The IP VPN sector is the fastest growing networking sector today, and is now a viable WAN option for the global enterprise. IP VPNs are used to ensure the privacy of WAN data over shared IP network infrastructure and to support convergence of applications and networks where classes of service (CoS) are provided.

IP VPN technology has boomed because it meets many of the needs of multinationals. Such companies need to extend their business practices to allow efficient electronic transactions among members of a business community – commonly called an extranet. They need to create a business environment that allows vendors and partners to exchange data – quickly, efficiently and securely. They also need to support multiple branch offices and large numbers of workers outside the office ensuring they can work efficiently and seamlessly, as if they were in the office environment. They also need to reduce costs, with an improved return on investment through right-sizing the network configuration to address application requirements.

However an IP VPN differs from traditional WAN technologies and the right type of IP VPN to fit the end-user’s needs must be selected if these benefits are to be realised.

An IP VPN is not a single product, but rather a collection of technologies that have been brought together in a common cause. The idea is to preserve the openness of the protocol yet provide a common security framework. An IP VPN could be defined as a partitioned private network constructed over a shared IP-based backbone using technologies to ensure privacy of data, either self-provided or provided by an IP-based service provider. It may connect dedicated sites and/or remote users to corporate sites, provide authentication of remote users, and encrypt data.
To address these requirements, companies have traditionally used a mix of private and public infrastructures. High performance is provided through leased lines and private networks – but maximum reach, such as to remote locations, is provided via the internet. Security is achieved through traditional firewalls and encryption.

There are predominantly three types of IP VPNs:

- **Private IP VPNs supported by a private IP network** – usually MPLS-based and offering a CoS that has been built to support users within a closed user group environment
- **Public IP VPNs via the internet network offered by one provider or in a multi-provider environment** – these are usually created with IPSec and offer an inexpensive alternative to private services
- **Hybrid IP VPNs using some private and some public components** – for example, a public IP VPN mixed with a secure private IP VPN for flexible/cost-effective WAN access to remote sites

Private IP VPNs are built around dedicated IP backbones and wholly owned and managed infrastructure. They are secure, high-performance network configurations. Typically, private IP VPNs employ MPLS technology to speed up and improve the switching of network traffic across various data protocols. MPLS is the next step in the convergence of network infrastructures, supporting both time-sensitive and time-insensitive applications across the same bandwidth. IP networks using MPLS and related protocols have quality of service (QoS) capabilities that allow users to establish different priorities for different packets of data, depending upon their time sensitivity.

Public IP VPNs, on the other hand, provide a cost-effective network solution using the internet and either single-provider or third-party networks to extend the IP VPN service to virtually anywhere in the world. This type of arrangement is especially applicable to those sites that may have historically been prohibitively expensive to reach through Frame Relay access, for example. It may also be the right choice at those sites that only require messaging or file transfer and not the CoS provided in a secure private IP VPN arrangement.
Hybrid IP VPNs, which mix both private and public IP VPNs, offer the advantage of both private and public infrastructure access. A user’s core may be provided over fully managed network elements secure enough for service level agreement (SLA) guarantees but linked to extended sites across the globe providing another level of flexible, cost-effective access.

**Capitalising on the Benefits: Network Configuration**

How IP VPNs support extranets and remote users is evident by the nature of the technology and choice of a private, public or hybrid configuration. Cost savings that produce a positive ROI on the IP VPN investment can be achieved even when migrating from an existing WAN structure, but the benefits of IP VPN technology must be leveraged fully: the any-to-any network configuration; the potential to right-size the network configuration to suit applications; and, of course, convergence.

The VPN any-to-any network backbone has an obvious capacity impact for large multinational enterprises compared to the highly meshed legacy point-to-point infrastructure. The principal difference, in terms of bandwidth, is that the number and location of various sites becomes incrementally less important as the number of addressable sites grows with an IP VPN. In other words, each time a new node is established and configured on an IP VPN it is able to communicate "directly" with every other node.

Convergence is certainly the most touted benefit, and clearly IP VPNs’ ability to use the same link for both low and high demand applications allows users to support their business requirements on a more efficient access circuit network. Migrating traffic types for separate links onto one initially requires additional IP bandwidth to handle the additional traffic, but the cost of a higher-speed access link is lower than a second WAN connection.

Migrating, or even growing into, an IP VPN from a legacy VPN will most likely require a change to the dimensions and topology of the existing network. The overall site redundancy requirements, cost implications, and other factors will dictate the best design for a company or site.
**Implementing an IP VPN**

The future for IP VPN uptake looks bright, analysts IDC predict the market will grow to U.S.$14.7 billion by 2006.

Cost effective, increased reach is not enough to ensure that the boom continues; companies must be confident that IP VPNs can continue to meet the demands of their mission-critical, voice, data and multimedia applications. This ability will be determined immediately in the first decision made while implementing an IP VPN: whether to do-it-yourself or rely on a carrier-managed IP VPN.

**DIY versus Carrier-Based IP VPNs**

DIY is still the most popular method of IP VPN provisioning. Many companies perceive that it increases their control and ability to capacity plan the network, while also reducing costs. A DIY VPN is based either on leased lines or on the open internet.

The leased line-based IP VPN allows for managed network performance but requires considerable investment and operational expertise. The open internet type is the commonly used DIY concept, but end-to-end security is limited to sites where appropriate encryption technology and expertise are deployed. QoS with performance SLAs might be provided in the case of a single provider but is non-existent in a multi-provider environment.

On the other hand, a carrier-based solution has the advantage of using a service provider with the expertise and staff specifically dedicated to the day-to-day management and operations of the WAN. This means that the customer can benefit from guaranteed network performance and customer support. Legacy WANs have traditionally been run and managed by carriers, so many network managers may look to take up a similar management solution for their IP VPN. A carrier-managed IP VPN frees up those responsible for managing the WAN to do just that – manage the WAN, removing the need to internally operate the network on a day-to-day basis.
The appropriate IP VPN solution will ultimately depend on the type, performance, behaviour and mixture of the enterprise applications, as well as the company's outsourcing policy, cost factors, type of e-business partners, security requirements and traffic topology.

There are four factors that a company needs to address to ensure its IP VPN successfully meets the original business goals: security, flexibility, guaranteed SLAs based on class of service, and cost savings.

The private nature of an IP VPN provides an additional layer of security for information transported over a WAN. A dedicated, protected private network guards critical applications from compromise, slowdowns or denial of service. The additional features of MPLS, which were originally aimed at providing predictable network performance via QoS features, also provide security in an IP VPN. The two most common methods of providing data privacy are encryption and traffic partitioning through the creation of a VPN or via leased lines.

**Encryption**

IP VPN encryption relies on IPSec incorporated into the IP protocol. Currently, IPSec is the dominant mechanism for providing public IP VPN tunnelling. IPSec encryption comes in two varieties: the data encryption standard (DES) and the more robust triple DES (3DES). These provide two levels of authentication: with or without public key infrastructure (PKI), a digital certificate or with shared key. Encryption protects VPN users from other internet users and provides high levels of authentication and integrity. It is a relatively inexpensive way to extend service to sites on the internet or, likewise, sites supported by third-party providers on the internet. Performance and service characteristics of the extensions differ from the core private IP sites.

**Traffic Partitioning**

Traffic partitioning offers a high level of security to private IP VPNs, equal to that of a Frame Relay service. Currently MPLS is the most common technology used to separate specific data streams from other traffic using the same, shared network. The idea is that closed user groups are dynamically set up for a specific user's IP VPN using MPLS. Such a group
is dependent on a membership list rather than a pre-defined site-to-site connection.

An IP-based network will connect to all other internet connections, potentially exposing the network to unknown traffic. This can put the customer’s network at risk from malicious users looking to attack chosen destinations with, for example, a denial-of-service (DoS) attack. The most reckless DoS attack is one of "bandwidth consumption" that takes advantage of the very thing that makes the internet so useful – its openness. An attacker, using an internet-based platform, first launches a recognisance mission to search for a network’s open IP ports. This is then followed by an attack that can consume the available bandwidth within a service infrastructure, using the large network resources of other networks to flood a victim’s location.

IP VPN’s benefit of convergence means that corporations can take an application-defined approach to network planning. Users have increased control over the destination of data and its transportation, the ability to partition traffic, along with the options of utilising both public and private networks.

Efficient use of Capacity
The integration of VoIP, video, multimedia with low demand applications is one example of the access circuit re-organisation that IP VPNs allow. Of course the obvious flexibility inherent in convergence is the efficient use of capacity. Companies deploying IP will usually have a parallel standard switched telephone network connection for common telephony. As the deployment of general and mission-critical IP-based applications grows so will the IP networks over which they run. The increasing availability of IP capacity eases the decision to migrate voice traffic. A regular PSTN connection will remain functional for many years, but could be easily offloaded to an IP VPN to decrease total bandwidth requirements. This will also result in an efficiently planned and maintained network with no QoS issues.

Class of Service Options
Class of service (CoS) is a critical factor in building networks to support the applications a business needs to operate. It ensures that the performance characteristics of all network traffic are met by separating different
streams of traffic. CoS in the core of the network will ensure high quality and consistent levels of performance, regardless of class.

There are usually three to five CoS that can be supported by a private IP VPN infrastructure, ranging from best effort for simple IP access to critical, real-time processing for voice, video and multimedia.

The multiple CoS options guarantee different performance levels for different applications and also allow more efficient use of available access bandwidth by using idle capacity for non-latency sensitive applications. This allows voice or file transfer applications to be added to the same port. Another key by-product of CoS is the segregation of IP VPN traffic into separate physical or logical virtual circuits from public internet traffic. VPN traffic is contained within the service provider’s network and does not transit public peering points.

Public IP VPN is usually thought of as a uni-class service, where applications are still combined, but be aware that no distinction is made between time-sensitive and time-insensitive applications.

A network service level agreement (SLA) for on-net service should address basic parameters such as availability, round-trip delay, and packet loss. Voice services should also include a jitter component and potentially even an MOS (Mean Opinion Score) measure to quantify actual voice quality.

**Service Level Agreements**

The SLAs offered will depend on the location of the sites that are being connected and the end-user’s network. Different performance SLAs are available for each CoS. Additional value is realised by Web-based reporting options to support the SLA, resulting reports can include network statistics, link utilisation and router health.

Any-to-any connectivity provides default connections to other business sites without having to purchase connectivity to each site, thus reducing complexity and simplifying administration. A combined private and public network IP VPN offers the cost effectiveness of a shared network, along with network management and the reduced billing associated with converging data,
voice, and video over a single infrastructure. IP VPN’s ability to support new applications with their own inherent cost savings, such as VoIP, provide another method to leverage the IP network.

**A Mature WAN Technology**

IP VPNs are now joining other solutions as a mature WAN technology, while offering the advantage of meeting the aggressive ROIs that multinationals are demanding out of their IT investments. The rapid growth of the IP VPN market is sustainable since IP VPNs uniquely support globalisation requirements more efficiently, whether it be extranets that create a business community with vendors and partners, or creating virtual office environments for telecommuting workers and remote branch offices. However, an IP VPN’s benefits will only be realised through active network planning and management. This means multinationals should factor in more than just the cost difference when making the decision between a DIY versus a carrier-managed IP VPN.

**About Infonet**

Infonet Services Corporation, known for its quality of service, is a leading provider of managed network communications services, for nearly 3,000 multinational entities.

Employing a unique consultative approach, Infonet offers integrated solutions optimising the complex relationship between enterprise applications and the global network. Extensive project management capabilities are the foundation for the services and solution offerings (broadband, Internet, intranet, multimedia, video conferencing, remote and local access, provisioning, application and consulting services) positioning Infonet as a single-source partner for multinational entities. In particular, Infonet IP VPN solutions offer multinationals a unique combination of Private and Public IP services as well as a full set of Managed Security Services.
Rated “Best in Class” overall in Telemark’s survey of Global Managed Data Network Services, Infonet has also won “Best Customer Care” and “Best Carrier” at the World Communication Awards. Founded in 1970, Infonet owns and operates The World Network®, accessible from more than 180 countries, and provides local service support in over 70 countries and territories.

Infonet’s stock is traded on the New York Stock Exchanges under the symbol IN. Additional information about the company is available at www.infonet.com.