WHITE PAPER

Choosing the Best Enterprise IP VPN or Ethernet Communication Solution for Business Collaboration

Sponsored by: AT&T

Nav Chander
June 2015

EXECUTIVE SUMMARY

Today's enterprise information and communications technology (ICT) staff are demanding increasingly larger amounts of bandwidth and an extremely reliable set of converged virtual private network (VPN) services from their service providers so that they can deliver a rich suite of voice, video, and business-critical data applications to their users with the desired level of performance and quality of service (QoS). Service providers must be prepared to offer a suite of WAN services that can be tailored to their customers' needs rapidly and cost-effectively.

This IDC white paper analyzes the trends and business drivers that are propelling enterprises toward network-based IP VPN and Ethernet WAN services and the types of applications and vertical segments that are leading the adoption of these popular services. The paper first examines the major differences between an Ethernet WAN and a network-based IP VPN and then discusses the benefits and advantages of the two technologies. The paper reviews some typical examples of when it is best to use a network-based IP VPN solution, an Ethernet WAN solution, and a combined hybrid IP VPN/Ethernet WAN solution based on different enterprise requirements. Both IP VPN and Ethernet WAN services offer enterprises a range of technology and business benefits and perform best when deployed in environments that closely match their capabilities.

SITUATION OVERVIEW

Introduction

WAN connectivity options for enterprises range from traditional private line, frame relay (FR), and ATM-based WAN connectivity to newer services such as network-based IP VPN services and Ethernet WAN services. IP-based WANs are widely available and ubiquitous and offer QoS that is the foundation of network-based IP VPNs. Therefore, many enterprises are opting for network-based IP VPNs and Ethernet WANs as their WAN service of choice.

Today's IP VPNs are based on multiprotocol label switching (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:

1. 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.
2. 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 premise 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 2014 *U.S. Enterprise Communications Manager Survey*, 42% of U.S. business respondents across company size segments utilize network-based IP VPNs.

Ethernet

Ethernet's popularity as a WAN technology is gaining rapidly because it 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 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 it 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 extend 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 increasing popular choices for organizations that are currently employing packet services.

Enterprise Data Application Drivers and Challenges: State of the Ethernet WAN and IP VPN Services Market

IDC research indicates that over 55% of enterprises are currently running their VoIP over their corporate VPN or Ethernet service, and an additional 30% of enterprises plan to transition to IP-based voice and video services over their corporate WAN within the next one to two years. Unified communications, videoconferencing, video surveillance, and mobile enterprise applications are driving increasing bandwidth requirements and the need to prioritize the applications for enterprise ICT managers. Video services alone are pushing the limits on bandwidth requirements in the WAN. IT decision makers have to balance end-user application needs with WAN connectivity requirements and associated budgets.

CIOs are increasingly looking to consolidate their datacenters (DC virtualization) to a small number of datacenter locations to reduce space, energy, equipment, personnel, and maintenance costs and adopt cloud-based service models while providing uniform WAN access to all applications in a reliable manner. With this approach, a WAN plays a vital role, connecting all enterprise office locations to the datacenters, to each other, and to the Internet.

Another cost-saving strategy that CIOs are employing is to move away from building and managing their own WANs based on the use of ATM, frame relay, or leased line services. Instead of using these technologies, some CIOs are procuring Ethernet WAN and IP VPN services, which allow them to focus on their core business. Consequently, the reliance on Ethernet WAN and IP VPN services has become critical.

According to results from IDC's 2014 *U.S. Enterprise Communications Manager Survey*, continuing enterprise focus on convergence is the single most important driver fueling adoption of network IP VPNs, as customers realize the cost benefits of migrating their voice, data, and video applications to a single IP-based network compared with running three different expensive networks for each of these applications. As the market migrates to network IP VPNs to take advantage of the network's ability to support traffic prioritization through class of service (CoS), there is a growing focus on network and application performance monitoring tools. These tools are critical for the success of an IP VPN implementation as customers migrate to a converged architecture and demand more control over the applications they wish to run on the network.

Ethernet WAN services are flexible and can carry multiple types of traffic, including voice and video, as well as non-IP-based traffic and storage traffic. Ethernet WAN is a Layer 2 solution, which appeals to organizations that prefer to maintain control over their routing tables and are looking for an alternative to Layer 3 IP VPNs.

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.

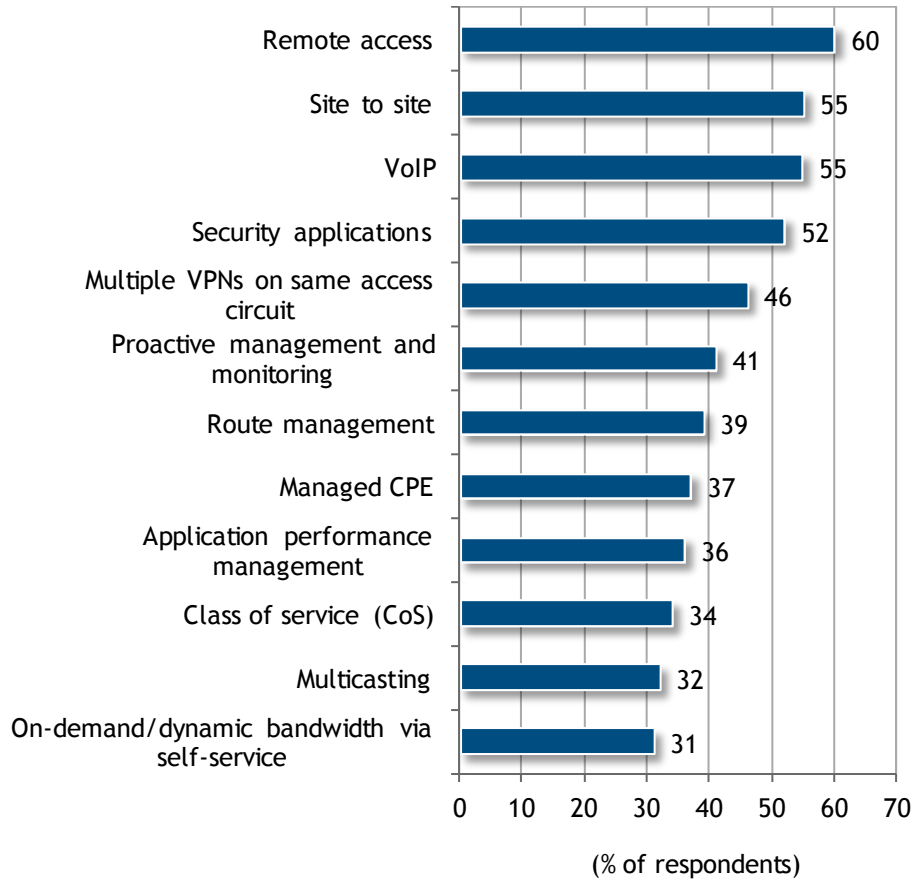
Today's MPLS network-based IP VPNs are the foundation of many enterprises' distributed data communication. IP VPNs are often the communication platform of choice to enable additional value-added enterprise applications on top of their VPN, such as VoIP, security, videoconferencing, and unified communications.

IDC's 2014 *U.S. Enterprise Communications Manager Survey* offers insights into the Ethernet and IP VPN WAN adoption criteria and usage of enterprise IT personnel, providing a good indication of the leading requirements for VPN selection and indicators of migration options from legacy WAN packet and private line WAN services. According to IDC's 2014 *U.S. Enterprise Communications Manager Survey*, 60% of respondents currently use IP VPNs for remote WAN access, making it the most widely used feature. 55% of respondents now use IP VPNs to transport VoIP traffic as the second most widely used feature, a 5% increase from IDC's 2012 *U.S. WAN Manager Survey* as VoIP adoption accelerates. The survey indicates that enterprises increasingly are using IP VPNs for smaller locations and Ethernet connectivity for large sites or datacenters with fiber access.

Figure 1 depicts the IP VPN use case adoption.

FIGURE 1

Key IP VPN Adoption Criteria



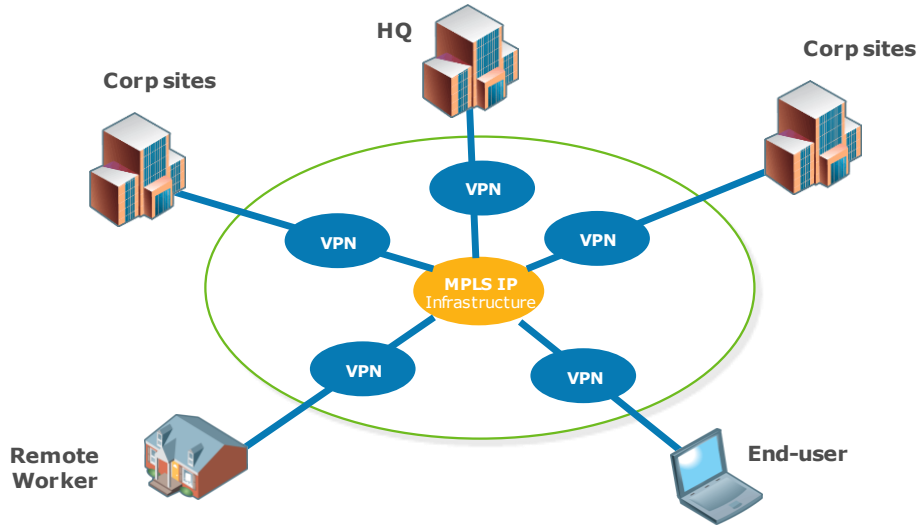
U.S. only n = 274

Source: IDC's *U.S. Enterprise Communications Manager Survey,* 2014

Figure 2 is a typical network-based IP VPN topology.

FIGURE 2

Network-Based IP VPN Topology



Source: AT&T, 2015

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. 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 (56K 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:

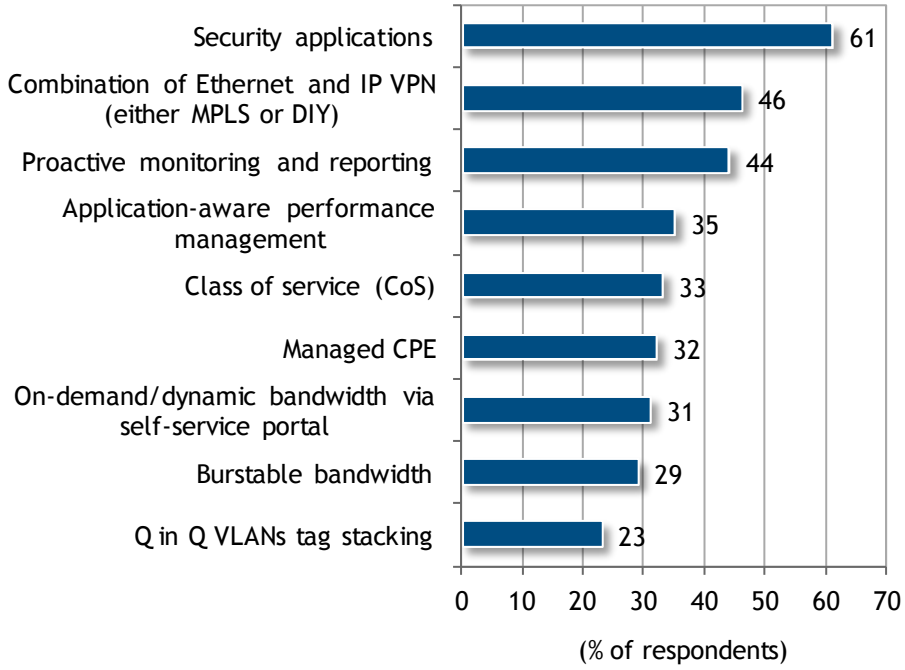
- **Finance/banking.** Regulatory changes, mergers and acquisitions, and technology changes are impacting financial and retail banking WANs. Often these WANs are an amalgamation of separate WANs, some still operating legacy banking applications that support multiprotocols. Access speeds vary from higher 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, 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. IDC interviews with enterprise IT/communications managers revealed that rapid adoption of Ethernet WAN services has been driven by cost, ease of implementation, and a familiarity with Ethernet architecture already employed in corporate LANs.

FIGURE 3

Key Ethernet WAN Features



n = 526

Source: IDC's *U.S. Enterprise Communications Manager Survey,* 2014

Ethernet WANs utilize Ethernet and employ industry-standard technologies, such as the following:

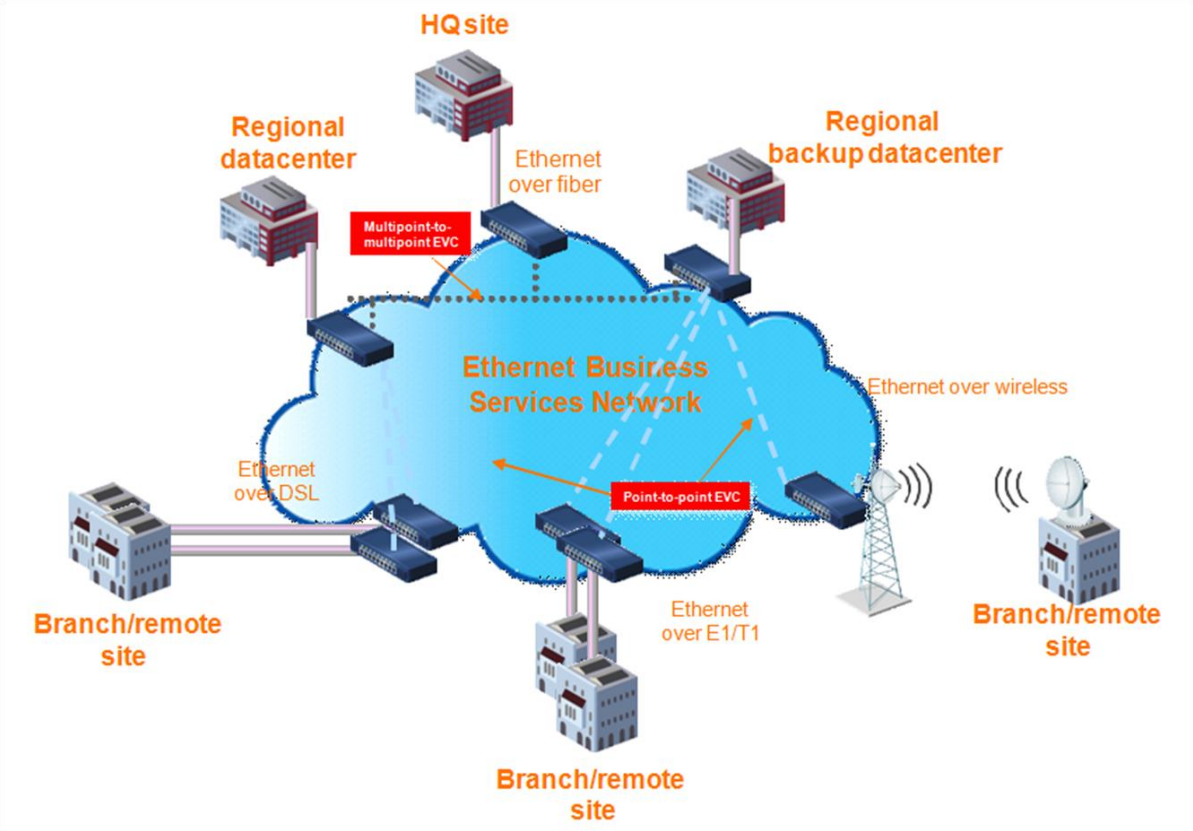
- **MAC address learning** is defined in the IEEE 802.1 standard to help minimize traffic on the attached LANs by storing source MAC addresses so that only packets destined for a given address will be sent to that address, improving the network performance.
- **VLANs** refers to a group of logically 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 its 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 results from IDC's 2014 *U.S. Enterprise Communications Manager Survey* shown in Figure 3, 46% 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 feature, with 61% usage. Figure 4 shows a typical Ethernet WAN with several applications, including datacenter connectivity.

FIGURE 4

Ethernet WAN



Source: IDC, 2015

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, IPX, and others, 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 (IEEE) 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. Though 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 software as a service (SaaS).** A growing number of enterprise software companies such as Salesforce.com, Google, Citrix, SAP, Oracle, and many others 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.

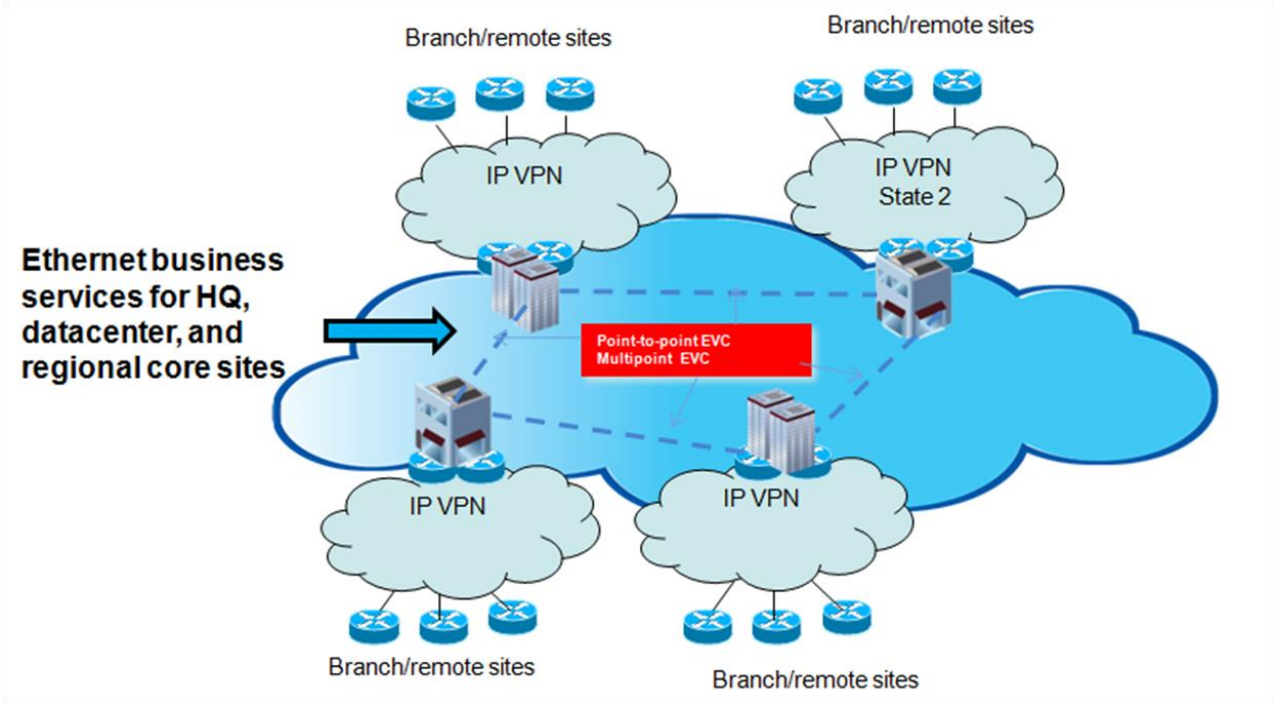
Hybrid Ethernet and IP VPN WAN Solutions: Coexistence of Ethernet WAN and Network-Based IP VPN Services

A majority of the respondents from IDC's 2014 *U.S. Enterprise Communications Manager Survey* choose to "mix and match" 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. For example, Figure 5 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 to connect to other sites on the network. The smaller branch office/remote sites use an IP VPN service to connect to any site on the network.

FIGURE 5

Ethernet WAN and Network-Based IP VPN Services



Source: IDC, 2015

Table 1 compares the requirements of Ethernet WAN services and network IP VPN services.

TABLE 1

Comparing Ethernet WAN Service and Network-Based IP VPN Service Requirements

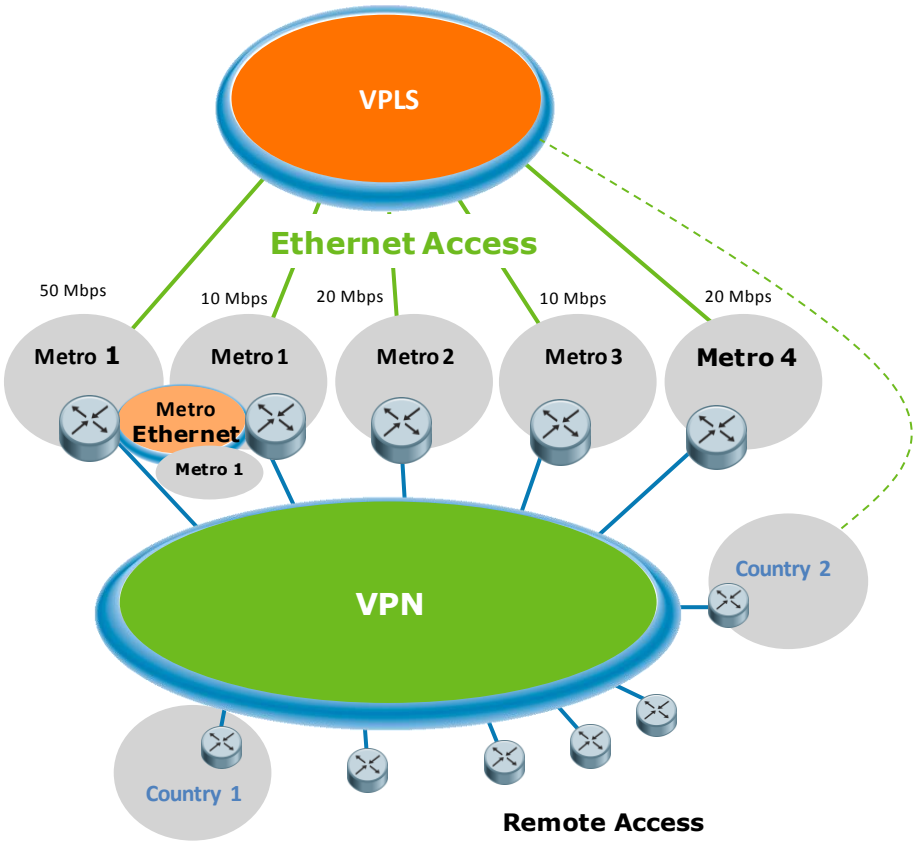
WAN Requirement	Ethernet WAN	Network IP VPN
Protocol transparency (non-IP)	✓	
Enterprise manages WAN connectivity	✓	
Routing control outsourced to service provider		✓
Connection speeds	1Mbps–10Gbps	56Kbps–1Gbps
Managed connectivity to large number of sites, globally distributed		✓
Diverse access choices (PL, DSL, FR) for smaller enterprise sites	✓	✓
Enterprise self-provisioning of bandwidth changes	✓	
High-bandwidth connectivity between core sites and datacenters plus managed connectivity for branch sites	✓	✓
Support for multiple CoS	✓	✓
Support for enterprise VoIP within a VPN service	✓	✓

Source: IDC, 2015

Figure 6 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.

FIGURE 6

Hybrid Network Using Metro and Regional Ethernet WANs, Ethernet Access, and Network-Based IP VPN



Source: AT&T, 2015

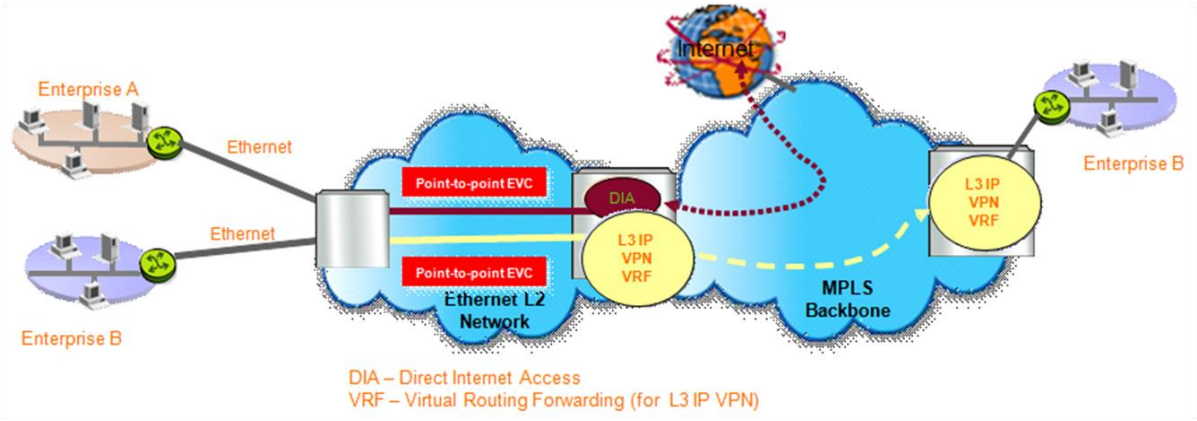
The following vertical enterprise segments illustrate how hybrid networks are used in enterprises:

- **Financial services.** 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 of the enterprise sites. This hybrid solution provides the enterprise with the flexibility to leverage the appropriate service based on its needs.
- **Healthcare.** 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 7 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 a Ethernet WAN for high-bandwidth point-to-point connections between datacenter and headquarters or as a gateway to offload traffic to the public Internet.

FIGURE 7

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



Source: IDC, 2015

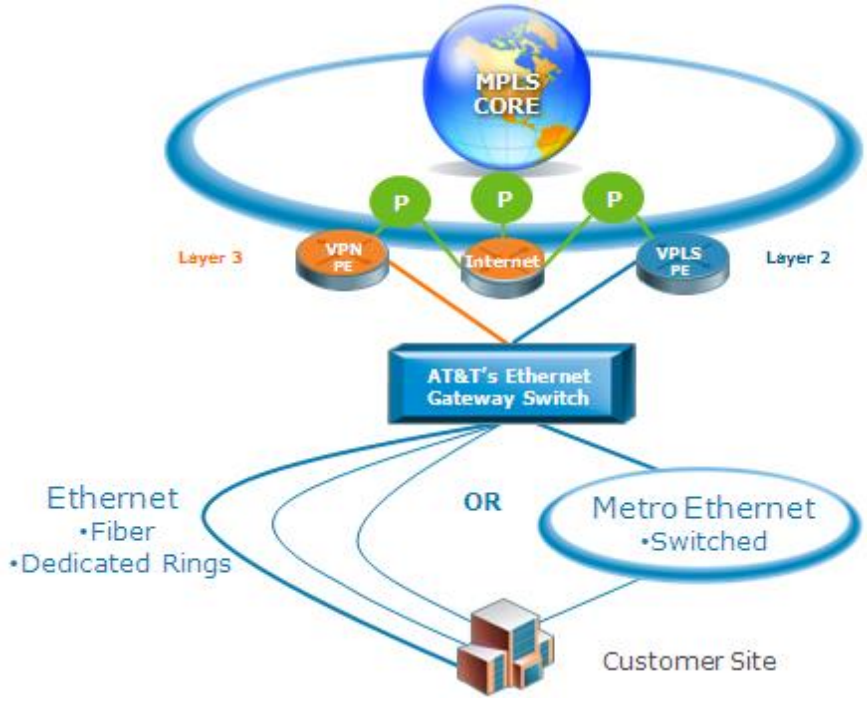
Ethernet Access to Hybrid Ethernet WAN and IP VPN

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, as shown in Figure 4 and Figure 8. 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 a IP VPN service, as depicted in Figure 7, 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 PoP.

FIGURE 8

Ethernet Access to the Internet, IP VPN, and VPLS



Source: AT&T, 2015

SUMMARY

Network-based IP VPNs and Ethernet WANs are two of the most popular WAN connectivity alternatives for many of today's leading enterprises. Enterprises should select service providers that offer robust solutions based on an MPLS/IP backbone network that have the flexibility to deliver either type of service, including hybrid solutions utilizing both services.

Both network-based IP VPN services and Ethernet WAN services offer enterprises a range of technology and business benefits but perform best when deployed in environments that closely match their capabilities. Network-based IP VPN provides a flexible platform to unify communications across an enterprise's distributed locations, and Ethernet WANs are best at supporting high-throughput applications within a more limited footprint and are often used to connect multiple LANs in a single metro area or interconnect metro WANs. By evaluating their needs across the appropriate range of criteria outlined in this paper, enterprises can match the networking capabilities to their business needs and evaluate carriers with an established background of offering a comprehensive suite of

global network-based IP VPN and Ethernet 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