



**Secure
Resilient
Networks**

May 2008

Whitepaper

IP-based networks overtake proprietary technologies for wide area networks

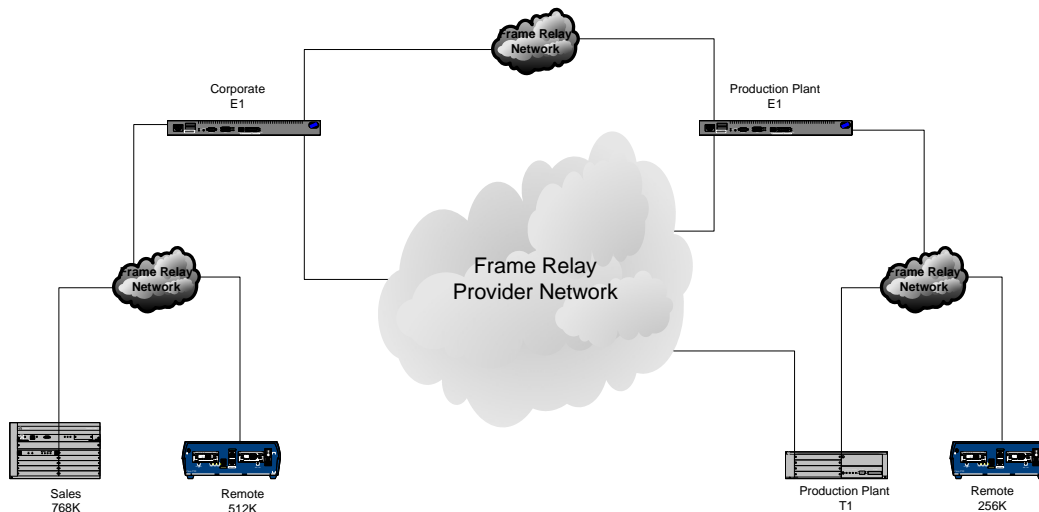
By: Andy Conway

Professional Services Director, CI-Net Ltd

IP WANs overtake proprietary technologies

For quite some time IP networks have been the technology of choice for LAN's. It was thought to be totally inconceivable that IP based networks would overtake proprietary technologies such as ATM and Frame Relay for wide area networks (WANs). However, that is exactly what has happened.

Typical Legacy Frame Relay



There are a plethora of decisions to be made on how to deploy an IP based WAN and various technologies that have the potential to meet the many and varied requirements. Should you wish to deploy a layer two or layer three network there are a number of questions that need to be answered:

- How do IP Sec VPN and SSL VPN fit in?
- Is it necessary to implement MPLS?
- Do you move over in a phased approach or does it have to be 'big bang'?

In this whitepaper we hope to dispel some of the myths surrounding IP WAN's, provide a clear understanding of the various drivers for the different technologies and some information on how best to roll out an IP based network.

Common 'must haves' for a WAN

A WAN should be the vehicle that allows ALL disparate parties to communicate in a secure and reliable way. This includes the Head Office, Regional Offices, International Offices, Trading Partners, Remote Workers and Home Workers. As technologies converge so the WAN can be the transport infrastructure for all traffic whether it be data, voice or media. Whilst each Wan is different and each company will have specific needs the core requirements will almost certainly remain the same.

1. **Reliability:** a reliable network that is available to support your business without interruption.
2. **Quality:** you will want your packets to arrive in such a way that the service is usable. For example if you are using VoIP it is important that voice traffic be given priority when there is congestion on any part of the network to avoid jitter in the call. This can be achieved by using a different 'Class of Service' for different traffic.
3. **Privacy:** as company confidential data is pinged around the WAN you need to be certain that no one can tap the data stream and steal your proprietary information. This has long been the strength of legacy networks, but has come at considerable cost.
4. **Secure Internet Access:** – Whilst you may want to avoid using the internet as part of your inter-office WAN it will be important for email and for browsing. It is important therefore to have up-to-date firewalls, anti virus and anti spam, and to consider controlling and auditing the sites employees are accessing.
5. **Home Workers** – as employers become more flexible and we all become more aware of the effects of global warming, reducing unnecessary travel home working is now common practice in many organisations, this offers the added benefit of providing workers with an office environment should the main office be unavailable due to disaster.
6. **Secure Remote Access:** it is not just access from home offices; many employees need access when travelling. This access will typically be from a hotel room or increasingly from wifi hotspots and you need to ensure your WAN is not exposed.
7. **Business Continuity:** Should the need for business continuity arise in the event of terrorism, epidemic or natural disaster , the network should either automatically fail over to DR locations or be quickly configurable to provide access to remote systems.

MPLS Networks

A key driver for IP based WANs is the need for a cost effective network that supports convergence and allows prioritisation across the network. Many think that Multi Protocol Label Switching (MPLS) is the only show in town. However, this is simply not the case. Whilst MPLS does offer some advantages, there are a number of limitations that need to be taken into account.

MPLS was originally developed to overcome a problem that is now obsolete, namely to address performance differences between layer 2 switches and layer 3 routers. With the development of new hardware this performance difference has evaporated, but MPLS remains and can be implemented in either layer 2 or Layer 3.

Layer 2 MPLS: a cost effective alternative to point-to-point higher bandwidth leased lines it is used by many wholesale network vendors as this type of transit is protocol independent and allows anything running over a LAN to be sent over the WAN without the need to use routers to convert packets up to Layer 3.

Whilst there are advantages of this approach they tend only to be only available at higher bandwidths from wholesalers and do not support point-to-multipoint, which means they are not often used in enterprise WAN's.

Layer 3 MPLS: more suitable for multisite enterprises where there is a mixture of high and low bandwidth sites, such as Head Office and retail outlets, it has often been used as a replacement for Frame Relay and ATM networks. However, MPLS is not the real requirement and does have some significant limitations:

1. Layer 3 MPLS, like Frame Relay and ATM are proprietary networks, which means you are tied to one provider and one network.
2. The MPLS provider must have control over the entire network infrastructure in order to establish an MPLS path.
3. MPLS can be expensive to implement and maintain.
4. The management of MPLS networks can be cumbersome. For example, changing a Class of Service can take more than five days to roll out across a medium size network and some carriers charge for prioritization.
5. Data is not encrypted across the network leaving a security risk from data tapping or back-door access from shared carrier infrastructure. While standards have been proposed for interconnecting MPLS networks there are significant business, financial and technological barriers to overcome before this practice becomes accepted. This cuts across the whole concept of a private network and would require additional security features such as encryption.



**Secure
Resilient
Networks**

May 2008

Virtual Private Networks

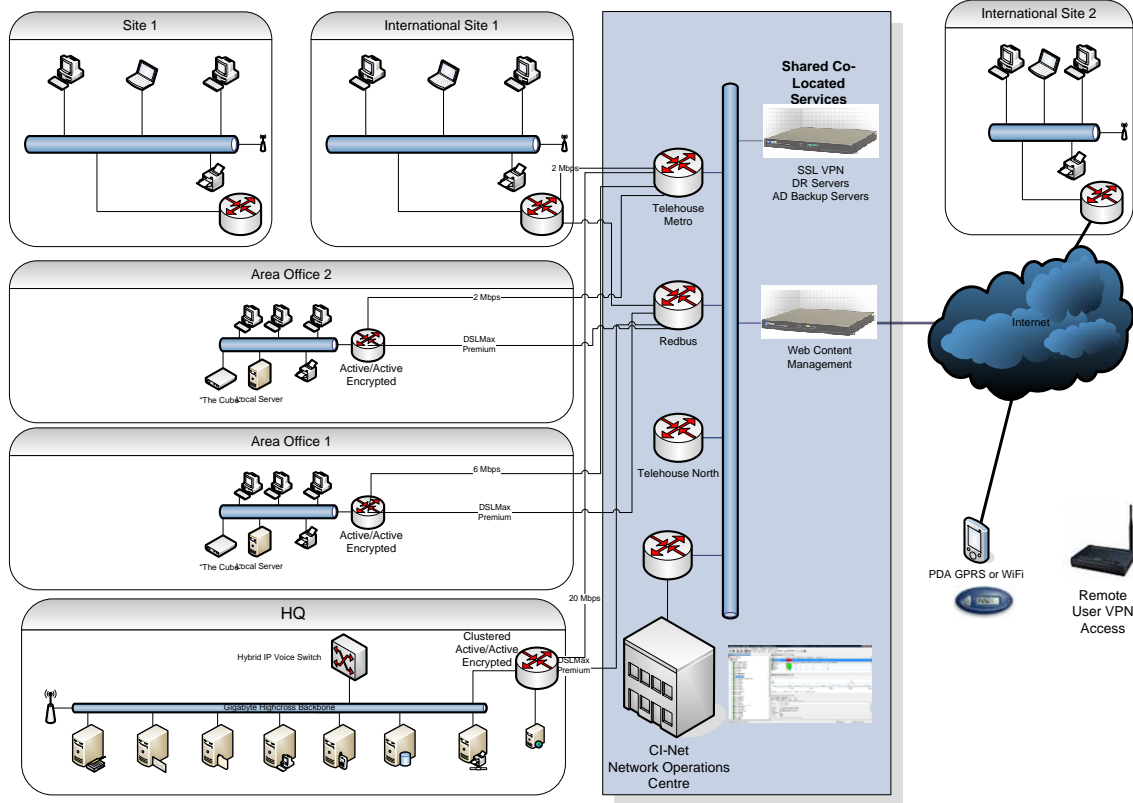
With the advent of IP and IPSec (Layer 3) technologies more cost effective and flexible solutions are available. Service providers like CI-Net are able to utilise the carrier class shared network to build Virtual Private Networks (VPN's). The great advantage being that these networks **provide the same bandwidth and security as private networks but at a fraction of the cost**. In addition all data is encrypted to minimise the risk of data being tapped. Finally these are not proprietary so you are not tied to a single vendor and can substantially ease the pain of migration.

In the past maintaining IPSec based networks has proven complicated, with each separate link needing to be defined on each site. However, technology has emerged over the last four years that enables fully meshed VPN's to be simply maintained via a central management console, introducing the point to point flexibility of MPLS networks whilst maintaining the security and value of IPSec networks.

All carriers have limitations on their reach which means that proprietary ATM, Frame Relay and MPLS networks are invariably unable to provide a total solution - certainly not at a justifiable cost! As the number and locations of an enterprise's WAN points expands so the flexibility of using multiple carriers becomes more attractive.

Unlike VNO's tier 2 carriers like CI-Net can harness their own infrastructure to create a network which remains completely separate from the Internet, using a private IP addressing schemes and cost effective standard communication channels such as Leased Lines, Ethernet, DSL and emerging wireless/cell based technologies. In addition IPSec and SSL can safely use any providers' IP transport.

IP VPN with carrier and technology resilience



IP VPN Centralised Management

In order to deploy and manage an IP VPN the rules are held in each of the customer premises equipment (CPE). At first sight this might seem to be a retrograde step, and a highly intensive infrastructure to manage. However, in order to overcome the deployment and configuration issues CPE hardware vendors like Stonesoft have developed sophisticated management centre software with easy to use drag and drop capabilities. This allows the network manager or 3rd party managed service provider to easily deploy and maintain the most complex of networks, even across multiple carriers. Central Management of the entire infrastructure provides a global view of network health and effectiveness independent of the communication technology deployed.



In conclusion, the implementation of this technology provides a solution to the common must have criteria adding the flexibility to deliver across multiple communication channels anywhere in the world.

Glossary of terms

- IPSec VPN** Internet Protocol Security is a suite of protocols used to implement secure exchange of packets at the IP layer.
- SSL VPN** A VPN accessed via HTTPS from a browser. SSL VPNs require minimal client configuration to allow access to private resources in the corporate network.
- CoS** A way of managing traffic in a network by grouping similar types of traffic (e.g. voice, email and file transfer) together and treating each as a class with its own level of service priority.
- QoS** Quality of Service refers to various schemes to prioritise groups of traffic ensuring they delivered in preference to less important traffic.
- SMC** The StoneGate Management Center forms the core of the StoneGate Platform, providing unified management for StoneGate Firewall, VPN and IPS solutions.