoop. For example, MapReduce jobs are distributed among the data copies on different nodes; network latency can and will affect performance. Elasticity and Scalability (Pillar IV) are also a key requirement, as assets are commissioned and decommissioned based on the demands of the scheduled workloads. Failure to deploy infrastructure that addresses these unique scale-out requirements translates into longer wait periods for network reconfiguration, poor resource optimization, and potentially inefficient use of valuable assets leading to higher sustainment costs and constant "bolt-on" fixes which can spiral out of control.

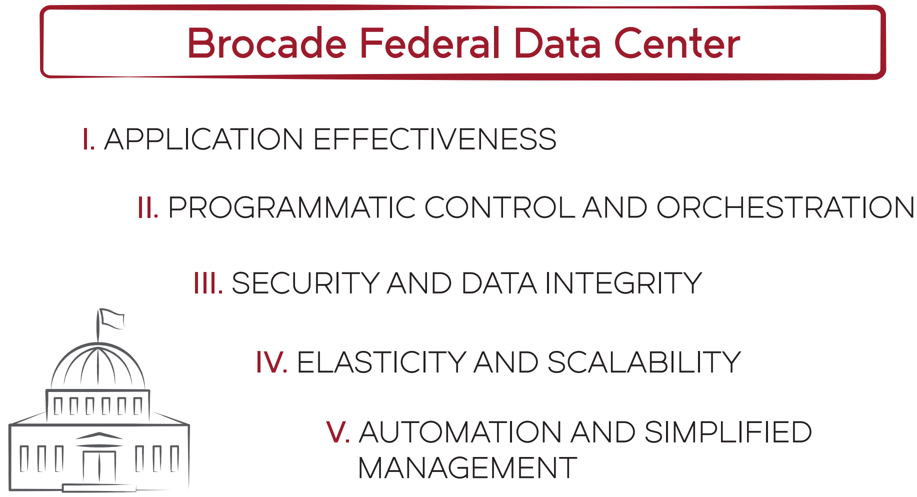


Figure 2: Brocade defines the Five Pillars of Data Center Excellence.

Tactical or Transportable Data Centers

Tactical or transportable data centers support battlefield operations, remote business, disaster recovery locations, and industrial environments. Transportable data centers are also used as modular expansions to existing facilities (as an alternative to facility renovation or construction). The on-demand availability of information in fixed-infrastructure environments creates an increasing dependency on having this information available when users are mobile or are located in more austere environments. For the military, this explosion of data requires information and computing power to be located closer to the warfighter. For these data centers, Size, Weight, and Power (SWaP) are the overriding critical constraints and are a major factor in Elasticity and Scalability (Pillar IV). A tactical data center is most likely bandwidth-limited and possibly out-of-network for long periods of time.

These data centers must be able to operate as standalone centers; that is, they must be able to run applications on the battlefield and in remote regions without requiring a WAN connection. When such centers are connected, Security in Transport (Pillar III) for synchronizing and backing up mission data is critical.

Brocade data center architectures provide the flexibility, adaptability, and elasticity required for enterprise-wide deployments of computing infrastructure and applications. A network architecture based on Brocade technology ensures maximum bandwidth availability to applications, flexible Virtual Machine (VM) workload location and movement, and elastic resource addition and provisioning. All of these maximize the service level of an application, while reducing the infrastructure and administrative costs to support and maintain it. This paper presents the Five Pillars of Data Center Networking from Brocade and the ways in which Brocade is working to change the existing paradigm and make the network a responsive source of innovation.

Pillar I: Application Effectiveness

Today's business and mission priorities require data centers that deploy new applications quickly and efficiently, provide fast and reliable data access, meet or exceed stringent service levels with zero downtime, all while maximizing investments by reducing costs. A high-performance, intelligent network infrastructure is the key to enabling application effectiveness.

For example, Brocade and Microsoft have co-developed a 100,000-subscriber Microsoft Lync reference architecture, which has been tested by both companies to ensure that service metrics and service targets are met or exceeded. This architecture uses state-of-the-art converged Brocade Fibre Channel and Ethernet fabrics, core routing, application delivery controllers, and software networking for dynamic resource

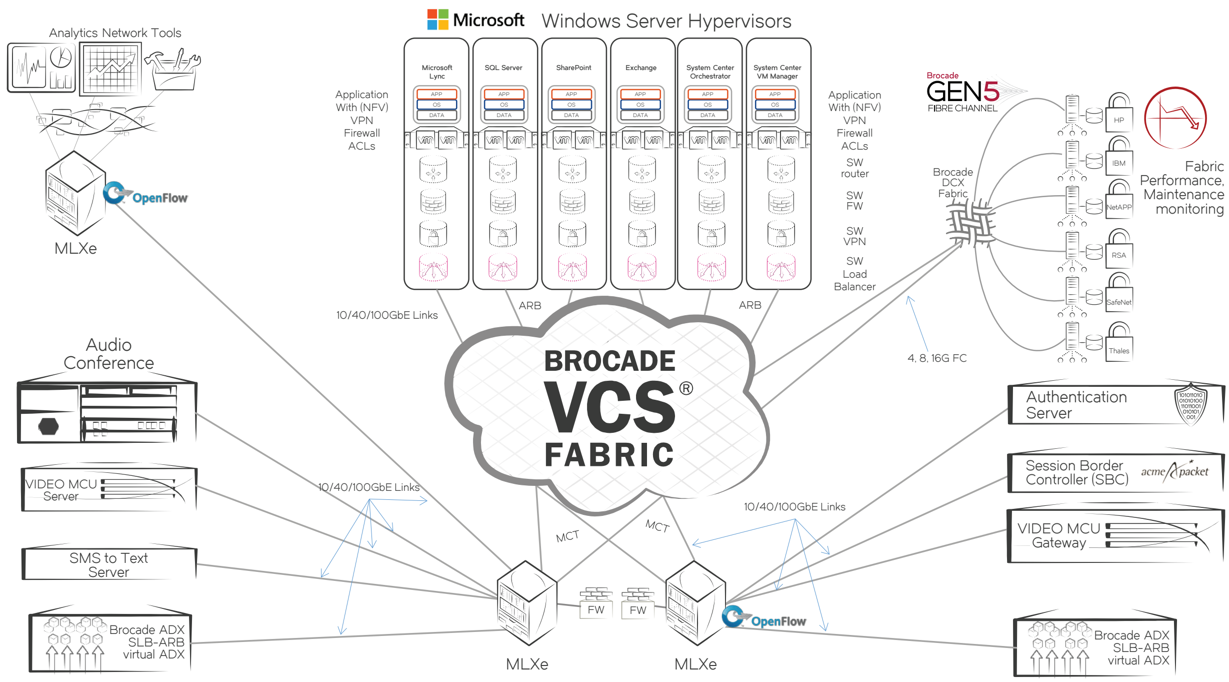


Figure 3: The Brocade-Microsoft Reference Architecture has been tested by Microsoft and Brocade to enable Lync solutions in excess of 100,000 active unified communications subscribers.

expansion. As part of load simulation testing, Brocade has validated the following metrics:

- Instant messaging, conferencing, voice, and unified messaging meet worst-case service targets of 99.9 percent.
- User interface responsiveness and Lync client connection time meet or exceed a top-end limit of 1.5 seconds.
- Lync call setup time was 2 seconds or less.

These key metrics were achieved in a cost-effective architecture for a hosted Unified Communications (UC) deployment, which included multiple technology components. The architecture includes not only the Lync configuration, user workload profiles, and server, storage, and network elements, but also real-time services gateways for SIP trunking, Public Switched Telephone Network (PSTN) access, video conferencing, Session Border Controller, and switched firewalls. The Microsoft solutions of choice for networking components include Brocade® MLXe® core/WAN routing and switching, Brocade VDX® Ethernet fabrics with Brocade VDX Switches, Brocade Gen 5 Fibre Channel fabrics, and the Brocade Application Delivery Controller.

As part of this architecture, the Brocade MLXe Core Router provides high availability and best-in-class scalability with secure connectivity to regional and branch sites, using encryption technology that is Suite B-capable. The Multiprotocol Label Switching (MPLS) capability of this router allows inter-data center connectivity at Layer 2, via MPLS Virtual Private LAN Services (MPLS-VPLS), over a Border Gateway Protocol (BGP), IPv4, or IPv6 backbone network. The Brocade MLXe Core Router also provides a telemetry traffic filtering and redirection capability that optimizes Big Data toolsets. This ensures that only traffic of interest reaches these tools, decreasing the time spent processing uninteresting traffic and thus increasing productivity while controlling server scaling rates.

The 70 percent market share Brocade has in traditional Fibre Channel Storage Area Network (SAN) fabrics is built upon a foundation of performance, simplicity, and automation. When Brocade developed its Ethernet Fabric technology, this heritage was leveraged to bring the same benefits to Ethernet switching. Brocade VDX switches use Brocade VCS® Fabric technology to provide a high-performance Ethernet fabric. These high-density cut-through switches enable traffic flow between application servers with the lowest latency in the industry. Brocade VCS fabrics, based on the Transparent

Interconnection of Lots of Links (TRILL) protocol, enable all links within the data center to be active and load sharing, which enables maximum utilization of available bandwidth. The lowest latency and deepest buffers enable the handling of microbursts. With the addition of fine-grained labeling, this platform provides massive scale-out and traffic separation for large multitenant environments. Brocade is an original member of the Gartner Ethernet Fabrics category, shipped the first commercially available product, and continues to be a technology leader in this space.

The Brocade Application Delivery Controller performs Layer 4 through Layer 7 switching and Global Services Load Balancing (GSLB), which provide the ability to redirect traffic, rewrite URLs, and load-balance server traffic between workloads to ensure that flows are serviced across available resources.

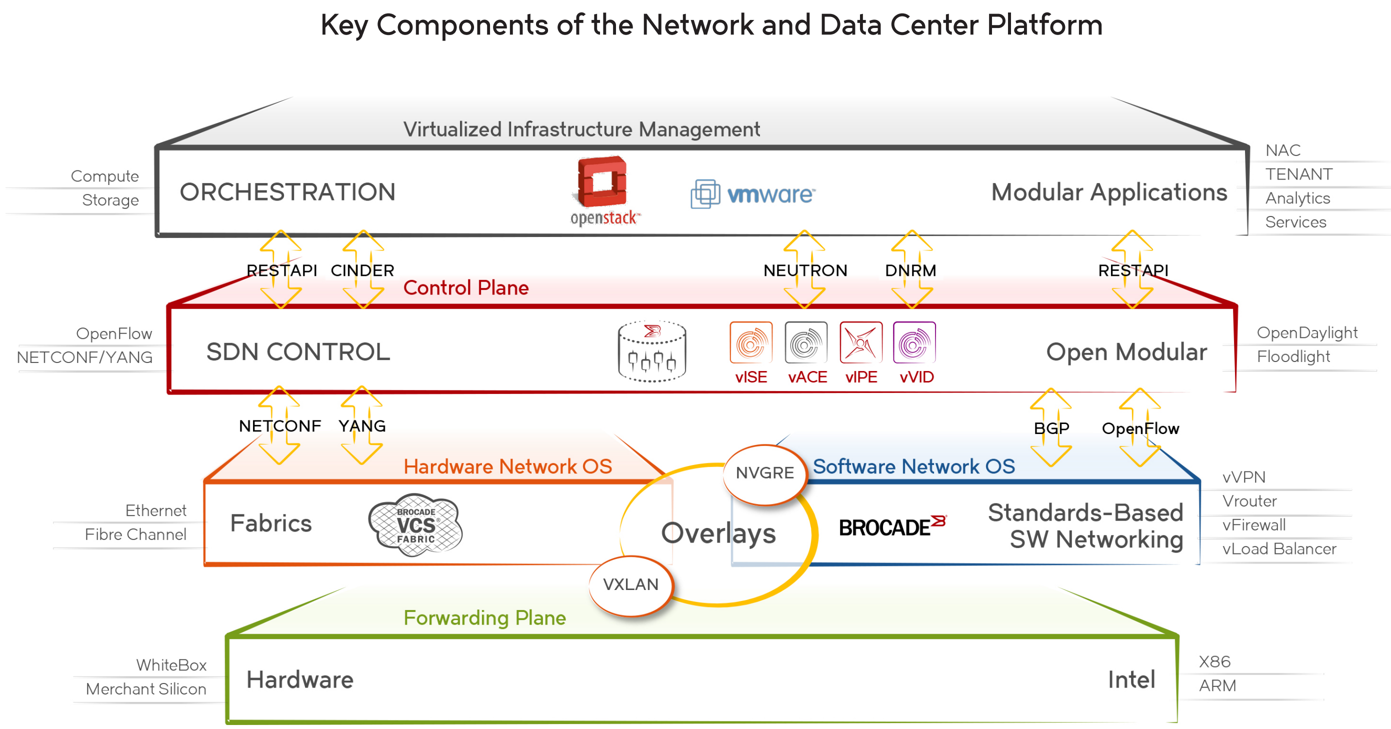
The Brocade ADX® switch also uses the Brocade Application Resource Broker feature, which optimizes compute resources. (This is discussed in more detail in Pillar 4). The Application Resource Broker software interacts with VMware vCenter, the Brocade Virtual ADX Switch and the network infrastructure to deliver multi-tenancy, capacity-on-demand, and the ability to operate in an active-active data center framework.

Pillar II: Programmatic Control And Orchestration

Programmatic control and cross-platform orchestration are the primary methods that service providers and cloud data center operators want to leverage to reduce their operational costs. Programmatic control, in the form of Software-Defined Networking (SDN), deals specifically with the decoupling of network control from the data forwarding function, as well as the abstraction and direct programmability of network control by higher-level applications. Orchestration is a key element of Software-aDefined Data Centers (SDDCs) and provides for "single pane of glass" provisioning of all elements in the architecture by administrators or, within predefined resource pools, by end users themselves.

To encourage wide adoption of SDN, the communications protocol between the network and controller should be open standards based. The emerging standard, OpenFlow, is being developed by the Open Networking Foundation (ONF). Implementing SDN via an open standard promises to reduce service development and operational costs and free network administrators to integrate best-of-breed technologies as they are developed. An example of the network control function is an open-source SDN controller initiative, OpenDayLight.

Figure 4: Brocade has defined the SDN architecture that transforms the government data center into a service delivery platform. By adopting the Brocade SDN platform, agencies are ensured the ability to adopt open solution elements and avoid vendor lock-in from proprietary software models.



The OpenDaylight controller provides REST-based northbound APIs that can be used to manipulate network infrastructure through a suite of southbound protocols, which include NETCONF, BGP-LS, and PCEP, in addition to OpenFlow. This broad range of southbound protocols makes OpenDaylight ideal for real-world, brown-field SDN deployments and migrations.

As an early proponent of SDN, Brocade quickly supported OpenFlow 1.0 in Brocade MLX routers and Brocade CER 2000 routers. Brocade now supports OpenFlow 1.3 in hardware across the entire Brocade Ethernet switching and routing portfolio: Brocade MLX and CER 2000 routers, Brocade ICX® campus Ethernet switches, and Brocade VDX data center Ethernet fabrics. As a means of facilitating SDN adoption, Brocade also supports an OpenFlow hybrid mode that seamlessly integrates with existing networks to enable SDN in conjunction with traditional networking capabilities. Hybrid port mode provides the ability to run OpenFlow enabled services and traditional routing services over the same ports. This allows the selective application of OpenFlow policies to a subset of network traffic that is critical to a smooth migration to SDN. Organizations can maintain their traditional forwarding policies and all the established operational processes that keep that traffic flowing while selectively enabling OpenFlow into their environment to create their own Communities of Interest (COIs) with segregated traffic flows. This keeps the data of Department of Defense (DoD) and other federal agency SDN-based transport networks segregated from the production enterprise data that uses legacy protocols.

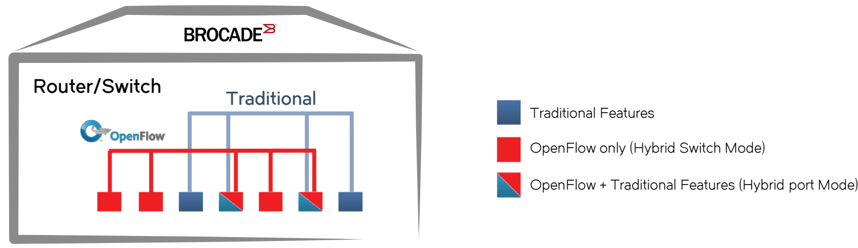


Figure 5: Brocade implements "hybrid" mode. Getting the approach to SDN right the first time requires vision and the willingness to innovate without forcing customers through continual forklift upgrades to their data centers. With hybrid port implementations, the network may be migrated to SDN without investing in dual access or core layers in the network infrastructure.

As a part of its SDN strategy, Brocade has adopted the OpenDayLight controller as the basis for the Brocade SDN Controller. The Brocade SDN Controller is the first commercial distribution built directly from OpenDaylight Helium code, without any proprietary extensions or platform dependencies. Organizations can freely optimize their network infrastructures to match the needs of their workloads, and develop network applications that can be run on any OpenDaylight-based controller (see Figure 6).

The Brocade SDN Controller package includes tools and services to quickly and confidently implement software-defined networks within existing environments. Brocade provides multivendor compatibility testing and complete, single-source support for Brocade SDN Controller environments, backed by the expertise of leaders within the OpenDaylight developer community. The approach of Brocade to its BVC OpenDaylight-supported release is compared to how Red Hat commercialized the first releases of Linux for the open source Linux community. Brocade combines deep networking expertise with a highly collaborative approach to open-source networking. Brocade views the OpenDaylight community as a force multiplier for innovation with and on behalf of controller users. The multifaceted support provides to organizations helps them achieve maximum architectural flexibility and develop skillsets for self-service innovation. Adopting SDN can help organizations accelerate the delivery of new services while optimizing their business operations. OpenDaylight APIs (REST) platform services network service functions Service Abstraction Layer (SAL) extensions network applications, orchestration, and services network applications, orchestration, and services controller platform southbound interfaces, and protocols data plane elements (such as virtual switches and physical device interfaces), user interfaces with other standard protocols (such as ONF and IETF), and OpenFlow vendor-specific interfaces.

Another critical element of the Software-Defined Data Center is orchestration. OpenStack technology was originally developed by NASA as part of the Nebula computing platform to dynamically streamline provisioning of compute

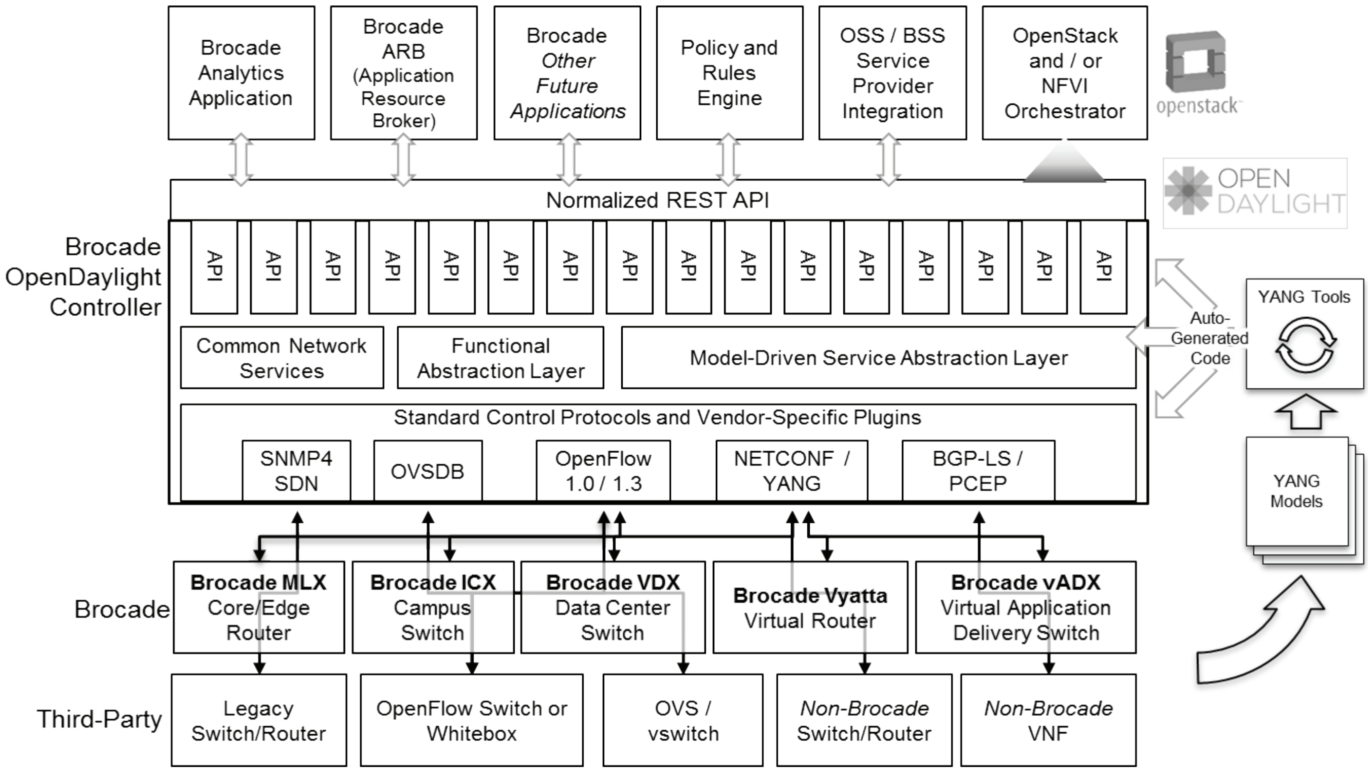


Figure 6: The OpenDayLight SDN controller framework enables a platform in which SDN may be implemented using orchestration from REST APIs (northbound), special applications, and southbound interfaces to SDN and traditional network transmission platforms.

resources and storage for users who must run certain applications using a cloud-based model. Hardware and software vendors write to the provided APIs and integrate into a central OpenStack controller that can provision resources in a cloud framework. Some examples of the provisioning targets consist of active components such as VMware vCenter for creating an operating system, as well as storage management tools from VMWare, NetApp, or EMC for storage space. Brocade has worked to integrate its data center network offerings to support orchestration tools such as OpenStack by developing API plugins for several Brocade products. Brocade is also developing plugins and extensions for its products that will allow OpenStack to provision networking and SAN platforms, network services, and communicate with an OpenDaylight controller such as the Brocade SDN Controller.

The ability to provision services using open cloud data center enablers such as OpenStack, and then create dynamic WAN connectivity using OpenFlow controllers and SDN applications, introduces a new paradigm in research data accessibility and user access control that was never before available. To ensure support of these innovations, Brocade routers and converged Brocade VCS Fabric technology are provided with these cloud provisioning and SDN protocol abilities built in, which future-proofs the solution sets.

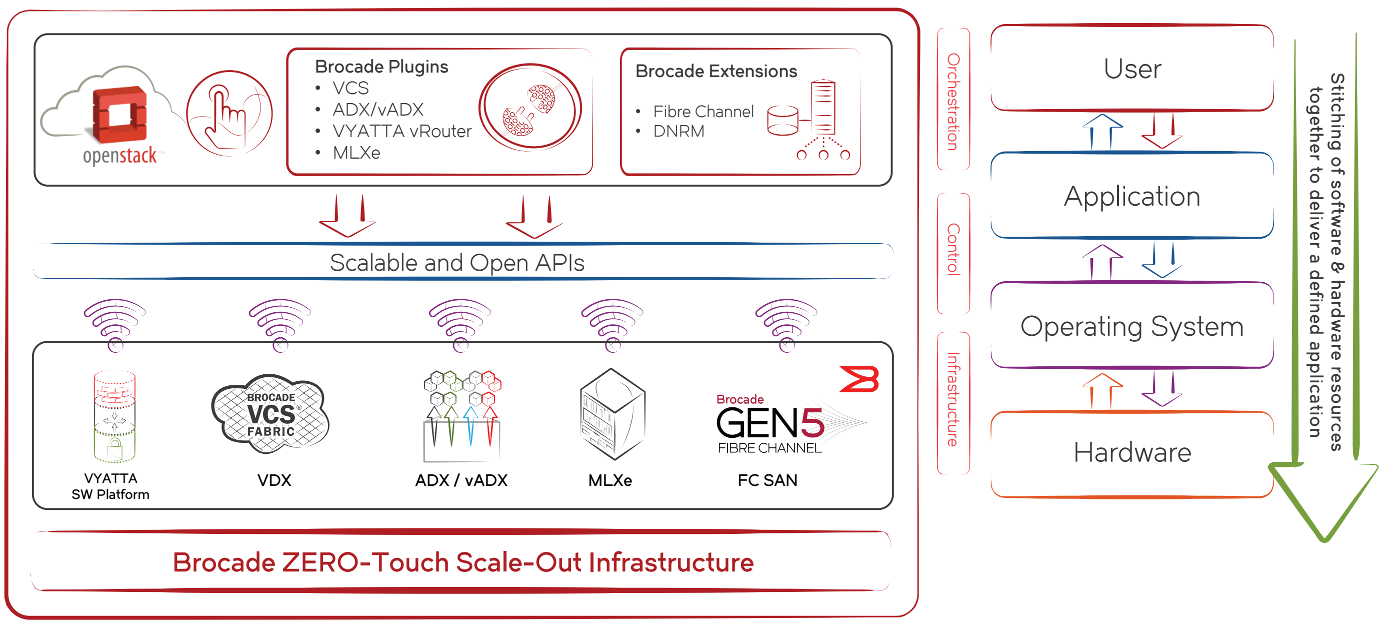


Figure 7: Brocade Zero-Touch Scale out Infrastructure and the OpenStack "cloud-ready" services model. Brocade uses scalable open API's to interface the orchestration layer using network (Neutron) and storage (Cinder) plugins for OpenStack.

Pillar III: Security and Data Integrity

When considering cyber-security protection for a data center network, it is important to keep in mind that the prominent underlying objective of a cyber-attack is the actual information itself. From a networking perspective, where the transport of information is the primary function, a key aspect of information protection is securing data while data is traversing the network. Although intrusion detection and prevention techniques are valuable, ever-evolving cyber-attack methods make identifying incursions a constant effort to understand, update, and maintain signature information. With networks, and especially U.S. government networks, being constantly under attack, the most efficient approach is often the most direct approach. In a network environment, securing the data though encryption is a very effective countermeasure to ensure data security. By protecting the lowest common denominator within a network—the data itself—the risk of data interception is essentially nullified.

Network link encryption has been utilized for some time to provide protection of data in transit, but the highest classifications of data generally require purpose-built Government-Off-the-Shelf (GOTS) devices. With the processing capabilities of modern CPUs, commercially available products can now utilize the complex algorithms needed for the highest classification categories. The redefinition of national information assurance standards to include Suite B cryptography now provides the ability to secure network data with Commercial-Off-the-Shelf (COTS) solutions as part of the NSA's Commercial Solutions for Classified (CSfC) program. This program allows government agencies to more quickly adopt new network technologies and capabilities by providing a framework of cryptology methods that can be accomplished without highly specialized devices and yet still achieve highly secure transmission of data through the network.

Brocade provides a multipronged approach to the securing of data across the network to ensure protection end-to-end. These capabilities extend across a wide spectrum:

- Wide Area Networks (WAN)
- Local Area Networks (LAN)
- Within the server as VM to VM
- Server to storage array

By protecting these multiple areas, Brocade provides data protection not just "outside the facility" but internally as well. With today's data center consolidation, multitenant environments are the standard operating practice, and internal protection is a consideration, to ensure

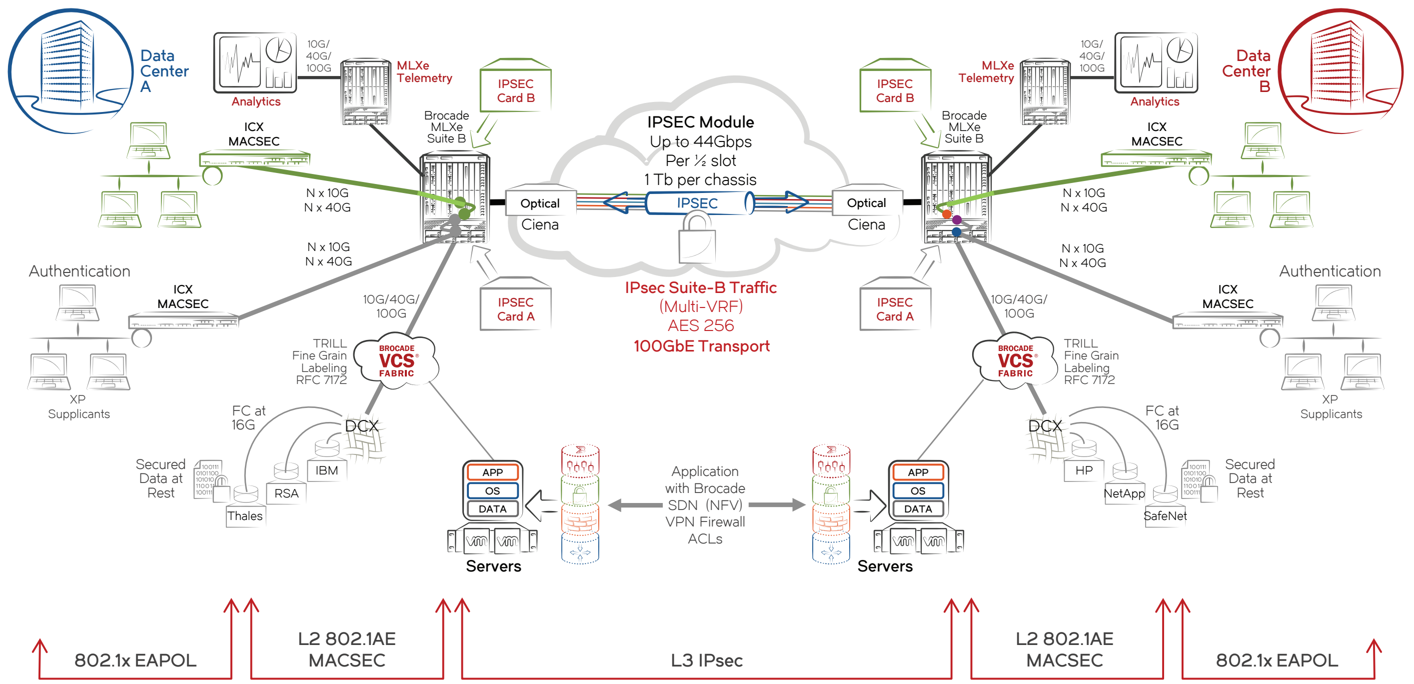


Figure 8: Brocade end-to-end security architecture for the data center. Brocade provides internal security between users and applications and external security between workloads in a multiple data center environment. With 42G+ goodput per card (up to 32 cards) this solution is currently the highest-performing Suite B level encryption platform on the market.

against inappropriate data exposure. To accomplish data protection in these different network areas, Brocade supports data encryption capabilities on multiple products.

For data protection across the WAN, the Brocade MLXe series of high-performance routers provides hardware-based encryption with inline ports, helping to ensure data protection without compromising performance or requiring complex deployments. By leveraging

Suite B cryptographic algorithms, the Brocade MLXe router provides the industry's first terabit-per-second IPsec routing in a single chassis with four wire-speed 10 Gigabit Ethernet (GbE) ports and four 1 GbE ports per half-slot module. The Brocade MLXe has deep buffers that easily handle encrypted dynamic voice, video, and data traffic. Investment protection is maximized for new security capabilities with a programmable architecture built on Brocade VersaScale Packet Processor Field-Programmable Gate Array (FPGA) based technology. The use of Suite B IPsec encryption on the Brocade MLXe router fully secures data at Layer 3 to provide data protection across the WAN between facilities, or from private cloud to public cloud provider data locations.

To provide link data protection within the LAN, Brocade utilizes encryption based on 802.1AE Media Access Control security (MACsec). As a Layer 2 encryption methodology, MACsec provides hop-by-hop encryption across the multiple links in a LAN environment. MACsec is ideal for fast, low-latency, easy-to-deploy encryption within a campus network, and it provides the additional benefit of enabling policy to be applied to network traffic at the switch or router as it traverses the network. From the WAN edge to the core, and down to the access layer, the Brocade MLXe router and the Brocade ICX 6000 and 7000 family of campus Layer 2/Layer 3 switches all support MACsec capabilities.

1. Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting National Security Systems (NSS). Suite B includes cryptographic algorithms for encryption, key exchange, digital signature, and hashing.

2. As MACsec is specifically a link encryption methodology, and IPsec security is dependent on the tunnel origination point within the network in regards to full end-to-end data encryption, Brocade supplements its IPsec and MACsec capabilities with further encryption technologies at the VM level within a server. The

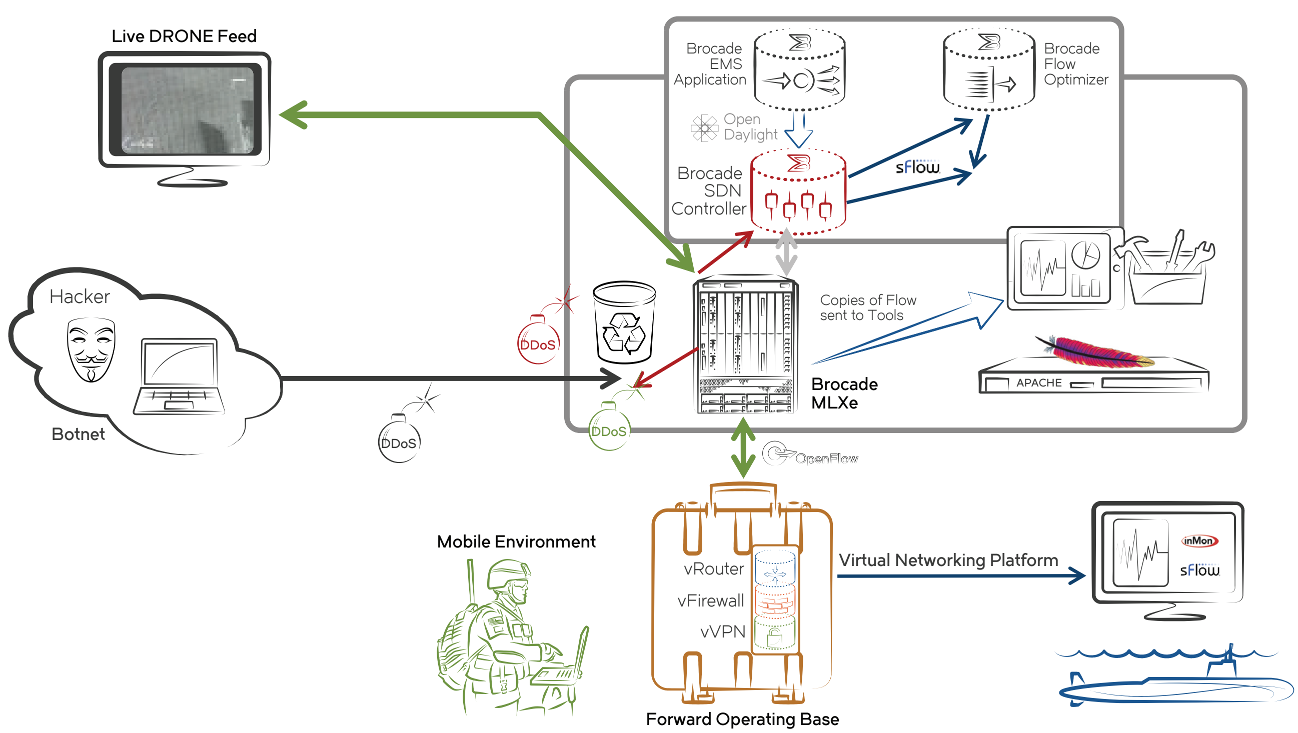
Brocade vRouter family of virtual routers support IPsec encryption at the closest point possible within an application environment by providing IPsec tunnel endpoints within the server itself. To facilitate IPsec tunnel termination, the Brocade Virtual Routers support both traditional static point-to-point and Dynamic Multipoint VPN (DMVPN) IPsec capabilities. With IPsec encryption at the server level, combined with MACsec and IPsec encryption at the router/switch level, Brocade is able to provide the layered defense-in-depth security needed to ensure the proper data protection throughout the entire network.

To provide further coverage data protection from the server, Brocade also includes link encryption capabilities within the Brocade Gen 5 Fibre Channel SAN switch and director products. This capability ensures protection of information not just from the server egress to the IP network, but also from the server egress to the storage arrays. Within this same family are the SAN extension products from Brocade, which accelerate and optimize replication, backup, and migration over any distance, enabling the following: multisite synchronous and asynchronous disk replication, centralized SAN backup, recovery, and archiving, and global data migration, distribution, and sharing. With multiple layers of encryption capabilities across multiple network areas, Brocade ensures the complete fundamental integrity of information within the data center. With the rapid advancements being made in SDN, applications are being introduced that enable a number of use cases that afford operators the ability to begin implementing security measures in their networks. The Brocade Flow Optimizer and the Brocade SDN Controller can provide the ability to redirect traffic flows over preferred or optimal paths, as well as implement policies that would dynamically thwart activities such as Directed Denial of Service attacks (DDoS). As SDN matures, look for more capabilities that would enable network planners to take proactive approaches to security by manipulating IP Flows, dynamically redirecting or sending copies of the IP flow traffic to Big Data toolsets for analysis.

Pillar IV: Elasticity and Scalability

Even with the great strides that have been made in virtualization technology, the operational environments of many of today's data centers are largely static. This is due to the fact that network administrators are constantly struggling to keep up with the demands of new application deployments. This is also an outcome of the network itself being largely

Figure 9: Brocade SDN Controller-driven security provides options that go beyond traditional layered firewall and encryption and security measures. By using sFlow-RT reporting, policy, and an SDN controller (above), a DDoS attack may thwarted immediately due to the implemented policy driven dynamically by the Brocade SDN Controller.



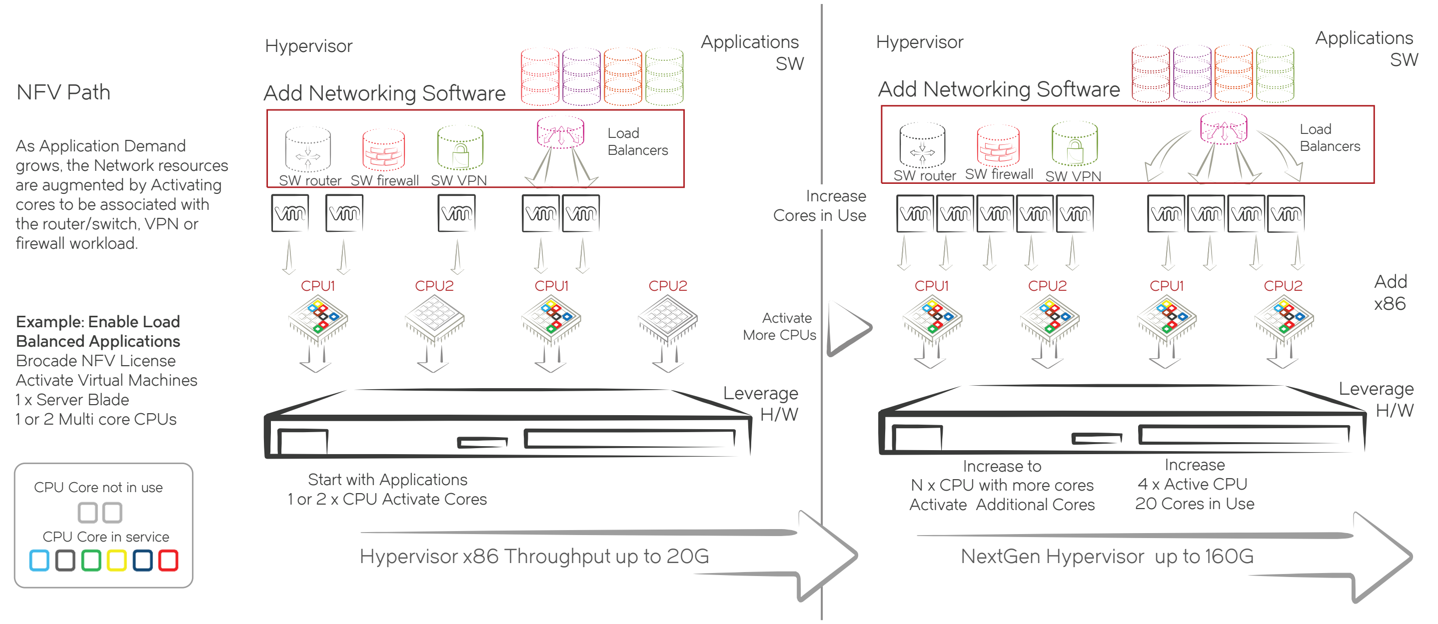


Figure 10: Brocade NFV technology proves there is no longer box dependency in networking. NFV enables an application lifecycle to be decoupled and unaffected by traditional network lifecycle churn points, while ensuring SDN compatibility.

static; outside of standard release features, there has been little innovation in the network over the last 10 to 20 years. This lack of innovation has resulted in networks that are fragile at scale, overly complex, and typically, are configured manually. The inability to fully utilize available bandwidth (due to legacy network protocols) and dynamically optimize workload placement has resulted in enterprises paying for largely unused compute and network capacity.

As a result, the configuration of the network and network appliances to accommodate new or changing customer requirements results in weeks of lead time and delays. Brocade software networking innovations transform legacy data center architectures by replacing static, hardware-based services with software-based services that are scalable, elastic, and deployable on demand. As data center fabrics and SDN technologies are adopted and put into production in support of virtualization, it is critical for new network resources and services to be deployed rapidly and to be optimally located with supported virtualized compute and storage capacity. Network Functions Virtualization (NFV) takes historically hardware-based networking functions, such as routing, firewalls, VPNs, and load balancing, and puts them in software that runs on general-purpose x86-based machines as either in either a bare metal instantiation or as a virtual machine. Brocade has been at the forefront of this industry movement through the acquisition of the Vyatta vRouter in 2012 (now known as the Brocade vRouter), the development of the Brocade Virtual ADX Application Delivery Switch, the addition of the SteelApp portfolio of application deployment controllers in 2015 to its NFV portfolio, In addition, Brocade has acquired assets to address network visibility and analytics through the addition of VistaPointe for carrier grade visibility and Connectem to address SDN principles/ in mobile wireless networks.

The Brocade vRouter software image includes robust routing, switching, firewall, and VPN features. Brocade vRouters can be deployed on a bare metal x86 server or on any of the industry-leading hypervisors as a VM. The Brocade Virtual ADC, SteelApp Application Delivery Controller (ADC) software, Brocade vRouter, and Broade SDN Controller products comprise the Brocade software networking portfolio.

The Brocade Application Delivery Controller product adds the ability to deploy a Layer 7 application delivery controller with integrated Web Content Optimization (WCO) and Web Application Firewall (WAF). The Brocade SteelApp family enables a more flexible application delivery strategy and provides a common delivery and control platform that can scale according to business needs.

The Brocade virtual Traffic Manager is a software-based Layer 7 application delivery controller designed to deliver faster, high performance user experience, with more reliable access to public Web sites and enterprise applications, whether they run in a public cloud, private cloud, or virtualized environment, while maximizing the efficiency and capacity of Web and application servers.

Brocade Service Director cost-efficiently automates the deployment, licensing, and metering of application delivery services. Each application is given a dedicated application delivery controller instance in a high-density multi-tenanted platform. Organizations allocate charges to each client application based on hourly metering, offering ADC-as-a-Service to customers and applications.

The Brocade Virtual Web Application Firewall is a scalable solution for application-level security, both for off-the-shelf solutions and complex custom applications, including third-party frameworks. It can be used to apply business rules to online traffic, inspecting and blocking attacks such as SQL injection and cross-site scripting (XSS), while filtering outgoing traffic to mask credit card data, and help compliance with PCI-DSS and HIPAA by filtering of outgoing data.

Brocade Web Accelerator software extends Application Delivery Controller scalability and reliability for enterprise and Web applications to end users. It accelerates page load times up to four times for public Web sites and applications, and improves the business results from a huge range of Web-based services including Microsoft SharePoint, public Web sites, intranet portals, and cloud applications.

The Brocade vRouter is programmatically controlled, giving it the capability of being deployed quickly in conjunction with the application it supports. Performance of the Brocade vRouter can be scaled up or down by adding CPU cores to the VM. As shown in Figure 10, there is no longer a need for the application lifecycle to be dependent upon a box-based network lifecycle. Resources can be added quickly to both parts of the service delivery equation with velocity and predictable cost. This is now done without the strain of network redesigns, lengthy acquisition cycles, or unavoidable reconfiguration churn activities that are normally associated with the legacy approach of providing constituent services. In fact, the legacy approach has run its course, as NFV provides a clear path to delivering a cost-effective application lifecycle.

An additional benefit to software networking is the reduction in SWaP in comparison to traditional network devices and appliances. Instead of paying the space and power tax to operate a physical hardware box that may be only partially utilized, organizations can provision and scale software networking applications as needed and de-provision them when not in use based on well-known operational procedures that are currently utilized for virtual machine management.

As mentioned in Pillar 1, the Brocade Virtual ADX switch not only performs Layer 4 through Layer 7 switching, Global Server Load Balancing functions, optimal path selection in a multitenant environment but it also works in conjunction with the Brocade Application Resource Broker (ARB) , SDN controllers, and an ADC to manage application workloads by monitoring application utilization. When utilization reaches a predetermined usage threshold, Brocade ARB will send a signal to the hypervisor to activate additional VMs. The switch then adds these new VMs to the pool over, which are then load balanced. ARB also uses a Global Server Load Balancer (GSLB) feature that integrates with DNS whereby these additional resources can be located locally or remotely at another facility. This is a tremendously helpful tool to ensure that every CPU core and license is used across the enterprise and between data centers to handle the demand of the applications. When application utilization descends below set thresholds, the Brocade Application Resource Broker returns the computing resources to the available pool. By running the Application Resource Broker across the enterprise data center architecture, organizations gain higher utilization density of valuable resources, while also increasing survivability. This capability ensures that enterprises can meet peak application demands without overspending on resources.

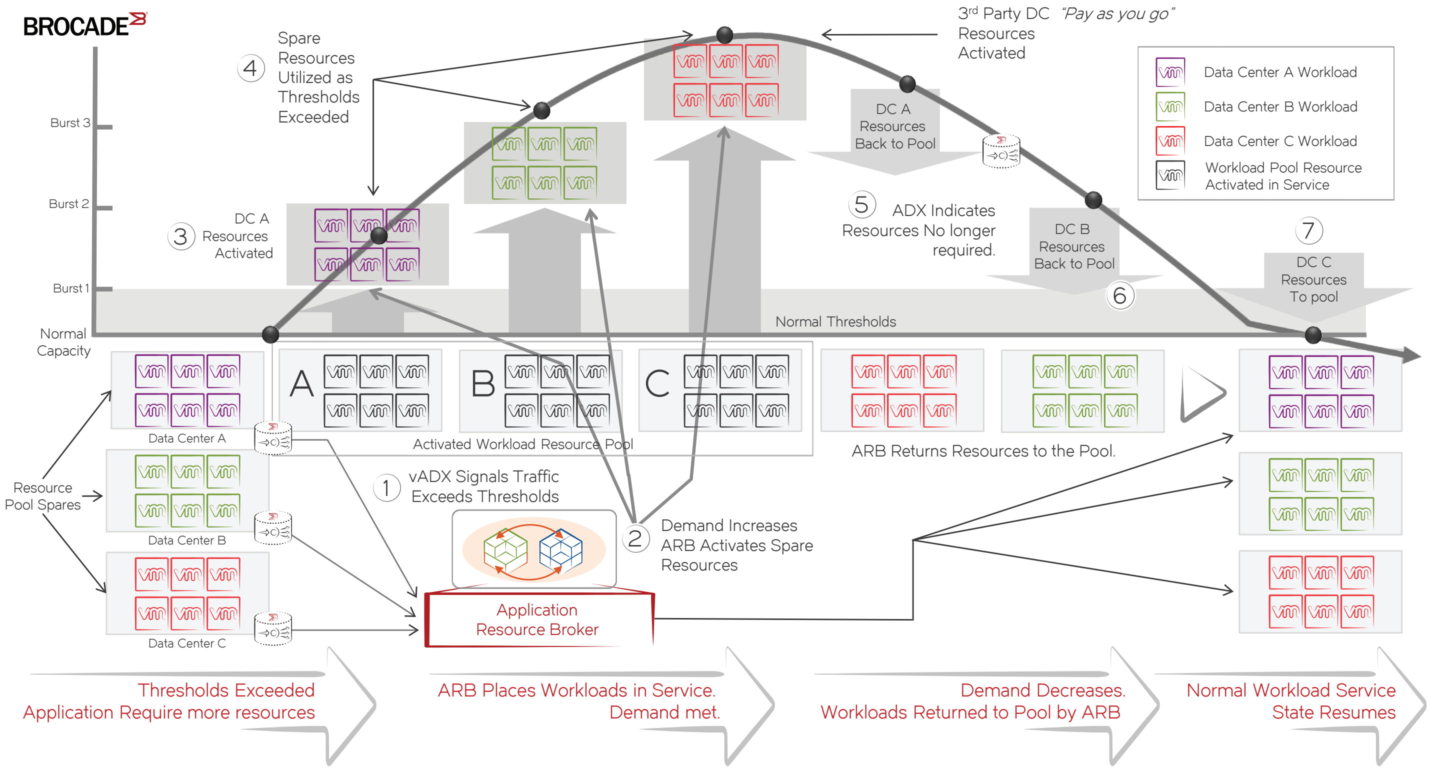


Figure 11: The Brocade Application Resource Broker manages resource pools effectively within and between data centers. The solution enables pooled spare resources to be enabled for applications requiring more processing, placing them into service during application usage bursts. It places resources back into the availability pool after the application no longer requires additional resources, becoming available for other applications. The result is a high-density utilization model for applications, computing platforms and virtual machines.

Figure 11 illustrates how Brocade and Ciena have developed a joint solution that leverages the Brocade Application Resource Broker to automate not only remote, threshold-based VM provisioning, but also the associated optical transport between data centers. The Brocade Application Resource Broker can configure the Ciena V-WAN REST API to dynamically increase bandwidth between data centers, thus ensuring sufficient capacity to load balance the traffic. This solution can be leveraged for cloud bursting, dynamic capacity-on-demand, and Disaster Recovery with Continuity of Operations (DR-CoOP) based use cases. With the Application Resource Broker, organizations can now burst both workload resources and bandwidth to other data centers in the cloud or at CoOP sites. As previously stated, when demand subsides and conditions return to normal levels, the resources from the burst pool are automatically removed. This automation ensures that organizations pay only for extra compute, network, or storage resources when they are needed, thus reducing the overall cost of the service.

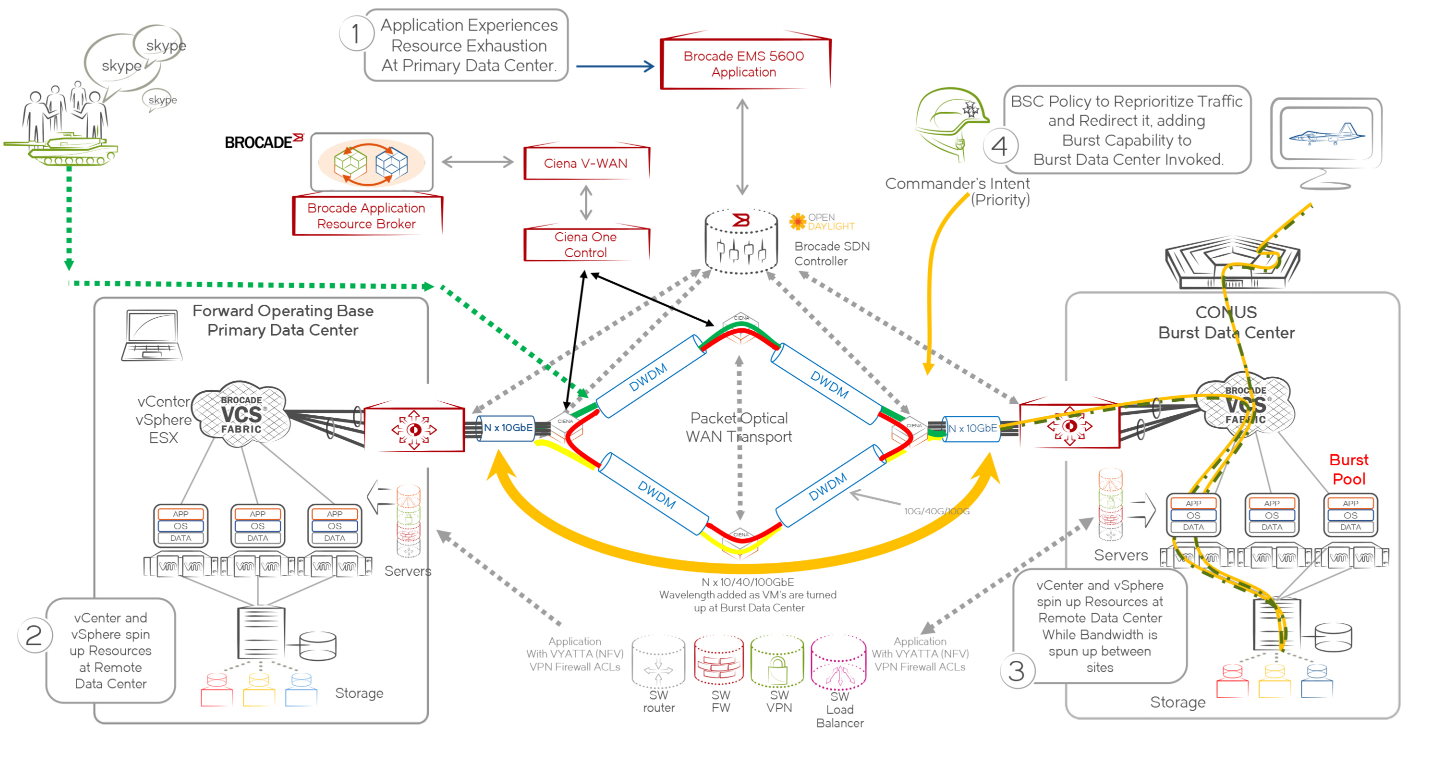


Figure 12: Brocade-Ciena joint solution for cloud bursting. By expanding application workloads and deploying new bandwidth between centers in a dynamic fashion, services are delivered across enterprise data centers. Aided by a Brocade SDN Controller (BSC), the lower priority traffic of the "Skype" users may be dynamically rerouted while a commanders preferred drone traffic is placed on a higher priority WAN transport. In addition, as application workloads increase, new resources are "spun-up" in data center B, along with dynamically-added bandwidth (wavelengths) are added by the combination of Brocade SDN-based ARB and SDN-based Ciena One Control application.

Pillar V: Automation and Simplified Management

The management and operations of a data center network can create a series of complex tasks, and it is often assumed that this complexity is inherent within the network and cannot be changed. Brocade challenges that assumption with new technologies and enhanced capabilities that are specifically intended to make the network simpler. Behind this approach is the belief that a data center network should "just work" and that network complexity is not set in stone—it can be greatly reduced. There are two key characteristics necessary to accomplishing network management simplicity: automation and visibility.

Automation can mean different things, but from the point of view of making the network simpler, automation does not just mean taking a manual process and putting it in a script. Automation to make the network simpler is about the network having the intelligence and knowledge to take actions on its own. Brocade provides this type of network intelligence with Brocade VCS Fabric technology, which provides the capability to have multiple physical network devices join together as a single logical entity that is called a "fabric." In a network fabric, details of devices and VMs attached to the individual fabric nodes are automatically distributed among other nodes in the fabric, so that any network event can be automatically adjusted to. If new network ports are needed, a new physical device can be merged with the existing fabric simply by using a matching "Fabric" ID and the physical connection of one or more links. The links are automatically configured, and all system-wide configurations are automatically applied to the newly added network device. If new links are added between nodes in the fabric for additional bandwidth, the traffic is automatically rebalanced. If an individual node is removed from a fabric, traffic is automatically rerouted. These automated self-forming, self-healing, and self-balancing capabilities are the foundation for network simplification in the data center. However, in the heavily virtualized data centers found today, these are not the only necessary capabilities.

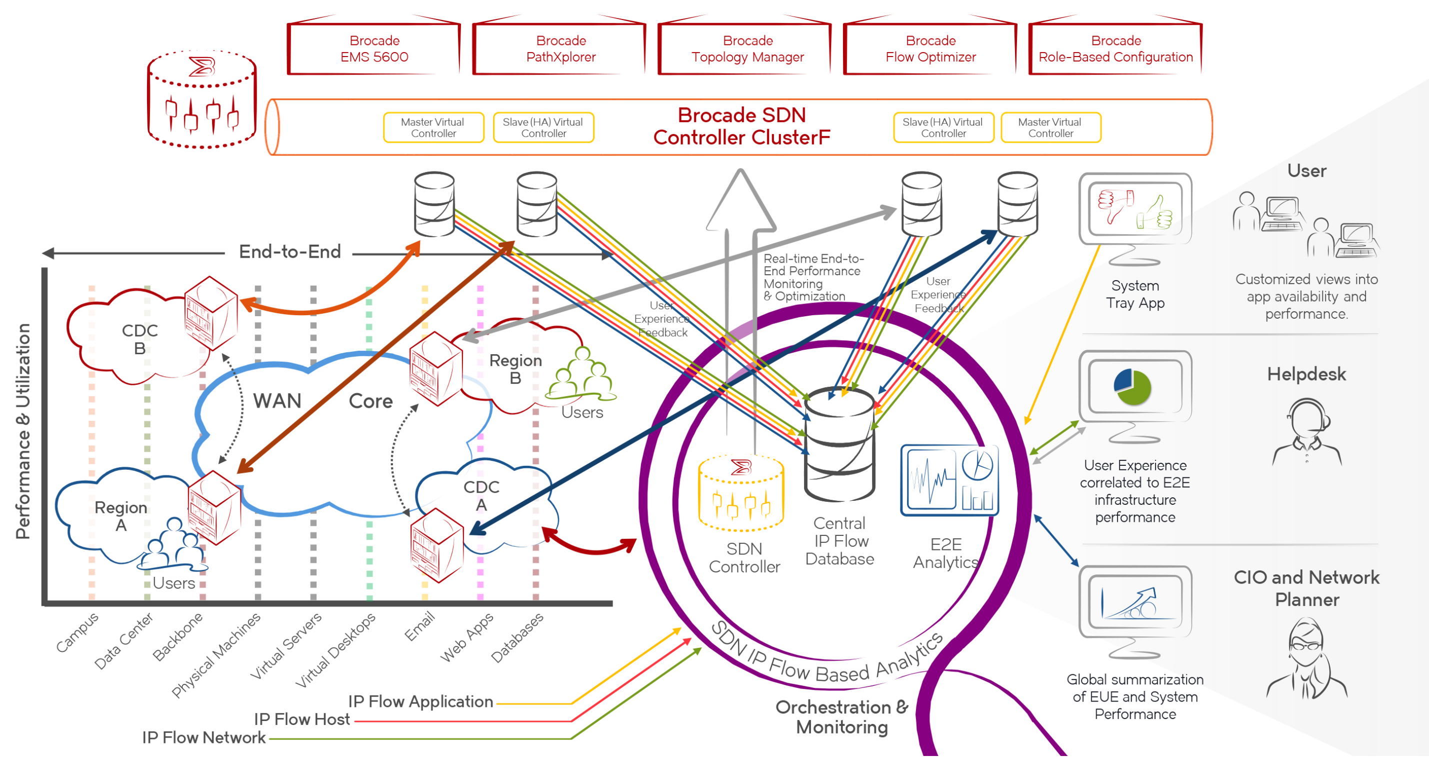
Also important to network simplification in the data center is the ability of the network to be "virtualization-aware " and to be able to automatically respond to changes with those VMs. Brocade VCS Fabric technology simplifies the management of VMs by providing the capability to automatically provision the network ports that are associated with those VMs such that they contain the needed network parameters—such as VLAN ID, associated access lists, and required Quality of Service (QoS) parameters. By matching VMs with specific port profiles, Brocade VCS technology automatically tracks the VM to the physical server in which it resides, and then automatically assigns the appropriate parameters to the network port for that server. If the VM moves to a different physical server, the network parameters that the VM needs are automatically moved as well. Without any manual intervention, the network is now automated.

All of these automated capabilities provided by Brocade VCS Fabric technology are in integral part of the product hardware and software design. This functionality does not require an outside "management shim," which is often found in other vendor implementations to provide the illusion of built-in automation. With such an effectively high level of automation, meaningful network simplification can be achieved by directly lowering the level of operational resources needed to perform these functions in a complex environment. Operational functions that would otherwise require complex manual interactions can now be achieved more quickly and cost-effectively.

Network simplification is not only improved by automation, but also by network visibility. The ability to easily and quickly determine a network fault or to prevent a network fault from occurring is another key characteristic. Two capabilities that Brocade utilizes for enhancing network visibility are Brocade Fabric Vision™ technology for SANs and sFlow technology within the Brocade Ethernet product lines.

Brocade Fabric Vision technology offers a full suite of capabilities providing breakthrough hardware and software solutions that maximize uptime, simplify SAN management, and provide unprecedented visibility and insight across the storage network. Offering innovative diagnostic, monitoring, and management capabilities, Brocade Fabric Vision technology helps administrators avoid problems, maximize application performance, and reduce operational

Figure 13: In this illustration of mission trend and situational awareness across the enterprise, sFlow provides reports that support the specific functions of IT team members' requirements. Using SDN supporting applications, IP data flows may be tracked across disparate regions of the network and correlated for end-to-end status, utilization, and reporting in support of network operations, planning, and subscriber uses.



costs. By providing built-in monitoring for issues such as traffic bottlenecks and automated correction capabilities for link errors, Brocade Fabric Vision technology drastically reduces the manual troubleshooting and restoral efforts required by SAN operational staff. With advanced tools to analyze traffic flows and to test the physical cabling infrastructure, detailed analysis can be conducted without additional costly tools and with less disruption to the SAN. Brocade Fabric Vision technology enables SAN administrators to maintain fabric-wide configuration, monitoring, and visibility on these systems, with unmatched 99.9999 percent availability. Brocade Fabric Vision technology includes Flow Performance Monitoring that provides non-disruptive visibility of performance conditions without the use of signal-degrading taps.

Brocade DCX® switches with Brocade Fabric Vision technology provide best-in-class Gen 5 Fibre Channel SAN fabrics. Brocade switches with DCX technology provide multi-tenancy to storage arrays through logical partitioning. These switches also enable zoning with service level agreement driven QoS priorities for different types of flows.

sFlow technology within the Brocade Ethernet product lines is built into the hardware for every network port, to provide detailed traffic flow information and statistics. This visibility capability provides the needed network information for identifying and resolving network issues; it provides the specific traffic flow information to better understand traffic trends and to improve capacity planning; it provides options for better real-time congestion management (see Figure 13). By increasing the ability to understand how individual traffic flows within the network are behaving, sFlow subsequently enhances the ability to make better informed decisions on correcting and improving network efficiency.

Summary

Emerging SDDC architecture goals cannot be met using traditional Ethernet networking technologies. A network that is built upon the five pillars discussed in this paper will be well-positioned to provide lower OpEx and CapEx costs to its operators, as well as higher levels of availability and faster delivery of new services to its customers. Brocade data center network fabrics provide intelligence and automation in the underlay, to ensure the successful operation of overlay networks and virtualized network functions. Programmatic control of Brocade hardware and software-based networking products provide the ability to translate service level requests into network policies and topologies, without the need to configure every network element individually. Orchestration and network applications are able to manipulate this centralized control plane to dynamically provision and monitor not only the network, but the compute, storage, and application environments it supports.

- Brocade application-specific reference architectures are designed to exceed the requirements of the enterprise and are validated to ensure the highest availability.
- The Brocade Application Resource Broker feature enables the enterprise to gain a greater efficiency in resource utilization density and avoid the ripple effect of costs associated with overbuying capacity.
- Brocade telemetry solutions enable Big Data analytics to mine only relevant data and avoid the rapidly increasing costs to scale those tools.
- Brocade secures the data from workload to workload, server to server, and site to site across the enterprise.
- Brocade solutions are not only priced competitively, but they also cost less to operate through a lower cost warranty and decreased demand on the energy infrastructure.

For more information about Brocade solutions, visit www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com