White Paper

Software-Defined Access: Enabling a Digital Transformation Fabric for Enterprise Networks

Sponsored by: Cisco

Brandon Butler
March 2019

EXECUTIVE SUMMARY

Enterprises around the globe continue to invest in digital transformation (DX) in an effort to take full advantage of important technology innovations such as cloud computing, artificial intelligence-enabled automation, and advanced big data analytics tools. The network is a critical component for enabling enterprise usage of these technologies. Hence, as DX initiatives continue to ramp up, this increasingly leads to investments in network transformation as well. According to IDC's 2018 *Worldwide Semiannual Digital Transformation Spending Guide*, DX spending will increase from $1.2 trillion in 2019 to $1.9 trillion by 2022.

As enterprises look to upgrade their networks to enable DX, intent-based networking (IBN) has emerged as an architectural model that can address the need for greater agility, scale, and efficiency, bridging the gap between organizational needs and what IT can deliver. There are a handful of principles guiding IT's purchasing and architectural decisions. Top of mind for any technology decision is security. In a world where the threat landscape is varied and ever-changing, foundational tools can be used to help protect both users and enterprise networks. Cisco has sought to deliver intent-based networking and to address these security challenges through its Cisco Digital Network Architecture (Cisco DNA) — an open software-driven architectural model powered by intent and informed by context. Cisco DNA seeks to address the DX imperative through software-defined networking (SDN), virtualization, automation, analytics, and cloud. Within this framework, Software-Defined Access (SD-Access) provides end-to-end segmentation to keep user, device, and application traffic separate without a redesign of the network. Leveraging the machine learning ethos of Cisco's DNA framework, SD-Access allows for the automation of access policies for users, devices (wired and wireless), and applications from cloud to device and from WAN to edge.

Enterprise networks continue to be complex environments. But management platforms that leverage the latest in access policy for users, devices, and applications have enabled a new wave of innovation, driven by DX initiatives. A successful DX project, however, increasingly requires network transformation too. This includes faster enablement of not just the network infrastructure components but also — and perhaps even more important — the software-based management, analytics, and security platforms that run atop them. As enterprise networks continue to expand to new areas, complexity is the enemy of agility. These problems can be solved only with simple, intuitive, and scalable management platforms that integrate with all aspects of the ever-evolving enterprise network.

SITUATION OVERVIEW

The Digital Transformation Imperative for the Enterprise

Digital transformation leverages cloud, mobile, social, and big data technologies to improve organizational efficiency and creates new revenue streams while enhancing the customer experience. As global competition has raised requirements across many industries and all industries face continued pressure to cut costs and optimize operations, DX is not a solution in search of a problem but an enterprise imperative. To compete in the global economy, enterprises must increase organizational efficiency and agility while effectively and innovatively engaging employees and customers through 3rd Platform technologies (cloud, mobility, big data, and social business).

Organizations across the world are responding to the DX imperative. IDC's 2017 *Digital Transformation MaturityScape Benchmark Survey* found that more than 90% of the 413 responding organizations are in some stage of the digital transformation process: 27% are at the opportunistic stage of exploring new digital opportunities; 31% have established some repeatable successes as digital players; 29% have more sustained, managed DX efforts; and 7% are at the highest stage — optimized (aka "digital disruptor").

DX efforts are aimed at myriad business initiatives throughout the value chain. Table 1 breaks out the different categories of DX and where IDC measured their spend as a percentage of total DX efforts in 2015 and where it sees these percentages going in 2020.

The data in Table 1 illustrates that the benefits of DX will be far-reaching, but back-end operations and customer experience (e.g., Omni-Experience DX) are the dominant factors in today's DX investments. These will remain important in 2020, but Table 1 shows that the role of DX in transforming the use and management of data will become a more common vector of DX investment. In any case, DX is leading to a need for new enterprise IT investment. This is particularly true for the network. Consider the following: Enterprise users are increasingly mobile.

TABLE 1

Digital Transformation Spending by Business Initiative, 2015 and 2020 (%)

	2015	2020
Leadership DX	1	1
Omni-Experience DX	28	25
Information DX	19	33
Operating Model DX	49	38
WorkSource DX	3	3

Source: IDC, 2017

Cloud applications are one of the top driving factors to enterprises creating and constantly evolving their enterprise mobility and BYOD policies. Engaging in such evolution is increasingly becoming a benefit not just for operations but also for savings. According to IDC's 2018 *Enterprise Mobility Decision Maker Survey* (n = 457), over 64% of United States-based respondents indicated that their organizations have saved money as a result of having a BYOD strategy. The largest driving factor was reduction in device procurement costs, followed by savings in employee data plan costs and IT device management costs. In fact, IDC's interviews with network practitioners reveal that it is not uncommon for enterprise employees to connect three or more wireless devices to the network. The increased mobilization of common cloud-based applications (e.g., CRM, ERP, collaboration) further promotes the use of mobile devices in the enterprise. Naturally, employee-owned devices carry a degree of security risk when accessing the network and benefit from network segmentation and policy setting to ensure proper access and security protocol on the corporate network. This only increases the urgency for granular access and security policy functionality on the network.

Internet of Things Is Now an Enterprise Reality

Also contributing to this urgency for granular security is the rapid uptake of IoT devices in the enterprise network. IDC has forecast that the worldwide IoT installed base will grow from just under 15 billion in 2016 to over 30 billion by 2020 and to over 80 billion by 2025 (see *Worldwide Internet of Things Installed Base by Connectivity Forecast, 2017-2021,* IDC #US42331917, March 2017). IoT will have several effects on the enterprise network. It will flood the wireless network (and, in some cases, the wired network) with new endpoints that must be provisioned, connected, and managed. Connecting IoT devices will not necessarily be challenging from a bandwidth perspective as many IoT devices have low data rate requirements.

The true challenge with IoT on the enterprise network, however, is twofold. First, IoT devices are headless; once connected to the network, they access it without human intervention. Second, the scale at which IoT is penetrating many enterprise networks is untenable for manual configuration and policy setting. A new paradigm of automated and flexible network segmentation, policy management, and security enforcement must emerge so that networks can support IoT without interruption, limiting where IoT devices go on the network so that they do their jobs without introducing new risks. In the case of a security threat or breach, enterprise IT must be able to react quickly to thwart bad actors and prevent future attacks.

Applications Are Shifting to the Cloud

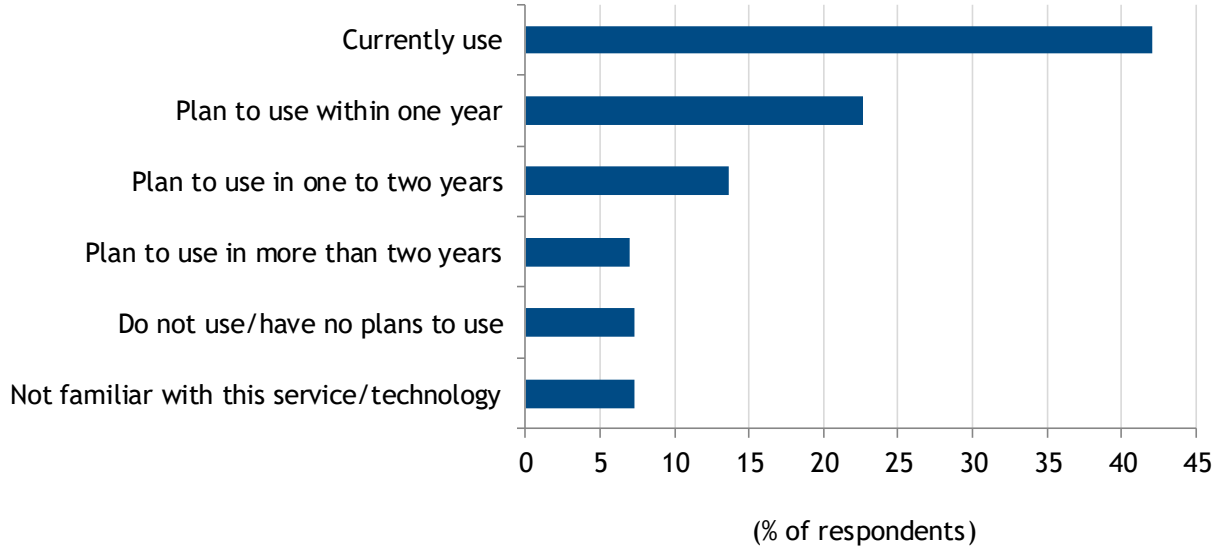
Increasingly, applications are hosted not in an on-premise datacenter but out in the cloud as SaaS, IaaS, or PaaS. Delivering applications from the cloud has become a strategy frequently employed by enterprises in their quest to offer greater efficiencies and to improve the customer experience. Mobile-enabled and stationary cloud applications (e.g., Microsoft Office 365, Salesforce) are breaking down barriers regarding time and place, allowing employees to seize opportunities to create value as they arise. Figure 1 highlights enterprise adoption of SaaS applications in United States-based organizations now and in the near term to midterm.

All the previously profiled categories of DX are driven in part by the proliferation of public cloud applications and thus depend on a robust network infrastructure. This means that the enterprise network must be ubiquitous, carrying the highest service levels to keep the digital business up and running. In addition, cloud applications elevate the role of user and application policies on the network. The ability to set, monitor, and adjust nuanced access policies and security measures at user, device, and application levels is critical to network performance and uptime, as well as the protection of sensitive data.

FIGURE 1

Enterprise Adoption of Software as a Service/Cloud Computing

Q. *Software as a service (SaaS)/cloud computing — Are you implementing or do you plan to implement any of the following services/technologies?*



n = 1,201

Base = all respondents

Notes:

This survey is managed by IDC's Quantitative Research Group.

Data is not weighted.

Use caution when interpreting small sample sizes.

Source: IDC's *U.S. Enterprise Communications Survey,* March 2017

Security and Compliance

The explosion of mobile devices, IoT, and cloud in the digital enterprise has increased the threat surface dramatically, leading to new security and compliance challenges. The ability to provide granular segmentation and access control for users, devices, applications, and things is a critical first step in complying with regulations and preventing the downtime and compromising of data associated with a security breach. With the rise of outside devices and public cloud applications, the network security perimeter has moved from the enterprise edge to the public cloud. Threat defense now must take on both an "outside in" approach and an "inside out" approach while being natively integrated throughout the network stack.

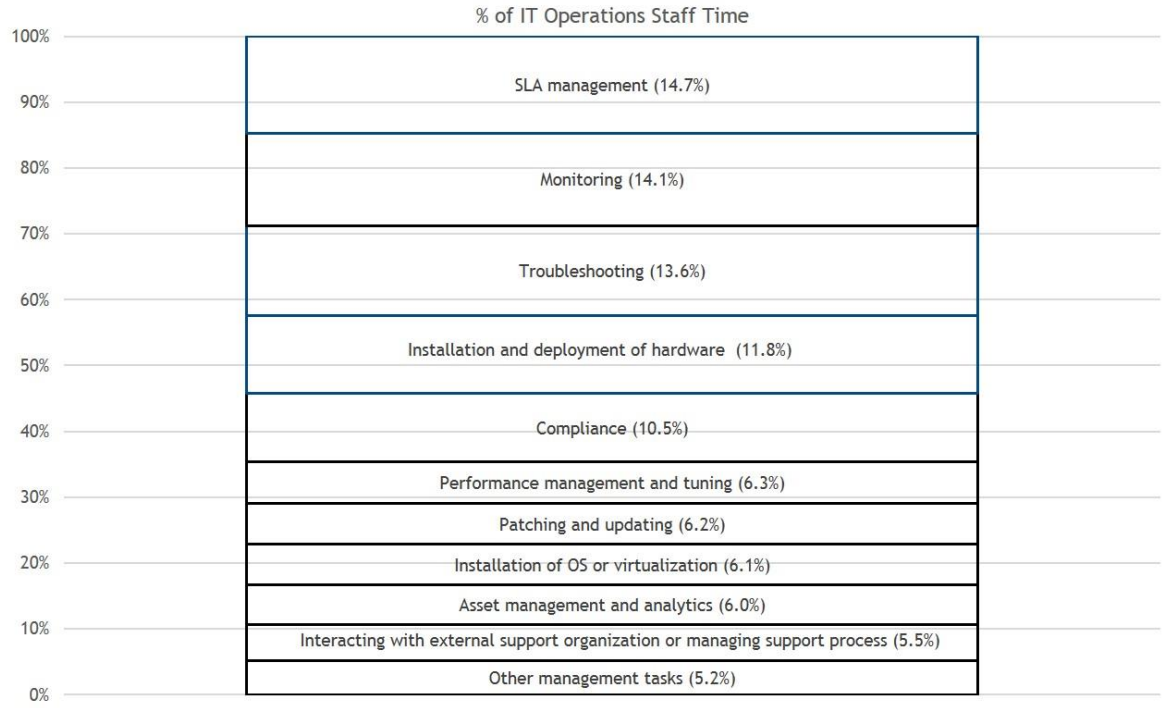
Enterprises Embrace Automation

While IoT is one of the main factors elevating the importance of automation in network provisioning and configuration, automation is a force that is being seen across the enterprise. Artificial intelligence, machine learning, and robotics are leading to new business value opportunities across all verticals as task automation

promises significant opex reduction. The growth of enterprise automation has a two-sided impact on the enterprise network. First, the network must securely support automation applications. Second, enterprise IT desires to realize the benefits of automation on network operations and management. It is also worth reiterating the established relationship between headless endpoints, such as IoT and many robotics devices, and network automation and programmability. Automation is a necessary component of achieving true DX within every function of enterprise IT. Figure 2 demonstrates how the majority of IT staff time in many organizations is spent on manual tasks. IDC believes that most enterprises will embrace automation as a means to redirect IT staff time to more strategic, business initiative–oriented work.

FIGURE 2

IT Operations Staff Time Allocation by Task



Note: For more information, see *The Impact of Automation on Network Consulting and Integration Services* (IDC #WC20170525, May 2017).

Source: IDC, 2017

What Will Be Required of the Enterprise Access Network?

The rapid shift of applications to the cloud and the emergence of the mobile internet and IoT necessitate that the application access network evolves to better serve the new paradigm in terms of performance, security, reliability, and efficiency. Otherwise, many DX opportunities are at risk of being missed. This is because legacy network infrastructures do not meet the scalability, flexibility, and manageability requirements of the digital enterprise.

Many enterprises still manage discrete LANs and WLANs, alongside siloed WAN connectivity, and they do so manually. However, cloud and mobility have rendered the WLAN equally mission critical to business operations, with DX only accelerating this trend. The need for more holistic policy setting, network monitoring, and threat detection across increasingly distributed networks (including remote workers) mandates a new level of convergence that combines wired and wireless LAN, WAN, and cloud with single-pane-of-glass management and visibility and dynamic policy configuration for the full campus and branch network stack. With end users accessing public cloud applications over wired and wireless LANs, the interplay between the WAN, the cloud, and the LAN is at unprecedented levels. Thus, a consistent and converged policy, security, and quality-of-service (QoS) management framework becomes necessary.

This raises an important point: The WAN architecture also needs to evolve to serve the new application access requirements. Because cloud and mobility are foundational to DX, the shortcomings of the traditional enterprise WAN have come into focus. The traditional branch-centric WAN, which came of age in the client/server era, was not architected for the cloud, nor was it intended to facilitate DX. A new WAN paradigm is required for digital success. To this end, first there was "hybrid WAN," a WAN architecture that included at least two WAN connections from each branch office, leveraging two or more different networks (e.g., MPLS, 4G/LTE, broadband internet). More recently, the idea of hybrid WAN has been extended to the more transformational architecture of software-defined WAN (SD-WAN).

SD-WAN leverages hybrid WAN in an active/active configuration and also includes a centralized, application-based policy controller; analytics for application and network visibility; a secure software (virtual) overlay that abstracts the underlying transport networks; and an SD-WAN forwarder (routing capability). These technologies are combined in the SD-WAN to provide application-driven intelligent path selection across WAN links (MPLS, broadband internet, LTE, etc.) based on policies centrally defined on the controller. The business benefits of SD-WAN should include providing cost-effective delivery of business applications, satisfying the requirements of the modern branch/remote site, accommodating SaaS- and cloud-based applications and services, and improving branch IT efficiency through automated service provisioning. Another critical benefit that should derive from SD-WAN involves meeting the demands of application SLAs, which directly results in greater enterprise productivity and business agility. Figure 3 provides enterprise end-user considerations of SD-WAN benefits.

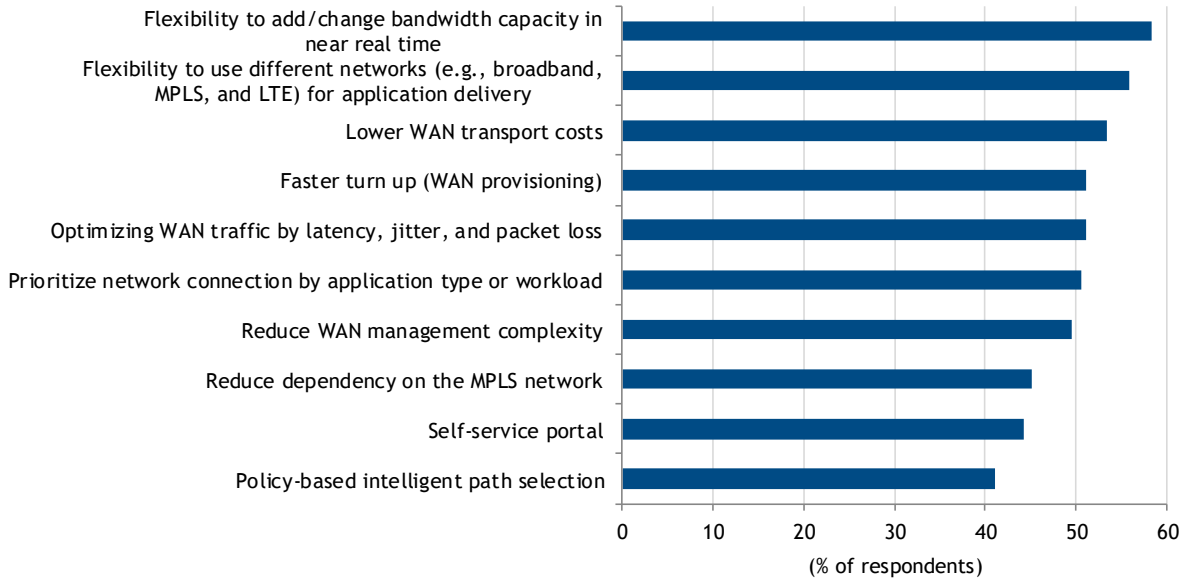
These benefits do not have to stop at the WAN. Integrating SD-WAN with a broader software-defined enterprise campus network infrastructure for end-to-end policy automation (core to campus to remote branches) will also be important for DX. Enterprises will be required to be agile in spinning up new branches and adjusting policy and security rules in an ever more dynamic environment. The ability to propagate policy context (i.e., network segmentation and identity) will be a critical new requirement for branch automation.

According to IDC's March 2017 *U.S. Enterprise Communications Survey* (n = 772), end-user organizations are seeking myriad potential benefits from SD-WAN as they bring their networks up to speed for the digital era. At the same time, this talk of benefits goes far beyond casual discussion. The emerging worldwide SD-WAN infrastructure market (comprising the hardware and software used to enable SD-WAN) recorded revenue of $1.3 billion in 2018 and is expected to grow to $4.5 billion by 2022, representing a significant early uptake (see *Worldwide SD-WAN Infrastructure Forecast, 2018–2022,* IDC #US44182618, August 2018). IDC believes this reflects two important trends: the cloud, mobile, and IoT-driven digital transformation of the enterprise and the growing comfort of the enterprise campus and branch with adopting software-defined network architectures.

FIGURE 3

SD-WAN Selection Criteria

Q. Which of the following attributes of an SD-WAN service or solution are the most important considerations when choosing an SD-WAN solution for branch office connectivity? Rank order from 1 to 5, with 1 the most important.



n = 772

Base = respondents who indicated their organization plans to deploy SD-WAN as an overlay framework on existing WAN/network connections within two years

Notes:

This survey is managed by IDC's Quantitative Research Group.

Data is not weighted.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

Source: IDC's *U.S. Enterprise Communications Survey,* March 2017

SDN Starts to Take Hold in the Enterprise Campus and Branch

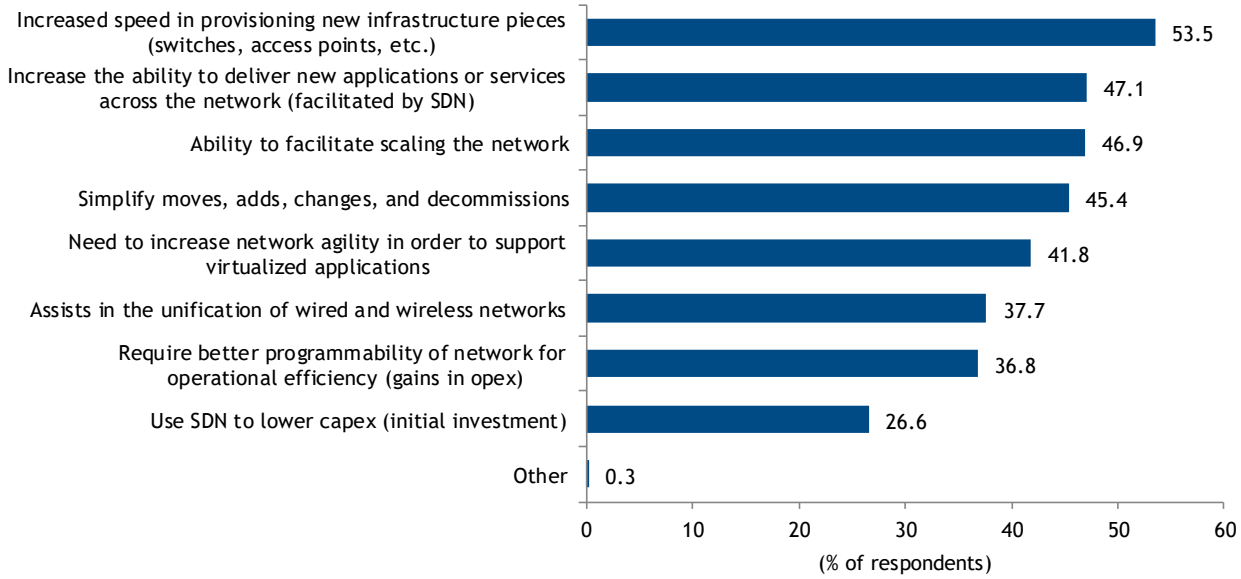
Software-defined network is an emerging architecture that decouples the network control and forwarding functions, enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services. This dynamic, manageable, cost-effective, and adaptable architecture helps better align network infrastructure with the needs of application workloads through automated (thereby faster) provisioning; programmatic network management; application-oriented, networkwide visibility; and direct integration with cloud orchestration platforms. These capabilities can translate into significant operational savings while providing adopters with the means of achieving expeditious time to business value.

The earliest adoption of SDN was in the datacenter, but unsurprisingly, the promise of greater IT agility and flexibility alongside lower operating costs is also compelling to enterprise campus and branch network decision makers. In IDC's *Campus Network Innovation Survey,* enterprise network decision makers were asked to choose from a list of potential campus SDN benefits, indicating their most motivating factors for considering campus SDN. Figure 4 illustrates their responses.

FIGURE 4

Ranked Drivers for Campus Network SDN

Q. Which of the following factors is the primary motivation for considering or implementing SDN in the campus network?



n = 240

Base = respondents who indicated their organization has deployed/plan to deploy SDN

Notes:

This survey is managed by IDC's Quantitative Research Group.

Data is weighted by number of companies.

Multiple responses were allowed.

Use caution when interpreting small sample sizes.

Source: IDC's *Campus Network Innovation Survey,* October 2015

What Is Software-Defined Access?

There is great reason to believe that as organizations look to increase network flexibility and agility through automation, programmability, and single-platform control of wired and wireless environments alongside WAN convergence, they will look for SDN solutions oriented toward the campus and branch access network; in other words, "software-defined access." And these solutions have begun to emerge slowly. Whether a campus or branch prefers to deploy a more open source–type deployment or a more

proprietary single-vendor architecture, more options are becoming available. Before delving into the benefits and considerations of software-defined access, we need to establish a definition.

IDC defines "software-defined access" as being able to provide consistent and secure access (to any user, endpoint device, or application) through the application of SDN's data-plane and control-plane abstraction to enterprise campus and branch network infrastructure, such as Layer 2–3 Ethernet switching, WLAN access points and control infrastructure, and access routers. While many SDN topologies heavily leverage open source SDN controllers and standardized hardware such as white-box switching, software-defined access infrastructures can also be designed from proprietary network infrastructure.

Key Benefits of a Software-Defined Access Approach

The innovation that a software-defined access approach can bring first arises from the separation of the intelligent functions of software from hardware. This allows for a centralized software platform to provide end-to-end network control and visibility for all the elements that have been abstracted. In research into this emerging technology, IDC has noted the high potential for several critical benefits:

- **Increased security and compliance.** SD-Access provides a framework for integrated threat defense by allowing a suspicious user to be "quarantined" networkwide. In addition, the automation of security policy propagation will be necessary for dealing with the scale of IoT. An SD-Access framework allows rapid and consistent policy updates across the entire network regardless of the location, VLAN, or IP address of a user, a device, or a thing. At the same time, insights and telemetry can harness the power of analytics to proactively identify and resolve security issues.
- **Reduced cost and increased agility.** The benefits of SDN such as programmability, automation, and unified visibility ultimately promise reductions in capex and opex. Moving former hardware functions into software can greatly reduce capex in new network infrastructure, while automation, programmability, and unified visibility have the potential to reduce IT department staffing costs (while potentially redirecting IT staff efforts to more proactive, business value–generating projects). Moreover, network upgrades and changes can be achieved through centrally administered software updates instead of time-consuming manual reconfiguration of hardware. This helps minimize network downtime and provides enterprise IT more capacity to work on longer-term strategic initiatives. Furthermore, a complete software-defined access solution will support a broad range of standards-based northbound and southbound APIs, customizing the enterprise network with all the network services required for digital success.
- **Enhanced monitoring and troubleshooting.** Centralized SDN controllers provide visibility into all network elements, encompassing wired and wireless and cloud connectivity through the WAN. This provides better ability to monitor the network and ensure that it is running as expected, enabling faster detection — and remediation — of network anomalies. Unifying wired, wireless, and the cloud connection through the centralized controller also means that consistent access and QoS policies can be applied to applications regardless of how or where they are being accessed. In addition to unifying visibility and policy control for the wired and wireless LAN, SDN is also a framework for automation of policy and QoS enforcement across the unified network.

Considering Cisco

Cisco has recently introduced its Software-Defined Access solution as part of its centralized network management framework Cisco DNA Center. SD-Access is designed to bring the demonstrated benefits of SDN to the enterprise campus and branch, leveraging years of Cisco research and innovation as well as the foundation of Cisco's long history in enterprise networks.

Cisco SD-Access provides end-to-end segmentation to keep user, device, and application traffic separate without a redesign of the network. It automates user policy so that organizations can make sure the right policies are set for any user or device with any application across the network. This is done with a single network fabric to enable a consistent user experience anywhere without compromising on security, meaning common user policy for LAN, WLAN, WAN, and cloud.

Cisco's Strategic Approach

As a longtime leading vendor in the enterprise access network space, Cisco needed to provide an agile software-defined access network solution that could respond to the DX imperative. Cisco SD-Access is just one element of Cisco's recent innovations in enterprise campus and branch networking (see Figure 5). At its foundation is the notion of intent-based networking. Intent-based networking uses machine learning, cognitive computing, and deep analytics to build intuition throughout the network topology. This deep understanding of the network's operation, in turn, helps the infrastructure baseline the network's "normal," anticipating actions and improving security through faster anomaly detection and self-healing. This detection of variances from baseline operation also allows end-to-end policy automation across wired and wireless. Cisco's recent innovations include:

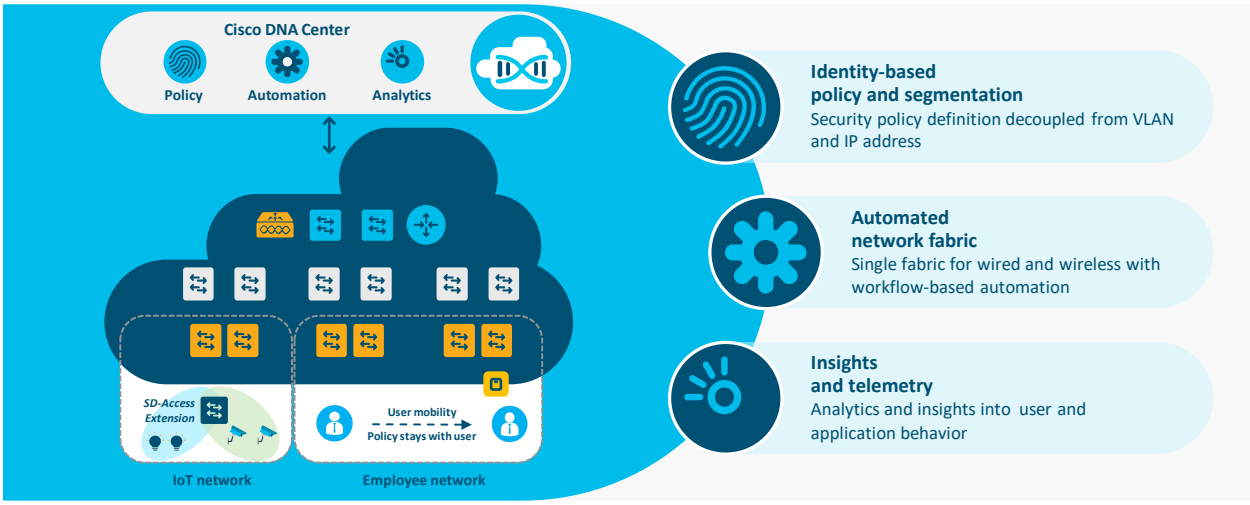
- **Cisco Digital Network Architecture.** Cisco Digital Network Architecture is an open and extensible, software-driven architecture that simplifies and accelerates the enterprise network architecture. Leveraging the benefits of programmability, automation, and analytics, Cisco DNA can benefit IT staff by allowing them to spend less time on manual, repetitive, and reactive network configuration and troubleshooting tasks, instead focusing on proactive, future value-creating strategic initiatives that better align the network with business outcomes. Cisco DNA is designed with foundational security in mind, reducing gaps between network infrastructure and security tools and allowing network security staff to spend less time on reactive and remedial tasks. Cisco DNA also provides IT visibility into the activities of users, devices, and applications. This visibility can provide insights for improved business decisions.
- **Cisco DNA Center.** The result of rewriting over 20 years of code for the digital era, Cisco DNA Center is Cisco's new overarching management framework that incorporates elements from Cisco's first campus and branch SDN framework – APIC-EM – and Cisco's incumbent Prime network management software. The goal of Cisco DNA Center is to "manage the [enterprise] network as one entity," ensuring command of network design, policy, provisioning, and assurance.

  With a user-friendly interface as its backdrop, Cisco DNA Center allows enterprise IT to design the network using intuitive workflows and set secure policy through drag-and-drop, granular user and device profile-based network segmentation. Cisco DNA Center relies on the deep analytics and machine learning capabilities of intent-based networking to provide service assurance and proactively monitor, troubleshoot, and optimize the network. In an acknowledgment of the realities of digital era networking, Cisco has introduced native third-party integrations for select security tools in Cisco DNA Center, such as Palo Alto Networks firewalls and Tufin security management.

- **Fabric-based topology.** SD-Access is enabled through a single network fabric and controller-based management via Cisco DNA Center with single-pane-of-glass orchestration and visibility.
  The fabric consists of a programmable overlay connecting users and devices with a standards-based control plane (enabled through Cisco's LISP routing protocol) and a VXLAN-enabled and standards-based data plane. VXLAN is an encapsulation protocol that enables network segmentation at scale, addressing the limitations of legacy VLAN segmentation in the mobile and IoT era. In most cases, VXLAN allows for the usage of legacy infrastructure, reducing the likelihood of a rip-and-replace effort.
- **Group-based policy.** A mechanism that supports Cisco's network segmentation and policy automation capabilities, group-based policy allows network administrators to group devices and users, regardless of IP address or VLAN, within Cisco DNA Center through Cisco TrustSec technology. This promises to reduce the friction of granular policy setting that is experienced on many legacy networks.
- **Assurance.** End-to-end assurance is a differentiating tenet of Cisco SD-Access. Through machine learning and fabric-orchestrated intent, SD-Access provides proactive operations and predictive network optimization that affect not only the network at large but also the individual client and application. Moreover, assurance is both underlay and overlay aware.

FIGURE 5

Cisco's Vision of Software-Defined Access



Source: Cisco, 2017

Value Proposition of Cisco SD-Access

IDC believes that there is a strong value proposition behind SD-Access. The enterprise network has become the backbone that enables end-to-end business operations. As such, the network must perform with consistency and robustness with high levels of security and service assurance. Just as important are the underlying mechanisms that allow for high service and security levels. By providing intuitive, single-platform, and drag-and-drop user, device, and application traffic segmentation, Cisco SD-Access

leverages a network fabric to provide enterprise IT with a simple means of ensuring a secure, always-on network with application prioritization. Additional benefits of SD-Access include:

- **Policy-based automated network provisioning from cloud to edge.** Distributed network topologies and the widespread use of cloud-hosted "as a service" applications require more policy consistency from cloud to edge. IoT deployments, at scale, make automated provisioning an absolute necessity so that IoT devices stay where they are supposed to on the network and are not exposed to forces that could lead to a breach.
- **Open APIs and turnkey automation.** SD-Access leverages open APIs and turnkey automation to quickly enable both third-party and in-house-developed network services, spanning a wide range of functions.
- **Wired, wireless, and WAN as a unified entity.** IDC has long noted the benefits that wired and wireless unification can bring to the enterprise network, with better visibility, uniform application policy setting, and reduced time to remediation being chief among them. In the age of the cloud-hosted SaaS applications consumed through the web, WAN visibility must be brought into this equation. The Cisco SD-Access network fabric enables a consistent user experience for wired and wireless LAN, WAN, and cloud.
- **Machine learning and analytics to fuel user experience.** The combination of Cisco SD-Access network fabric, unified policy setting, and Cisco DNA's underlying analytics and assurance engine means that users enjoy a consistent experience regarding QoS and access capabilities.
- **Potential to lower opex.** Cisco SD-Access generally does not require a "rip and replace" to be implemented. In most cases, existing Cisco customers can layer SD-Access onto their current Cisco infrastructure and immediately start harnessing the benefits of programmability, automation, unified network fabric, and analytics-based baselining and remediation.

Overall, SD-Access is a solution with many promising benefits well suited to the needs of the digitally transforming enterprise. With Cisco DNA underpinnings enhanced by programmability and machine learning, SD-Access is well positioned to continually evolve in lockstep with the needs of users, devices, and applications on the enterprise network. The viability of any software-defined access solution will be measured by its ability to be applied seamlessly from end to end on the network, its ability to port credentials and authorization from AAA systems and, ultimately, its ability to deliver lower opex.

CHALLENGES AND OPPORTUNITIES

There are challenges that Cisco will need to address with customers if they are to be successful with the SD-Access strategy. First, unlike many SDN-oriented solutions, Cisco SD-Access runs on proprietary network infrastructure. This may not appeal to enterprise network decision makers who have come to abide by a "best of breed" multivendor approach. In this case, Cisco must demonstrate its proof points as to why the single-vendor approach would work well for any given customer. It is worth noting again, however, that Cisco is allowing for strategic third-party software integrations through Cisco DNA Center. In addition, Cisco SD-Access represents several changes for many traditional Cisco networking customers.

While automation, programmability, and machine learning have many proponents touting a number of anticipated benefits, there are also those that fear the obsolescence of certain networking skill sets and jobs as these technologies rise. It is incumbent upon advocates of SD-Access and similar technologies to use this transition as an opportunity to thoroughly train networking professionals on

how to manage networks in the coming era of end-to-end SDN. An important part of this is orienting networking teams to the opportunities that can arise amid moving from the reactive and manual "keeping the lights on" style of management for legacy networks to the more proactive and strategic style that is becoming associated with SDN. There is a real opportunity for networking professionals to learn new skills, especially programming skills, while learning how to work more closely with the lines of business to affect organizational strategies. This mindset shift must begin with a real commitment from the C-suite to making DX and SDN work for everyone in the organization.

CONCLUSION

The explosion of users, devices, applications, and data that DX is bringing to enterprise networks worldwide has created urgency for enterprise network practitioners to evaluate their network topologies and ensure that they are equipped for DX. This means a constantly growing and shifting ecosystem of devices and applications are supported amid transformation. Gone are the days when LAN, WLAN, WAN, and cloud functioned in disparate silos. Today's network requires end-to-end visibility, programmability, and automation to dynamically ensure performance, security, and user experience for a unified wired and wireless network connected to many clouds. Also, today's network architecture requires the agility for enterprise IT to quickly make changes and adjustments when needed. IDC believes that Cisco Software-Defined Access provides the visibility, programmability, automation, segmentation, and intent-based networking capabilities that can support a network throughout its digital transformation journey and beyond.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com