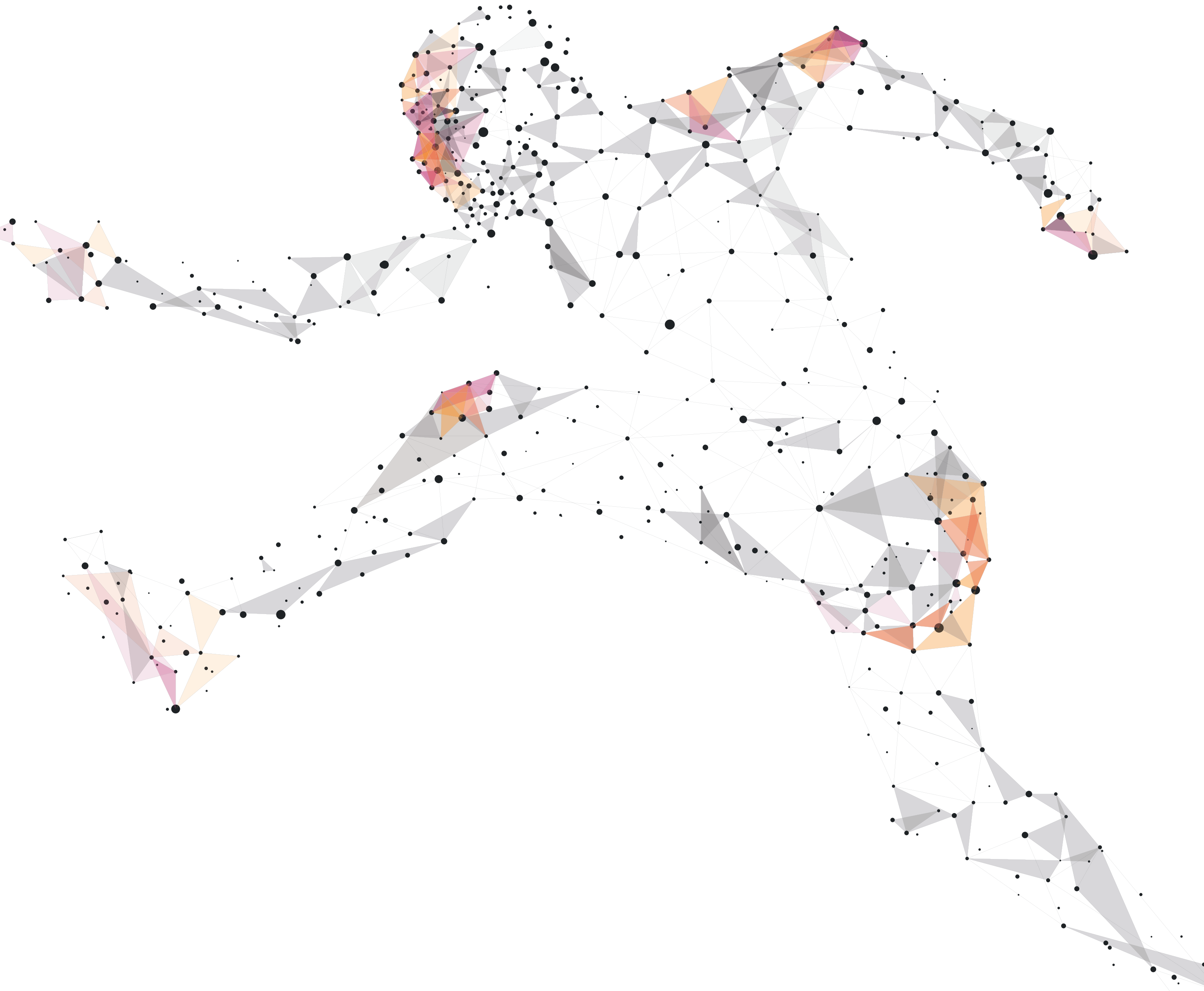
ideal
Defining customer experience

CISCO

THE NETWORK OF INTENTIONS:

HOW SOFTWARE DEFINITION RECONNECTS THE ENTERPRISE

- Understand the challenges facing legacy network technologies
- Discover how software definition enables a move to intent-based networking
- Explore the possibilities, benefits and risks of our software-defined future



Contents

1. Introduction

The old tools are blunt

2. Software defined access and the network of intent

The network. Intuitive

3. Trust in the machine

The internet of risk

4. Agile resources in the app age

Building IT resources

Network time travel

Spring forward

5. Accelerating digital transformation

The future network fabric

Demands

Solutions

6. The next generation of access control

Architecture evolving

7. Summary

Stepping into the future

SD Access' four core benefits

Introducing Ideal

References

Introduction

Your business has changed. How could it not? Your customers are online, operations are 24/7, apps and systems extend into the cloud, and with digital transformation your focus is increasingly on facilitating the customer journey. Data is fundamental, your devices are more varied than ever, and everything is held together by the network - which has barely changed in years.

Network technology has failed to keep pace with the transformation in network use. Today's enterprise IT network is the fabric that connects stalwarts like PCs and servers with mobile devices, and an ever-expanding array of smart systems and things. New devices are hooked up daily, and systems, users and their data need protection from threats that are becoming more sophisticated and persistent.

Despite this, IT teams still try to provision, support and defend network technologies with the same labour-intensive, error-prone tools and processes they had a decade ago. In an age of flex, of fast-moving, customer-led business demands, network administration is still a tedious journey through spreadsheets and command-line interfaces, while network management is hampered by a lack of visibility across multiple, disparate systems.

NETWORK INSIGHTS

One million new devices connect to the internet every hour[1]

Network demand is dynamic, and increasingly app-based, but 80-95% of network operations are manual[2]

The median time to detect a breach exceeds three months[3]

The old tools are blunt

As IT functions come under increasing pressure, the consequence of outmoded manual management and administration is more than just a pinch on resources. The lag between business demand and network response becomes an issue that threatens the delivery of organisational goals, and the lack of visibility stops you optimising your network as well as raising the prospect that security issues and breaches will go undetected.

In at least five areas, conventional IT environments are a constraint on digital enterprise:

1 **They're a drain on resources.** As local area networks become more and more complex, they become more expensive to operate and maintain efficiently, and - with up to 95% of network changes performed manually[2] - their operation ties up resource. Troubleshooting becomes more involved, and the IT team are called on more and more for support, diverting them from higher-level responsibilities.

2 **They can't maintain performance.** Manual network configuration is inherently error-prone, making it difficult to maintain standards and assure quality. Resilience suffers: a minor mistake can cause an outage.

3 **Network security suffers.** As 'smart' endpoints such as CCTV cameras and connected building systems are added to networks, they can pose a security threat. With conventional LAN technology it's hard to effectively segregate Internet of Things (IoT) devices, raising the risk that they become weak points or backdoors into the network. Edits to the network configuration may require security exceptions that aren't closed down again afterwards - Cisco research has found that 70% of policy violations are down to human error.

4 **They can't respond to operational challenges.** Conventionally managed networks can't offer the flexibility and security required by the business. Often the network becomes a damper on change, as reconfigurations are complex and have to be performed manually.

5 **They don't deliver value.** Operational and management resources are occupied by troubleshooting, and in trying to achieve visibility of the health or otherwise of the network. Cisco research suggests that 75% of network OpEx is spent on network visibility and troubleshooting.[4]

As business' operations and network infrastructure continue the move into a new digital era, there's an urgent and growing need for network provisioning, management and visibility to follow suit. Networks that underpin global, dynamic, expanding and agile organisations need the intelligence not only to respond, but to anticipate, understand and facilitate all the demands and needs of the business.

Technology partners, too, must move with the times: updating and deepening their core network expertise, and wrapping it in a wider strategic awareness of digital transformation and its impact on the organisation. Increasingly, experts like Ideal are called on for their interpretation of digital change: we continually invest in our in-house skills to ensure we can offer the strategic guidance and vision our customers expect, while maintaining focus on delivering the network you need.

Underneath it all, the fact is that networks are becoming too complex for manual design and management to be effective. Simply put, a new era of business demands the next generation of network.

Software defined access and the network of intent

The future network functions in an entirely different way. Managed centrally through a single pane of glass, the network is designed and configured automatically to deliver what the business needs. Where legacy networks are planned by spreadsheet, defined through lines of text and managed by hand, this software-defined network (SDN) leverages the intelligence of network devices to plan, provision, manage and secure the infrastructure through software, based on the business' intent.

The network of intent solves the fundamental challenges plaguing network management today. Staff are freed from time-consuming manual configuration, and the network is spared the consequences of their errors. Security policies are implemented and managed centrally, increasing visibility and ensuring compliance. The network becomes flexible, with major changes planned quickly and enacted in moments, rather than painstakingly applied across the enterprise. Operational and management resources are freed up, delivering value.

SDN is the near-future of networking, and Cisco has taken the first important step to delivering this vision of the intuitive network, with **Software-Defined Access** (SD Access). An exciting prelude to the next-generation of enterprise infrastructure, SD Access is an innovative technology that delivers policy-based automation of users, devices, and things from the edge of the network to the cloud. Delivered through a centralised management console - **Cisco DNA Center** - SD Access brings automation and visibility to complex network systems that currently require heavy manual intervention to maintain legacy levels of availability and security.

Breaking dependencies - how SD Access revolutionises network provisioning and management

SD Access lets you easily design, provision, apply policy, and assure network services with full visibility across the entire network, simplifying the delivery of consistent, highly secure, identity-based policy for users and devices across wired and wireless networks. It's a step-change in the way users and devices are managed on the network, made possible by the application of intelligence in Cisco's latest generation of switches, access points and routers.

In the legacy network, policies are enacted by careful provisioning of physical ports, user accounts or groups, but **SD Access** breaks the conventional dependencies between IP address, identity and location. Devices and users are authenticated on the edge of the network and granted the appropriate access as they traverse the entire estate.

The benefits are manifold. Users and devices are managed through **Cisco DNA Center**, a single interface that eliminates the need for multiple or interdependent configuration changes.

The network. Intuitive

In the intent-based network, the ideal is that the network team simply describes, in plain language, what they want to accomplish, and that the network will make it happen. But acting on intent requires intuition, and in a network that starts with the intelligence not just to understand business objectives and policy, but to break them down into the many actionable configurations and instructions that are required to make them a successful reality.

Ultimately, intent-based networking means taking in a high-level scenario, and creating a secure and predictable outcome, architected according to established best practice, that reflects the original business intent. It's an involved and complex task that, until recently, could only be performed by human experts, so why are things changing now?

The simple answer is that at the same time that conventional networks have become a bottleneck to business ambitions, the intelligence available in networking devices has grown markedly. The latest generation of Cisco switches, access points and routers have a level of sophistication way beyond what was even imaginable when legacy management practices evolved. Why not apply this intelligence to solving network problems?

As it develops and matures, intent-based networking will become key not just to solving the increasing demands on networks at the time they are provisioned, but to ensuring that the network continues to meet the original intent in changing circumstances - for example as an organisation grows, or as new device classes or roles emerge. Through machine-learning, the network will automatically ensure that service levels are maintained, identifying and alerting us to issues, and ultimately fixing or reconfiguring itself to resolve them.

Trust in the machine

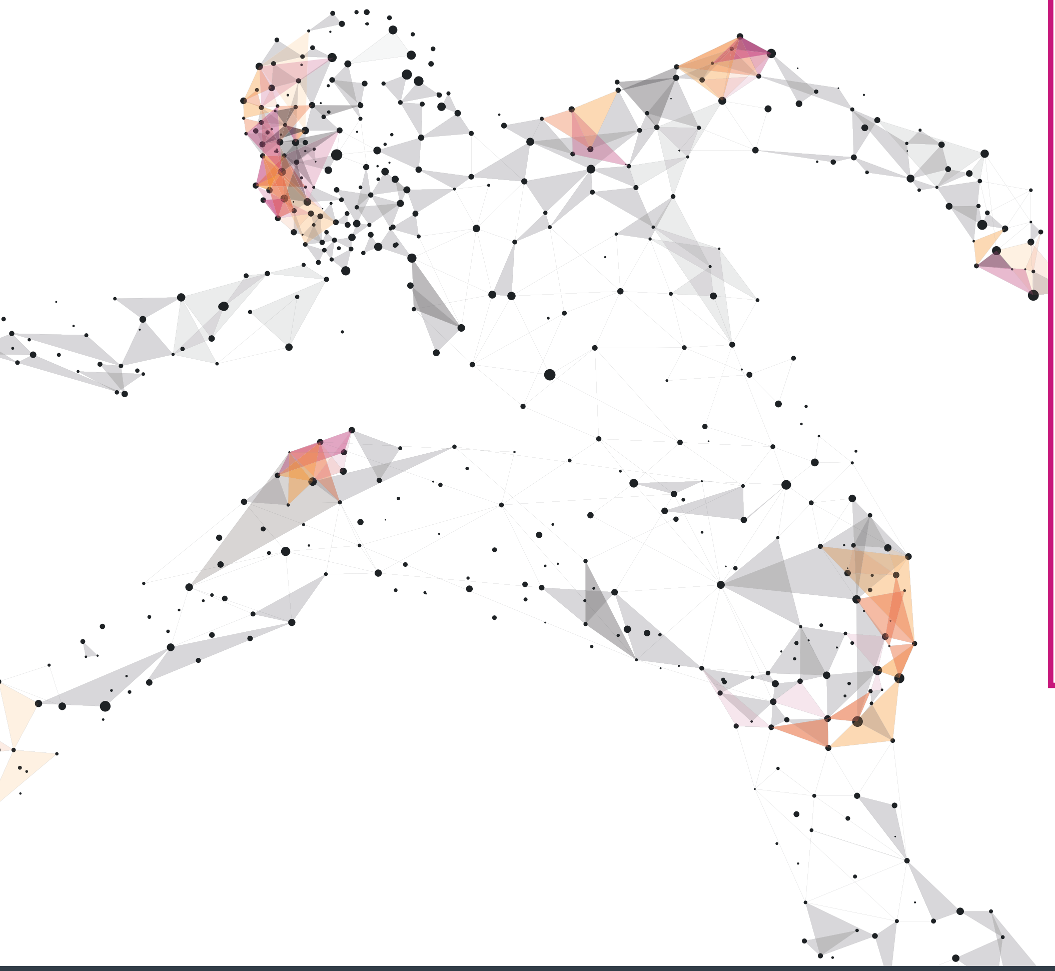
It's a powerful vision, but - in common with other fields where artificial intelligence promises to reduce human involvement - it raises legitimate concerns. How do network architects, until now central to the painstaking design of best-practice infrastructure, learn to trust the outcome of an algorithm?

"Network configuration can be a menial task from which you might want to free up your IT staff," says Richard Harvey, Ideal's solution architect for network infrastructure. "But when it's a manual process, somebody is at least thinking about the impact of the changes they're making on the rest of your systems. Removing people from the equation is… powerful."

"Fortunately, we're talking not about removing people, but freeing them up to perform higher up the stack. Human oversight and quality control will ensure - at least until these systems are fully matured - that network outcomes are matched to intent."

It's here that the expertise of technology partners such as Ideal will prove essential. Networking environments are complex, and it will be some time yet before automation and machine learning allow them to provide for every scenario. In the meantime, the experience and insight of highly qualified network architects like Richard will be required to cater for unusual and bespoke scenarios, and to ensure that the reality of the software-defined network matches the intent behind it.

And of the future? "Ultimately, intelligence in networks may introduce new risks," says Richard, "for example, an incredibly powerful central interface that must be strongly defended from abuse. Overwhelmingly, though, they will remove existing weaknesses. Skip forward a few years and the kind of security failings created by human error will just be a memory."



The internet of risks?

The Internet of Things (IoT) suffered from being over-hyped for much of this decade, but it's now commonplace in the home and in business. Everything from white goods to building systems are getting connected, and businesses are increasingly able to leverage sensors, connectivity and burgeoning intelligence to improve and streamline processes and reduce costs. By 2020 it's forecasted[5] that more than 26 billion things will be connected. What does that mean for the network?

The number, scope and sheer diversity of the IoT presents a problem: innumerable devices, multiple vendors with different stances on security, and no unified system for managing updates. Already we've seen examples of smart non-traditional endpoints co-opted into malicious activity: the 2016 distributed denial of service (DDoS) on Dyn involved a botnet of compromised IoT devices. Organisations need the tools to embrace IoT securely.

With current networks, that's a huge challenge. While the best practice is to segment IoT devices, isolating them from other business systems, the reality isn't so straightforward. Legacy segmentation tools such as VLANs are time-consuming to configure and test, and can be especially challenging to extend across multiple sites.

SD Access presents a simple, estate-wide solution. IoT devices can be identified at the edge of the network, assigned the appropriate access and restrictions, and securely segregated from the rest of the network. If a class of device is insecure, or in the event that devices are compromised, the network is protected, and their access can be easily managed or revoked.

Agile resources in the app age

Intelligent and secure, **SD Access** applies intent-based solutions to the challenges of the legacy network, but the result isn't just a legacy network that's easier to manage. Supported across latest-generation Cisco network hardware, **SD Access** is the first important step in a new generation of network performance and optimisation.

Business today is faster. Opportunities are more fleeting, challenges more pressing, so the organisation needs to work in a more agile, customer-focused way. Network users increasingly want to consume IT resource in the same app-based, on-demand way they use their personal phones. Through software definition, the provision, configuration and optimisation of networks is finally entering the same digital era - responding to organisational requests at the speed the business demands.

In the past, network requests would typically have been made by business functions, looking for resources to support an expansion or project. By the time a project had been designed and costed, the business case made and approved, and the systems provisioned and commissioned, months - even years - could have gone by. And while that may still be good enough for planned, core business functions, agile business also demands an agile IT response.

Software definition changes the game, enabling networks to move on from project-based, CapEx expansion to a cloud-like, infrastructure as a service (IaaS) model. In this brave near future, network resource may be on premises, hosted, or in a private or public cloud: software definition abstracts the details. As IT consumption becomes increasingly driven by apps and outcomes, network users simply request and receive the resources they need.

Building IT resources

"If legacy networks are like a big, mixed-use building, major changes require planning. A new project might need walls knocking down or even an extension being built. The result is capital investment and delay.

The Software-defined network lets us use that space more flexibly. If a business team needs space to prototype an idea, we can quickly partition it off - nobody else will notice or care. If we run out of space, we simply lease another building, or rent a secure, partitioned space elsewhere. Software definition means that all our users see are the resources they need, arriving as quickly as they need them."

Daren Vallyon, Ideal solutions architect

Network time travel

With **SD Access**, Cisco brings many of these capabilities to today's network. The **Cisco DNA Center** console transforms the management of the network, bringing deployment, management and optimisation into a single pane of glass. Performance data is gathered and stored centrally, where holistic analysis of network-wide traffic enables new levels of visibility, troubleshooting and optimisation.

Cisco DNA Center is a new approach, providing tools that slash the time lost to tedious network troubleshooting. Its more complete, easily accessed overview of network performance makes it easier to find, diagnose and solve issues.

As an example, take a common support desk scenario: on Monday morning a network user reports they had problems connecting at 7pm the previous Friday. Immediately there are possibilities: a device problem, network congestion, or perhaps a key access point or server was unavailable. Getting to the bottom of the problem will mean digging into thousands of lines of log data, potentially across multiple devices, so either the issue goes undiagnosed, or a skilled staff member spends hours tracking it down.

Cisco DNA Center not only gives staff a holistic view of network performance, it saves detailed historical data, enabling it to recreate the full picture of what was happening at a given time. In the above scenario, the team can wind the clock back to 7pm on Friday and see the exact circumstances to get quick insight into the problem and identify measures that might be needed to prevent it happening again.

Spring forward

This ability to 'time travel' on the network isn't limited to looking backwards. DNA Center can apply its intelligence to model different usage patterns, and help staff predict and respond to future demands.

Take the example of a UK-wide meeting at the company headquarters, where 200 colleagues are going to be converging on a conference area that's currently served by two access points. If each person has a smartphone and laptop, the network team needs to look ahead and assess whether user experience will suffer.

DNA Center allows you to run projections for such a scenario, modelling an additional 400 devices against likely demands and seeing a forecast for how the network will perform. This ability to peer into the future gives the team vital insight, and the agility to not only respond to but anticipate business needs.

Digital transformation makes new demands on network strategy - demands that can only be satisfied by a foundational shift. As traditional, siloed business structures are broken down in favour of responsive, customer-focused operations, the power in networking shifts away from the IT function and toward developers and lines of business.

Today's network connects clouds, applications, users, staff and their devices, and secures them and their data from a threat landscape that, too, is evolving to make the most of new opportunities. The best business, with the best applications, can only be as good as the network it's built on.

There's an inherent contradiction at play. As networks increasingly move towards a consumable resource, available on demand and rarely considered, they become more vital: their security is taken as a given, and business operations are built on the assumption of their availability and performance. Network demands are higher than ever, yet as the network is backgrounded, it becomes less valued by the business.

There's a strategic imperative for the network to evolve, to move from a legacy system responding to legacy demands, to an intent-driven ecosystem that responds, anticipates and adapts to the goals of the business. The industry shift in focus from hardware to software enables the network of intent. Suddenly intelligent, adaptive, responsive and empowered, the network releases its chokehold on agility and moves to the forefront of delivery. The network of intent becomes the key enabler and accelerator of digital transformation in the enterprise.

The future network fabric

Cisco has already taken the most comprehensive and evolved step towards this future network, producing a new generation of network hardware with the intelligence demanded by the evolved, software-defined network. Already the network of intent is coming to life in fast-evolving products like **SD Access**. In the near future, the IT estate will provide flexible resources on demand to a business that consumes them as apps and services. What are the primary requirements of the future network fabric, and underneath it all, what will it look like?

Demands

The near-future enterprise LAN faces a continuation and escalation of familiar challenges. As businesses become increasingly digital - using technology internally and externally to raise productivity, lower costs and gain competitive advantage - the network needs to offer its support through increased scale, application awareness, policy enablement and programmability.

Flexibility comes increasingly to the fore, with growing use of private and public cloud to deliver rapid and innovative services, or to add flexibility in hybrid systems. By 2019, it is forecast that 60% of enterprise workloads will be cloud hosted.[6] Containerisation and other software technologies will help ensure the portability of workloads across physical and virtual resources.

Staff and visitors already access corporate apps and data from mobile devices. As enterprises increasingly move infrastructure to the cloud and offer IT and networking as a service, mobile devices will be users' entry point to the hybrid cloud infrastructure. And as the IoT adds billions of device-to-device connections, the network will need to support and secure the additional influx of connectivity.

Security remains fundamental, with the network doubly under threat from its expanding scale and complexity, and the increasing sophistication and motivation of malicious actors seeking to compromise it. The network needs to apply intelligence to the behaviours it observes - even in encrypted traffic - picking out potentially malicious activity in real-time and at scale.

Solutions

The biggest change to network hardware is already underway: a revolution in the intelligence of devices, and in the flexibility and speed with which this intelligence can be applied. The future enterprise LAN requires that hardware is both programmable and easily updated, to adapt to innovation and support new features. Network operating systems need to continue moving away from their monolithic, proprietary past, into a future where they're open, API-driven and modular. To support centralised, single-view visibility, telemetry and analytics interfaces must be standards-compliant.

Virtualisation will continue to be key to flexible delivery of business demands. As the IT environment moves to a hybridisation of on-premises, hosted, co-located and/or cloud resources, virtualisation technologies are vital to abstracting the details: breaking the dependencies between workloads and the hardware they're running on. To support this, switching technology needs to support virtualised environments as comprehensively as physical ones.

Conversely, virtual environments themselves need to support virtualised devices, with consolidation and cost-saving achieved through running infrastructure such as firewalls and intrusion protection as services. The virtual network lends itself to rapid and secure network expansion. From the campus, virtual network services can be more easily provisioned and managed to the branch, data centre or cloud. Security demands will only be satisfied through embedded intelligence, deeply integrated into the infrastructure. Policy and identity-based access - as implemented by **SD Access** - will be imperative to ensuring security throughout the enterprise, not just at its perimeter.

The next generation of access control

In the future enterprise LAN, traditional VLAN-based segmentation is replaced by software-based segmentation, a simpler, more practical approach to security policy. With this approach, a central policy engine defines and manages security group tags (SGTs) to enforce access policies for users, applications and devices, allowing the enterprise to streamline security policy management across domains, and quickly scale and enforce consistent policies. Lateral movement of threats can be restricted with micro-segmentation, and group-based policies can control access to regulated applications for compliance requirements such as PCI DSS. In short, SGTs enable user and device segmentation without the need to redesign the network, while simplifying the management of access to enterprise resources

Architecture evolving

Supporting these new operational demands will drive, and in some cases require, evolutionary changes to network architectures. Key among these will be:

- Wired/wireless convergence - wireless is fast becoming the primary method of network access, so policies for security, quality of service (QoS), bandwidth, application performance and packet treatment must be applied consistently across wired and wireless traffic.
- Convergence of non-IP networks - other connections on the enterprise campus, such as security or utility networks, would benefit from a single, IP-based fabric. Converging them would enable consistent operation, administration, security, management and visibility of each.
- Enhanced performance - as traffic and reporting loads increase, so too must the capabilities and availability of campus switches.
- Novel connectivity models - as user mobility increases and lines of business introduce their own custom applications, the enterprise needs an architecture flexible enough to accommodate any connectivity requirement.
- Automation and central visibility - With so many connected devices, so much data and analytics, and such high security requirements, the future enterprise LAN requires precise automation and orchestration. Delivering this only becomes possible through an adaptable, always-learning network.

Parallel to this evolution in the network will be a change in the role and skills of those who manage it. Liberated from labour-intensive administration, the IT team's focus will shift further toward optimising the performance and value of existing and new technology investments, demanding a 'skilling-up' of the team. Furthermore, as IT delivery becomes more aligned to business intent, teams will require and develop an increased awareness of strategic business goals and their role in delivering them.

Trusted technology partners such as Ideal will be central to both making the most of these opportunities and managing the challenges they present. Through on-the-ground technical expertise and remote support capabilities, partners will be key to helping ensure that new technologies are deployed and performing as expected. Further up the stack, partners' strategic and management experience will be an important tool in optimising return on investment.

Summary

Stepping into the future

Cisco's SD Access, running on latest-generation Cisco network hardware and delivered through DNA Center, delivers many future network capabilities today. Bringing the ability to identify, classify and manage users and devices from the edge of the network, right the way through to the cloud, SD Access centralises and simplifies the provisioning and management of the network, and greatly enhances visibility across the enterprise.

Core SD Access benefits:

1 Confidence. SD Access gives you confidence in the security and performance of your network. Highly secure, identity-based policies span your wired and wireless networks, and centralised, single-pane-of-glass management gives you enhanced visibility. Next generation management intelligence allows you to simplify deployment, scale quickly, and add and secure IoT devices with confidence.

2 Accelerated digital transformation. SD Access is the foundation for an intelligent, agile network with simplified deployment and management. Software capabilities move the network on from a damper on change to an enabler of innovation and an accelerator of digital transformation in your organisation.

3 Relief of resourcing headaches. With increased intelligence in the network, and simplified planning, provisioning, management and visibility, the network team is free to focus on optimisation rather than troubleshooting. Your IT team regains the time to focus on better outcomes and higher-priority business initiatives.

4 Accelerated pace of IT. With a network that helps you plan ahead, and which can scale and adapt at speed, the time between business request and IT response is slashed. New devices, users and workloads can be added and secured at an accelerated rate and your business begins to pick up speed, responding with a new agility to opportunity or threat.

SD Access is the first step into an exciting future, but it's a future that will require changes in the way networks are planned, deployed, maintained and used. Key to a successful outcome will be the selection of a specialist network partner that can help design, implement, manage and support bespoke systems that exceed your business goals. Working with Ideal as your partner will ensure that you reap the benefits of an IT estate that's architected, installed and maintained for the optimal outcomes.

Introducing Ideal

Ideal designs, provides and manages secure infrastructure for organisations who see IT as a core business enabler. With over 100 customers across all industries, we deliver brilliant business outcomes through innovative, secure technologies and services. Our work is distinguished by excellence in communication and delivery, and by the width and depth of our in-house expertise.

With the experience and vision to advise organisations on how their IT estate can deliver and accelerate their business goals, Ideal is a trusted advisor for enterprises seeking to deploy, refresh and future-proof their network systems.

Ideal's extensive, 10-year partnership with Cisco is enhanced by the Advanced Enterprise Networks Architecture and Advanced Security Architecture specialisations. We architect, install and support high-performance network and unified comms infrastructure for clients including Caffyns, IKEA, OneFamily, the Rugby Football Union, SITA and Skanska.

ideal
Defining customer experience

Reference

1) IDC https://blogs.cisco.com/enterprise/2017-enterprise-network-security-trends
2) McKinsey Study of Network Operations for Cisco, 2016
3) FireEye M-Trends 2018 https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
4) https://blogs.cisco.com/cin/techwisetv-dives-into-enterprise-service-automation-and-easy-qos
5) Gartner https://www.gartner.com/newsroom/id/2636073
6) 451 Research https://451research.com/blog/1910-by-2019,-60-of-it-workloads-will-run-in-the-cloud

ideal
Defining customer experience