Analyzing MPLS from an ROI Perspective

Site Interconnection

In most cases, a Virtual Private Network (VPN) is considered a means of connecting various locations using a public or private IP network. Increasingly, businesses require a fully meshed network permitting "any to any" connectivity. It is important to determine the need for a meshed network, as the resources and costs associated with creating and maintaining a meshed network are directly impacted by the specific VPN technology deployed. This white paper discusses the most common VPN technologies and highlights hidden costs, which should be considered when deploying a VPN.

Network meshing and the addition of subsequent nodes are automatic functions of "connection-less" technology, including MPLS and IPSec. However, Frame Relay, a "connection-oriented" technology, requires separate "permanent" virtual circuits to be manually programmed, in order for each node to be meshed. Network expansions are time consuming and necessitate the need for accurate record keeping and skilled IT resources. The amount of resources required increases exponentially as the number of sites in the network increase.

Throughput Speed

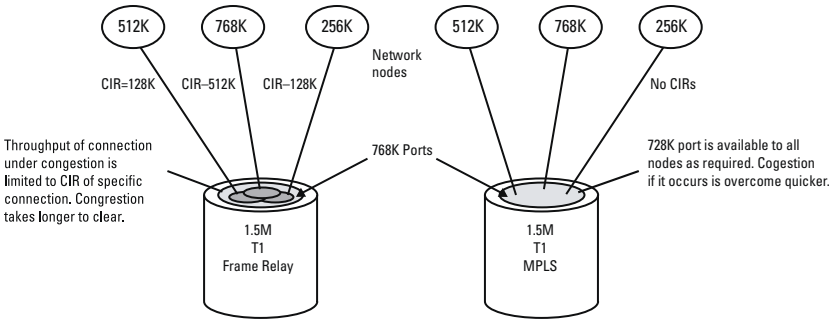
Throughput speed results from a combination of the connecting network circuits' bandwidth and the effects of any congestion that may exist within the network. It is therefore important to understand the manner in which bandwidth is managed within different network types.

In regards to Frame Relay, Permanent Virtual Circuits (PVCs) are established and maintained between sites. End-users subscribe to a minimum bandwidth, Committed Information Rates (CIRs), which is contained within the PVC. For example, over a Frame Relay network, you could have a PVC with 768K of bandwidth, but a CIR with 128K of bandwidth. (CIR must always be equal to or less than the port bandwidth.) It is the CIR rate that will fundamentally affect the price being charged for the Frame Relay circuit.

Under normal circumstances, the full 768K of bandwidth may be available for use. However, when congestion occurs within the carrier's network, data that exceeds the CIR would be deemed 'discard eligible,' because the throughput

Throughput Speed (cont.)

of VPN circuits under congestion is limited to the CIR bandwidth. Under these conditions, data marked as discard eligible would need to be retransmitted, which is unacceptable for time sensitive or real-time applications. Applications such as VoIP, which are latency sensitive, will experience static, crackling, or will drop altogether. Since MPLS does not require PVCs with CIR, congestion is handled more efficiently. The following diagram demonstrates how full port speed would be available to overcome the congested conditions under MPLS or IPSec. With Frame Relay, only the bandwidth of the associated CIR would be available; therefore, congestion recovery would typically occur faster in a MPLS or IPSec VPN.



It is important to consider how end-user business could be affected by congestion. Customers should select the type of VPN that best matches the applications being deployed. For example, if real-time transactions are being processed (i.e. point of sale transactions), congestion between nodes may be deemed unacceptable. Any costs associated with provisioning a higher capacity network may be offset by the additional business gained as a result.

While an equivalent Frame Relay PVC may cost less than or equal to that of MPLS, an equivalent CIR will generally result in increased Frame Relay circuit costs.

Data Prioritization

The type of network being adopted needs to match the application being deployed. While Voice over IP (VoIP) exemplifies the classic need for real-time data prioritization, to avoid dropped calls and transmission distortion, there are many scenarios in which data needs to be prioritized in order for businesses to function efficiently. Internet surfing or e-mail should take lower priority in comparison to point of sale transactions, to ensure that a business is capable of generating maximum revenues.

Although Frame Relay allows for data prioritization, 'Priority PVCs,' which are available from some vendors, add substantial IT resources and associated costs. Implementing 'Priority PVCs' is not automatic; manual intervention is required in many cases at both the customer level and at the carrier level. In an MPLS environment, data prioritization is fundamental. Quality of Service (QoS) facilitates packet prioritization, and with its relatively simple implementation, is invariably a cheaper solution.

Security

MPLS and Frame Relay are equally secure. Frame Relay utilizes Data Link Circuit Identifiers (DLCIs) to address traversing data packets, whereas MPLS uses tags or labels. IPSec is often adopted by organizations that are required to comply with HIPAA, since IPSec relies on encrypted data transfers. However,

IPSec tends to carry a price premium over MPLS and requires specific hardware configurations. After studying various MPLS white papers written by technology manufacturers and IT managers, many healthcare organizations are becoming comfortable claiming HIPPA compliance when utilizing MPLS VPNs.

Remote Access

IPSec allows access to the customer's corporate VPN from remote locations. This encryption method is seen within the industry as the preferred method of connection, ensuring data is not compromised prior to entering the VPN.

However, IPSec does not provide data prioritization, because traversing packets are encrypted, and as such, is not generally suitable for real-time applications.

Disaster Recovery & Reassignment

MPLS resides on an IP over SONET network and can automatically route around points of failure to a disaster recovery location within the meshed network. However, with a Frame Relay network, connection paths are pre-determined; PVCs need to be manually reassigned to the recovery site by the network provider and IT resources at the end-user level. While providers may offer a 'PVC Redirection Service,' it is essentially a manual reassignment. The time to complete reassignment increases exponentially as the number of nodes in the network increases or the need to mesh nodes increases.

An intermittent failure within a Frame Relay network can leave a business in an undesirable predicament. If a circuit fails, the customer is faced with the following question: should he invoke circuit reassignment and incur the cost associated with it, or should he wait to see if the failure could be quickly rectified? Acting too soon could incur unnecessary costs, but acting too late could negatively affect business. In addition, once the problem is resolved, it is likely that the network would have to be reassigned back to its original configuration, incurring additional costs. Under an MPLS configuration, the situation would have been automatically resolved, since PVCs do not exist. Network resilience is therefore greater with MPLS than Frame Relay.

Strategic Planning

All market reports show that Frame Relay is an aging and declining technology, unable to match the rich feature set that MPLS offers. MPLS is the de-facto standard for future services and for applications requiring packet prioritization. Packet prioritization is essential in the VoIP domain, preventing clipping and distortion and ensuring prioritization of data transfers. Regardless of VoIP's presence, good business practice dictates that priority business applications, such as point of sale transactions, reservations, etc, take priority over such items as Internet browsing.

MPLS also permits consolidation of Voice and Data services, thereby reducing communications overhead. Frame Relay is purely a data network, which was not designed for convergence.

Conclusion

There are hard and soft costs associated with a VPN deployment. While hard costs, such as circuits and CPE, are easy to measure, soft costs, such as IT resources and throughput, are equally important.

As technology progresses and businesses look towards technology to keep them at the leading edge of their field, the deployment of networks with embedded intelligence to enable the highest level of efficiency and business continuity with minimal human intervention become an increasingly desirable proposition. While other forms of VPN have desirable characteristics, only MPLS provides the network intelligence businesses demand with the reassurance of future capabilities. With its ability to reduce in-house IT resources, coupled with its inherent resilience, MPLS provides the most cost- effective and beneficial VPN solution.