Mobility and Collaboration

Remote Meeting Technology

Remote Meeting Technology

Several technologies and services exist that allow organizations and individuals to meet "virtually." These applications are typically web-based and either install extensions in the browser or client software on the host system. These technologies also typically allow "desktop sharing" as a feature. This feature may allow the viewing of a user's desktop. Some organizations use dedicated equipment such as cameras, monitors and meeting rooms to host and participate in remote meetings. These devices are often integrated with Voice over Internet Protocol (VoIP).

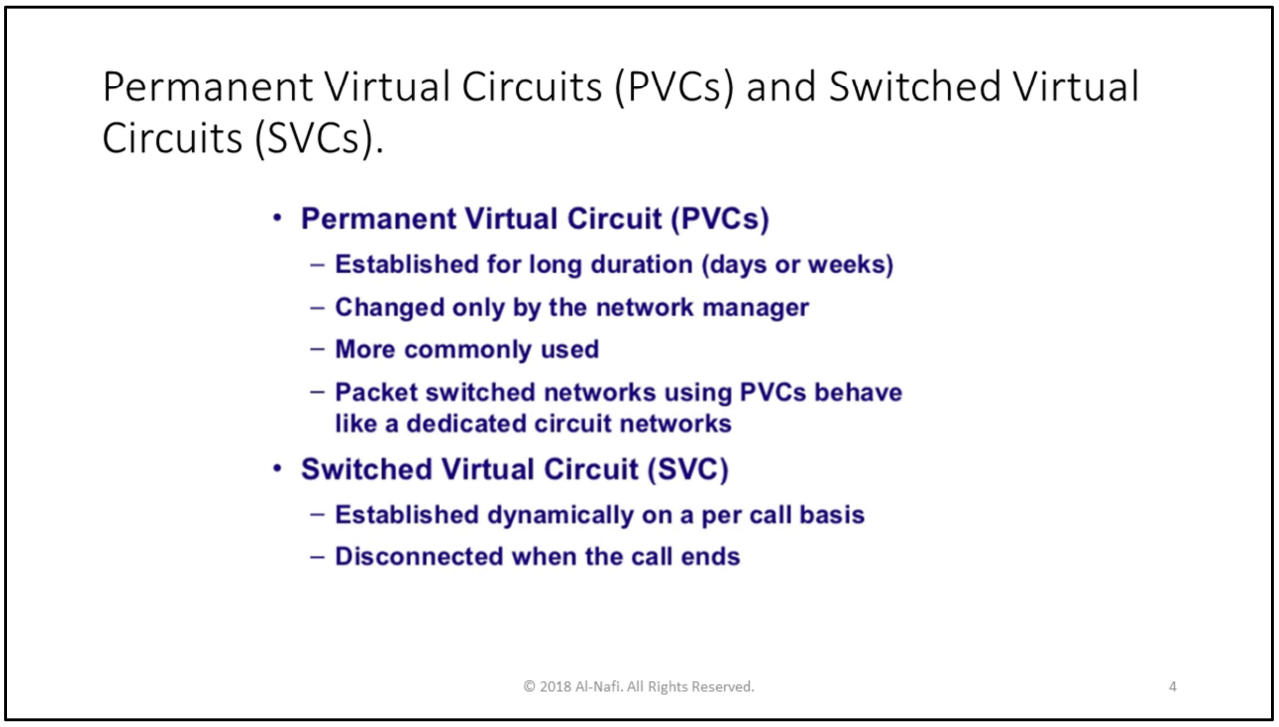
Remote meeting technology risks include the following:

- Some software may allow control of another system when the desktop is shared
- Vulnerabilities in the underlying operating system or firmware

Virtualized Networks

Within the realm of circuit switched networking arose two types of virtualization, namely;

- Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs).
- Circuit-Switched Networks

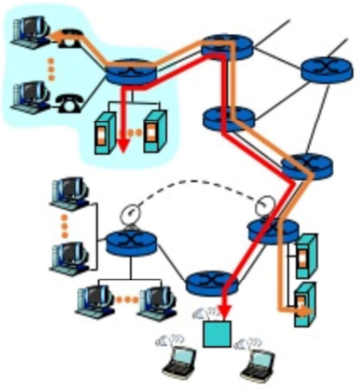


Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs).

Virtual circuits provide a connection between endpoints over high bandwidth, multiuser cable or fiber that behaves as if the circuit were a dedicated physical circuit. There are two types of virtual circuits based on when the routes in the circuit are established. In a permanent virtual circuit (PVC), the carrier configures the circuit's routes when the circuit is purchased. Unless the carrier changes the routes to tune the network, respond to an outage, etc., the routes do not change. On the other hand, the routes of a switched virtual circuit (SVC) are configured dynamically by the routers each time the circuit is used.

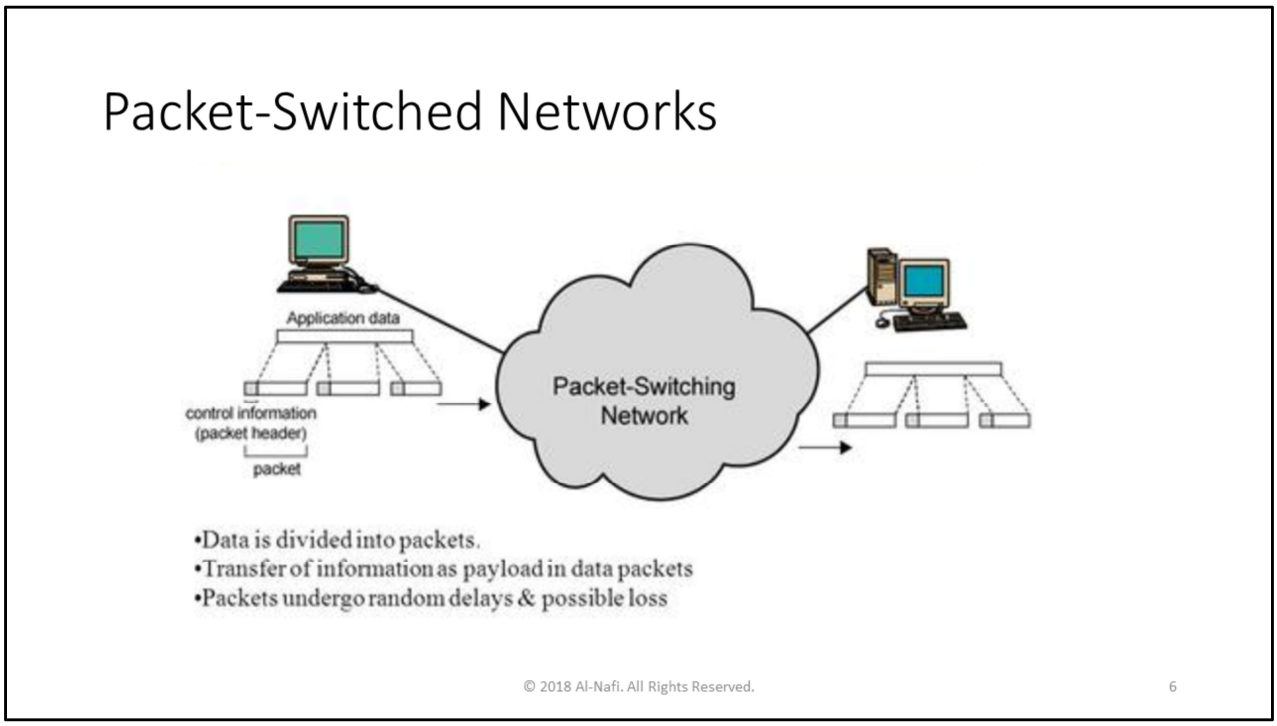
Circuit-Switched Networks

- Circuit switching is a technique that directly connects the sender and the receiver in an unbroken path.
- Telephone switching equipment, for example, establishes a path that connects the caller's telephone to the receiver's telephone by making a physical connection.
- With this type of switching technique, once a connection is established, a dedicated path exists between both ends until the connection is terminated.
- Routing decisions must be made when the circuit is first established, but there are no decisions made after that time



Circuit-Switched Networks

Circuit-switched networks establish a dedicated circuit between endpoints. These circuits consist of dedicated switch connections. Neither endpoint starts communicating until the circuit is completely established. The endpoints have exclusive use of the circuit and its bandwidth. Carriers base the cost of using a circuit-switched network on the duration of the connection that makes this type of network only cost-effective for a steady communication stream between the endpoints. Examples of circuit-switched networks are the plain old telephone service (POTS), Integrated Services Digital Network (ISDN), and Point-to-Point Protocol (PPP).



Packet-Switched Networks

Packet-switched networks do not use a dedicated connection between endpoints. Instead, data is divided into packets and transmitted on a shared network. Each packet contains meta-information so that it can be independently routed on the network. Networking devices will attempt to find the best path for each packet to its destination. Because network conditions could change while the partners are communicating, packets could take different paths as they transverse the network and arrive in any order. It is the responsibility of the destination endpoint to ensure that the received packets are in the correct order before sending them up the stack.

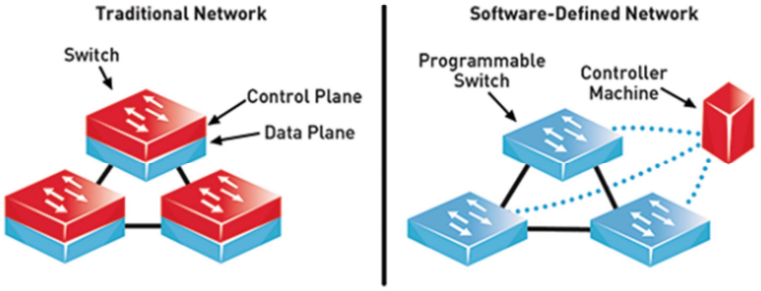
The modern virtualization of networks and the associated technology is called Network Function Virtualization (NFV) or alternately referred to as virtual network function. The objective of NFV is to decouple functions, such as firewall management, intrusion detection, network address translation, or name service resolution, away from specific hardware implementation into software solutions. NFV focus is to optimize distinct network services. With the focus on network service management and not hardware deployment, NFV readily supports capacity

management since there is a more thorough utilization of resources. As service providers struggled to keep up with the quick deployment needs and faster growth models, the slowness of hardware-based solutions was exposed. A number of these service providers came together and founded The European Telecommunications Standards Institute (ETSI) and worked to formalize NFV standards.

The following benefits are sought for utilizing NFV:

- Support transition from capital expenditure to operational expenditure (CapEx to OpEx).
- Reduce wait time in time-to-market ventures.
- Increase service consumption agility.

Software-Defined Networking (SDN)



https://www.youtube.com/watch?v=Z5Gi2Bpd82M

 7

Hardware reigned supreme in the networking world until the emergence of software-defined networking (SDN), a category of technologies that separate the network control plane from the forwarding plane to enable more automated provisioning and policy-based management of network resources.
SDN's origins can be traced to a research collaboration between Stanford University and the University of California at Berkeley that ultimately yielded the OpenFlow protocol in the 2008 timeframe.

OpenFlow is only one of the first SDN canons, but it's a key component because it started the networking software revolution. OpenFlow defined a programmable network protocol that could help manage and direct traffic among routers and switches no matter which vendor made the underlying router or switch. In the years since its inception, SDN has evolved into a reputable networking technology offered by key vendors including Cisco, VMware, Juniper, Pluribus and Big Switch. The Open Networking Foundation develops myriad open-source SDN technologies as well.

"Datacenter SDN no longer attracts breathless hype and fevered expectations, but the market is growing healthily, and its prospects remain robust," wrote Brad

Casemore, IDC research vice president, data center networks, in a recent report, *Worldwide Datacenter Software-Defined Networking Forecast, 2018–2022*. "Datacenter modernization, driven by the relentless pursuit of digital transformation and characterized by the adoption of cloudlike infrastructure, will help to maintain growth, as will opportunities to extend datacenter SDN overlays and fabrics to multicloud application environments." SDN will be increasingly perceived as a form of established, conventional networking, Casemore said.

IDC estimates that the worldwide data center SDN market will be worth more than $12 billion in 2022, recording a CAGR of 18.5% during the 2017–2022 period. The market generated revenue of nearly $5.15 billion in 2017, up more than 32.2% from 2016. In 2017, the physical network represented the largest segment of the worldwide datacenter SDN market, accounting for revenue of nearly $2.2 billion, or about 42% of the overall total revenue. In 2022, however, the physical network is expected to claim about $3.65 billion in revenue, slightly less than the $3.68 billion attributable to network virtualization overlays/SDN controller software but more than the $3.18 billion for SDN applications.

“We're now at a point where SDN is better understood, where its use cases and value propositions are familiar to most datacenter network buyers and where a growing number of enterprises are finding that SDN offerings offer practical benefits,” Casemore said. “With SDN growth and the shift toward software-based network automation, the network is regaining lost ground and moving into better alignment with a wave of new application workloads that are driving meaningful business outcomes.”

What is SDN?

The idea of programmability is the basis for the most precise definition of what SDN is: technology that separates the control plane management of network devices from the underlying data plane that forwards network traffic. IDC broadens that definition of SDN by stating: “Datacenter SDN architectures feature software-defined overlays or controllers that are abstracted from the underlying network hardware, offering intent-or policy-based management of the network as a whole. This results in a datacenter network that is better aligned with the needs of application workloads through automated (thereby faster) provisioning, programmatic network management, pervasive application-oriented visibility, and where needed, direct integration with cloud orchestration platforms.”

The driving ideas behind the development of SDN are myriad. For example, it promises to reduce the complexity of statically defined networks; make automating network functions much easier; and allow for simpler provisioning and management

of networked resources, everywhere from the data center to the campus or wide area network. Separating the control and data planes is the most common way to think of what SDN is, but it is much more than that, said Mike Capuano, chief marketing officer for Pluribus. “At its heart SDN has a centralized or distributed intelligent entity that has an entire view of the network, that can make routing and switching decisions based on that view,” Capuano said. “Typically, network routers and switches only know about their neighboring network gear. But with a properly configured SDN environment, that central entity can control everything, from easily changing policies to simplifying configuration and automation across the enterprise.”

How does SDN support edge computing, IoT and remote access?

A variety of networking trends have played into the central idea of SDN. Distributing computing power to remote sites, moving data center functions to the edge, adopting cloud computing, and supporting Internet of Things environments – each of these efforts can be made easier and more cost efficient via a properly configured SDN environment. Typically in an SDN environment, customers can see all of their devices and TCP flows, which means they can slice up the network from the data or management plane to support a variety of applications and configurations, Capuano said. So users can more easily segment an IoT application from the production world if they want, for example.

Some SDN controllers have the smarts to see that the network is getting congested and, in response, pump up bandwidth or processing to make sure remote and edge components don’t suffer latency.

SDN technologies also help in distributed locations that have few IT personnel on site, such as an enterprise branch office or service provider central office, said Michael Bushong, vice president of enterprise and cloud marketing at Juniper Networks. “Naturally these places require remote and centralized delivery of connectivity, visibility and security. SDN solutions that centralize and abstract control and automate workflows across many places in the network, and their devices, improve operational reliability, speed and experience,” Bushong said.

How does SDN support intent-based networking?

Intent-based networking (IBN) has a variety of components, but basically is about giving network administrators the ability to define what they want the network to do, and having an automated network management platform create the desired state and enforce policies to ensure what the business wants happens.

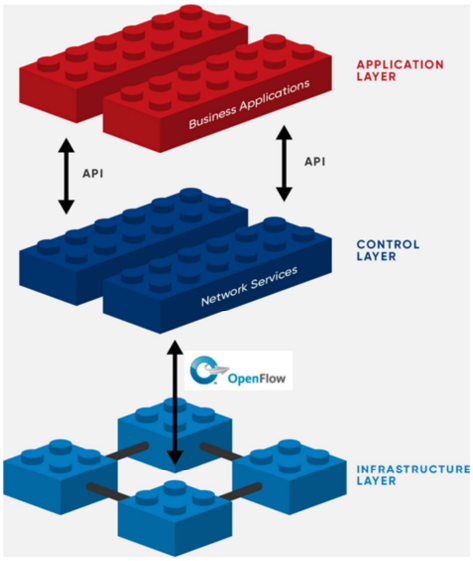
“If a key tenet of SDN is abstracted control over a fleet of infrastructure, then the provisioning paradigm and dynamic control to regulate infrastructure state is

necessarily higher level," Bushong said. "Policy is closer to declarative intent, moving away from the minutia of individual device details and imperative and reactive commands." IDC says that intent-based networking "represents an evolution of SDN to achieve even greater degrees of operational simplicity, automated intelligence, and closed-loop functionality."

For that reason, IBN represents a notable milestone on the journey toward autonomous infrastructure that includes a self-driving network, which will function much like the self-driving car, producing desired outcomes based on what network operators and their organizations wish to accomplish, Casemore stated. "While the self-driving car has been designed to deliver passengers safely to their destination with minimal human intervention, the self-driving network, as part of autonomous datacenter infrastructure, eventually will achieve similar outcomes in areas such as network provisioning, management, and troubleshooting — delivering applications and data, dynamically creating and altering network paths, and providing security enforcement with minimal need for operator intervention," Casemore stated.

While IBN technologies are relatively young, Gartner says by 2020, more than 1,000 large enterprises will use intent-based networking systems in production, up from less than 15 in the second quarter of 2018.

Software-Defined Networking (SDN) continued..



 8

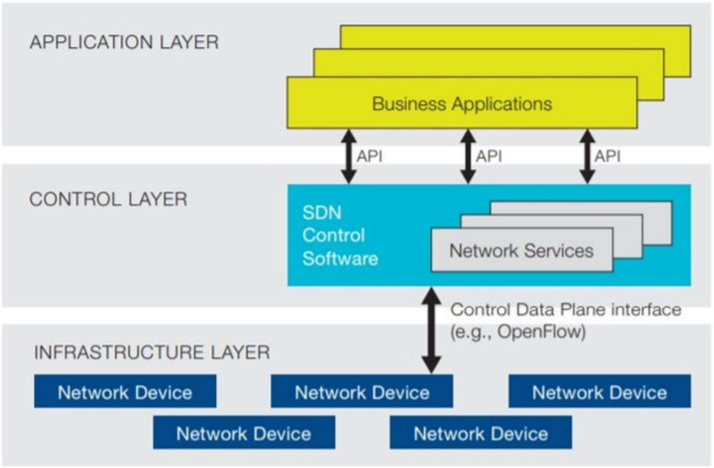
How does SDN help customers with security?
SDN enables a variety of security benefits. A customer can split up a network connection between an end user and the data center and have different security settings for the various types of network traffic. A network could have one public-facing, low security network that does not touch any sensitive information. Another segment could have much more fine-grained remote access control with software-based firewall and encryption policies on it, which allow sensitive data to traverse over it.

"For example, if a customer has an IoT group it doesn't feel is all that mature with regards to security, via the SDN controller you can segment that group off away from the critical high-value corporate traffic," Capuano stated. "SDN users can roll out security policies across the network from the data center to the edge and if you do all of this on top of white boxes, deployments can be 30 – 60 percent cheaper than traditional gear."

The ability to look at a set of workloads and see if they match a given security policy is a key benefit of SDN, especially as data is distributed, said Thomas Scheibe, vice

president of product management for Cisco's Nexus and ACI product lines. "The ability to deploy a whitelist security model like we do with ACI [Application Centric Infrastructure] that lets only specific entities access explicit resources across your network fabric is another key security element SDN enables," Scheibe said. A growing number of SDN platforms now support microsegmentation, according to Casemore. "In fact, micro-segmentation has developed as a notable use case for SDN. As SDN platforms are extended to support multicloud environments, they will be used to mitigate the inherent complexity of establishing and maintaining consistent network and security policies across hybrid IT landscapes," Casemore said.

Software-Defined Networking (SDN) continued..

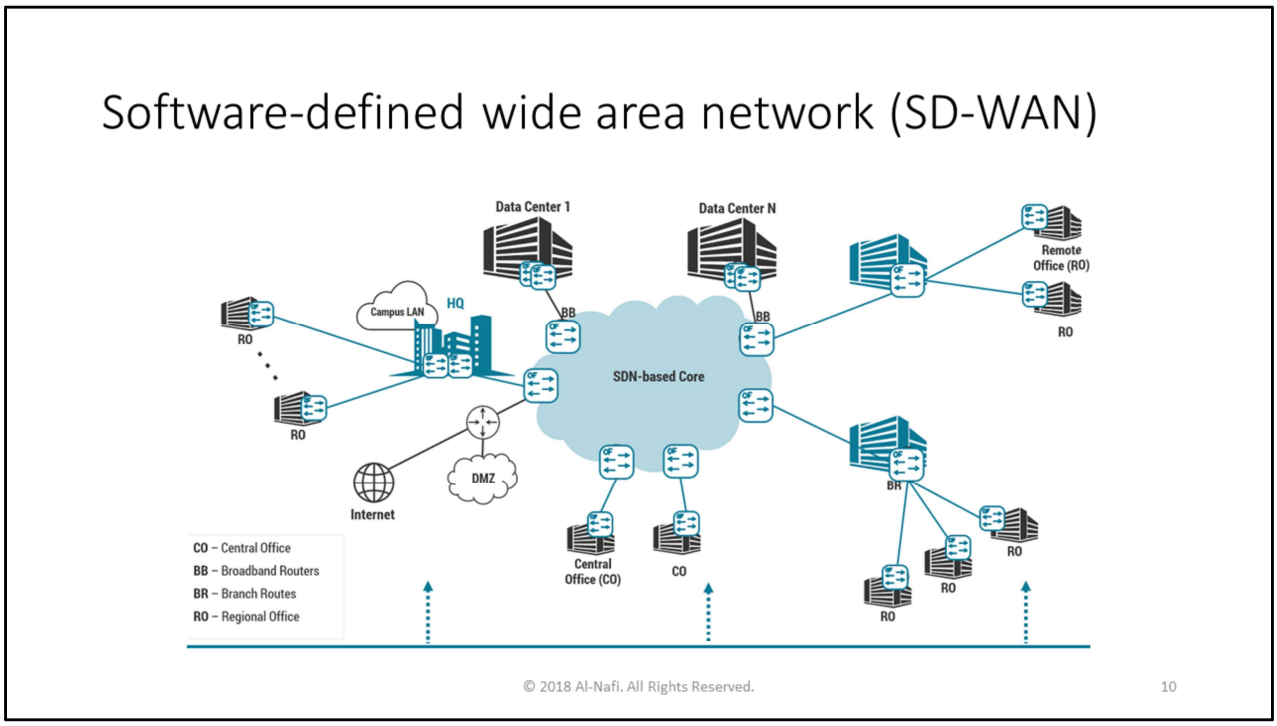


 9

What is SDN's role in cloud computing?

SDN's role in the move toward private cloud and hybrid cloud adoption seems a natural. In fact, big SDN players such as Cisco, Juniper and VMware have all made moves to tie together enterprise data center and cloud worlds. Cisco's ACI Anywhere package would, for example, let policies configured through Cisco's SDN APIC (Application Policy Infrastructure Controller) use native APIs offered by a public-cloud provider to orchestrate changes within both the private and public cloud environments, Cisco said. "As organizations look to scale their hybrid cloud environments, it will be critical to leverage solutions that help improve productivity and processes," said Bob Laliberte, a senior analyst with Enterprise Strategy Group, in a recent Network World article. "The ability to leverage the same solution, like Cisco's ACI, in your own private-cloud environment as well as across multiple public clouds will enable organizations to successfully scale their cloud environments." Growth of public and private clouds and enterprises' embrace of distributed multicloud application environments will have an ongoing and significant impact on data center SDN, representing both a challenge and an opportunity for vendors, said IDC's Casemore. "Agility is a key attribute of digital transformation, and enterprises will adopt architectures, infrastructures, and technologies that provide

for agile deployment, provisioning, and ongoing operational management. In a datacenter networking context, the imperative of digital transformation drives adoption of extensive network automation, including SDN," Casemore said.



Where does SD-WAN fit in?

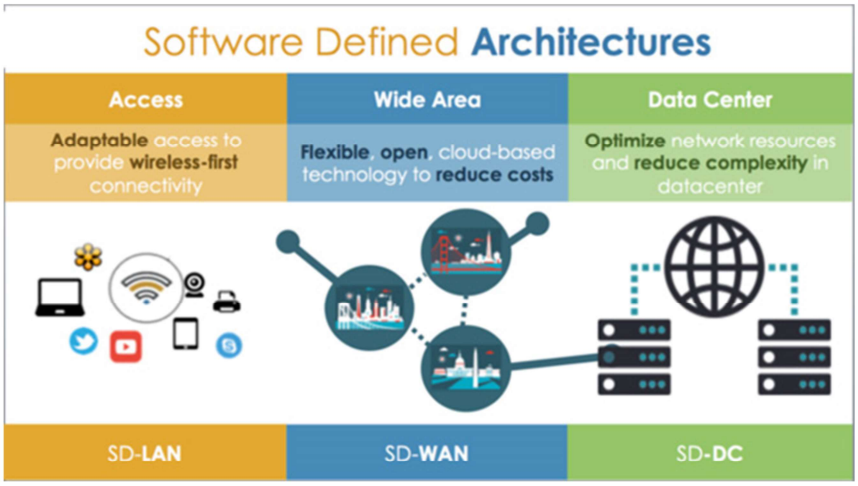
The software-defined wide area network (SD-WAN) is a natural application of SDN that extends the technology over a WAN. While the SDN architecture is typically the underpinning in a data center or campus, SD-WAN takes it a step further.

At its most basic, SD-WAN lets companies aggregate a variety of network connections – including MPLS, 4G LTE and DSL – into a branch or network edge location and have a software management platform that can turn up new sites, prioritize traffic and set security policies. SD-WAN's driving principle is to simplify the way big companies turn up new links to branch offices, better manage the way those links are utilized – for data, voice or video – and potentially save money in the process. SD-WAN lets networks route traffic based on centrally managed roles and rules, no matter what the entry and exit points of the traffic are, and with full security. For example, if a user in a branch office is working in Office365, SD-WAN can route their traffic directly to the closest cloud data center for that app, improving network responsiveness for the user and lowering bandwidth costs for the business.

"SD-WAN has been a promised technology for years, but in 2019 it will be a major driver in how networks are built and re-built," Anand Oswal, senior vice president of engineering in Cisco's Enterprise Networking Business, said a Network World article earlier this year. It's a profoundly hot market with tons of players including Cisco, VMware, Silver Peak, Riverbed, Aryaka, Fortinet, Nokia and Versa. IDC says the SD-WAN infrastructure market will hit $4.5 billion by 2022, growing at a more than 40% yearly clip between now and then.

From its VNI study, Cisco says that globally, SD-WAN traffic was 9% of business IP WAN traffic in 2017 and will be 29% of business IP WAN traffic by 2022. In addition, SD-WAN traffic will grow five-fold from 2017 to 2022, a compound annual growth rate of 37%.

Software Defined Architectures is now everywhere… no need for tons of physical hardware anymore.



11

What is in the future for SDN?

Going forward there are a couple of developments to watch for, Cisco's Scheibe said. One involves the increased ability to automate the provisioning of data center services, to make it easier to horizontally extend access to data. The second expected development is the ability to more easily allow customers to work across domains to monitor and track what is going on across the infrastructure. According to Cisco's most recent Global Cloud Index research, SDN might streamline traffic flows within the data center such that traffic is routed more efficiently than it is today. "In theory, SDN allows for traffic handling policies to follow virtual machines and containers, so that those elements can be moved within a data center in order to minimize traffic in response to bandwidth bottlenecks," Cisco stated.

Most major hyperscale data centers already employ flat architectures and SDN and storage management, and adoption of SDN/NFV or network function virtualization (which virtualizes network elements) within large-scale enterprise data centers has been rapid, Cisco stated. Over two-thirds of data centers will adopt SDN either fully or in a partial deployment by 2021. As a portion of traffic within the data center, SDN/NFV is already transporting 23%, growing to 44% by 2021.

Cisco found that there are also ways in which SDN/NFV can lead to an increase in both data center traffic and in general Internet traffic:

Traffic engineering enabled by SDN/ NFV supports very large data flows without compromising short lived data flows, making it safe to transport large amounts of data to and from big data clusters. SDN will allow video bitrates to increase, because SDN can seek out highest bandwidth available even midstream, instead of lowering the bitrate according the available bandwidth for the duration of the video, as is done today. The future of SDN is shaped by operational needs and software innovation, Bushong said. “While trends like cloud-native design certainly impact SDN engineering, the operational side of SDN is likely to really benefit from the innovation happening around machine learning and AI, and these innovations also benefit from the accelerated pace of software and hardware innovation happening in prominent public clouds.”