# White Paper

# Transforming the Enterprise with Managed Hybrid Networks and Cloud Connectivity Services

## EXECUTIVE SUMMARY

The IT sector is undergoing digital transformation (DX), driving migration to hybrid wide area network (WAN) and local area network (LAN) environments. Mobile, social, cloud, and big data tools that are required to manage the vast amounts of data are driving changes to the network and forcing companies to rethink existing network operating procedures.

These developments drive increased complexity in managing the enterprise LAN/WAN infrastructure. Implementing digital transformation is complex and costly within the constraints of static IT budgets and growth of shadow IT operations within the enterprise. This leads to a perennial struggle in managing the complexity of emerging technologies; consequently, managed network services will offer significant benefits.

Most enterprises are currently in the early stages of digital transformation, and managing change is complex and expensive. Many companies are still developing their strategies for the long term. Network services delivered in a managed services model continue to meet the needs of enterprises looking to transfer the cost of owning and managing their network to third-party providers. The role of the network in guaranteeing high levels of availability and performance has never been more important, given the diverse requirements for legacy and cloud-native applications.

There is an avalanche of cloud-native applications, new technology solutions like software-defined networking (SDN), software-defined WAN (SD-WAN), and service delivery models (hosted and cloud) that are forcing enterprises to reevaluate the viability of their current architecture, operational procedures, and in-house technical skills. These are critical factors to consider for enterprises looking to managed services as a means of bridging the gap between their legacy and new 3rd Platform environments.

The majority of large enterprises reported that outsourcing LAN/WAN operations will facilitate capex/opex savings while reducing complexity for IT managers (see Figure 1). The adoption of managed services will help companies face the challenges of maintaining adequate network security, 24 x 7 network monitoring, and business continuity.

## FIGURE 1

**Enterprise Adoption of Third-Party Service Provider Managed Services**

*Q.      Which of the following services is managed by a service provider?*
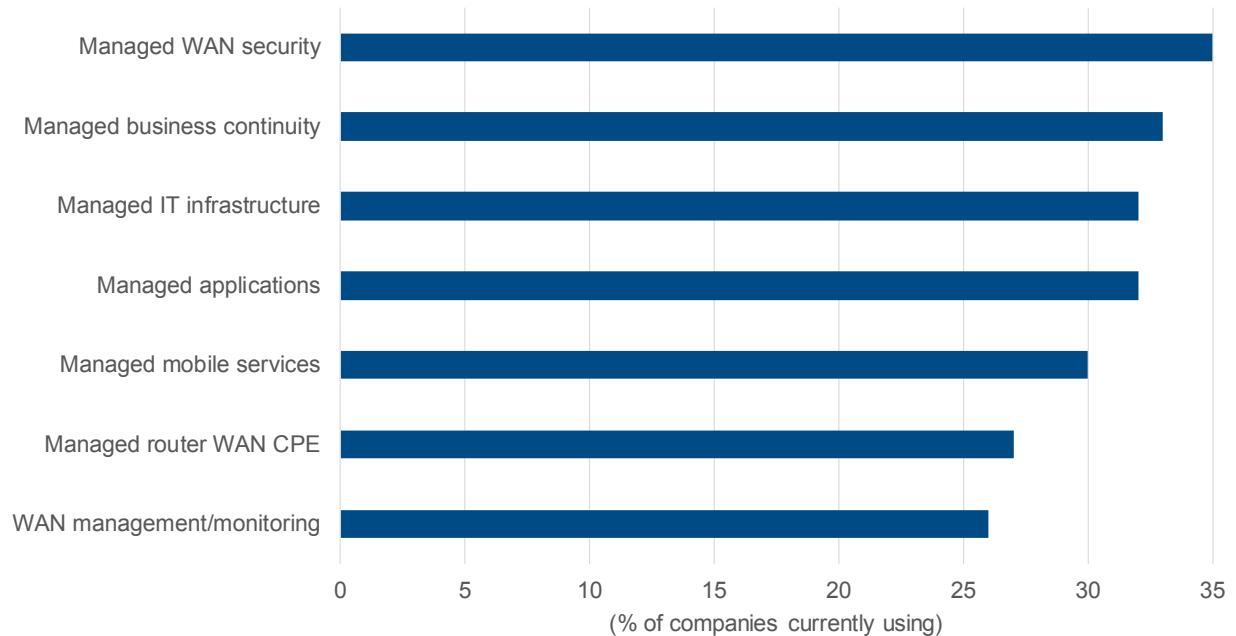


n = 905

Source: IDC's *Enterprise Communications Survey,* 2015

Most global multinational corporations (MNCs) now rely on dozens of IT suppliers for global networking coverage and IT services, a situation that will become even more acute with the transition to cloud platforms. The advent of cloud computing, mobility, and the internet of things (IoT) presages a larger dependence on a diverse range of infrastructure and service providers. Enterprises will increasingly leverage multiple IaaS, PaaS, and SaaS providers to meet the full range of IT and application requirements. One of the most significant challenges for CIOs will be the management of multiple, disparate cloud computing and network service providers. When organizations increasingly rely on more than one network service provider, the ability to have visibility in such a hybrid environment becomes essential.

## IN THIS WHITE PAPER

This IDC White Paper highlights the evolving enterprise requirements for managed hybrid WAN network connectivity, managed LAN, and managed virtualized or cloud-based services that can also support the growing need to connect enterprise locations to both public and private cloud-hosted services and cloud service providers (CSPs). This white paper examines new alternatives such as managed SD-WAN, managed virtualized services, and managed internet-based solutions. In addition, this document discusses how organizations can significantly improve network and applications management by outsourcing LAN/WAN network management to an external partner.

## SITUATION OVERVIEW: MARKET TRENDS AND EVOLUTION

According to IDC's recent *Cloud Connection Survey,* enterprises in North America and Western Europe will leverage up to 13 cloud providers in 2017, up from an average of 9 cloud providers in 2015.

IDC predicts that the scale-up of digital migration strategies will drive more than half of enterprise IT spending within the next 24 months as the amount of IT spending on cloud-based technologies will rise to 60% of total budgets by 2020 (see Figure 2). "Cloud first" will become the new mantra for enterprise IT because virtually none of the other 3rd Platform technologies or major digital transformation initiatives is possible in scaled-up implementations without the cloud as the foundation. IDC predicts that by 2020, enterprise spending on cloud services, the hardware and software to support cloud services, and the services for implementing and managing cloud services will exceed $500 billion, more than three times what it is today.

This fundamental shift also means that enterprises will require secure, high-bandwidth, and reliable access to information stored on private and offsite environments. The management of vast amounts of information about products and customer requirements will be essential for IT infrastructure managers.

## FIGURE 2

**Enterprise CIOs Evaluating Cloud Connect**

By 2018, **60%** of enterprise apps will be cloud enabled.

Public internet access to cloud resources can result in potential exposure to DDoS attacks and malware, limited throughput, and inconsistent performance.



By 2018, **60%** of IT spending will be cloud enabled.

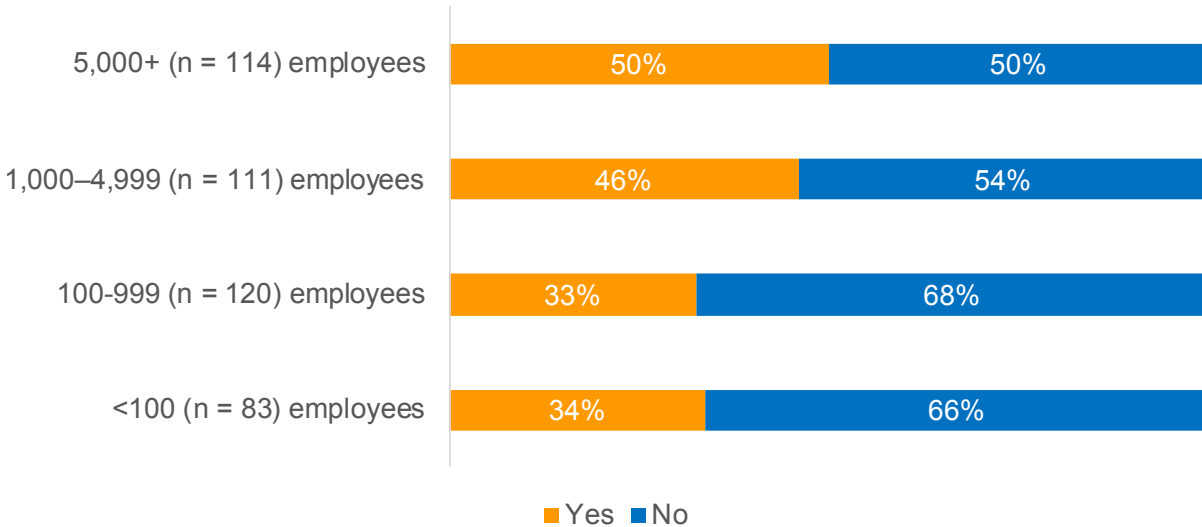Source: IDC's *Enterprise Communications Survey,* 2015

What are some of the major drivers of this new fundamental shift to DX?

- The IoT will be one of the most fertile areas for DX. IDC predicts that by 2018, the number of devices on the IoT will more than double to 22 billion and drive the development of 200,000 new apps and solutions that take advantage of those devices. Both the devices and the solutions have the potential to redefine competitive advantages in virtually every industry.

- Cognitive systems are already providing critical assistance to organizations dealing with the tsunami of data. Spending on cognitive software platforms is forecast to surpass $1 billion in 2016 and will scale up dramatically over the next three years. IDC predicts that by 2018, more than 50% of developer teams — up from less than 1% today — will embed cognitive services into their apps to leverage their data pipelines and improve customer personalization.

- In the expanding digital economy, industry cloud platform and community participation will become increasingly vital to scale up digital supply chains and digital distribution channels by as much as 100-fold to 1,000-fold. IDC predicts that by 2018, as the digital economy compresses pricing in many sectors, 60% of B2B enterprises and 80% of B2C enterprises will overhaul their "digital front doors" — and the customer engagement systems behind them — to support 1,000-10,000 times more customers and customer touch points than they do today.

- The role of cloud-native applications and SaaS will evolve. Large organizations source increasingly more IT capability from cloud software services and less from conventional licensed software deployments. IDC's data indicates that large organizations are very interested in shifting dollars toward SaaS/public cloud-type deployments.

- IT buyer patterns and influence are shifting. The role of LOB and applications development personnel within the enterprise is impacting IT buying behavior in multiple ways: While IT/networking managers and CIOs still dominate the IT buying process, LOB managers and applications developers are exerting increasing influence on the buying process. According to IDC's most recent *Enterprise Communications Survey,* LOB and applications developers now constitute 25% of enterprise IT buyers. In addition, large MNCs increasingly source networking services from multiple communications and cloud providers (see Figure 3).

FIGURE 3

**Procuring Networking Services from Multiple Providers**

*Q.        Do you procure networking services from multiple providers?*



Source: IDC's *Enterprise Communications Survey,* 2015

- ▪ Hybrid cloud WAN is a viable option for many organizations. IDC believes that there is a marked shift away from enterprises managing their own IT and WAN infrastructure, including servers and datacenter-based functions, to more of a managed environment that includes both public and hosted private cloud services. This shift is affecting the WAN network communication requirement choices as enterprises try to plan for both external cloud-connected environment and traditional WAN environment within the confines of a flat IT budget. At the same time, enterprises are becoming more aware and familiar with SDN and SD-WAN technology choices, and IDC believes that in 2016, there will be a shift toward these new services.

## MANAGED NETWORK SERVICES REQUIREMENTS IN A CLOUD-CONNECTED ENVIRONMENT

Enterprise IT executives are faced with increasing demand to integrate their cloud-hosted applications and new cloud-native applications with their existing premise and datacenter applications. This may include migration of support for enterprise applications that lines of business may have hosted or developed in the public cloud (often without the support of IT) or need to connect to hosted SaaS software applications such as salesforce.com, Microsoft Office 365, or SAP.com. The requirements for integrating cloud services are having a significant impact on the traditional LAN/WAN environment.

One change amounts to a SaaS approach to network administration, whereby management consoles and device configuration screens sit in a cloud service and are accessed via browsers and use web APIs to push changes to remote network equipment. This type of orchestrated provisioning is often achieved via a web portal.

Another change entails delivering WAN services over the public network. Although public cloud services inherently rely on the internet, they are obviously not all public services – companies have tunneled private traffic over the internet using VPNs for years. Salesforce.com Inc. and Workday use the cloud to deliver dedicated instances of enterprise applications, but key concerns for enterprise IT executives are the data security and access to authorized users, especially when "shadow IT" users have to be integrated into this WAN strategy.

Enterprise managers will also encounter more cloud-hosted solutions such as cloud-based WiFi, cloud-hosted VoIP, and cloud VPN or SD-WAN options for their LAN/WAN networking requirements. Managing network connectivity will include connecting traditional datacenter host-based legacy applications and hybrid cloud environments across a hybrid WAN network of internet, private VPN, and Ethernet environments. This complexity is truly an enterprise dilemma and will only increase as enterprises leverage more cloud service providers, use more hybrid networks, and leverage more broadband access for smaller locations.

New networking technology advancements and market dynamics are driving the need for IT and networking professionals to give consideration and even rethink their existing network architectures – LAN, WAN, datacenter, wireless, and security – and how they work in concert for delivering upon and meeting the needs of the business. New technologies such as SDN, network function virtualization (NFV), and SD-WAN provide the promise of simplification, increased agility and insight, and improved cost management but must be integrated in collaboration with, and awareness of, other enterprise networking initiatives. IDC believes that before enterprises can leverage these benefits, developing a holistic network strategy in alignment with the business will ensure successful adoption of any new networking initiative.

For most enterprises, this can prove overwhelming. Leveraging professional services to help define a clear strategy and road map will be essential for success. This requires bringing together the appropriate stakeholders from across the organization, including IT and business leadership, to prioritize applications and workloads, define policies for security and governance, and establish new processes for operational efficiency. Professional services can provide organizations the right resources, such as people, processes, and tools to evaluate, deploy, integrate, mitigate risk, and optimize new architectural approaches for the LAN, WAN, and datacenter networks.

The rapid integration of automation and analytics capabilities has the potential to enable enterprises to optimize and adapt to new business models and achieve new levels of customer engagement that translate into more service agility and improved user experience. Automation coupled with analytics can help drastically reduce mean time to resolution and drive incident prevention. Instead of manually resolving issues, automation leveraging virtual engineer technology can automate problem identification and resolution. Analytics can examine failure patterns across platforms and processes and prevent issues more effectively by addressing their root causes, before they impact the network.

In addition, the integration of traditional networking, public and private cloud services, and enterprise connectivity with these professional services requires a change in managing a mix of dedicated connectivity for low-latency, high-performance applications along with variable workloads and applications that use internet delivery means. Maintaining enterprise security policies across this evolving hybrid network includes connectivity to public cloud services with off-net broadband and wireless cellular access as well.

This is increasingly important as enterprises are optimizing WAN access services to cope with increasing bandwidth requirements of 20-30% at branch offices per year while budgets remain flat. This means evaluating the use of broadband internet access and also 3G/4G cellular options for

connectivity along with Ethernet access but ensuring that security and encryption requirements also take into account the connectivity options at each branch.

The transport-agnostic approach is becoming a key part of the managed services strategy even as navigating such an approach can be time consuming and costly. Working with a partner that understands an organization's applications and workloads, cloud strategy, and premise-based architectures, along with key business priorities coupled with the right transport relationships, will be critical for successfully adopting this strategy.

Enterprises also expect their cloud providers and managed service providers (MSPs) to employ and leverage software-defined networking technology to integrate the best of SD-WAN, SDN, NFV, analytics, and open source vendor solutions. Enterprises believe that virtualized services and new SDN and SD-WAN networking options will provide the flexibility for the future of their managed services. Figure 4 shows that there are many diverse attributes that enterprises look for in these new virtualized services, and they have expectations that MSPs will be able to support many of these virtualized services.

Automonitoring and remote support for diverse locations are additional requirements for global companies.

## FIGURE 4

### Attributes of a Virtualized Service
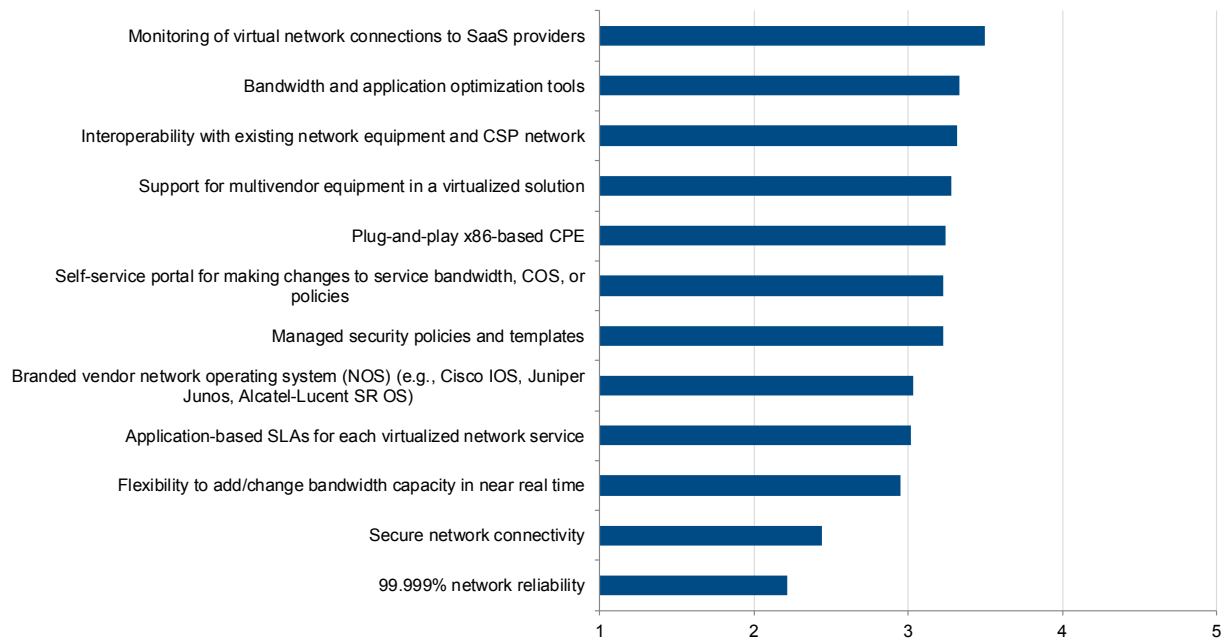


n = 744

Note: Respondents were asked to rate the importance of the attributes on a scale from 1 to 5, with 1 being not at all important and 5 being important.

Source: IDC's *Enterprise Communications Managers Survey,* 2015

## KEY IT CHALLENGES FOR ENTERPRISE NETWORK MANAGED SERVICES

Efficiently managing legacy and business-grade cloud applications and workloads across IT and WAN/LAN infrastructure underlies the need for a more holistic integration with emerging cloud services, including orchestration across multiple cloud environments over a secure network.

Enterprise internal IT organizations will need to develop an architecture or platform strategy that involves enterprise IT taking ownership to develop and extend WANs to various cloud services. This is a challenging and complex task because it involves significant resources and time to develop and implement solutions that support hybrid public cloud-based and private cloud-based enterprise applications. Developing a set of application-based use cases and service-level agreement (SLA) parameters is helpful in advance of discussions of these requirements with cloud providers.

Enterprises can outsource the development and hosting of their hybrid cloud networking strategy to an IT outsourcing company, but these enterprises then face the daunting task of developing the "magic integration" of the cloud services to the CSP that provides WAN connectivity. This can lead to issues of compatibility and often compromises flexibility to change cloud services or manage the performance of applications.

Enterprises can evaluate available CSP WAN cloud connectivity solutions that are a combination of a managed multiprotocol label switching (MPLS) VPN or a public internet and a separate hosted cloud service. Enterprises should be careful to avoid CSP cloud connectivity solutions that are offered only by the CSP for a specific suite of cloud services and do not allow enterprises the flexibility to use their own cloud service or easily connect to another third-party cloud service. Integrated SLAs and performance metrics for these two separate services are challenging, especially where the CSP may even use two different internal networks that are supported and handled by two different business units within the CSP.

There is also the added complexity of managing multiple CSPs' technology providers, and hybrid IT infrastructure is becoming very challenging for enterprise CIOs. This is perpetuated further as the WAN evolves to become a hybrid network that supports internet access, MPLS VPN connectivity, and connectivity to cloud services. This new role for the WAN also presents new challenges for IT administrators who now have to also manage the use of new cloud-based enterprise applications, including unified communications (UC), web conferencing software like WebEx or GoToMeeting, and CRM software services from salesforce.com, that are accessible to all users in remote, branch, and large offices often via the MPLS VPN.

Enterprise IT managers are faced with challenges in supporting a wide range of branch-office communication options such as internet access, Ethernet services, and IP VPN services using broadband, 3G/4G Ethernet, and MPLS networks cost effectively. Requirements include application agility, performance, and ubiquity while delivering efficiency, security, and privacy.

Implementing and maintaining security across this hybrid network environment present additional challenges, particularly for integrating third-party services or networks to access the managed services. Operational challenges include the following: How do IT managers have a single view of their hybrid network and each of its providers? How do security policies and encryption tools work in a cloud-connected environment?

Security is more challenging as more virtualization of enterprise IT infrastructure and network services occurs. Critical apps cannot be open or susceptible to hackers, viruses, denial-of-service (DoS) threats, and so forth – both on the WAN and when connecting to a public cloud or a private cloud service in a multicloud environment. Regulatory compliance can also become an issue (e.g., retailers need to comply with the PCI DSS data encryption security standard for all credit card transactions), and there are HIPAA requirements to comply with in the healthcare sector.

Implementing SDN and cloud-based networking in a hybrid IT environment in the enterprise datacenter is one of the areas where enterprises have varying levels of expertise internally. Managing a network environment made up of multiple legacy, virtualized, and software-defined network technologies requires cross-IT domain expertise and experience to ensure seamless network interoperability with applications and all of IT. When these new technologies are extended to include remote branch locations, where there is little or no IT expertise, this can become a larger issue for IT executives.

Managing internal IT skills and complex IT networking platforms such as SDN across a WAN environment with a single management view can be a considerable technical challenge and require an investment in money and resources that may be better spent in other business-critical areas.

Enterprises that are implementing digital platforms, automation, and analytics to improve their own IT services to end users and are also embracing agile application development are likely to be the most innovative in terms of adopting hybrid WAN solutions. IT executives face the decision to design, develop, and construct a DIY hybrid WAN from a multivendor, multinetwork solution or partner with an MSP that can design and provide managed hybrid WAN solutions from a number of best-in-class service providers that can reduce the enterprise investment in IT staff for troubleshooting, problem resolution, help desk, and complex network transport scenarios.

## ABOUT IBM NETWORKING SERVICES

IBM, a New York-based multinational technology and consulting business, contains the Global Technology Services (GTS) business division. Within this division is Networking Services, a distinct unit that combines networking, a holistic view of all infrastructure assets, and a greater focus on and investment in networking technologies and consulting best practices. IBM Networking Services has a presence in 170 countries and manages over 240,000 network devices and 650,000 telephony end points across its approximately 18,000 contracts worldwide.

IBM Networking Services utilizes a life-cycle approach that includes planning, design, integration, managed, and optimization services. IBM does not develop or manufacture networking technology or provide transport services, and this enables flexibility to partner with a broad set of network technology and service provider companies to provide best-of-breed client solutions. Clients can engage with IBM at any point in the life cycle of services, with requirements ranging from small, project-based engagements to fully managed networks. Technology partners and service providers play a key role in IBM's strategy, in which IBM invests significantly in its industry certifications, its best practices, and its own repeatable methodologies for consulting, optimization, and management in support of its customers' complex networking environments. IBM is an integrator of network solutions and services that are designed to support customers' business and technology requirements while positioning customers to innovate and differentiate on their current and future initiatives.

The IBM Networking Services portfolio is designed to meet clients' business and technology objectives, with a focus on delivering on business outcomes while delivering high ROI and TCO returns. The portfolio is organized into three core segments that integrate with IBM cloud, analytics, mobility, social, security, and traditional IT solutions. All network services are designed to help clients achieve business outcomes by understanding the clients' business priorities, applications, and workloads, all in support of the clients' journey toward software-defined architectures:

- **Network consulting services.** Align networking and communications strategy with key business and technology requirements and objectives while leveraging IBM's expertise in new networking technology advancements. Services include strategy, assessment, and planning around software-defined networks, NFV, and network infrastructure and application optimization to support hybrid cloud and IT-as-a-service strategies.

- **Project-based services.** Consolidate, integrate, and virtualize networking environments for improved availability, reliability, performance, and security. Implement projects based on a clear strategy with the goal of obtaining the value of SDN, NFV, automation, analytics, and open standards.

- **Network managed services.** Simplify and automate network and connectivity management to enhance availability, reduce complexity, and better manage costs. Longer-term engagements encompass LAN, WAN, and collaboration.

Differentiated IBM Networking Services solution offerings are as follows:

- **SD-WAN management services.** These services dynamically manage a customer's WAN traffic across a combination of MPLS and internet connections using multiple carriers across multiple geographies. The services create a seamless global WAN for improved network capability, reduced cost, and simplified network management.

- **Networking services for SDN.** These services include design, deployment, and managed services for software-defined datacenter networks. Based on software-based programmability of networks, network virtualization, and network function virtualization, IBM can deliver a proven reference architecture to align networks and applications. At IBM's Client Innovation Centers, enterprises can build, integrate, and test client SDN solutions to select the best technology option before deploying solutions in a production environment.

- **Network managed services.** These services are an IBM catalogue for customizable services for monitoring, management, and reporting of IT assets including the network, whether the assets are on-premise or on SoftLayer or reside in any cloud. Using automation, analytics, standardized processes, and cross-IT domain expertise, IBM manages a broad range of network technologies, technology providers, and networking equipment across numerous network types. The services include datacenter networks, wireless networks, SDNs, virtualized networks, enterprise WANs, hybrid cloud networks, and campus networks and LANs.

- **Converged fiber networks.** These services build converged networks leveraging passive optical technology and distributed antenna systems to run a full range of IT, communications, and building services on the same network while delivering a highly engaged and secure venue experience for industries such as sports and entertainment, healthcare, education, hospitality, and retail. Both SDN and NFV provide network strategy, design, and implementation services to create a programmable and centralized software-defined network environment as an integral part of a software-defined infrastructure to quickly deploy cloud-based workloads.

## Opportunities

IBM Networking Services affords customers the opportunity to leverage capabilities across other IBM divisions and resources to deliver complementary service offers, such as security, mobility, hosting, managed, and cloud services. IBM also has the ability to view a client's infrastructure in a holistic manner to encompass compute, storage, and applications and their impact on the network across the globe and in many verticals.

IBM presents a robust breadth of client satisfaction measurement systems and client retention programs. It is also developing specialized services offers, such as network optimization services, to ensure ongoing client satisfaction and network readiness.

## Addressing Challenges

Over the past year, IBM has undergone its own transformation, realigning and reinvesting its own services practices within the GTS business unit. Specifically, the Networking Services group has redefined its position in the networking consulting and integration space. It has hardened its core network infrastructure offers around key growth areas of LAN, WLAN, wireless, cloud datacenter, and Ethernet networking as well as invested in new network technologies such as SDN, NFV, and hybrid IT. In addition, IBM has expanded into new differentiated offers – such as network managed services, SD-WAN, and converged fiber networks – to provide customers higher levels of automation, agility, and choice for managing and optimizing their networking assets.

IBM has significant global scale and has developed a portfolio of network consulting, project-based services, and managed services to support customers as they move toward cloud and mobility initiatives. In recent strategic moves, IBM has continued to focus more intently on developing and expanding its services portfolio while lessening its stake in traditional network hardware.

As customers look to align technology investments with business outcomes, their trusted advisor must be able to speak this language and provide appropriate guidance. Fortunately, pan-IBM capabilities allow the company to address business challenges that can be solved through technology. IBM Networking Services will need to fine-tune its offers in the development of KPIs for measuring network investments to solve business outcomes. This may prove difficult in many cases because KPIs are "softer" to measure.

## ENTERPRISE HYBRID WAN USE CASE

IDC examined a typical enterprise example. A global tax and legal services advisory enterprise operates in over 75 countries and has an MPLS WAN network to connect its proprietary business applications for employees across its own datacenters, remote offices, and headquarters and at partner or client sites. The company also uses two public cloud providers to leverage compute and storage resources for some of its R&D and product development teams. The company currently utilizes a single MPLS CSP for all of its WAN connectivity and uses the internet to connect to one of the public cloud service providers and an Ethernet connection to connect to the other public cloud provider. This company also uses over 40 ISPs for broadband internet access for manual backup and currently backhauls all of its internet traffic to the MPLS POPs. The company plans to expand its use of cloud connectivity by extending redundant MPLS VPN cloud connectivity to one of the public cloud service providers as well as IBM SoftLayer.

The issues with this solution are little network diversity and lack of integration between broadband and cloud service providers. There is also no single network or service management portal view for the different WAN networks and connectivity to the cloud services that provide visibility to the enterprise legacy applications performance. Also, the company has to wait 90-120 days to get a new MPLS VPN site on-net. The MPLS WAN service provides inherent security, but when the network goes down, a manual switchover to broadband at remote offices goes over another unsecure broadband network, meaning security is potentially compromised; this vulnerability is critical because this is an entrance point to its network by not only the remote office but also potential hackers.

Figure 5 depicts an example of an integrated managed hybrid WAN solution that is a managed IBM network solution (IBM MultiNetwork WAN Services) for this enterprise. The solution provides a diverse mix of three different MPLS transport providers for connection diversity and also the ability to add another connection (like broadband internet or cellular) to supplement the traditional MPLS circuits. Diversity reduces costs and brings failover capabilities. Typically, a WAN is connecting two networks, and there will be a router on each end — usually manually configured (which is why it always seems to take so long for a company's IT department to bring a remote location online). This configuration can be automated with the managed hybrid WAN solution.

This solution also allows the enterprise to leverage the broadband connection for certain applications by analyzing the bandwidth, performance, latency, and security as well as load balance the access between the MPLS circuits and broadband internet. IBM has created peering network routing sites that provide a transport-agnostic MPLS solution with a managed network-based firewall. This solution also provides local internet breakout to avoid backhauling all of the mission-critical internet traffic across an expensive MPLS circuit.

In addition, IBM MultiNetwork WAN Services can provide application awareness and application performance optimization, including connecting to new cloud providers as well as existing cloud services from a "single pane of glass" view. This simplifies the IT operations for this enterprise's remote locations. With IBM managed services, this enterprise can also quickly roll out new sites or add more WAN capacity by leveraging broadband internet bandwidth to augment the MPLS network instead of trying to orchestrate the IT, network, and software changes or purchase more MPLS capacity. This type of SD-WAN or hybrid solution enables this flexibility.

FIGURE 5

## Enterprise Hybrid Cloud WAN Use Case
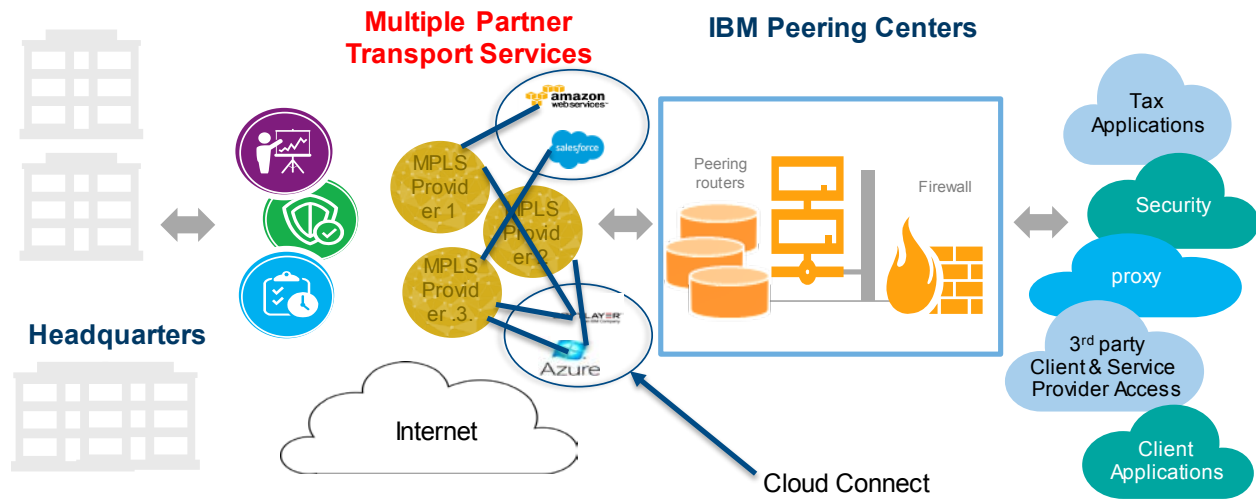


Source: IBM, 2016

## IMI FOR NETWORKING USE CASE

A large provider of IT security services and solutions was looking for a partner that could manage its complex and heterogeneous network environment along with the rest of its IT infrastructure. This company – which helps enterprises protect, identify, and manage data using intelligent information management solutions for large and complex IT environments – was looking at device integration and management across network, server, and storage environments. IBM's IMI for Networking Services provided 24 x 7 network management and monitoring for over 2,380 network devices, including switches, routers, firewalls, load balancers, WAN optimizers, and wireless devices from multiple network technology providers across multiple technologies.

Key features of the solution include:

- **Monitoring and ticketing:** 24 x 7 monitoring and automatic generation of tickets based on the alerts received from each system
- **Management:** Tools and 24 x 7 remote management for all the network devices
- **Reporting:** Periodic reports provided for all the managed services and shared with the company via an IBM service portal
- **Service management:** Level 3 technical support for the maintenance of the network devices

Using the power of dynamic automation and advanced analytics, IBM helped reduce the mean time to resolution and improved incident prevention while providing greater insight into the networking environment. The solution ensures continuous availability of critical business applications with proactive network monitoring, management, and reporting services. Centralized IT management of network devices, servers, and storage allows the company to work with a single provider for all its IT management needs.

## ESSENTIAL GUIDANCE

IDC has recommendations for MSPs looking to address enterprise requirements in terms of enabling hybrid WAN communications and cloud connectivity. The managed network services segment is experiencing a significant shift in the customer engagement process. Enterprise managers have a set of influencing factors that drive their selection of a managed services partner, and most of them indicate a desire to forge a more strategic relationship. The key decision factors include the following:

- Strong professional and consulting service capabilities
- Ability to provide IP, tools, automation, and people at the right time
- Solid ecosystem of technology and connectivity partners
- Holistic understanding of an enterprise's LAN, WAN, wireless, datacenter, and security architectures
- Strong knowledge of an enterprise's business
- Availability of dedicated support resources
- Ability to provide a level of customization in the managed service solution offered

Enterprises require a managed network service provider with the ability to manage a diverse array of networking capabilities, including Layer 2 topologies such as fiber and Ethernet services. In addition, the service provider should be adept at managing Layer 3 networks including MPLS and IP networks. Most importantly, the provider should have the ability to integrate and manage global network-to-network interfaces (NNIs), spanning multiple countries and topologies. The optimal service provider also must be able to facilitate a cost-effective and simplified management of multiple backbone and local loop contracts. Multinetwork management capabilities should include the following:

- Legacy and IP WAN connectivity
- Secure LAN networking
- Managed security intrusion and threat detection
- Managed VPN hybrid cloud networking
- Professional services

## CONCLUSION

Growth of hybrid network requirements calls for deep global relationships with a wide variety of service providers to facilitate smooth orchestration and asset management among various providers, as well as 24 x 7 monitoring of network performance. These service providers include large incumbents, cable multiple system operators (MSOs), specialized ISVs, and cloud service providers. The global managed network service provider should have the ability to integrate a wide variety of multivendor hardware and software platforms including legacy and emerging hybrid cloud such as IaaS, SaaS, and PaaS cloud environments.

Most importantly, the global managed network service provider should have the expertise to offer a cost-effective integration road map that can simplify the complex management of a global multinetwork environment. This includes an integrated portal capability that spans multiple global environments. The ability to deal with disparate regulatory and compliance regimes is also paramount.

Global multinational corporations face the challenge of a rapidly evolving IT environment. The ideal global managed service provider will have the expertise to offer a long-term vision to facilitate agility in leveraging dynamic IT trends. The ability to offer secure and efficient orchestration of IT asset management in a secure environment is an essential attribute. This spans the migration from legacy to IP and cloud environments. The ability to provide proactive managed security including threat detection and intrusion is also paramount.

## 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