White Paper

The Future of the Distributed Enterprise: IP VPN and Ethernet Wide Area Networks Enhanced by SD-WAN and Virtualized Network Solutions

Sponsored by: AT&T
Courtney Munroe
June 2017

EXECUTIVE SUMMARY

Today's enterprise information and communication technology (ICT) requires flexible, diverse, and reliable bandwidth options. Bandwidth demand is increasing exponentially, and networking methods are diverse, ranging from private multiprotocol label switching (MPLS) networks to public IP over secure wired and wireless broadband. This new hybrid IT scenario requires a new technology architecture that can provide agile and guaranteed performance depending on the specific applications in use. The foundation for secure, reliable hybrid IT networking is a communication service provider (CSP)-managed virtual private network (VPN) service capable of delivering a rich suite of voice, video, and business-critical data applications to the entire range of enterprise locations including headquarters (HQ), datacenter, and remote offices. This can be implemented via an access-agnostic wide area network (WAN), with rapid provisioning, flexibility, and transparency leveraging a seamless software-defined network (SDN)-based managed virtualized service incorporating MPLS and software-defined solutions.

This IDC white paper analyzes the trends and business drivers that are propelling enterprises toward the implementation of hybrid ICT services that can leverage the security and reliability of IP VPN, on-demand Ethernet, and software-defined networking services, including SD-WAN. CSPs are enhancing hybrid ICT with diverse access and virtualized network solutions that are tailored to provide the optimal performance of applications and vertical use cases.

SITUATION OVERVIEW

Introduction

WAN connectivity options for enterprises have evolved from traditional SONET-based private line, frame relay (FR), and ATM-based WAN connectivity to newer services such as network-based IP VPN services, Ethernet, and software-defined services including SD-WAN. IP-based WANs are widely available and ubiquitous and offer quality of service (QoS) that is the foundation of network-based IP VPNs. The availability of fiber-based broadband service as well as mobile broadband access provides another cost-effective option for enterprises seeking to rationalize networking costs. While many enterprises are opting for network-based IP VPNs and Ethernet WANs as their WAN service of choice, software-defined access that leverages broadband and LTE circuits has emerged as a viable option.
Today's IP VPNs are based on MPLS technology. MPLS is an IETF standard that defines a packet label-based switching technique, which was originally devised to perform fast switching in the core of IP networks, helping carriers and large enterprises scale their networks as increasingly large routing tables become more complex to manage.

Today, MPLS is widely used by service providers to connect organizations’ data networks with multiple, dispersed locations. By encapsulating these varying protocols in "labels," an MPLS network can make packet-forwarding decisions without understanding the contents of the packet. Enterprises can eliminate multiple complex overlay networks and transport many new and existing voice, video, and data applications over a single MPLS network.

**IP VPN Services**

An IP VPN service is a site-to-site connection with the service provider managing the end-to-end network and can be deployed in one of two methods:

- **A network-based IP VPN** is also sometimes referred to as a private IP VPN when it uses the secure infrastructure of a single network provider.
- **A public IP VPN (or internet VPN)** carries "best effort" data across multiple and nonspecified IP backbone infrastructures, often using customer-owned or customer-managed premises equipment (CPE) and IP Security (IPSec) tunneling, which is an end-to-end security scheme that encrypts every IP packet.

Network-based IP VPN services are enabled over a carrier’s private MPLS network. Their unique attributes enable the creation of virtual circuits that can scale nationally and even globally to connect a large number of remote networks. While organizations still maintain their unique LAN infrastructures and varying WAN access approaches in these configurations, MPLS unifies them.

Because a private IP VPN carries traffic across a single infrastructure, the provider can deliver greater and more standard security, manageability, and connectivity service attributes than a public service that relies on disparate network infrastructures. Private IP VPNs offer enterprises traffic prioritization, security, data integrity, and higher QoS guarantees supported by contractually binding SLAs than an equivalent public internet-based VPN employing IPSec. According to IDC's 2017 *U.S. Enterprise Communications Manager Survey*, 71% of U.S. business respondents across company size segments utilize MPLS IP VPNs.

**Ethernet**

Ethernet's popularity as a WAN technology has emerged because the technology offers a wide range of high-speed connections (from Mbps to Gbps) at lower cost compared with SONET services of similar speeds. Ethernet is a cost-effective option in part because of its underlying support of ubiquitous Institute of Electrical and Electronics Engineers (IEEE) industry standards for Ethernet physical interfaces in the LANs and because it works across homogeneous hardware that is readily available from multiple vendors. This makes Ethernet inexpensive compared with alternatives such as frame relay or ATM.

An Ethernet WAN service is a VPN service operating at Layer 2 of the Open Systems Interconnection (OSI) model, which is a reference model that describes the seven-layer structure of how data flows between telecommunication and computer networking products. Layer 2 provides framing of packets and error correction. The Ethernet WAN service enables enterprises to maintain control of their routing policies and also extends their existing virtual LAN (VLAN acts like an ordinary LAN, but connected
devices don't have to be physically connected to the same LAN segment) architectures to connect their enterprise WAN sites. Ethernet WAN services typically operate at higher speeds (ranging from 1Mbps to 10Gbps), and enterprises are increasing their use of higher bandwidth (typically 100-200Mb services), where direct fiber connections are available. In addition to fiber access, new Ethernet-over-copper solutions are extending the availability of Ethernet WANs to connect additional regional or branch sites. Ethernet WAN services such as Ethernet virtual private line (EVPL) and Ethernet virtual private LAN service (VPLS), which is based on MPLS technology, are becoming increasingly popular choices for organizations that are currently employing packet services.

The Emergence of Software-Defined Hybrid WAN Services

The emergence of Ethernet and broadband access has stimulated strong growth in hybrid wide area networking. A typical hybrid WAN includes at least two WAN connections from each branch office, leveraging two or more different access technologies (MPLS, broadband internet, 3G/4G, etc.). This facilitated cost-effective path divergence and business continuity for branch networking.

Some CSPs have been offering a hybrid VPN or hybrid WAN solution to try to address the need for a more flexible internet-based connectivity as an alternative or in conjunction with their MPLS VPN service to address the branch office connectivity needs of the enterprise.

However, the "hybrid WAN" as a concept has been rejuvenated by the emergence of cloud services, software-defined networking, and the lure of low-cost, high-speed internet circuits. A hybrid WAN combines the "traditional" network transport (including MPLS) with the substantial use of dedicated and broadband internet access. It frequently involves two connections to each site, which can be selected according to traffic type and performance parameters.

Figure 1 shows how an enterprise WAN solution that leverages MPLS at its core can be configured to incorporate a diverse mix of access methodologies. Branch sites can be configured based on their application and performance requirements for use with MPLS, IPSec circuits, or SD-WAN technology.
MPLS VPNs are ideal for supporting mission-critical, premise-based applications that require low-latency routing, higher performance, security, and QoS for delay-sensitive applications. This includes extending the enterprise MPLS VPN sites to be able to leverage CSP cloud connect services through a CSP’s gateway. Hybrid WANs can also make better use of wireless LTE access, even to MPLS, and they allow users to allocate premium MPLS bandwidth to applications that really need it, mitigating the need for costly port or circuit upgrades or allowing for a reduction in MPLS bandwidth (and cost). For many enterprises, a hybrid WAN is also a way to begin to transition away from the back-haul architecture that MPLS networks often employ to access internet-based services.

An SD-WAN service is an emerging service and is a type of hybrid WAN that is flexible and resilient. It utilizes centralized, cloud-managed, policy-enabled network or service control to leverage a software abstraction policy layer that can dynamically set up and manage all branch office Layer 3 WAN connections for enterprise communications services such as VPNs, WAN optimization, VoIP, and network-based firewalls. CSPs are beginning to position SD-WAN services as an alternative or a complementary service offering to traditional network-based MPLS VPNs or router-based IPsec VPNs for cost savings, increased agility, and simplification.

Figure 2 shows that the provisioning of an alternative transport to MPLS for non-mission-critical traffic or cloud-based software-as-a-service (SaaS) applications uses any access network in a simplified and cost-effective manner with IPsec. Increasingly, more than 40% of enterprise data traffic is migrating from traditional private WAN connections to the internet.
FIGURE 2

SD-WAN Features

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 being the most important and 5 being the least important.

- Reduce dependency on the MPLS network
- Prioritize network connection by application type or workload
- Policy-based intelligent path selection
- Reduce WAN management complexity
- Optimize WAN traffic by latency, jitter, packet loss
- Faster turnup (WAN provisioning)
- Flexibility to use different networks (e.g., broadband, MPLS, LTE) for application delivery
- Flexibility to add/change bandwidth capacity in near real time
- Lower WAN transport costs
- Self-service portal

n = 772
Base = respondents who indicated that their organization plans to deploy SD-WAN as an overlay framework on existing WAN

Source: IDC’s U.S. Enterprise Communications Manager Survey, 2017
SD-WAN leverages hybrid WANs, but it includes a centralized, application-based policy controller; analytics for application and network visibility; a software overlay that abstracts underlying networks; and an optional SD-WAN forwarder (routing capability) that together provides intelligent path selection across WAN links. The business benefits of SD-WAN include cost-effective delivery of business applications, meeting the evolving operational requirements of the modern branch/remote site, optimizing SaaS and cloud-based services, and improving branch IT efficiency through automation.

The adoption of cloud-based applications, unified communications, videoconferencing, and mobile enterprise applications is driving increasing bandwidth requirements and the need for cost-effective, reliable alternatives to legacy access circuits. IDC research indicates that over 73% of enterprises are currently leveraging broadband, Layer 2 Ethernet, and mobile broadband services for last-mile access. The need for real-time dynamic bandwidth configuration and rapid provisioning of services are key drivers orchestrating this evolution.

According to results from IDC's 2017 U.S. Enterprise Communications Manager Survey, leveraging cloud infrastructure and implementing hybrid infrastructure to ensure reliable data backup and business continuity are essential drivers for enterprises. Accordingly, software-defined networking leveraging IP VPNs and multiple access options such as Layer 2 Ethernet and broadband services are important aspects of the enterprise CIO strategy.

Use cases for SD-WAN solutions by specific vertical sectors include:

- **Financial sector**: Companies in this sector, such as banking and insurance, utilize a large number of small branch locations. Many of these locations require a reliable backup access circuit for business continuity or to offload noncritical transactions. An SD-WAN solution is a perfect complement for off-peak data transfer over broadband or a backup access for ATM machines. The backup circuit capabilities also leverage the high SLA requirement for availability, latency, and other performance characteristics of a transactions-oriented industry.

- **Retail sector**: Companies in this sector can utilize the application performance monitoring and management capabilities of SD-WAN instantaneously.

**VPN Service Choices: Ethernet or IP VPN, or Both? Services, Solutions, and Benefits**

**Network-Based IP VPN Services**

Network-based IP VPN services have been available for over a decade and are currently offered by many of the leading service providers worldwide. An increasingly large number of enterprises have adopted this type of service, allowing them to interconnect hundreds or thousands of disparate regional, national, and global locations in a very efficient manner.

Today's MPLS network-based IP VPNs are the foundation of many enterprises' distributed data communication. IP VPNs are often the communication platform of choice for enterprises to enable additional value-added enterprise applications on top of their VPN, such as VoIP, security, videoconferencing, and unified communications.

Figure 3 depicts the benefits of implementing IP VPN.

Figure 4 depicts a typical network-based IP VPN topology.
**FIGURE 3**
Key IP VPN Adoption Criteria

Q. What features/use cases have you currently implemented on your network-based MPLS IP VPN?

- Remote access
- Security applications
- Voice over IP
- Site-to-site
- Multiple VPNs on same access circuit
- Proactive monitoring and reporting
- Class of service (CoS)
- Route management
- Multicasting
- Managed CPE
- On-demand/dynamic bandwidth via a self-service customer portal
- Application-aware performance management
- None of the above

n = 401
Base = respondents who have network-based MPLS IP VPN

Source: IDC’s U.S. Enterprise Communications Manager Survey, 2017
Benefits of Network-Based IP VPNs

There are benefits and advantages of a network-based IP VPN that are specific to the service provider; however, the most important characteristics of a network-based IP VPN service have the following important benefits:

- **Outsourced routing control**: With network-based IP VPNs, enterprise IT managers gain a single and centralized solution for WAN connectivity, eliminating the operational and resource planning inefficiencies of maintaining separate duplicative networks and thus enabling a focus on the enterprise’s core competencies. Enterprise IT staff can rely on the service provider as a trusted partner to help prioritize the different traffic types such as latency-sensitive voice and video and utilize the class of service (CoS). The service provider is responsible for managing and maintaining enterprise WAN connectivity. The enterprise outsources routing and traffic policies for data, voice, and video applications to the service provider, relying on the expertise of the service provider to create policies that prioritize mission-critical data and real-time applications above other applications and ensure that there is sufficient bandwidth. Any changes to the enterprise applications that require routing control changes are managed by the service provider.

- **Flexible access connectivity**: Access service refers to the last-mile telecom connection between a network device at the enterprise location to the local exchange carrier, and it also provides the service interface to the IP VPN. IP VPN supports a range of access options, including leased line, Ethernet, FR, and ATM. Remote/branch sites typically have lower-speed...
connectivity options (56Kbps up to T1/E1 or n*T1/E1 speeds). Larger sites may have higher-speed connections (DS3/E3/OC-3/STM-1/Ethernet), but they are typically a much smaller subset of VPN access connections. This variety of access options provides users with a simpler migration path from the current standard ATM/FR/TDM connectivity toward an IP VPN solution.

- **Scalability:** IP VPNs are routed and offer a highly scalable platform for supporting very large enterprise networks (with hundreds or thousands of enterprise locations) that require site-to-site and any-to-any connectivity. The service provider's IP VPN infrastructure and network access enable rapid scaling.

- **Extensive service reach:** IP VPN services tend to be offered by a larger number of service providers and thus provide a larger geographic coverage and service reach to enterprises that are highly distributed or expanding.

- **Inherent security:** Internal and independent label addressing schemes for additional security prevent denial-of-service (DoS) attacks.

The following vertical enterprise segments illustrate how IP VPNs are used in enterprises:

- **Finance/banking.** Regulatory changes, mergers and acquisitions, and technology changes are impacting financial and retail banking WANs. Often these WANs are an amalgamation of separate WANs, some still operating legacy banking applications that support multiprotocols. Access speeds vary from higher speeds at datacenters or headquarters to moderate speeds at branch offices and lower speeds at ATM terminals or kiosks. This distributed architecture makes it difficult and expensive to maintain technical support resources at every site. Today's IP VPNs can support legacy and IP protocols and voice traffic and work across all speed links, providing a managed and secure network that reduces the amount of financial services enterprise IT management resources.

- **Insurance:** Regional and national insurers typically employ a large headquarters for data warehousing and claims processing and a highly regionalized employee base to service customers. Collaboration and communication between central administration and remote field offices are important. IP VPNs enable an integrated network by lowering operating costs for insurers, while providing uniform access to information accelerates decision making and improves customer satisfaction.

- **Retail:** Retail chain stores operate large national or regional networks connecting each store's voice, data, and video (surveillance) traffic. Access is also required to the headquarters for inventory update and transaction reporting, datacenters, and a common web database of store product items and services. Network IP VPNs can interconnect all the stores, offices, datacenters, and web hosting sites and network all applications, including voice.

- **Manufacturing:** The voice and data networks of manufacturing companies are highly meshed, interconnecting a myriad of developers, suppliers, partners, and dealers. In fact, connections are as dynamic as the nature of their business. IP VPNs interconnect bandwidth-intensive CAD/CAM applications, videoconferencing, and storage backup as well as lower-speed connections to dealers and suppliers and for inventory tracking and replenishment.

**Ethernet WAN Services**

Ethernet WAN services have evolved during the past five years, initially offered in metro networks and now offered in metro, regional, and global networks from leading service providers worldwide. Enterprise IT/communications managers interviewed by IDC revealed that the rapid adoption of Ethernet WAN services has been driven by cost, ease of implementation, and a familiarity with the Ethernet architecture already employed in corporate LANs.
Ethernet WANs utilize Ethernet and employ industry-standard technologies, such as the following:

- **MAC address learning** is defined in the IEEE 802.1 standard to help minimize traffic on the attached LANs by storing source MAC addresses so that only packets destined for a given address will be sent to that address, improving the network performance.

- **VLANs** refer to a group of logically networked devices on one or more LANs that are configured so that they can communicate as if they were attached to the same physical network, providing flexible bandwidth and resource optimization.

- **CoS**, which enterprises already utilize in their LANs, is a way of classifying and prioritizing packets based on application type (voice, video, email, file transfer, transaction processing, etc.), user type (VIP or normal, etc.), or other ways of classification. A "first class" priority label is assigned to data applications (such as mission-critical data transactions or video or voice transmissions), which require faster turnaround, while a lower-priority label is assigned to less time-sensitive traffic (such as email and web surfing).

These Ethernet WAN services can be either point to point (EPL/EVPL) or multipoint to multipoint (ELAN/VPLS).

Enterprises continue to choose Ethernet services because of Ethernet's relative price/capacity, flexibility, and low cost, and these remain the most widely used business criteria. Another reason for Ethernet's popularity is access to IP VPN and internet services.

According to the results from IDC’s 2017 *U.S. Enterprise Communications Manager Survey* shown in Figure 5, 48% of respondents currently utilize the hybrid Ethernet/IP VPN features combining the best of both Layer 2 and Layer 3 services (34% of respondents plan to employ these hybrid features in the next year). Support for security applications remains the most popular Ethernet WAN feature, with 63% usage.

Figure 6 shows a typical Ethernet WAN with several applications, including datacenter connectivity.
FIGURE 5

Key Ethernet WAN Features

Q. Which of the following Ethernet WAN service features do you currently use?

- Security applications
- Proactive monitoring and reporting
- MPLS and Ethernet
- Application-aware performance management
- Managed CPE
- Class of service (CoS)
- Self-service/on-demand dynamic bandwidth
- Burstable bandwidth
- Q VLAN tag stacking

n = 681

Base = respondents who indicated that their organizations’ more than 0% business sites are currently connected using Ethernet WAN service technologies

Source: IDC’s U.S. Enterprise Communications Manager Survey, 2017
Benefits of Ethernet WAN Services

Ethernet WAN services offer enterprises a number of benefits, including standardized services, scalability, reliability, service management, and flexibility. Ethernet WAN services have the following important characteristics:

- **Routing control**: Routing control in the WAN is maintained by the enterprise, which is typically favored by enterprises that prefer not to share their routing tables. With an Ethernet WAN service, the enterprise autonomously implements and controls its own end-to-end networking and routing decisions and can also manage and change its routing environment without having to involve the service provider in order to maintain security and privacy and manage it with internal staff.

- **Protocol transparency**: Ethernet WANs have the inherent ability to transport all legacy application protocols, such as SNA, DECnet, and IPX, because Ethernet, as an OSI Layer 2 protocol, can support any higher-order protocol, making it an ideal method of supporting legacy application protocols that are still in use by some enterprises.
- **Ethernet operations and maintenance (OAM)**. Ethernet WANs offer a more comprehensive OAM toolkit than FR/ATM. The Metro Ethernet Forum (MEF), the International Telecommunication Union (ITU), and the Institute of Electrical and Electronics Engineers are developing a number of OAM standard features that will provide advanced means to monitor and manage communication on the Ethernet WAN.

Bandwidth-intensive WAN applications are ideally suited for Ethernet, which enables bandwidth rates from 1MB to 10GB.

The following vertical enterprise segments illustrate how Ethernet WANs are used in enterprises:

- **Healthcare**: Healthcare organizations are required to comply with an increasing set of medical regulatory requirements related to patient medical records, images, and medical data while facing cost reduction pressures and improving patient care. These healthcare organizations are migrating to digital patient information, digital images, and faster communication, requiring significant amounts of bandwidth data exchanged between doctors, hospitals, medical offices, datacenters, and insurance companies’ facilities. Ethernet WAN enables doctors to rapidly view and share patient x-rays, medical imaging, and medical records securely and quickly from a large hospital, secondary hospital, medical office, or clinic. Ethernet WAN also enables a large hospital network to use CoS to prioritize interactive video for live surgery, imaging, and real-time data between key locations on the WAN at high bandwidths (a typical MRI is 50Mb). HIPAA requires that healthcare organizations have a disaster recovery and backup facility for all medical records, and that can be enabled by an Ethernet WAN linking the healthcare datacenters, backup centers, and administration locations. Telesurgery, which is live remote surgery, is another new and emerging application for Ethernet.

- **Government**: Many government agencies depend on a network of distributed datacenters, which are becoming increasingly expensive to maintain and operate, preventing governments from realizing economies of scale and reducing cost. While there are efficiencies in consolidating datacenter operations into a single location, consolidation introduces the possibility of a single point of failure, which is not acceptable for government services. Although redundancy and uptime can be enhanced through database or SAN replication and backup to an alternate location, the required connections are latency and packet-loss sensitive. An Ethernet WAN service provides a high-speed, low-latency dedicated or virtual connection that can support datacenter to head office connectivity and also connectivity to a secondary backup storage facility or alternate site or datacenter on a secure WAN.

- **Financial services**: Financial services organizations that generate or process a high volume of data, including securities trading, commodities, exchanges, institutional investment, and commercial lending, often require low latency, high bandwidth, high availability, redundancy, and the ability to provision their own CoS as part of their network requirements. Ethernet WANs can enable the low-latency and bandwidth-intensive financial trading applications that often require 500Mb and higher bandwidth rates. Some of the important low-latency financial applications include data streaming, financial transaction reconciling, and live trading, which require millisecond response times. Many trading organizations also have to comply with regulatory requirements to have a secondary, redundant offsite storage of financial and transaction data, which can be accommodated with an Ethernet WAN. Videoconferencing and other collaboration applications are also enabled with the Ethernet WAN. High-speed secure WAN connections to global financial exchanges are most often supported by Ethernet WAN services.
• **Campus LAN extension:** Connecting corporate enterprise, government, and education campus sites in metro networks and across the WAN using high-speed LAN interconnectivity is an increasingly important requirement as content and applications become more bandwidth intensive. Distance learning applications, videoconferencing, and desktop sharing are examples of applications that demand extremely high throughput, but in a relatively limited geographic area. Ethernet WANs such as VPLS can support the required connections and high-bandwidth requirements and allow enterprises to utilize their existing enterprise VLAN policies across the WAN.

• **Cloud computing services and SaaS:** A growing number of enterprise software companies such as salesforce.com, Google, Citrix, SAP, and Oracle are moving away from selling software licenses and instead are selling their technology in a pay-per-use model. IT WAN managers face the challenge of how to plan for adoption of their SaaS offerings, and conventional WAN connections can quickly become congested. Ethernet WAN services offer high-speed connections that can scale very rapidly and often can be configured for bursting of traffic at higher rates or enable customers to self-provisioning additional bandwidth.

• **Contact center connectivity:** High-speed Ethernet WAN services can interconnect global or regional enterprise call centers and also provide high-bandwidth connections to datacenters with CoS to ensure fast data retrieval to deliver satisfactory customer service. Using Ethernet GigE connectivity ensures that customer data is available to contact center employees instantly.

• **Video or other rich content delivery:** Many enterprises are increasing the use of video on demand for employee skills training, HR compliance training, corporate town hall meetings, and customer support. The throughput requirements are many magnitudes higher than those of traditional data access, and an Ethernet private line (point to point) service can provide the scalable bandwidth to enable enterprises to easily meet demand as needed.

**Hybrid Ethernet and IP VPN WAN Solutions: Coexistence of Ethernet WAN and Network-Based IP VPN Services**

Enterprises can leverage Ethernet and IP VPN services that are specific to their enterprise requirements for bandwidth, cost, flexibility, QoS, and IT control. This hybrid VPN solution combines and optimizes the best WAN service based on enterprise business application and bandwidth availability at the enterprise WAN locations.

Figure 7 illustrates where an Ethernet WAN service is ideally suited for WAN connectivity between headquarters, datacenters, and regional sites where high-bandwidth, low-latency, and high-performance applications such as document storage, video streaming, or on-demand video or application sharing can use a configurable CoS Ethernet WAN capability, which the enterprise can manage. For other applications such as peer-to-peer applications, web applications, transactions, and voice, these larger sites can use the IP VPN service to connect to other sites on the network, whereas the smaller branch office/remote sites use an IP VPN service to connect to any site on the network.
Figure 8 illustrates another example of how Ethernet WANs using VPLS, Ethernet access, and metro Ethernet can provide an interconnection between each of the four metro fiber-based sites and then use an IP VPN to interconnect these same four sites to the corporate IP VPN for regional, global, and remote access connections to the VPN.
The following vertical enterprise segments illustrate how hybrid networks are used in enterprises:

- **Financial services** organizations can utilize a combination of an Ethernet WAN service for high-bandwidth, low-latency connections between datacenter locations and backup sites and network-based IP VPN services deployed at regional office locations where voice, data, and videoconferencing applications are used between all the enterprise sites. This hybrid solution provides the enterprise with the flexibility to leverage the appropriate service based on its needs.

- **Healthcare** organizations often require hybrid networks to support a myriad of applications. High bandwidth and high availability are key requirements supported by Ethernet WAN services for medical imaging applications that are transmitted from a hospital to other medical facilities. High-speed storage of medical records also benefits from using Ethernet WAN services, which are ideal for low-latency storage protocols such as VMware. IP VPN services support the healthcare voice network, email, patient data, and other applications requiring connectivity between hospitals, doctors, insurance providers, laboratories, and other providers of services that are part of the extended healthcare network.
Figure 9 illustrates a typical example of how enterprises can connect their branch offices, regional offices, and datacenters using a managed IP VPN service for any-to-any connectivity and an Ethernet WAN for high-bandwidth point-to-point connections between datacenters and headquarters or as a gateway to offload traffic to the public internet.

**FIGURE 9**

---

**Ethernet Access to the Internet, IP VPN, and VPLS**

---

**Ethernet Access to Hybrid Ethernet WAN and IP VPN**

Ethernet access is no longer limited to a fiber-only connection to reach the end-customer site. There are other flexible access options for implementing an Ethernet WAN service or as an on-ramp to an IP VPN service. In addition to Ethernet over fiber (Active Fiber, PON, SONET/SDH), Ethernet access is supported and available over PDH (T1, DS3), copper (EFMCu), wireless (WiMAX, broadband wireless, and microwave), and HFC/DOCSIS (see Figure 10; refer back to Figure 6). Ethernet access enables higher-access bandwidths, often at rates much higher than T1/T3.

The enterprise customer for Ethernet WAN services has also evolved from large enterprises located in fiber-rich metropolitan centers to those with globally distributed operations and midsize businesses in suburban and rural settings. Many of those same enterprises already use an IP VPN service for their WAN. Ethernet access can also provide access to an IP VPN service (as depicted in Figure 10) as Enterprise B interconnects two branch locations: one using Ethernet access to connect to the IP VPN service (on the right) and the second branch to an Ethernet point to point (PoP).
FIGURE 10

Enhancing Existing IP VPN Service to a Hybrid Network Using Ethernet WAN

DIA = direct internet access  
VRF = virtual routing forwarding (for L3 IP VPN)  
Source: IDC, 2017

SUMMARY

Hybrid WAN networking leveraging software-defined networking based on network-based IP VPNs and a diverse mix of access circuits is emerging as a key transformative driver for enterprise WANs. Enterprises should select service providers that offer the most robust and diverse solutions based on an MPLS/IP backbone network and SDN-based virtualized services as well as SD-WAN options. Together these solutions offer the flexibility to manage today’s challenging requirements for secure access to cloud applications over a hybrid private or public environment.

Enterprises can continue to leverage traditional trusted technologies such as network-based IP VPN services and Ethernet WAN services. Software-defined platforms such as AT&T FlexWare and SD-WAN solutions provide additional flexibility for the secure access of corporate applications over a variety of disparate public IP infrastructure.

MPLS has traditionally been considered secure because it provides isolation. Integration with Layer 2 services such as Ethernet access provides a secure path and managed access to cloud platforms. Software-defined network can provide both isolation and end-to-end network encryption. Integrated security and segmentation is becoming a requirement in many sectors such as financial services and healthcare. Key elements of these new CSP SD-WAN service offerings will leverage encryption, path control, policy management, overlay networks, and on-demand subscription capabilities of the underlying technology, which are embedded in the various network equipment of a vendor’s solutions.
IDC believes that, in 2017, enterprises should consider SD-WAN alternatives and be prepared to purchase services or solutions from vendors in the next one to two years, as well. Recent data from IDC's 2017 U.S. Enterprise Communications Manager Survey confirms that 17% of enterprises plan to migrate to SD-WAN in the next year and 29% plan to do the same in the next one to two years.

By evaluating their needs across the appropriate range of criteria outlined in this white paper, they can match the networking capabilities to their business needs and evaluate carriers with an established background of offering a comprehensive suite of global software-defined WAN services including network-based IP VPN and SD-WAN features, along with network planning, management, WAN optimization, and managed application service choices. Enterprises should choose a carrier that can partner with them on a network WAN strategy on a regular basis, proactively advising them on improving and optimizing the network as their business and network applications evolve.
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-insights-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2017 IDC. Reproduction without written permission is completely forbidden.