EXECUTIVE SUMMARY

Today's enterprise WAN networking environment is characterized by global coverage, an end-to-end IP-based application environment, increasing use of on-demand applications, and a wide variety of network topologies, network carriers, and access services. Enterprise adoption of hybrid network-based IP virtual private network (VPN) services that combine MPLS-enabled VPNs for larger sites and IPSec network-based VPNs for smaller locations, mobile users, and mobile remote access is increasing. Enterprises of all sizes expect flexible, secure, and robust VPN connectivity for business applications from anywhere at any time.

This IDC white paper discusses the following:

- Combining an MPLS VPN and network-based IP VPN network for remote access offers a unique opportunity for enterprises to connect all of their existing high-speed data, voice, and video enterprise applications over this hybrid private/public VPN network platform with inherent security, quality of service (QoS), and low latency.

- IDC believes that enterprises are most likely to select a VPN communication service provider (CSP) that offers a platform for both managed network services such as managed security and a managed MPLS VPN and that can integrate an internet-based remote access IPSec VPN service. This provides access to business applications regardless of location, access technology, or type of mobile device.

- AT&T's MPLS-enabled VPN and network-based IP VPN platforms combine to provide secure private IP and public internet VPN access that allows enterprises to connect their applications between offices, users, or locations, including access to public and private cloud services.
IN THIS WHITE PAPER

This IDC white paper examines enterprise MPLS and IPSec VPN network applications and recommendations for hybrid network MPLS and IPSec VPN platforms. It also discusses the benefits of the AT&T network MPLS and IPSec VPN platforms for secure remote access and network services.

ENTERPRISE TRENDS AND NETWORK VPN MARKET OVERVIEW

Market Overview

Network-based IP VPNs are the most important component of a managed network service because enterprises increasingly depend on VPNs to support access to VoIP, enterprise data, storage, and security applications between all of their business sites and remote workers.

According to IDC, in 2015, the $8.4 billion U.S. market for network-based IP VPN services was made up of $6.7 billion in managed MPLS VPN services and $1.7 billion in IPSec VPN services. IDC's 2015 U.S. Enterprise Communications Manager Survey found that 69% of all United States-based enterprises with a VPN use an MPLS-based solution. Approximately 32% continue to use CPE-based IPSec VPN solutions. The majority of enterprises still prefer to use a managed network-based IP/MPLS-based solution. With increasingly complex commercial cloud, mobile, and other IP-based collaboration software, robust WAN IP network connectivity solutions are more important than ever, and the IT staff of many enterprises face challenges managing the mix of DIY and various managed network IP VPNs that will include the use of more on-demand network resources. Also, IDC's 2015 U.S. Enterprise Communications Manager Survey found for the first time that less than 41% of enterprises manage all or part of their own DIY VPN with internal IT resources, with this trending toward managed VPN.

MPLS network-based VPNs provide enterprises with the best choice for managed, secure private WAN IP network connectivity from any on-net enterprise location to any other on-net location for a whole range of business applications, including large data transfers, security, VoIP, telepresence, storage, image, and video transfers.

MPLS VPN customers can continue to maintain their own IP addressing plans and also take advantage of a service provider's class of service (CoS) per application to enable the appropriate quality of service. Enterprise application-specific traffic requirements such as performance, latency, and QoS map to the contracted service provider's SLA for a managed MPLS VPN service.

As business organizations decentralize their workforces to be closer to customers or encourage more flexible home-work environments, employees find themselves more disconnected from corporate resources. The mobile remote worker is likely to have access to any combination of broadband, wireless 3G/4G, and/or WiFi networks and needs to securely connect to the VPN with a variety of wireless devices such as laptops, smartphones, or tablets. The integration of devices, applications, and services for onsite workers and remote workers within the same VPN network is critical, and user experience and network performance are equally important in both environments.

For remote mobile workers, remote access network VPN services employing IPSec enable ubiquitous IP access, which is probably the single most important characteristic of a VPN (secure access over the internet or any IP connection for maximum reach for single users or small sites).
IPSec can be used to create secure VPNs over the internet or to add security features in an overlay of an MPLS VPN. When used over the internet, IPSec provides point-to-point connections. IPSec enables an extra level of protection through encryption and authentication and allows the enterprise to maintain its own IP addressing plan through tunnels between sites. IPSec is ideal for connecting isolated company sites and mobile remote workers as well as enabling temporary connections to a VPN (events, pop-up stores, exhibitions). It also serves as a temporary backup for an MPLS VPN network recovery.

Today, many enterprises employ more than one type of VPN service: a managed MPLS VPN for some locations, a separate IPSec VPN for remote access, and possibly even an SSL-based VPN solution for some employees. Integrating application performance requirements across an enterprise is extremely complex. Consider, for example, point-to-point IPSec tunnels – when a new tunnel is added, customer premise equipment will need to be reconfigured in accordance with the changed logical network topology. In addition, packet characteristics may be hidden inside an IP tunnel, preventing the recognition of high-priority flows and making CoS usage difficult and limited to the edge of the network.

Enterprises continue to use one or both, and sometimes, new applications such as telepresence or business continuity can be extended to a larger number of sites and users by employing a hybrid network IP VPN solution.

**ENTERPRISE APPLICATIONS FOR NETWORK MPLS VPN, REMOTE ACCESS IPSec VPN, AND HYBRID VPN**

Today, enterprises have a clear choice of network IP VPN offerings – managed or unmanaged and MPLS or IPSec based. According to IDC’s 2015 *U.S. Enterprise Communications Manager Survey*, remote access, site-to-site connectivity, and security applications are the three most important criteria for selecting an IP VPN service (see Figure 1). The results are very similar to IDC's 2014 survey, with security emerging in 2015 as one of the top 3 issues.
FIGURE 1

Enterprise IP VPN Usage Trends, 2014 and 2015

Q. What features do you currently use on your network-based MPLS IP VPN? Select all that apply.

This section reviews some enterprise use cases and applications for each of the following types of VPN deployments:

- Managed and unmanaged MPLS VPN service
- Managed and unmanaged IPSec network-based IP VPN
- Hybrid managed MPLS and IPSec network VPN

For managed or unmanaged MPLS VPN service, enterprises choose a private IP VPN service that delivers a high degree of service quality and any-any connectivity for all of their locations that are directly accessing the network IP VPN. This ability to prioritize applications by CoS has been one of the key drivers for many enterprises in adopting MPLS VPNs. Using CoS to prioritize business-critical or delay-sensitive applications is becoming increasingly important because some of these applications, such as VoIP, telepresence, and WebEx, require lower latency. Also, mapping multiple VPNs to the same access port has become more important as more enterprises segment their internal business units or departments into workgroups to control access to certain applications, especially as SaaS and software licensing of applications per user have evolved.

In the case of an unmanaged VPN service, the enterprise is responsible for providing the CPE device; configuring the CoS, multiple VPNs, and security attributes; and managing the impact on the VPN network when a new business application is introduced or a change to an application is instantiated. The enterprise has to self-monitor network performance.

Source: IDC's U.S. Enterprise Communications Manager Survey, 2015

n = 346

Base = percentage of respondents who use network-based MPLS IP VPN

For managed or unmanaged MPLS VPN service, enterprises choose a private IP VPN service that delivers a high degree of service quality and any-any connectivity for all of their locations that are directly accessing the network IP VPN. This ability to prioritize applications by CoS has been one of the key drivers for many enterprises in adopting MPLS VPNs. Using CoS to prioritize business-critical or delay-sensitive applications is becoming increasingly important because some of these applications, such as VoIP, telepresence, and WebEx, require lower latency. Also, mapping multiple VPNs to the same access port has become more important as more enterprises segment their internal business units or departments into workgroups to control access to certain applications, especially as SaaS and software licensing of applications per user have evolved.

In the case of an unmanaged VPN service, the enterprise is responsible for providing the CPE device; configuring the CoS, multiple VPNs, and security attributes; and managing the impact on the VPN network when a new business application is introduced or a change to an application is instantiated. The enterprise has to self-monitor network performance.

Source: IDC's U.S. Enterprise Communications Manager Survey, 2015

n = 346

Base = percentage of respondents who use network-based MPLS IP VPN

Source: IDC's U.S. Enterprise Communications Manager Survey, 2015

This section reviews some enterprise use cases and applications for each of the following types of VPN deployments:

- Managed and unmanaged MPLS VPN service
- Managed and unmanaged IPSec network-based IP VPN
- Hybrid managed MPLS and IPSec network VPN

For managed or unmanaged MPLS VPN service, enterprises choose a private IP VPN service that delivers a high degree of service quality and any-any connectivity for all of their locations that are directly accessing the network IP VPN. This ability to prioritize applications by CoS has been one of the key drivers for many enterprises in adopting MPLS VPNs. Using CoS to prioritize business-critical or delay-sensitive applications is becoming increasingly important because some of these applications, such as VoIP, telepresence, and WebEx, require lower latency. Also, mapping multiple VPNs to the same access port has become more important as more enterprises segment their internal business units or departments into workgroups to control access to certain applications, especially as SaaS and software licensing of applications per user have evolved.

In the case of an unmanaged VPN service, the enterprise is responsible for providing the CPE device; configuring the CoS, multiple VPNs, and security attributes; and managing the impact on the VPN network when a new business application is introduced or a change to an application is instantiated. The enterprise has to self-monitor network performance.

Source: IDC's U.S. Enterprise Communications Manager Survey, 2015

n = 346

Base = percentage of respondents who use network-based MPLS IP VPN

Source: IDC's U.S. Enterprise Communications Manager Survey, 2015

This section reviews some enterprise use cases and applications for each of the following types of VPN deployments:

- Managed and unmanaged MPLS VPN service
- Managed and unmanaged IPSec network-based IP VPN
- Hybrid managed MPLS and IPSec network VPN

For managed or unmanaged MPLS VPN service, enterprises choose a private IP VPN service that delivers a high degree of service quality and any-any connectivity for all of their locations that are directly accessing the network IP VPN. This ability to prioritize applications by CoS has been one of the key drivers for many enterprises in adopting MPLS VPNs. Using CoS to prioritize business-critical or delay-sensitive applications is becoming increasingly important because some of these applications, such as VoIP, telepresence, and WebEx, require lower latency. Also, mapping multiple VPNs to the same access port has become more important as more enterprises segment their internal business units or departments into workgroups to control access to certain applications, especially as SaaS and software licensing of applications per user have evolved.

In the case of an unmanaged VPN service, the enterprise is responsible for providing the CPE device; configuring the CoS, multiple VPNs, and security attributes; and managing the impact on the VPN network when a new business application is introduced or a change to an application is instantiated. The enterprise has to self-monitor network performance.
In a managed MPLS VPN, enterprises can securely access network reports and monitor the performance, latency, and bandwidth usage of their private data, voice, and video traffic via a unique customer portal that is part of the service offering and sometimes included as part of an SLA. The ability to adhere to data governance, industry compliance, regulatory, and privacy requirements is another important factor in considering a managed MPLS VPN versus an unmanaged MPLS VPN because of the cost and complexity involved with developing and administering VPN policies.

IPSec-based network IP VPNs are increasingly a popular choice for enterprises trying to connect small offices/home offices (SOHOs), retail locations (restaurants, stores, kiosks), and remote workers to their corporate VPN. Customers use a VPN gateway router to provide an encrypted IPSec connection to access the internet via a broadband or wireless network or even another service provider’s fixed network for these smaller sites. For remote workers, thin VPN client software can be installed on smartphones, tablets, and laptops that enables simple plug-and-play VPN connectivity choices with built-in security policies. Individual employees can also access the IPSec VPN service via public WiFi hotspots.

The third use case involves combining both managed MPLS and IPSec network-based IP VPNs into a hybrid solution to handle all of an enterprise’s on-net and off-net locations and workers.

Today, many enterprises have a mix of sites – including mobile workers, SOHOs, branches, and large datacenter and campus environments – that all need to connect to the same corporate network with secure, predictable network performance. A service provider that supports a hybrid network-based VPN, as shown in Figure 2, enables enterprises to maintain consistent service policies, application performance, and secure connectivity to corporate applications for workers from any location. However, hybrid network-based VPNs can also carry greater management challenges, making it crucial to develop a comprehensive network strategy and select the right service provider.

One of the more popular applications for employing a hybrid IP VPN solution is an enterprise telepresence service that extends telepresence sessions between corporate office locations that are part of the MPLS VPN network to remote access IP VPN sites or even individual workers accessing the VPN. This can be a cost-effective form of secure internal company communication, and it is gaining popularity as corporations reduce travel budgets and increase real-time collaboration.

One of the more interesting applications for this type of hybrid IP VPN solution is employing an IPSec-based VPN that provides temporary access to corporate MPLS network-based VPN resources. Disaster recovery and failover are two applications that can utilize 3G/4G cellular networks to provide alternative VPN connectivity for MPLS-based network sites that experience an outage. This application becomes very important if a location’s network VPN service is temporarily disrupted because of a cut fiber or copper cable or for wider-scale disaster recovery if a major natural disaster occurs and employees cannot travel to their business establishments.
Hybrid Network-Based IP VPN: Optimized for the Enterprise

Access to Core Business Applications Regardless of Location, Access Type, or Device

Today's service provider has to be able to offer a VPN platform solution that has the flexibility to support the use of hybrid network-based MPLS and IPSec VPN networks for diverse enterprise environments. These hybrid platforms increasingly have to provide 99.99% or 99.999% network availability and SLAs that enterprises are accustomed to with a managed MPLS VPN network.

The AT&T Network-based IP VPN Remote Access solutions are designed to provide highly secure access to critical business applications regardless of location, access type, or device across a unified global platform – the AT&T Global Network. Dynamic routing to AT&T MPLS VPN services via high-speed backbone infrastructure is based on MPLS network technology, offering enterprises consistent application performance on a global basis. The AT&T MPLS VPN solution supports service differentiation by employing CoS for latency-sensitive applications.

IDC recommends that enterprises consider a hybrid VPN solution based on the following six attributes that AT&T supports in an MPLS VPN platform and the AT&T Network-based IP VPN Remote Access IPSec platform:

- **Breadth of access and extended global reach.** AT&T’s VPN solution enables consistent application capabilities for small office locations, as if they were at headquarters with backup options for business continuity.
- **Flexibility.** AT&T’s network flexibility provides remote access to an enterprise’s intranet via the MPLS VPN, including simultaneous access to the internet via IPSec when connecting to public internet sites, WiFi hotspots, or cloud services.
- **Resiliency.** AT&T Network-based IP VPN Remote Access is easy to configure, and the on-premise AT&T VPN Gateway can be combined with wireless technology as a redundant connection, restoring VPN service very quickly. The AT&T network gateways are mirrored, geographically separated, and load balanced to ensure network uptime.

- **Security.** AT&T’s VPN Tunneling Service uses IPSec to create paths that carry encrypted enterprise data over public networks, creating a highly secure pathway. This enables integration of applications with enterprise core infrastructure from multiple types of connections, such as broadband, wireless, WiFi, or dial-up.

- **Proactive management and reporting.** AT&T provides VPN network management services, application performance reporting, and network monitoring of both MPLS- and IPSec-based VPN enterprise sites via a customer web portal.

- **Service agility.** AT&T Network-based IP VPN Remote Access is for telecommuters, mobile workers, and remote staff in an office setting. The AT&T VPN Gateway along with AT&T Network-based IP VPN Remote Access provides a complete solution for these settings. Mobility options include 3G/4G wireless or WiFi access to AT&T Network-based IP VPN Remote Access, providing fast connections and extending the reach of the enterprise VPN.

### OUTLOOK FOR HYBRID MPLS AND IPSec NETWORK VPNS

IDC believes that there is a growing market requirement from enterprises for a hybrid network-based IP VPN solution that can provide private IP/MPLS-based on-net VPN services and extend access to off-net services via a VPN that accesses the public internet or cloud service. Increasingly, enterprises will look for the flexibility to reach all of their locations with the security and privacy of a VPN.

Enterprises expect their own IP VPN network expansion requirements will include a mix of always connected on-net sites, remote small offices, remote workers, mobile workers, and external partner sites. A hybrid VPN platform solution that incorporates the best of both MPLS and IPSec VPN solutions will be more appealing and more cost effective for enterprises that have off-net users who infrequently access the VPN. The hybrid VPN will become important as IDC predicts that enterprise IT applications and hosting of applications will shift over time to cloud or mobile environments.

Best-in-class network IP VPN platforms can address the growing need to securely connect these business applications from any combination of wireless networks, the internet, public cloud providers, and private IP/MPLS networks.

Future advances in managing application session management and access diversity will also play a key role in leveraging remote access IP VPN solutions and optimize the customer’s application performance across multiple VPN networks from 3G/4G, broadband, and WiFi hotspots and then enable enterprises to prioritize between “lowest cost per bit” and lowest latency.
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

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 2016 IDC. Reproduction without written permission is completely forbidden.