



WHITE PAPER

Choosing a WAN Solution IP VPN vs. Frame Relay or ATM

Introduction

At MegaPath, we are committed to providing the right Wide Area Network (WAN) solution for your business. Our team of sales consultants and sales engineers work with you to assess your business requirements and determine the most appropriate WAN access, transport and security technologies based on the size and location of your sites and the applications you intend to use.

While some businesses may be well served with Frame Relay or ATM services, others demand the enhanced flexibility and scalability of an IP VPN solution – particularly one that leverages low-cost DSL, Cable and Satellite access. It all depends on your specific data communications requirements and business goals. The purpose of this document is to help you define those requirements and goals, so we can help you determine which type of WAN solution is right for your specific situation.

First, consider what networked applications you plan to use, the type of location, the profile of your end users and your overall business situation and goals. These considerations can then be placed in context of the different features and benefits the various WAN technologies have to offer. Next, analyze the economics of Frame Relay/ATM versus an IP VPN solution to ensure the approach you choose not only meets your functional requirements but is also cost-effective. Finally, determine whether you need a Managed Solution, whereby your service provider handles the configuration, monitoring and ongoing management of your customer premise equipment.

Using this document as a guide, MegaPath will work with you to create a customized WAN solution based on your specific business requirements – so you can achieve your business goals.



Business Profile

What are your business goals?

All businesses strive to increase revenues and lower costs, but what that means in terms of their day-to-day operations and strategies for growth may be considerably different. Some businesses are racing to launch new products or expand into new markets and need a flexible, scalable solution. Others may be actively acquiring or partnering with other companies and need a way to quickly connect them. And, many large companies are looking to lower costs and improve productivity.

Sometimes, the industry you're in can be a deciding factor. Manufacturing companies, for instance, can achieve significant efficiencies by integrating their supply and demand chains via an expansive extranet – so universal accessibility and scalability are paramount. Healthcare and financial services have stringent legal and market-driven security, as well as high-availability requirements, so encryption and redundancy are prerequisites. Firms in the media and entertainment industries need to transport large volumes of data so they need an efficient broadband solution. Pharmaceutical companies have large sales forces that need secure, high-speed connectivity at home and on the road. And, retail chains are looking for ubiquitous 'always-on' connectivity to migrate from analog to IP-based credit card authorization services and to utilize the latest online Point-of-Sale (POS) systems.

Another way to think about this is to identify your business' primary opportunities, challenges and threats. Many businesses have embarked on globalization efforts that place new demands on the capabilities and reach of their communications infrastructure. Others are looking for ways to leverage new technologies to be more productive or fend off competitors – or challenge incumbents. IP VPNs can play an integral role on both sides of this equation and have done a lot to drive down costs and incubate new technologies that boost productivity and facilitate globalization.

Where are your users and with whom do they communicate?

Different types of businesses have different types of communication requirements based on the topography of their users and the type of data they share or applications they need to access. Some businesses only need to connect a few branch offices to their headquarters or a central facility (e.g., a data center) and a simple hub-and-spoke network architecture will suffice. Others have dozens, hundreds or even thousands of locations (e.g., branch offices, retail stores and/or business partners) that need to connect back to headquarters. These locations may also need to communicate with each other, requiring fully-meshed network connectivity. And, some or all of them may need access to the Internet, with the proper security technology to protect against malicious attacks and block inappropriate web content.

To make sure you've considered all of your users' distinct needs, you should list the types of employees in each functional area of the business and then look at whom they share information with both inside and outside of the company. Here are some questions to facilitate this exercise:

- How many sites does your business have, where are they located, and how many employees are at each location?
- Which sites need Internet access?
- How many mobile users and/or telecommuters do you have?
- Do you need connectivity between your various locations and those of your business partners?

What information do they need to access and/or share?

This is perhaps the most difficult, yet important question, since it requires a deep understanding of your users' communications patterns and which applications your business plans to leverage in order to achieve its goals. The Internet has fueled the use development and use of many new and enhanced applications, from basic email, File Transfer Protocol (FTP) and Web sites to e-Commerce, to Distance Learning, Streaming Media, Sales Force Automation (SFA), Customer Relationship Management (CRM), Enterprise Resource Planning (ERP) and Supply/Demand Chain Management. Some newer applications are on the verge of widespread adoption, including IP Telephony using Voice over IP (VoIP), Web-based Collaboration and IP Videoconferencing, and there are certainly many more to come.

It's hard to foresee the next "killer-app," but you can identify the types of applications that are appropriate for your business today and the network-requirements for those applications. For example, if your business involves a lot of travel for meetings, it's possible that these could be done more efficiently via Web-based Collaboration and/or IP Videoconferencing. This application, like many newer ones, requires a lot of bandwidth and the usage tends to be very bursty. It also involves any-to-any communication and is very performance-sensitive, so it calls for premium quality data-delivery and a fully-meshed network architecture to provide the shortest, most direct connection between any pair/group of users. Other applications, such as ERP accounting packages, usually only involve communications between a few employees and a central database and can therefore be implemented with a hub-and-spoke network architecture.

Another important factor to keep in mind is whether the applications your business uses are designed to be used over the Internet via a Web browser. If so, this may be an important reason to consider an IP VPN, which can have distributed Internet access seamlessly integrated into the service.

The best approach is to list all of the applications you use or plan to use and evaluate their network requirement based on the following criteria:

- Do users access this application from a central location or do they use it to communicate with each other?
- Would users like to access this application over the Internet?
- What level of performance does this application require (packet loss, latency, jitter)?
- What are the implications/costs if this application is temporarily unavailable?
- How much bandwidth does the application require?
- Is this application's bandwidth usage consistent or bursty?
- Does it contain data that must be encrypted?

Next, we will assess the different features and benefits each of these WAN technologies provides as they relate to your applications and user criteria.

Features & Benefits

IP VPN

The most basic definition of an IP VPN is 'secure transport across a shared IP network.' However, there are several ways in which this can be accomplished, depending on the *network* used, the type of *transport protocol* and the means of *securing* the traffic.

Perhaps the simplest approach is to use the public Internet for network connectivity, native IP for the transport and a CPE-based firewall and encryption (i.e., IPsec encapsulation) for security. This allows you to connect sites that are located on different ISPs, and so it is often used to reach business partners, telecommuters, and mobile workers. However, this Internet-based approach only provides 'best-effort' performance and therefore may not support certain performance-sensitive applications. One can also use native IP and encryption across a single provider's network, which may afford better performance – or at least a single point of accountability – but has limited reach.

The ideal solution is to use a service provider that has Network-to-Network Interconnects (NNIs) with numerous other providers to extend its reach without compromising performance, and uses MPLS to keep each of its customer's traffic private without the overhead of IPsec encryption. Since MPLS is a switched transport service that keeps customers' traffic logically separated from one another, it is inherently as secure as Frame Relay and ATM – so you do not need encryption unless your security policy requires it. This approach lets you use private IP addresses, which are less susceptible to Denial-of-Service (DoS) attacks, and also takes advantage of the route optimization and QoS capabilities that MPLS affords.

MegaPath is one of the few IP VPN providers that currently utilizes MPLS in this manner and has NNIs with all the major DSL providers as well as the leading national Frame Relay and Satellite providers. So, you can choose from any of these access technologies or dedicated DS1/DS3 access circuits, depending on each site's specific needs. MegaPath also offers managed firewall services and IPsec encryption using state-of-the-art Cisco, Netopia and Adtran VPN routers to connect those sites that are connected via the public Internet. So, the IP VPN solution we propose may involve a combination of the options described above.

When is an IP VPN appropriate?

An IP VPN is the appropriate WAN technology if your business needs include the following characteristics:

1. Numerous Locations Nationwide or Worldwide

One of the inherent advantages of an IP VPN is the ability to use any ISP to access the network – all that's required is a VPN router, or gateway. With Internet access now available virtually anywhere in the world, this means true universal accessibility. Of course, it is preferable to connect directly to the

MegaPath network via one of our on-net access providers, to which we directly interconnect at Layer 2 to ensure premium performance.

2. Communication Among Sites

A partially-meshed or fully-meshed network topology is desirable if the various locations need to communicate with each other, versus a single hub location. An IP VPN is ideally suited for this requirement because the underlying transport protocols, IP and MPLS, provide any-to-any connectivity, whereas Frame Relay and ATM do not. That is, one doesn't have to specify the connection for any pair of endpoints; using MPLS, the network is pre-configured to route traffic directly between each pair of Provider Edge (PE) routers via the optimal path. This "any-to-any" optimal path routing capability can save considerable time and expense when compared with traditional data communication services that are priced and configured on a per-connection basis.

3. Remote Users

In the past, businesses maintained modem banks on their premises for mobile workers to dial-in to the corporate network. These systems, however, were notoriously unreliable and difficult to maintain. They also represent a considerable capital cost and require expensive toll-free or calling card service. Fortunately, with an IP VPN, mobile workers can now dial-in via a local call to their ISP or use the broadband or WiFi Internet access at their hotel, airport or local coffee shop. And, telecommuters can do the same from home using their residential DSL or cable Internet service.

4. Intranet and Extranet

In addition to providing branch offices and remote users with access to internal company resources (i.e., an Intranet), some businesses also want to connect with customers, suppliers and business partners via an Extranet. While this can be done using traditional WAN technology, it requires provisioning a new circuit whereas an IP VPN can be extended via each business' existing ISP connection and an IPsec capable router or device – even if they use different ISPs.

5. Branch Offices With Internet Access

With a traditional Frame Relay and ATM WANs, Internet access for branch offices (if they even have it) is funneled through a central gateway at the hub location. While this eliminates the need to secure each site, it can result in poor performance if Internet traffic exceeds the capacity of one or more Frame Relay/ATM Private Virtual Circuits (PVCs) or the central Internet gateway. Not only does the branch office user's Web browsing suffer, the bursty nature of Internet traffic can interfere with the company's business applications for which the Frame Relay/ATM network was originally designed. With more and more users accessing the Internet from branch locations, sending and downloading large files via email, FTP or the Web, this problem has only gotten worse – so much so, that some

branch offices have procured their own dedicated Internet connection. Some businesses even have a requirement to host Internet-accessible applications at the branch offices, so they can have immediate control over them. An IP VPN can solve this problem by seamlessly providing network-based Internet access via high-bandwidth connections at each site and secure Internet gateway(s) in the MPLS core. Since traffic is not confined to low-bandwidth, site-to-hub PVCs, this network-based Internet access approach can be easier and less costly to manage for large-scale deployments.

6. High Bandwidth

An IP VPN can provide higher bandwidth connections than traditional data communications services (up to 155 Mbps with an OC3) because service providers, like MegaPath, are able to provide this service using efficient, high capacity fiber optic networks. It is also priced lower than traditional Frame Relay and ATM data communication services for the same reason, and because IP traffic can be more efficiently distributed across the service provider's network. Likewise, customers can also use low-cost broadband access technologies, such as DSL, Cable and Satellite.

7. Bursty Applications

Many businesses that deployed Frame Relay networks for back-office applications have found that bursty Internet-based applications, like email, Web browsing and FTP are saturating these connection-based networks and degrading performance of their enterprise applications. And, similarly, point-to-point networks used for voice and videoconferencing have to be 'over-provisioned' to accommodate peak usage but go under-utilized much of the time. An IP VPN is an ideal solution for these types of applications, in part because it provides any-to-any connectivity and distributed Internet access, but also because as an IP service customers get access to the full "port" capacity of the circuit as opposed to a PVC. So, they can use bursty applications without performance degradation due to over-utilization.

8. Wide Variety of Applications – Convergence

Businesses with diverse user groups and numerous types of applications have in the past deployed separate Frame Relay/ATM WANs based on the specific requirements of each separate user scenario. While this appears to be the most practical approach at the time, the result is a hodge-podge of WAN platforms that are costly and difficult to manage and scale. An IP VPN solution can accommodate all types of traffic on a single platform. That means it costs less because it's easier to manage and more efficient, plus you are able to realize economies of scale as the number of locations and bandwidth needs increase.

Point-to-point, Frame Relay, and ATM

These traditional data communications services are the standard for most enterprise WANs because they've been available for much longer than IP VPNs, and because they offer inherent security and dedicated site-to-site bandwidth. A point-to-point WAN epitomizes the concept of a private network by providing dedicated site-to-site circuits, so you have the entire capacity available whenever you need it and there are no other clients sharing the circuit who could present a security threat. Of course, this also means that you do not enjoy the efficiencies, redundancy, reach and flexibility that a shared network affords. Frame Relay and ATM offer some of these benefits, but not to the same degree as an IP VPN because they are still based around providing dedicated bandwidth from site-to-site; instead of dedicated circuits, though, they offer Private Virtual Circuits (PVCs). Each PVC is allocated a certain amount of bandwidth, or Committed Information Rate (CIR), that must be reserved on the local loop and the providers' network. IP VPNs, on the other hand, are based on the Internet model of providing connectivity to all sites and so instead provide guaranteed levels of performance throughout. Frame Relay services also do not typically exceed DS1 capacity, and the protocol itself does not typically accommodate certain applications, such as voice and video. For these real-time applications, and for higher bandwidth levels, ATM is available for bandwidth requirements up to OC-12 capacity.

When are traditional data communications appropriate?

Traditional WAN technologies are most appropriate if your WAN requirements have the following characteristics:

1. Legacy Systems

If you already have a Frame Relay, ATM or point-to-point WAN connecting your legacy systems, it may require a considerable integration effort to replace it. More than likely, it probably makes sense to maintain the traditional data communication infrastructure, at least initially, and complement it with an IP VPN for those applications or user scenarios that would benefit (e.g., email, FTP, HTTP, videoconferencing). This is a more conservative approach, as it gives you the opportunity to test each legacy application over the new IP VPN service.

2. Hub-and-Spoke

In some cases, businesses only need connectivity from their branch offices back to a central location. This may be because users at the branch offices do not share applications with those at other branch offices; instead, most of the communications are between the *systems* at the central and branch offices.

3. *Dedicated Bandwidth*

Applications that require dedicated bandwidth between two sites are typically best served by a point-to-point private line, or Frame Relay/ATM service. However, an MPLS IP VPN offers similar performance in terms of latency and packet loss as Frame Relay/ATM, since it is also a switched service.

Security

WAN security is a complex discipline, but a simplified perspective yields three options: If your data requires the utmost protection, then you will probably use a point-to-point WAN with encryption – regardless of the benefits and lower costs other technologies afford. A lower cost option is a switched service, such as Frame Relay, ATM or an MPLS IP VPN. The third option is a CPE-based IPsec VPN, where all traffic is encrypted and sent over the public Internet. Or, one can use a hybrid MPLS/IPsec VPN in which on-net sites are connected directly to the MPLS network and off-net sites are connected via the public Internet using IPsec encryption. The latter allows one to extend the reach of the MPLS VPN to any site on the public Internet. All of these approaches provide adequate security of the data and source/destination information and the tools to ensure proper authentication and access controls.

If WAN users need access to the Internet, then this opens another area of security considerations. One needs to protect against viruses, spam, hackers and inappropriate web content. While this topic extends beyond the scope of this whitepaper, experts recommend a 'Defense in Depth' approach where protection is placed at the network perimeter, on the desktop, and at multiple points in between. Unified Threat Management devices placed on the perimeter of the WAN (i.e., at the Internet gateways) offer firewall, intrusion prevention, anti-virus, anti-spam and web content filtering capabilities. And, software installed on the PC offer similar protection. Given the complexity involved in specifying, implementing and managing these types of security systems, companies should select a WAN service provider that offers security services that utilize these systems to protect against such threats.

Economic Considerations

Aside from the different features and benefits of these traditional data communication services and IP VPNs, they are also priced very differently. Frame Relay and ATM services are priced based on access to the network (port charge) and the amount of bandwidth between each pair of sites (CIR per PVC). Point-to-point circuits, of course, are also priced based on the bandwidth (type of circuit) connecting each pair of sites.

IP VPNs, on the other hand, only have a port charge; the number of destination sites and the amount of bandwidth delivered between any pair of sites is not factored into the pricing because IP is inherently "any-to-any" connectivity. So, if you have many locations that need partially or fully-meshed connectivity, an IP VPN

will probably be much more cost-effective. And, the greater the geographic diversity and the higher the bandwidth requirements, the more likely it is that an IP VPN solution will be more economical. Of course, if any of the sites already have Internet access, the only incremental cost for connecting them via an IP VPN is the CPE and termination of the encrypted VPN tunnels using a VPN concentrator.

We will help you determine which types of WAN technologies are most cost-effective depending on your businesses network topology and traffic patterns.

Examples:

a) Small Hub-and-Spoke Network For Connecting HQ and Branch Offices

- Hub and spoke topology consisting of twenty sites
- DS1 port at headquarters location
- DSL or T1 port speeds at branch offices
- 128 Kbps minimum bandwidth requirement at each site (PVC)
- Local loop charges are comparable

Frame Relay Solution Monthly Charges:

1 Frame 1.5Mb CIR Port/Loop/Hub PVC x \$800	=	\$800
20 Frame 128k CIR Port/Loop/Hub PVCs x \$300	=	\$6,000
Total Monthly Charges	=	\$6,800

IP VPN Solution Monthly Charges:

1 DS1 x \$600	=	\$600
20 Varied Broadband Circuits x \$150	=	\$3,000
Total Monthly Charges	=	\$3,600

Savings	47%
---------	-----

b) Large Fully-Meshed Network with Business Partners

- Fully-meshed topology consisting of two hundred corporate sites and five business partner sites
- DS-3 / 9 Mbps port speed at main data center
- DS-1 port speed at remaining nine corporate sites and business partner locations
- Business partner locations already have DS-1 Internet access
- 128 Kbps minimum bandwidth requirement; bursting capability
- Local loop charges are comparable

Frame Relay Solution Monthly Charges:

1 Fractional 9Mb DS3 x \$5,000	=	\$4,000
9 Frame 1.5Mb CIR Port/Loop/Hub PVCs* x \$800	=	\$7,200
190 Frame 128k CIR Port/Loop/Hub PVCs* x \$200	=	\$85,000
Total Monthly Charges	=	\$96,200

* Does not include site-to-site PVCs for meshed topology

IP VPN Solution Monthly Charges:

1 Fractional 9Mb DS3 x \$4,000	=	\$4,000
9 DS1s x \$600	=	\$5,400
190 Varied Broadband Circuits x \$150	=	\$28,500
Total Monthly Charges	=	\$37,900

Savings	> 61%
---------	-------

Managed Services

If your business has a complex WAN and needs additional assistance specifying, installing and managing your network, MegaPath can help. We provide a wide range of services including WAN design, onsite installation and maintenance of your customer premise equipment, and proactive monitoring of all your network elements. In preparing your customized WAN Proposal, we will determine which of our Managed Services offerings are appropriate for you.

Conclusion

MegaPath is experienced at analyzing customer needs and has the expertise and services necessary to fit your needs. We look forward to conducting a personalized assessment for your technical and business requirements, and preparing a WAN Proposal that will help you achieve your business goals.