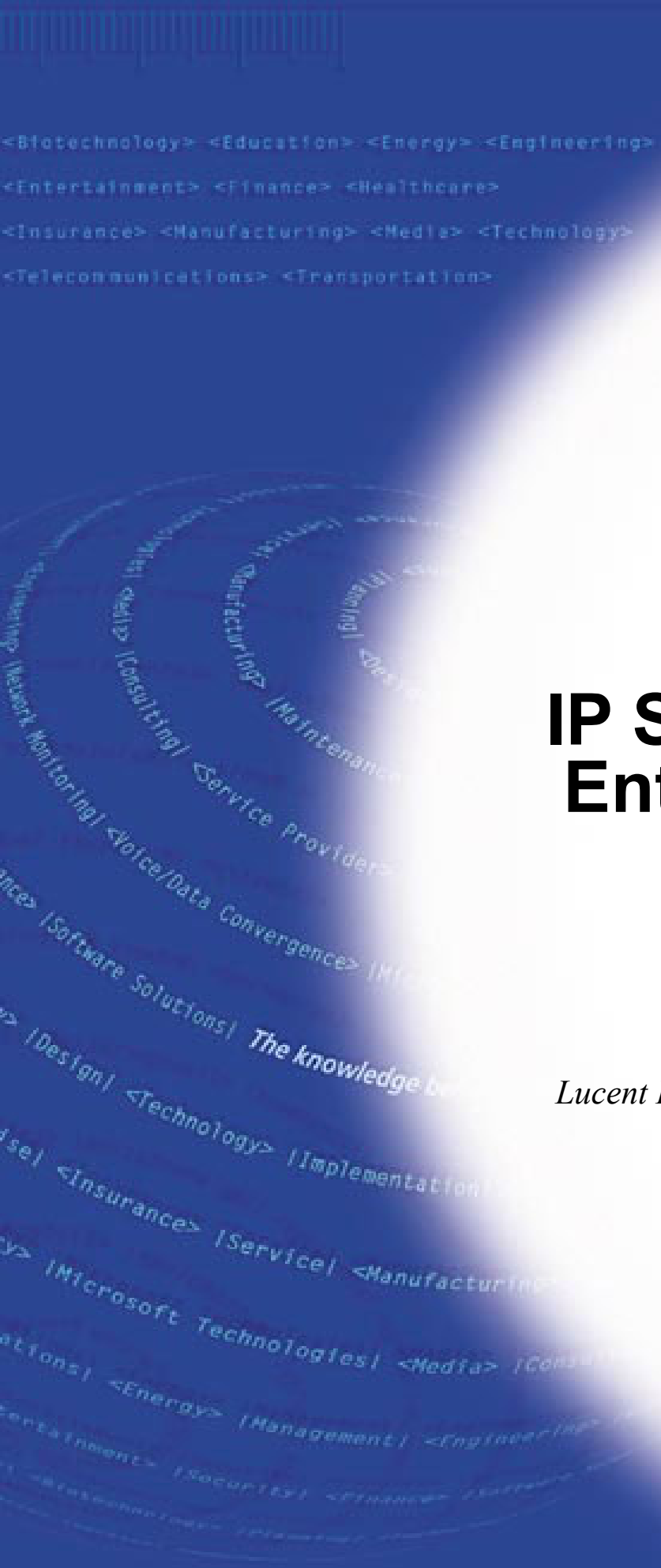



# IP Services – An Enterprise View

*By Gary Braver*

*Network Systems Consultant*

*Lucent Enterprise Professional Services*




# IP Services – An Enterprise View

*By Gary Braver, Lucent Enterprise Professional Services*

## Introduction

Over the last few years, network-based IP Virtual Private Networks (IP VPNs) have become widely available. Like frame relay, IP VPN technology provides a standards-based shared network infrastructure that can supply enterprises with a solution that is more cost effective, scalable, and reliable than a leased-line implementation. Unlike frame relay, IP VPNs are Internet Protocol-based, which allows for Internet connections to suppliers, customers, and home users; rapid deployment of new locations; and a far simpler network design.

As the number of sites on the network increase and traffic patterns increasingly become peer-to-peer (as opposed to hub-and-spoke), the flexibility of an "any-to-any" IP VPN produces a more efficient, easier-to-manage service. This simplification is accomplished by putting the complex traffic engineering function into the service provider's network, as well as having the layer 3 routing services performed and managed by the carrier. It also benefits enterprises by reducing the expertise and headcount required to configure and administer the network. This model leverages a flexible, virtual routing platform where one service provider management person can manage many customers' virtual routers. By providing secure access across the many sites that might comprise the customer network, IP VPNs can be provided in the same manner.

This white paper presents the enterprise view of IP VPNs, detailing the challenges facing enterprises and how an IP VPN network can functionally meet their needs in a cost-effective manner.

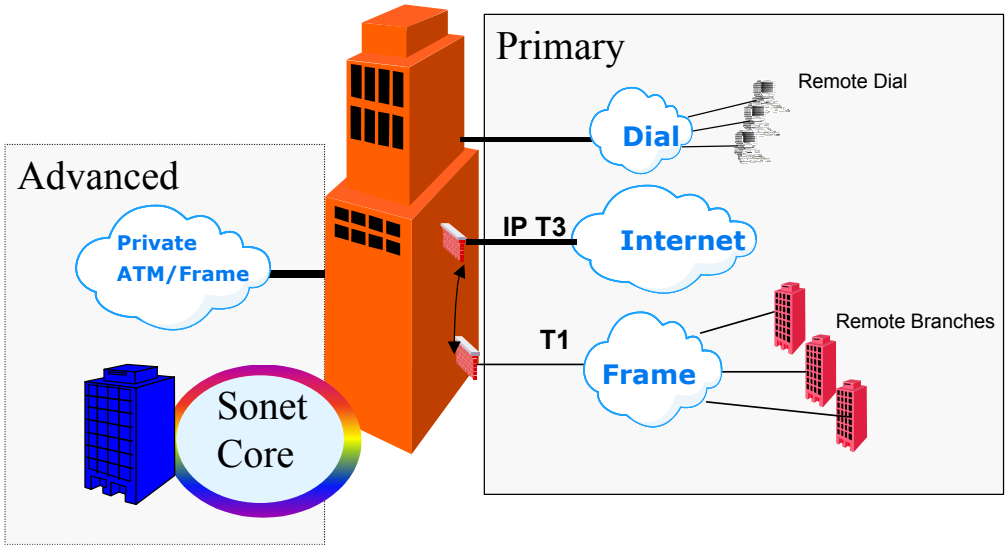
## Challenges to Today's Enterprises

Today's enterprise IT manager is responsible for providing many network services constructed from a variety of sources. Typical functions include:

- Network transport from the carrier (typically frame relay, ATM, and leased lines)
- Internet access (sometimes from a different carrier than the network transport)
- Dial modems for road-warrior employees (supported by dial-lines or 800-numbers provided by the carrier)

To meet these challenges network managers may deploy several types of purpose-built networks as shown in Figure 1.

**Figure 1: Typical Enterprise Networks**




A larger enterprise will typically have either an ATM or frame relay network to connect remote branch locations. The largest enterprises might even make investments in private transport networks based on frame relay or ATM over an optical fiber core.

These large enterprises will also provide some form of dedicated Internet access, which enables customers to access company web servers or employees to access the Internet from either a corporate location or from a remote location. Due to network complexity and security concerns in providing Internet connections at remote locations, branch locations will typically access the Internet through a centralized corporate location(s). Large corporations may provide multiple Internet gateways at scattered geographic locations.

In addition, enterprises may even provide remote access for traveling users or outsource the remote access to any number of service providers.

These multiple, "purpose-built" networks result in *higher physical line costs, inefficient bandwidth allocation, multiple points to secure, and increased complexity* – all of which leads to a substantially greater cost than providing for a single, integrated network. So, the question is: Why funnel all Internet traffic from remote branches back through corporate if you can provide a direct, secure, easy-to-manage, Internet connection at the branch location? Why provide for separate physical networks for Internet and frame relay, if one network will provide the security, reliability, and desired quality of service.

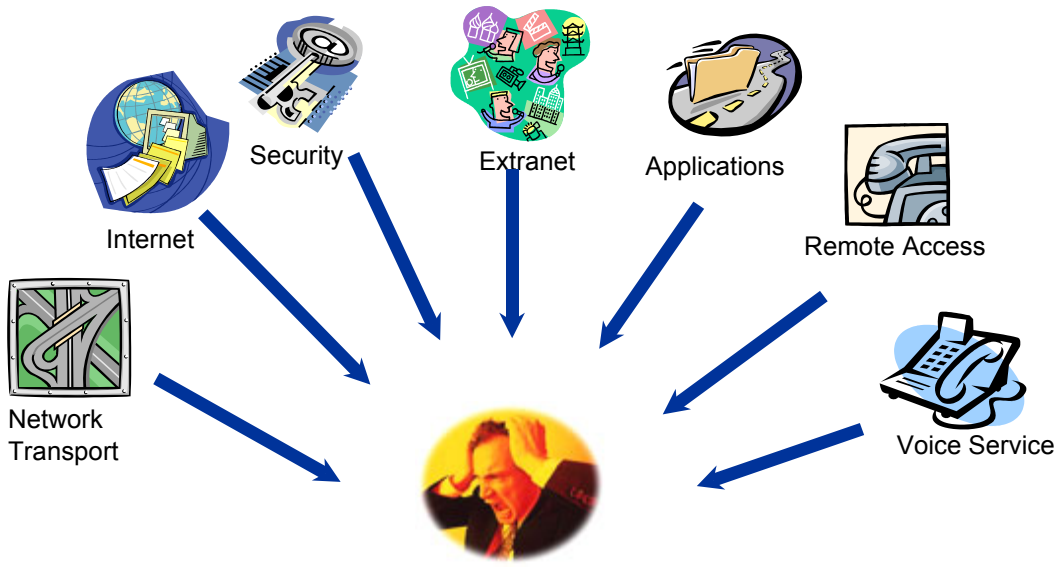
Even with multiple, purpose-built networks, enterprises typically still do not provide for:

- Broadband home-user access
- Secure supplier/customer extranet connections
- A simple way to add new remote locations
- An effective method for determining and allocating WAN bandwidth

All of these service requirements put a burden on enterprises, which have to compete with vendors and services providers for staff with the requisite IP networking expertise. This infrastructure burden is a necessary function because the enterprise has realized the benefits delivered by pervasive computing resources, computer networking, intranets, e-mail, e-commerce, and a mobile workforce. Enterprises are interested in the services that enable their business operation not necessarily the creation of those services, that is, they want to drink the water from the tap, but not build the plumbing behind the tap unless it is necessary or economically viable to do so.

Add to these challenges the task of integrating new applications and voice services and the pressures facing the typical IT manager become obvious (Figure 2).

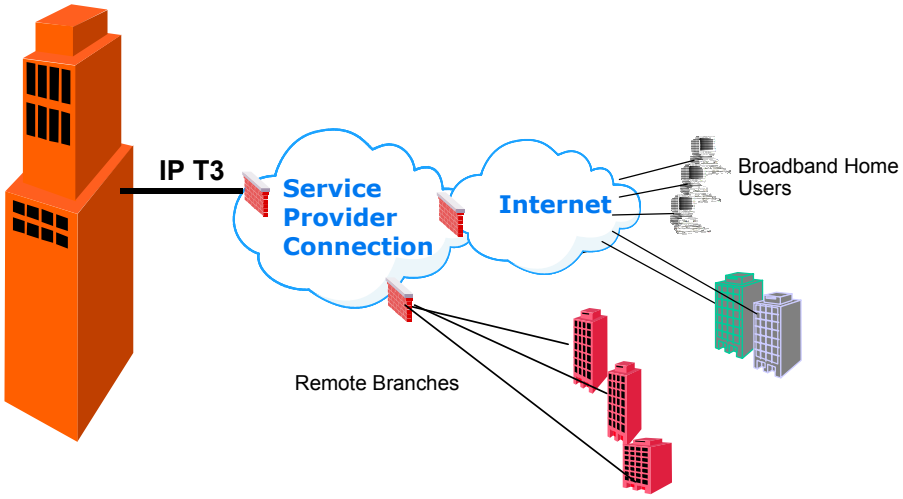
**Figure 2: Enterprise IT Manager Challenges**




### The IP Services View

In the network-based, IP services model, the frame relay or ATM network and the Internet connection are replaced with a public, IP-based network as show in Figure 3.

**Figure 3: Public IP-Based Network Model**




From a functional perspective, there is no difference in the services provided to corporate or remote branch locations with the public, IP-based network model compared to the multiple, purpose-built network model. All communications from branch and remote locations occur over an IP-based network as opposed to an IP-encapsulated frame relay or ATM network. This architecture allows for a reduction in physical networks, improved efficiencies in bandwidth utilization, and the capability to provide direct Internet connections to branch locations without having to funnel all Internet traffic through the corporate location. Direct Internet connections are possible because secure, guaranteed bandwidth services can be provided to each branch location.

To provide the required level of security to the branch office, firewall and network address management systems are provisioned and configured by the service provider in its network. The service provider would offer :

- A stateful firewall system (intelligent enough to understand the different protocols that pass through it) that can securely allow or block traffic as well as authenticate the use of services. With the stateful firewall function built into the network, there would no longer be a need for stand-alone firewalls at enterprise locations or a premises-based firewall system would provide additional security capabilities such as prevention of denial of service attacks.
- IP address management with network address translation/port address translation, and Dynamic Host Configuration Protocol (DHCP) to switch private, “non-legal” IP addresses to “legal” public addresses. In addition, the switches also use DHCP relay to provide for the address assignment. What this means is that new remote locations can be rapidly and simply brought onto the network because there would be no concern with obtaining scarce IP addresses. With the DHCP service, coupled with the stateful firewall functions, direct Internet connections could be provided to remote branch offices without having to home Internet traffic back to a centralized location.
- Packet capture capability on all interfaces. Packet trace includes the ability to store packet captures on flash, direct packet capture output to screen, convert packet capture to sniffer trace file, and trace a packet through the box. Remote monitoring equipment would no

longer be needed and a technician would not need to go on-site to diagnose a WAN network problem.

- Directory services that are repositories for policy information. The service switch should access directories to determine how to establish connections for traffic flows based on site and network service connection policies. Policy information can be distributed and stored in RADIUS servers, LDAP directories, and Microsoft's Active Directory. The standardized directory will allow for population of other systems (such as remote dial, security, server access) with the common directory information. This eliminates the need to manually re-enter user and site information for each separate system.

Additionally, the provider could offer an intrusion detection service to monitor and alarm any suspected intrusion “hacking” attack.

To provide for the required quality of services for key business applications or for delay- or latency-sensitive traffic such as voice, the provider could also offer various QoS levels or metrics.

With the first additional bandwidth service, a minimum bandwidth guarantee could be provided with the option of having bandwidth increased dynamically. An example of this would be hotel access on a high-speed line (such as xDSL), where bandwidth is available between 256 kilobits/second and one or two megabits per second. Incremental amounts of additional bandwidth can be provided as a service (e.g., the user may need more bandwidth to download large data files or access network based archive servers).

With a second additional service, the end-user could be allowed to prioritize traffic based on policies that can be predefined for each different type of traffic stream using the industry standard differentiated services (Diffserv) function. The network switch will examine the special IP header names (TOS field) and within that header determine queuing and bandwidth metrics for the packet. With prioritization, higher priority traffic will be passed through the network first during periods of heavy usage.

Within a single queue three different levels of conformance (conforming, caution state, non-conforming) are provided. There are numerous limits that can be set to gauge conformity. Some examples of these conformity settings are throughput (100k, 300k), priority level, or latency (how long has it been in the queue). There are also a number of choices in the caution state: dropping packets, shaping packets (hold it until you are back into conformance) or remarking packets (drop it down priorities – which could mean that the packet may eventually get dropped by the network). Finally, in a non-conforming state the packet can either be remarked or dropped.

Enterprises may contract for particular bandwidth partitioned between Intranet and Internet connections or between particular applications used on the corporate Intranet. For example, the user may use a particular application (e.g., sales force automation) and want to guarantee particular bandwidth for that application over others.

## Additional IP Services Capabilities

In addition to the base Internet and transport function the IP service provides, adding sites, establishing secure business location-to-location extranets, and providing connections for broadband users are now possible.

Adding remote sites is also simplified and less expensive because no network reengineering is needed to bring the network on-line. Full-mesh connectivity is provided by the IP-VPN network so that once a site is operational, communication occurs with all other allowed sites. There is no need to provision private virtual circuits (PVC's) and worry about site-to-site traffic patters.

## Financial Case Study

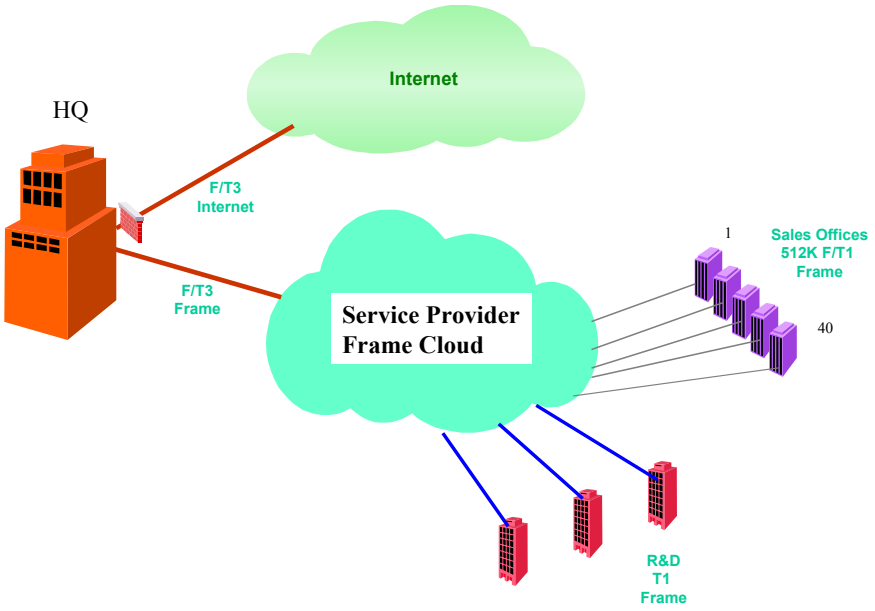
While an IP VPN service has clear functional advantages over the traditional frame relay and IP connection networks, new services can not be deployed unless they are cost justified. In the case of an IP VPN, these costs should be less than the combined cost of separate frame relay and IP connection networks as shown in the following case study based on a 2,500-employee, medical device manufacturer, which we will call "MedDev."

### *MedDev Overview*

- 1 co-located headquarters (HQ) and manufacturing location
- 3 research labs (each with a T1 frame relay connection)
- 40 domestic sales offices (each with a 512K F/T1 frame relay connection)
- 1 Fractional T3 (20 Megabits/Sec) frame relay connection at HQ
- 1 Fractional T3 (10 Megabits/Sec) Internet connection at HQ

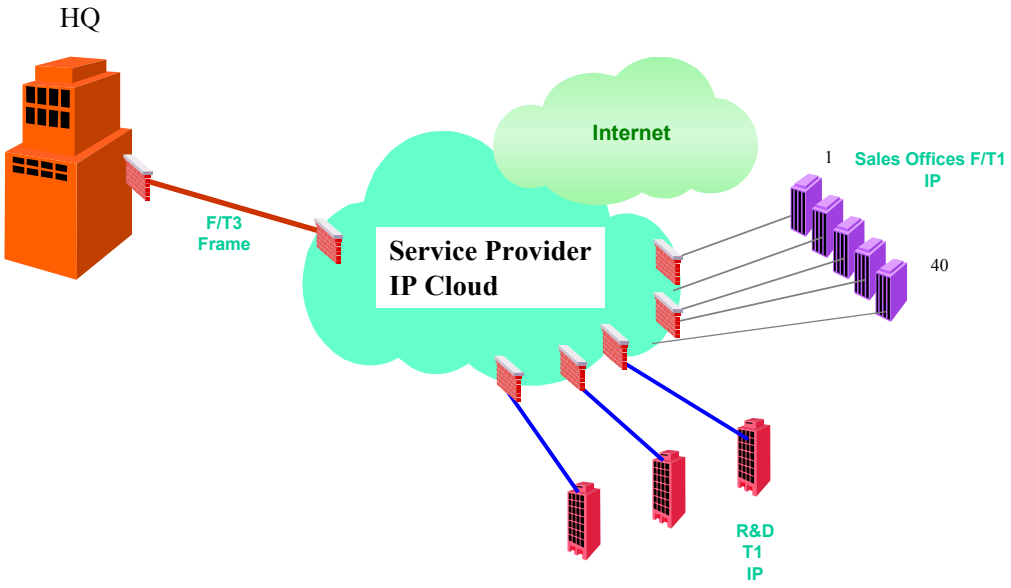
MedDev's basic network (Figure 4) provides for frame relay connections to the remote labs and sales offices. Internet connection is provided centrally through the HQ location. MedDev is unique in that all data traffic flows from all remote locations (branch and R&D) to one central HQ location. In most other mid-to-large size organizations, traffic would flow to multiple locations. The net result of this would be that many locations would have multiple PVCs adding a substantial cost to the frame network design. On top of this, the frame relay bandwidth requirements would typically be higher at the branch level than an equivalent IP VPN network because bandwidth does not have to be determined on a per PVC basis in an IP network.

**Figure 4: MedDev's Current Network**




To reduce costs and provide for additional capabilities, MedDev evaluated deployment of an IP VPN network (Figure 5)

**Figure 5: MedDev's Proposed IP VPN Network**



### *Cost Comparison*

Pricing for the current MedDev network differs from the proposed IP VPN network in two significant ways:

1. The F/T3 access line to the Internet in the current network is not required in the proposed network, and
2. The current network requires a separate ISP charge for Internet access.

The pricing comparison (Table 1) shows roughly a 10% saving for the IP VPN network compared to the traditional frame/Internet connection model.

**Table 1: MedDev Network Cost Comparison**

| | Current Network | Proposed IP VPN Network |
|---|---|---|
| Monthly frame relay line Port PVC costs | 142,146 | 142,826* |
| Monthly frame relay access line costs | 22,750 | 22,750 |
| Monthly ISP Internet access cost | 15,000 | 0* |
| **Total Monthly Costs** | **$179,896** | **$165,576** |
| **Total Annual Cost** | **$2,158,752** | **1,986,912** |

* Includes traditional intranet access plus Internet access. With the VPN transport network, there are no additional frame relay per PVC charges or ISP Internet access charges.

### *Managed Security*

MedDev can also reduce costs and increase its security capabilities by utilizing the service provider's managed security service, enabling it to eliminate two positions dedicated to firewall security (one staff, one consultant). Additionally, the managed security service provides better protection against denial of service (DoS) attacks, which MedDev estimates would cost $80,000 annually for it to provide using internal resources.

The managed security service costs $132,000 annually. However, eliminating two positions produces a savings of $275,000, for a net savings of $143,000, and a total benefit of $223,000, including the DoS benefit.

### *Managed Bandwidth*

MedDev can also use its service provider's managed bandwidth service to increase its capabilities and further reduce costs.

MedDev estimates that by being better able to determine specific bandwidth requirements they can further cut bandwidth costs by eight percent. Given the annual bandwidth charges of nearly

$2 million per year, this is an additional savings of approximately $160,000, or approximately $81,000 per year after the managed bandwidth service charge.

To guarantee key business applications will run effectively over the integrated IP VPN network, MedDev needs to dedicate a minimal level of bandwidth to these applications. Improved performance from guaranteed bandwidth often translates into productivity improvements that can lower costs. For instance, changing bandwidth parameters for the sales entry application via a self-service web-based system will provide $40,000 annually in productivity improvements for the sales force.

## Conclusion

Approximately ten years ago, leased lines were the predominate method used to build corporate networks. To build a network, an engineer would map traffic patterns and circuit costs and determine hub locations as well as circuit and hub redundancy scenarios. Network design was cumbersome, expensive, and not overly reliable.

In the mid 90's, frame relay became available. It provided for a standards-based, shared network infrastructure that could supply the enterprise with a cost effective, scalable, reliable, and easier-to-design network.

At first enterprises did not think a public network would be reliable or secure, or could provide for the bandwidth throughput they were accustomed to with private lines. But these fears abated and enterprises soon endorsed frame relay as the preferred method for large scale network delivery.

Today frame relay is still providing cost effective, scalable, and reliable corporate networking and is still a good fit for existing frame relay users that are expanding to additional corporate locations. However, enterprises are increasingly turning to IP VPNs for new networks and to provide capabilities frame relay can not address, as evidenced by the annual growth rates of the frame relay market (which will grow by an estimated 11% this year), and the IP VPN market (which is currently enjoying a 70+% growth rate). IP VPN services growth is forecasted to remain above 60% at least through 2004.

IP VPNs are not a panacea for all WAN related woes. An effective IP VPN deployment still requires selection of a service provider that can provide the required level of services, effective security policies and procedures for managing the connections, and integration with other operational and network management systems. These are areas where the experiences of multivendor network consulting organizations such as Lucent Enterprise Professional Services can be leveraged to provide for an effective plan, design, and implementation.

## About Lucent Enterprise Professional Services

Lucent Enterprise Professional Services provides a full lifecycle of services and solutions that help clients plan, design, implement, and operate networks in today's rapidly changing and complex environment. We have a proven track record of more than 15,000 consulting engagements worldwide. We also sell VitalSoft software for monitoring and managing network and application performance.

Lucent Technologies is headquartered in Murray Hill, New Jersey, USA. Visit the Lucent Services Web site at www.lucent.com/services.

Copyright © 2002, Lucent Technologies Worldwide Services

This is an unpublished work protected under the copyright laws. All trademarks and registered trademarks are properties of their respective holders. All rights reserved. Printed in U.S.A. Lucent Technologies, Inc.