PCM THE RIGHT TECHNOLOGY, DELIVERED™

NEXT GENERATION NETWORKS FROM PCM AND CISCO

Cisco Catalyst 9000 and DNA Center

ABSTRACT

Despite the promising USD 1.77M budgeted for Cloud spending in 2017[1], enterprises worldwide continue to ponder, “How can I lower the cost of managing network infrastructure in this increasingly complex world?”

There are no straight answers. Very few have embarked on this journey, confident that the solution chosen will be able to scale as the enterprise grows, and deter the many security threats that come its way. Yet, the emergence of virtual networks, ubiquitous connectivity, and an expanding device ecosystem have placed network engineers at the crossroads.

In this regard, Cisco’s new Digital Network Architecture (DNA) has been developed keeping these technological breakthroughs in mind. This paper discusses how the hardware and software components of the solution can help enterprises modernize their network and align with a rapidly-developing digital paradigm.

[1] *Forbes, Analytics, Data Storage Will Lead Cloud Adoption In 2017 accessed 24 August, 2017, https://www.forbes.com/sites/louiscolumbus/2016/11/20/analytics-data-storage-will-lead-cloud-adoption-in-2017/#4edfdce97e7a*

THE EXPANDING NETWORK FOOTPRINT

Although an enterprise network forms the backbones of IT operations, CIOs only seem to consider it when there is a serious issue to address. Digitization may have rewritten the rules of network management, but the mounting number of security breaches illustrate a stilted security posture requiring immediate intervention. To further complicate matters, the emergence of software defined networks (SDN), mobility, Cloud, video, and IoT pose a pertinent question – "Are mature networks built on the foundation of rapidly ageing hardware able to handle these new imperatives?"

Just consider the Cloud. It has established itself as a business enabler which can level the playing field, allowing small and medium companies to access previously unattainable IT capabilities. This has amplified competition across sectors, especially in response to increased customer expectations in terms of better connectivity, greater speed, and flexibility. Simply migrating to a dynamic, digitized, and always-on network, in order to follow these trends, however, comes with its own inherent set of risks.

Network administrators consider universal connectivity as the gateway for devastating security threats. According to recent reports, traffic from wireless and personal mobile devices will account for 63 percent of total IP traffic by 2021.[2] As enterprises embrace the mobile workforce culture by introducing BYOD and pro-nonlocal data access policies, the complexity of network operations is expected to increase phenomenally. The expanding device ecosystem and a growing number of users and applications will be generating an incessant stream of event and usage data.

To support remote access without compromising on network security, administrators will need mechanisms in place for authenticating and controlling user devices, while shielding enterprise data from unwanted access. Gartner predicts that over the next two years, IoT manufacturers will no longer be able to operate through weak authentication methods. This will open up the scope for launching attacks through connected devices.[3] After all, the average corporation experiences as many as two to three external cyber threats per month,[4] and 60% of these breaches are attributed to internal attacks.[5]

Given the gravity of the situation, enterprises must rethink their approach towards architecting the next generation, future-proof enterprise network. Although the conventional network quality parameters like availability and performance continue to be forms of worker and customer interaction. This, in turn, would entail simplifying and automating network operations, without taking the human operator out of the mix, and freeing them up to focus on more critical tasks.

[2] *Cisco, The Zettabyte Era: Trends and Analysis, accessed August 23, 2017, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf*
[3] *Gartner, Gartner's Top 10 Security Predictions 2016, accessed August 23, 2017, http://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/*
[4] *SC Media, The average company experiences two to three cyber-attacks per month, accessed August 22, 2017, https://www.scmagazineuk.com/the-average-company-experiences-two-to-three-cyber-attacks-per-month/article/570759/*
[5] *Harvard Business Review, The Biggest Cybersecurity Threats Are Inside Your Company, accessed August 22, 2017, https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company*

THE NETWORK EFFECTIVENESS GAP

Clearly, digitization is the new norm across industries. Worldwide spending is expected to hit USD 1.2 trillion in 2017 and climb to USD 2.0 trillion by 2020.[6] While enterprises work towards building a transition roadmap, they must take note of the tremendous innovations in networking – model-driven programming, network function virtualization (NFV), overlay networks, and open APIs. While they do offer enhanced operational efficiency and enable digital applications, adoption has been hindered by the difficulty of integrating critical functionalities such as automation, analytics, Cloud service management, and open and extensible programmability into a single unified architecture.

Large scale adoption of Cloud-based services, federated network applications, and the integration of IT with the supply chain continue to proliferate the number of edge devices connected to the network. This will diversify network topology and drive up the volume of data flowing in from these endpoints. This puts network administrators in a tight spot – managing the security of a network whose footprint is continually expanding while supporting many more devices per IT personnel.

For the enterprise, this means an additional USD 60 billion spent every year on network operation labor and tools.[7] It is an alarming situation as 95 percent of network changes are still performed manually, wherein 70 percent of policy violations occur as a result of human errors. Monitoring and troubleshooting these issues rapidly burn through 75 percent of the allocated OPEX budget.[8]

This is further exacerbated as the existing enterprise infrastructure is fragmented to a point where they tend to become progressively more opaque the closer it gets to the edge. This limits visibility required for predicting and detecting threats and responding to incidents. Reportedly, companies take approximately 191 days to detect malicious breaches and another 66 days to contain them. The average cost per breach can add up to an average of USD 3.62 million.[9]

Traditional firewalls are inadequate for maintaining network security posture, especially considering the highly diversified IT landscape of the 21st century enterprise. As BYOD, enterprise IoT, and services running on public Cloud blur the network's perimeter, it further expands the attack surface and increases risk exposure to sophisticated threats like encrypted malware and Zero-day exploits. Such threats are becoming harder to deter, or even comprehend since the underlying motives have evolved to include corporate espionage and intellectual property theft.

There is no denying that running applications in the Cloud offers immense cost benefits — virtualizing large swathes of the IT infrastructure and accommodating on-demand provisioning of computing power; however, there are significant drawbacks in terms of enterprise data security and vendor lock-in. The model relies entirely on the integrity of the network between users and the Cloud. As such, network administrators must have the capabilities to isolate resources, prevent misuse, and maintain confidentiality.

6IDC, IDC Forecasts Worldwide Spending on Digital Transformation Technologies Will Surpass $2 Trillion in 2019, accessed August 23, 2017, https://www.idc.com/getdoc.jsp?containerId=prUS40978116
7Cisco, A Smarter Way to Switch, accessed August 21, 2017, https://www.cisco.com/c/dam/en/us/products/collateral/software/one-subscription-switching/cisco-one-switching-infographic.pdf
8Cisco, TechWiseTV dives into Enterprise Service Automation and Easy QoS, accessed 23 August, 2017, https://blogs.cisco.com/cin/techwisetv-dives-into-enterprise-service-automation-and-easy-qos
9IBM, Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview, accessed 22 August, 2017, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

Considering most businesses move to the Cloud to reduce cost and bypass disruptions caused by planned and unplanned downtime, enterprises often don't factor in tools, automation, and orchestration for fortifying network security posture. The underlying reasons might vary between human error, cyber-attacks, and maintenance requirements, but IT downtime can cost companies as much as 17 percent of their annual revenue.[10] The cloud is almost never the complete solution because organizations must still secure their data and provide network connectivity, and security to wired and wireless devices within their organization.

The Cisco Catalyst 6500 has been the widely accepted industry standard switching platform central to campus, data center, WAN, and Metro Ethernet networks since its introduction in 1999 and has a $42 billion installed base, nearly 700,000 systems/110 million ports deployed and more than 25,000 customers worldwide.[11] For years the platform has set the bar becoming the first modular switch to showcase 40 Gigabit Ethernet interoperability in November 2010. However, the installed base is ageing rapidly and with the emergence of IoT, the need to revise enterprise network architectures is more critical than ever before.

A BLUEPRINT FOR A FRICTIONLESS NETWORK

The answer lies with Cisco's new Digital Network Architecture (DNA) which is poised to rewrite the network management playbook. It offers a new blueprint for extending the capabilities of the existing network to accommodate data centers, and Cloud and IoT infrastructures without compromising on availability, scalability, and performance. Supported by Cisco's Catalyst 9000 series of switches, the DNA infrastructure is designed to deliver network services that enable:

- Frictionless connectivity
- Security service that protect data and meaningfully gate user access
- Digital services for optimizing business applications
- Management services which lower operational cost

In effect, the DNA blueprint provides a platform which delivers digital solutions, empowering a mobile workforce while simplifying IT operations required for supporting it. The backbone of this new network architecture is the Catalyst 9000 which comes in three different versions — enterprises can choose from these, depending on the density and bandwidth required (Table 1).

[10] *Networking, The High Price Of IT Downtime, accessed 22 August, 2017, http://www.networkcomputing.com/networking/high-price-it-downtime/856595126*
[11] *Cisco, Cisco Readies Most Widely Deployed Network Switch to Tackle Next Decade's Networking Challenges, accessed 03 October, 2017, https://newsroom.cisco.com/press-release-content?articleId=434026*

PCM THE RIGHT TECHNOLOGY, DELIVERED™

NEXT GENERATION NETWORKS FROM PCM AND CISCO

Cisco Catalyst 9000 and DNA Center

Device	Description	Key Differentiators
Catalyst 9300	Fixed, stackable, switching access platform with modular 8x10G uplinks and power supplies capable of supporting 2.5G/mgig density	• Encrypted Threat Analytics for malware detection using behavioral and pattern recognition on encrypted traffic without the need of decrypting the application • Programmable everything with x86 CPU complex, programmable ASIC and programmable OPEN IOS-XE • Model-driven programmability and streaming telemetry • Inbuilt RFID and blue beacon capabilities • Highest UPOE density in the industry along with Perpetual PoE • Capability to create and manage applications that can be locally hosted on the switch in a container-based hosting environment • Converged wired and wireless network services across security (segmentation, Policy, ETA) for both user-operated and IOT devices.
Catalyst 9400	Modular access enterprise switching platforms that deliver state-of-the-art HA and supports up to 9Tbps	
Catalyst 9500	Fixed core and aggregation switching platform that is the foundational building block for software-defined access	

Table 1: A Smarter Way to Switch

This new product series leverages Cisco's UADP 2.0 ASIC, a new x86-based CPU with container based app hosting and the converged operating system, along with the open and programmable Cisco IOS® XE software. This promises to deliver advanced security and programmability capabilities. With network-based telemetry, the Catalyst 9000 acts as a threat sensor by feeding encrypted traffic data into a machine learning and behavior analytics engine to detect malware and support cryptographic audits.

For Cloud and mobility readiness, the Catalyst 9000 series come with a ready DevOps toolkit for zero-touch provisioning and model-driven programmability. These also ensure high network and application availability by supporting on-box app hosting and in-service software updates for rolling out system and security patches. In terms of enabling IoT convergence, the switches are embedded with NBAR and NetFlow for enabling full application delivery control (AVC). In addition, the integrated encapsulated remote switched port analyzer (ERSPAN) deliver unmatched IP surveillance, monitoring, and forensics for enhancing network security and device traceability.

THE CORNERSTONES OF PROGRAMMABILITY, SECURITY, AND ACCESSIBILITY

- RESTful interfaces, NETCONF-YANG, RESTCONF for device programmability
- APIC-EM – Cisco's flagship network service orchestration and operations tool. Essentially an SDN controller for enterprise LAN and WAN networking, it contains a policy-modeling engine that translates best practices sourced from Cisco Validated Design catalog into software controls.[12]
- Prime Infrastructure, Application Visibility and Control (AVC) or the WAN Automation Engine (WAE) for automation, orchestration, and managementfrom Cisco Validated Design catalog into software controls.

Since the network infrastructure itself is the enabler for digital transformation, it must support faster deployment of network devices and services, intuitive user management, and efficient troubleshooting. In this context, Cisco's DNA Center acts as a centralized network management application for handling end-to-end networks across the campus, branch, and WAN to the Cloud. Using structured workflows, DNA Center makes it easy to design the network, automate provisioning of new devices, simplify management of user policy, and diminish network downtime.

Integrating with APIC-EM, the network controller can deliver a policy-based, automated software-defined access (SD-access) network within the Cisco Network Data Platform (NDP). It accumulates streaming telemetry data, traditional NetFlow records, Simple Network Management Protocol (SNMP) events, and syslog information in real time to continually monitor device, user, and application performance. Once the data aggregation process concludes, the system establishes a baseline which is then used for performing network analysis – identifying outliers through event evaluation and correlation. This ultimately helps network administrators quickly discover root causes and determine the best course for issue resolution. The data can be drilled down even further, rendering it instantly actionable through the Assurance functions within Cisco DNA Center. The analytic insights are fed directly into the unified dashboard where they are aligned to specific tasks, thus enabling better service management.

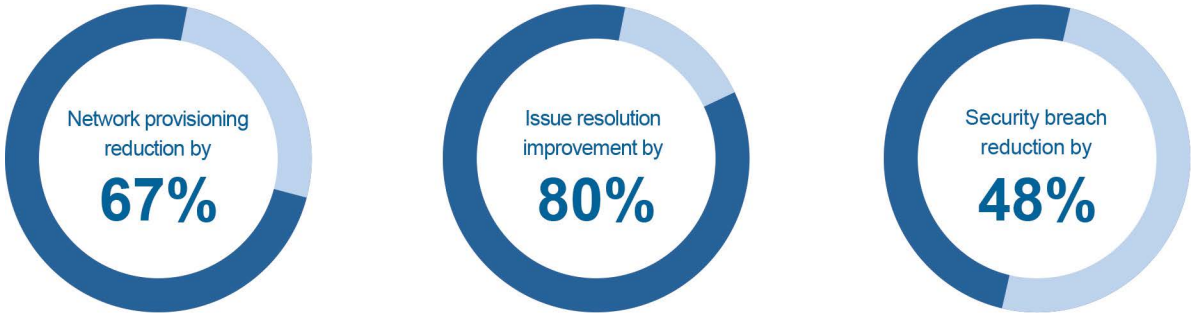
To further augment the security posture of the network, accelerate BYOD policy implementation, and enhance access control capabilities, enterprises will need to reimagine their approach towards managing user identities. In this regard, Cisco® Identity Services Engine (ISE) simplifies access control across wired, wireless, and VPN connections. Enabled by edge sensors and expansive user profiling capabilities, ISE provides superior visibility into who and what are accessing enterprise resources. It can share vital contextual data using technology partner integrations and can transform networks from a simple conduit for data into a security solution that ensures rapid threat containment. In combination with Cisco TrustSec®, ISE can also enforce role based access control at the routing, switching, and firewall layer by leveraging dynamic, software-defined user segmentation.

12 Cisco, Cisco Launches APIC-EM Controller for LAN and WAN Service Orchestration, accessed 03 October, 2017, https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/application-policy-infrastructure-controller-apic/ema-impact-brief.pdf

DIMINISHING OPEX, ENHANCING SECURITY

For network engineers, the Cisco DNA Center serves as a single view dashboard for monitoring end-to-end network performance. By rewiring the network as a software-driven, automated entity with built-in encryption capabilities and analytics, it enables scalability and reduces OPEX by 61%.[13]

With a logical workflow to design, provision, and set policies, network engineers can leverage the integrated, analytics-driven NDP to predict problems before they occur, and respond to changes faster —reducing overall downtime. The solution is also capable of discovering threats in encrypted packets at wireline speeds, leading to:[14]



This also eases the process of managing hardware and software lifecycles, helping IT meet compliance requirements and systematically plan for upgrades and refreshes. Moreover, the solution brings down the cost of managing network infrastructure by up to 70%, leveraging policy management and deployment instead of IP address tracking and other complex methodologies.

The Catalyst 9000 hardware itself is a resilient infrastructure, optimized for mGig access and designed to deliver unmatched universal power over Ethernet (UPOE) scalability. With an x86 CPU architecture, it makes room for faster MAC learning, thereby improving the enterprise's network security.

Built for scalability, the Catalyst hardware and the DNA center, if deployed in tandem, can lower total cost of ownership (TCO) by 70%. This can be achieved by simplifying guest and mobility tunneling, while removing dependency on a dedicated guest controller at enterprise branch locations.

13Cisco, Cisco unveils network of the future that can learn, adapt and evolve, accessed 24 August, 2017, https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1854555&utm_source=cisco.com&utm_campaign=Feature_1854555&utm_medium=RSS
14CIO Today, Cisco Launches New 'Intent-Based' Networking To Stop Cyberattacks, accessed 24 August, 2017, http://www.cio-today.com/article/index.php?story_id=021002JDKIV9

THE PCM ADVANTAGE

A Cisco-certified Gold partner, PCM is a USD 2.25 billion public company with over 4000 employees. Our Cisco Certified Internetwork Experts (CCIEs) and Firejumper teams have extensive experience deploying large scale networks for municipalities, stadiums, and major corporations that serve thousands of customers each day. We deliver unparalleled support for assessing, designing, implementing and managing these solutions – 24/7 and 365 days a year.

PCM also holds Cisco Master Security, Master Collaboration, Cloud & Managed Service Partner advanced certifications plus many more.

If you want to know more about what PCM can do for your network, our solution architects can perform a detailed network study and help you build a roadmap for digitally transforming your enterprise IT architecture.

Authors:
Phil J. Mogavero
Vice President, Network Solutions PCM

Jim Warman
Manager - Core Networking Team PCM

PCM
1940 E. Mariposa Ave,
El Segundo, CA 90245
800-700-1000
www.pcm.com