Secure Software-Defined Networks
Unlock Digital Information
SUMMARY

The classic enterprise network architecture has arrived at a complexity crossroad. As demand for network resources escalates and connections grow between information sources, companies find that traditional approaches to network design and operations don’t measure up to diverse workloads, changing load patterns, increased security postures and new services and capabilities coming from outside the data center. Increasingly, organizations are moving to software-defined networks (SDNs) to provide applications and users with the contextualized, just-in-time, secure information they need.
It is easy to say that, without networks, nothing would work. But the view of networks and their role is changing. By considering networks as core providers of the information, not just data, that flows through them, enterprises can tap into a whole new value proposition.

Businesses are dealing with major transformational shifts across platform, workplace and application domains. As a result, the network’s role is evolving to become more aware of the context for its applications, services and users.

No longer a collection of static appliances and cables, networks — the arteries that supply a company’s vital organs with information — must handle the flow of various types of data, accommodate changing demands, and take remediation actions automatically.

**New demands challenge the network**
Compute, storage and network requirements have always fluctuated with business needs in real time, but these routine variations are now amplified and broadened by new trends. Beyond the usual cyclical and periodic spikes, enterprises must deal with a whole new range of dynamic network demands.

The digital enterprise, with its focus on greater collaboration with customers and partners and its increasing use of cloud services, is creating high demand for network resources. Organizations have experienced an explosion of mobile devices. Application portfolios have expanded dramatically to serve these devices. A large, geographically distributed workforce and expanded global connectivity are adding to the demand.

The need for greater business agility also drives change. Enterprises must now deliver new, innovative services for users inside and outside the company. They must enter new markets quickly, without the delay of traditional provisioning cycles. They must manage costs while closely matching the capacity of the entire IT stack to rapidly fluctuating demands in real time.

In this environment, the modern enterprise network must be gradually enhanced by a set of programmable controls to support added functionality or to improve latency, protection, integration and collaboration. The result is a strong, stretchable fabric that enables integration and connectivity while improving the quality of service and experience.

By 2019, **45% of IoT-created data** will be stored, processed, analyzed and acted upon close to, or at the edge of, the network.

Source: [IDC FutureScape: Worldwide Internet of Thing 2016 Predictions, November 2015](#)
Stretched to the limit
Little about the traditional network is designed to effectively manage this new set of requirements, and its limitations sometimes slow the adoption of new technologies and platforms.

For instance, the method for matching capacity with demand usually entails a cost/benefit/risk tolerance model, which rarely results in the most efficient operating model in any given instance. Networks are too static to provide agility in light of technology demands on cloud platforms and digital services that flow critical information across an outside-in firm.

This lack of agility makes it challenging to support the continuous growth and fluctuation of traffic into and out of data centers — as well as a steady increase in intracenter traffic fueled by virtual machine migration, storage replications and other server-to-server applications with large-scale data requirements. As a result, organizations want to segment networks for a particular workload or data-flow pattern to improve specific throughput, security and efficiency requirements per traffic class. Additionally, organizations require finer control so flows can be managed per user, per class of service, per volume, or per time period — something difficult to obtain in traditional environments.

The static nature of traditional networks prevents them from rapidly adapting to changing usage patterns. They are often hard-coded and manually managed, making them rigid and difficult to scale and service. Plus, traditional networks don’t easily allow for the control and segregation of information at a sufficiently granular level.

Traditional networks execute their routing and switching algorithms over a large number of distributed network switches in addition to carrying out their essential traffic-forwarding functions. This distributed model has many limitations, including lack of global awareness, long convergence time, poor utilization and increased operational complexity. The operational

In 2018, surveyed companies expect that 56% of their networking infrastructure will use software-defined infrastructure (SDI). This is up from 38.5% in 2015.

Source: IDC Software Defined Infrastructure Survey, August 2015
complexity is primarily due to the switches’ diverse models, firmware releases and programming access methods.

Security is another concern. The growth of cloud computing and the mobile workforce means more data than ever is flowing beyond enterprise walls over the public Internet, as well as between new enclaves of differentially protected services. In highly regulated industries, these trends create concerns about data security and privacy, as well as the ability to defend critical information from the eventuality of an attack.

In short, current network designs limit the ability of organizations to take advantage of new technologies and platforms that improve agility and strike a balance among demand, performance, cost and security. These are the essential drivers behind the transformational shift to a radically new network architecture.

Elements of the software-defined network
In contrast to a fixed model of predefined and statically allocated capacity, software-defined networks (SDNs) measure network throughput in real time and proactively request additional bandwidth to complete important business functions. SDNs support the principles of loosely coupled architecture, where routing and switching functions are consolidated in a centralized controller (control plane) and decoupled from the traffic-carrying function in the network switches (data plane). To promote interoperability, Open SDN provides a consistent open source and open standards approach — important given the life cycle of typical network architecture and platforms.

Network function virtualization (NFV) is a technology that can be used in conjunction with SDNs to provide exceptional agility to the network estate and reduce capital and operational expenses. NFV uses virtualization technology to deploy network functions on industry-standard, high-volume servers instead of specialized and expensive appliances. This enables virtualized devices — such as firewalls, intrusion-detection systems and load balancers — to be easily configured, instantiated or replicated to provide for more reliability, management and automation.

This dynamic system has big advantages over the traditional diagnose-and-react manual process for application performance management often in use today. It enables the network to grow from a limited role of connecting devices to a strategic role that supports applications. SDNs easily facilitate the movement of data over the data plane in programmable flows, or virtual pathways, with a global context. Enterprise applications, which reside on the north side of the controller, communicate the network characteristics they need and leave it up to the controller to decide how these requests can be implemented.
The controller then programs the switches, residing in the south side, to accommodate the new flow requirements. If an endpoint moves, the control plane can redefine the flow to account for the move. If the service level drops for a given flow, an application alerts the controller, which can counter by changing quality of service (QoS) controls or by defining a new pathway where there is greater bandwidth availability.  

Modern networks support modern applications
Modern networks are closely aligned with enterprise applications’ dynamic requirements for underlying network resources that can flex on demand. With SDNs, an application can communicate its intent to the network, which in turn provisions the needed resources and continues to adapt during the application’s runtime based on changing demands.

Applications that make requests to the SDN controller can be categorized as either reactive or proactive. A proactive application has a good idea of what the network’s initial state should be and communicates a set of requests to the controller to configure the network. The controller implements the network flows and continues to revise the state based on real-time network measurements and further guidance from the application. An example of a proactive application is the rollout of virtual desktops, where location, typical demands, and density are known in advance.

A reactive application, on the other hand, starts from an initial blank network state, then builds and optimizes flows as it learns about events in the network. An example of a reactive application is one that implements Network Access Control (NAC) for users’ mobile devices as they connect to the network. There is no perceived knowledge about the user or service classes beforehand but the network resources are managed based on these events.

These adaptive behaviors follow a well-defined enterprise governance model for arbitration, prioritization and optimization. Operating within the services domain of the applications, and their users, provides the critical informational context for the digital enterprise.

Being software-defined, the network estate can also be simplified and instrumented by a consistent and pervasive programming paradigm, using a set of APIs, with a global view of resources. This makes it possible to successively and dynamically optimize the network, doing away with traditional complex configurations and their varying management methods. SDNs can help enterprises build more innovative, manageable, automated and deterministic high-scale infrastructure spanning data centers as well as private and public resources.

Here are a few use cases for SDNs:

- **Security and policy enforcement** to mitigate inbound threats and prevent outbound data leakage
- **Microsegmentation** based on services, classes of users, internal and external events, or other classifications
- **Application-aware routing policy** to address bandwidth requirements, resource optimization, security constraints or SLA thresholds
- **Operational controls** to support resource optimization, cost management and operational efficiency and resiliency

**Big help for big data**
Big data analytics can help manage enterprise applications that generate large amounts of data and require the analysis of
Network Data as a Source of Innovation

Extending the network beyond traditional enterprise boundaries means that the enterprise network is present during a greater number of customer and partner interactions. The modern software-defined network (SDN) contains data about fluctuating workloads and patterns, but it also contains a wealth of real-time data about the interactions of customers and partners. Capturing and mining this data is an important step in truly understanding — and even predicting — the customer and partner experience.

Analytics on network traffic data can increase raw performance and security, and they can also be a source of business innovation. Network traffic data can be transformed into insights on an industrial scale. We can feed data pipelines with continuous streams of network interactions. We can analyze these interactions using algorithms running in production. We can produce continuous insights and transform the business in small, meaningful chunks.

For example, by tracking traffic by named service endpoint rather than IP address, networks can record the ebb and flow of customer and partner service interaction. Service interaction data can be correlated with key customer events, such as sales. Imagine using network traffic as a real-time indicator of buyer intent, or using network traffic to anticipate shifts in a customer’s use of critical service value chains.

Modern platforms provide a greater ability to integrate disparate data, to put data into context and to provide situational awareness. When combined with the power of modern platforms, data from the modern network can be a new source of sustainable business value. This value can range from basic data about sales to the creation of new value nets. The shift to a modern network brings not only greater business agility, but also greater opportunity to understand and respond to customers.

— Jerry Overton, Data Scientist, CSC Distinguished Engineer

Big data also provides valuable input to modern networks. The rapid expansion of an extremely distributed IT estate has caused both the amount of data and the number of data sources to grow massively and more rapidly. Data shared between devices, data about application states, and data about the network are all growing. Big data analytics can be used to provide the network controller with near-real-time insights to make critical network decisions based on real-time network, device and application states.
End-to-end service management and operation
Software-defined networking is also a mechanism for managing service levels. Changes to the network controller can be dynamically requested to ensure that governing SLAs are met. Self-monitored devices communicate with the network about the resources needed to meet their individual performance, capacity, coverage or latency requirements.

This level of manageability provides agility and an opportunity for new integrated services. By using software-defined networking, IT can identify a potential problem and automatically prescribe a course of action before a service interruption actually takes place.

For example,

- Incident/event management can be improved by reactively re-provisioning or de-provisioning network resources, such as a desktop virtualization request for sufficient bandwidth for specific processing, improved access to IP storage, or the ability to shorten network convergence time when devices are deleted or added as a result of failure.

- Using knowledge management, an SDN can proactively provision network resources at deployment time to ensure services meet network-related SLA requirements.

- Using IT cost-management discipline with SDN programmable flow management, data center network racks can be turned off if they are associated with dormant flows during nonpeak hours, as a part of an integrated power management strategy to reduce operational expense.

- Data archive and replication can be de-prioritized to fill unutilized bandwidth differentially.

Network fabric for the Internet of everything
The adoption of modern network tools is essential to the integration of the billions of objects expected to join enterprise networks in the next few years. The domain of the Internet of Things (IoT) is characterized by a high number of devices, low-volume traffic, heterogeneous networks, differing priorities, and highly distributed, time-sensitive traffic. Devices such as sensors, actuators, heating/ventilation and air conditioning (HVAC) systems, lights, cameras, environmental controls, energy management systems, fire and safety controls, and audiovisual gadgets will be added to IT-managed IP-based networks.

This flood of devices will affect security, performance, capacity and latency of the network and will demand new monitoring capabilities, changes in policies and complex SLAs — all of which an SDN can effectively provide.

In addition to the advantages of flexibility and improved performance, SDNs offer better control over network traffic. IT can differentiate network access for users and applications based on qualifying metrics such as user privileges and connecting devices. By separating information flows, IT can better deal with individual service interactions at a finer level of granularity. For example, users in class X can access information and other services that are not available to users in class Y, with certain transactions enjoying higher-priority traffic than others.

SDNs provide three important mechanisms to implement a robust and complete end-to-end security architecture:

- Granular segmentation of the network to reflect complex security policies
Centralization of security policies and their respective configuration management

Automation of security remediation tasks

This means security can be built into business application logic, simplifying network security policy enforcement and auditing, and improving threat detection and response. Complex policies and remediation tasks can be implemented programmatically, taking into consideration application functions, various constraints, user classes, service categories, locations of traffic streams’ endpoints, time of day or week, cost of links, and external events. These capabilities not only strengthen existing security functions but can also improve the overall security posture and many of its operational aspects.

Consider, for example, a security mitigation function such as IP mutation, used to prevent distributed denial-of-service (DDoS) attacks. Attackers target a domain by first identifying an active IP address before flooding the server at that IP address with a large number of packets from multiple sources. This will eventually degrade the application and network performance to a point where the intended users for the service can no longer be served. An effective, established strategy against DDoS attacks is IP mutation. By constantly advertising a virtual IP address of the protected host and mapping responses back to the physical IP address, this approach prevents automated attacks from being effective. This is typically implemented either by using a specialized and expensive appliance or by utilizing a combination of Dynamic Host Control Protocol (DHCP) and Network Address Translation (NAT). However, the combination of DHCP and NAT can effect only a limited rate of change, so the host remains vulnerable to more sophisticated DDoS attacks.

SDNs offer an extremely effective and cheaper approach. When protected hosts advertise their assigned virtual IP addresses through DNS, an SDN network controller can randomly assign virtual IP addresses to these protected hosts at a very high rate. The temporary mapping between the virtual and physical IP addresses is pushed to the switches closest to the protected hosts, at the very edge of the network, where the translation can take place.

Another example is the operational improvement that SDNs provide for perimeter security during a firewall cluster migration. Firewall migration to a new platform is a challenging undertaking for enterprises, requiring extensive planning and experienced resources to manage its operational, financial and delivery risks. While most of the effort is spent analyzing the firewall rules, understanding the semantic relationships, and in implementing change management in an IT Service Management framework, SDN provides additional support. Since SDN is fundamentally about managing flows, an OpenFlow switch can front-end a battery of legacy firewalls, which can be programmed by an SDN controller to migrate rules incrementally in subsets to the new platform. These newly migrated rules can be further tested, versioned and rolled back if needed.

When it comes to threat detection and prevention, an SDN combined with in-line analytics provides powerful support for security improvements. It is critical that...
breaches are discovered quickly and dealt with swiftly, but the fact is that the gap between discovery and mitigation has been widening over the years, with some intrusions lasting for months. Visibility fabrics with taps and collectors are challenged by their limited scope of data sampling, isolation from the control plane, and their reliance on manual labor to diagnose and issue remediation.

On the other hand, SDN can use analytics to identify when compounded thresholds are crossed with preprogrammed mitigation plans that can immediately take effect in real time. Mitigation plans may include forwarding the traffic to a more specialized intrusion detection system, blocking or throttling suspicious traffic on a particular port. SDN can be used to implement infrastructure changes, with the ability to issue a recovery procedure given rich forensics capabilities over network flows’ history and logs. Since SDN applications can also receive events from outside the network, they can even execute a network remediation plan or a lock-down if physical security is breached. The very concept of automatic alerting and dynamic remediation brings a new form of agility to modern network security.

An Open SDN also abstracts a security vendor’s hardware differences and allows the design of security architecture that uses virtual chains based on the strengths of each vendor. This further improves the overall security model both at the time of design and during an attack.

Furthermore, when wired and wireless LANs are integrated into one controller, IT can establish tighter controls and more granular management over user-supplied devices. The network can, for example, easily detect jail-broken devices and prevent them from accessing the network. In addition, the SDN can find and eliminate threats by creating rules to spot suspicious patterns and act programmatically to shut down a link, quarantine a service, or isolate a user, without having to rely on operators to monitor and interpret the activity.

Centralized control, combined with the automation of software-defined networking, will enable adaptive and automated network security that ultimately results in a security-defined routing strategy. The ability to design the best route for each application, device and dynamic event (such as a triggered recovery plan) will change how IT secures networks, applications and devices.

**Where it’s all headed**

The networks and components described and automated by software are part of the move toward declarative IT, where all aspects of IT are provided as a service. By virtualizing the entire IT stack and running services on commodity hardware, the data center is being transformed. Bringing software constructs and abstraction concepts to the network domain opens up the possibility of applying programming methodologies to networks to create greater value.

As a result, the network is changing from a computer-centric communication infrastructure to one that supports many different types of devices, while becoming aware of context and information. The SDN makes it possible for the network to adapt dynamically and automatically to events and changing demands so it can deliver information at the speed of business.

This difference enables enterprises to maintain performance and head off potential problems before they arise.

**Getting started**

Whether an enterprise is modernizing and rationalizing an application portfolio, creating a hyperconverged infrastructure or adopting a cloud computing platform for an as-a-service model, every element of the next-generation IT stack relies on a modern network design. Indeed, an SDN should be included as part of any next-generation project’s design requirements.

From a strategic perspective, an enterprise must look at the full scope of the network estate, including the WAN, campus, data
Software-Defined Networks: The LEF Perspective

In the 21st century, digital assets and capabilities are an increasingly large proportion of the value and potential of our businesses. But digital assets are a bit like financial currencies — what makes them valuable is their liquidity. The value of digital capabilities and information lies in their accessibility and their ability to be exploited anywhere in our ecosystem in a timely fashion. High volumes, high speed, low latency.

At the same time, due to the consumerization of technology, customer and citizen expectations are sky-high and rising. To support increasingly open business models, ecosystem initiatives, enterprise agility and digital disruption, the networks that support and enable these services must continually evolve to provide the necessary liquidity.

Digital assets and capabilities may not appear explicitly on most companies' balance sheets, but be sure that whether your business is pens, pensions or power stations, digital capabilities will be an increasing source of your success in the next decades. You must ensure that they are liquid and exploitable.

The Leading Edge Forum (LEF) is the independent research arm of CSC.

center and cloud provider, as an integrated part of the end-to-end service delivery infrastructure.

With a common architectural design and control plane that can truly provision end-to-end connectivity, as well as service functions, the modern network provides a unique advantage for enterprises in the global business environment.

New business demands, connected devices, next-generation technologies and a multitude of modern services require a new, more granular type of network that can be provisioned far more rapidly to enable a governed flow of information.

The transformation is underway. With the growing abstraction of network hardware and adoption of software-defined networking, businesses are creating highly flexible and resilient networks able to service critical demands. These agile applications yield a more information-rich experience for employees, consumers, clients and partners alike.
CSC Partnerships Keep Networks Humming

CSC helps organizations connect their information systems to each other — across a campus, across a major metropolitan region or across the globe. CSC also helps organizations connect their IT systems to public cloud services, essentially treating the cloud as a logical extension of enterprise IT infrastructure.

CSC’s partner ecosystem is vital to making these connections. These partnerships provide integrated sets of complementary products that enable CSC to offer solutions that are managed, flexible and secure.

CSC’s enterprise LAN, WAN and Internet services are delivered through our partnership with AT&T. This arrangement enables CSC to offer a world-class carrier backbone along with our hardware- and software-based solutions.

By working with AT&T, CSC can offer a common cloud infrastructure that’s managed across our clients’ respective data centers. With CSC Agility Platform orchestration software, we’re also able to manage enterprise cloud workloads across hybrid, multivendor cloud environments.

Security is another benefit of the AT&T-CSC partnership. As more of our client organizations move to hybrid cloud environments, they’re asking CSC to help them extend these networks across the Internet with enterprise levels of security. To do that, CSC has integrated AT&T’s NetBond cloud-connectivity solution with CSC’s Agility Platform. AT&T NetBond is an implementation of an open source SDN controller to manage traffic across its global network to meet SLA requirements. The controller enables organizations to connect securely to public clouds using MPLS VPN technology while its instantiation and capacity are policy-managed and orchestrated by the Agility Platform. Together, they add simplified automation to reduce overhead and help organizations respond quickly to changing business needs. CSC Agility also integrates with open source controllers in the data center, which provides a unique advantage to manage network resources for a hybrid cloud, extending beyond the premises to include cloud service providers across the globe.

NFV is provided by AT&T’s Universal Customer Premises Equipment (uCPE), the hardware foundation of the AT&T Network Functions on Demand service. A single AT&T-branded x86 server can host several software-based virtual network functions (VNFs), depending on what functions are needed at each location, such as a firewall, load balancer or network accelerator. The uCPE platform is also dynamic and flexible: Supporting a different or additional function is just a matter of adding or replacing VNFs via a configuration button. Implemented in software, the hardware doesn’t change.

NFV, combined with SDN, supports new business initiatives at the lightning speeds required by today’s agile business. In addition, CSC’s LAN solutions combine hardware and software tools. While information is appropriately routed, policies are fully applied and alerts are issued if and when risks arise. CSC’s Network Security Services provide appropriate levels of protection. And CSC Enterprise Service Management keeps network administrators informed of any environmental state changes.

The end result: networks that not only enable the fast and secure transport of information among disparate systems, but also apply policies. Thanks to an integrated orchestration tool set, data flows across secure managed networks that connect both public and private services as if they were enterprise nodes. That’s the power of partnership.
Authors

Rafat Shaheen is a lead global solutions executive and a member of CSC’s CTO Office. His expertise includes IT transformation, service-oriented architecture, design methodologies, IT virtualization stack, hybrid cloud architecture, DevOps and architecture design.

rshaheen@csc.com

James Hanley is vice president of data center and platform offerings at CSC. He is responsible for driving growth in this sector, ensuring client satisfaction, and building strategic partnerships critical to the development of CSC offerings.

jameshanley@csc.com

Chris Swan is chief technology officer for Global Infrastructure Services at CSC, where he directs the vision, strategy and architecture for CSC’s infrastructure and managed services portfolios including cloud, workplace, data center, platform and service management. Chris also leads CSC’s shift toward infrastructure as code and being a data-driven delivery organization. He has previously held CTO and director of research & technology roles at Cohesive Networks, UBS, Capital SCF and Credit Suisse, where he worked on app servers, compute grids, security, mobile, cloud, networking and containers.

chrisswan@csc.com

*CSC’s ResearchNetwork contributed to this paper.*
Regional CSC Headquarters

The Americas
1775 Tysons Blvd.
Tysons, Virginia 22102
United States
+1.703.876.1000

Asia, Middle East, Africa
Level 9, UE BizHub East
6 Changi Business Park Avenue 1
Singapore 468017
Republic of Singapore
+65.6809.9000

Australia
26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(2)9034.3000

Central and Eastern Europe
Abraham-Lincoln-Park 1
65189 Wiesbaden
Germany
+49.611.1420

Nordic and Baltic Region
Retortvej 8
DK-2500 Valby
Denmark
+45.36.14.4000

South and West Europe
Tour Carpe Diem
31 place des Corolles
CS 40075
92098 Paris La Défense Cedex
France
+33.1.55.707070

UK, Ireland and Netherlands
Floor 4
One Pancras Square
London
NIC 4AG
United Kingdom
+44.020.3696.3000

About CSC
CSC leads clients on their digital transformation journeys. The company provides innovative next-generation technology services and solutions that leverage deep industry expertise, global scale, technology independence and an extensive partner community. CSC serves leading commercial and international public sector organizations throughout the world. CSC is a Fortune 500 company and ranked among the best corporate citizens. For more information, visit us at CSC.com.