UNIT 3 VPNS, INTRANETS AND EXTRANETS

Virtual Network management and planning – VPNs for small businesses – Secure remote access in VPNs – IPSec VPNs – Integrating data centers with Intranets – Implementing and supporting Extranets.

3.1 VIRTUAL NETWORK MANAGEMENT AND PLANNING

A VIRTUAL NETWORK IS A DATA COMMUNICATIONS SYSTEM that provides access control and network configuration changes using software control. It functions like a traditional network butis built using switches.

The switched virtual network offers all the performance of the bridge with the value of the router. The constraints of physical networking are removed by the logical intelligence that structures and enforces policies of operation to ensure stability and security. Regardless of access technology or geographic location, any to any communications is the goal.

The switch could be considered a third generation internetworking device. First generation devices, or bridges, offered a high degree of performance throughput but relatively little value, because the bridge's limited decision intelligence resulted in broadcast storms that produced network instability. Routers, the second generation of internetworking devices, increased network reliability and offered great value with firewalling capabilities, but the tradeoff was in performance. When routers are used in combination with each other, bandwidth suffers, which is detrimental for delay sensitive applications such as multimedia.

3.1.1 THE BUSINESS CASE FOR VIRTUAL NETWORKING

Both the business manager and the technical manager should find interest in this new virtual networking scheme. The business manager is usually interested in cost of ownership issues. Numerous studies from organizations such as the Gartner Group and Forrester Research have found that only 20 percent of networking costs are associated with capital equipment acquisition. The other 80 percent of annual budgets are dedicated to items such as wide area networking charges, personnel, training, maintenance and vendor support, as well as the traditional equipment moves, adds, and changes.

It is important for IS managers to remember that capital expenditure happens in year one, even though the equipment may be operating for another four years. Wide area network (WAN) charges can account for up to 40 percent of an organization's networking budget. For every dollar that the technical staff spends on new equipment, another four dollars is spent on the operation of that equipment. Therefore, focus should be on the cost of ownership issues, not necessarily the cost of the network devices.

3.1.2 Network Reliability

Business managers are also looking for increased reliability as the network plays a major role in the core operations of the organization. Networks have become a business tool to gain competitive advantage they are mission critical and, much like a utility, must provide a highly reliable and available means of communications. Every office today includes an electrical outlet, a phone jack, and a network connection. Electrical and phone service are generally

regarded as stable utilities that can be relied on daily. Networks, however, do not always provide comparable levels of service.

3.1.3 Network Accountability

Managers also can benefit from the increased accountability that virtual networks are able to offer. Organizational networking budgets can range from hundreds of thousands of dollars to hundreds of millions per year. Accounting for the use of the network that consumes those funds is a critical issue. There is no better example than WAN access charges. Remote site connectivity can consume a great deal of the budget, and the questions of who, what, when, and where with regard to network use are impossible to determine. Most users consider the network to be free, and the tools to manage and account for its use are increasingly a requirement, not an option.

3.1.4 The Technology Case for Virtual Networking

The IS manager's needs for higher capacity, greater performance, and increased efficiency can be met through the deployment of switched virtual networks. Each user is offered dedicated bandwidth to the desktop with uplinks of increasing bandwidth to servers or other enterprise networks. Rather than contending for bandwidth in shared access environments, all users are provided with their own private link. This degree of privacy allows for increased security because data are sent only to intended recipients, rather than seen by all.

The most attractive feature to the technical manager, however, may be the benefits gained through increased ease of operation and administration of virtual networks. A longstanding objective has been to deliver network services to users without continually having to reconfigure the devices that make up that network. Furthermore, many of the costs associated with moves, adds, and changes of users can be alleviated as the constraints of physical networking are removed. Regardless of user location, they can remain part of the same virtual network. Through the use of graphical tools, users are added and deleted from workgroups. In the same manner, policies of operation and security filters can be applied. In a sense, the virtual net work accomplishes the goal of managing the individual users and individual conversations, rather than the devices that make up the network.

3.1.5 Virtual Networking Defined

The ideal virtual network does not restrict access to a particular topology or protocol. A virtual network that can only support Ethernet users with Transmission Control Protocol/Internet Protocol (TCP/IP) applications is limited. The ultimate virtual network allows any to any connectivity between Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM), Internet Protocol (IP), Internetwork Packet Exchange (IPX), AppleTalk, or Systems Network Architecture (SNA) networks. A single virtual network infrastructure under single management architecture is the goal.

Network management software becomes a key enabling requirement for the construction of switched virtual networks. The greatest challenge net work designer's face is the separation of the physical network connectivity from the logical connection services it can provide. Many of the design issues associated with networks can be attributed to the physical parameters of protocols and the routers used as the interconnection device. A challenge for any manager is to remain compatible with existing layer 3 protocols and routers and still preserve the investment in existing local area network (LAN) equipment to the greatest extent possible.

3.1.5.1 Using Telephony as a Model

The principles of operation for switched virtual networks are concretely founded in the success of the global communications systems. Without doubt, the phone system is the world's largest and most reliable network. Built using advanced digital switches controlled by software, extensive accounting and management tools ensure the success of this highly effective means of communication. The connection oriented switch is the key. End to end connections across multiple switches and various transmission types ranging from copper to fiber optics to microwave to satellites allow millions of calls per day to be successfully completed, regardless of the type of phone or from where the user is calling. The telephony model is used throughout this chapter to help illustrate the workings of a virtual network.

3.1.5.2 FEATURES OF SWITCHING SOFTWARE

The software that runs on switches is just as important as the switches themselves. A salesperson from Lucent Technologies, Fujitsu, or Northern Telecom does not focus the potential customer on the hardware aspects of the telephone switches. On the contrary, the salesperson conveys the benefits of the call management software, accounting, and automatic call distributor (ACD) functions. Switched virtual networks should also be evaluated for their ability to deliver value because of the software features.

3.1.5.3 The Virtual Network Server

Network management software has traditionally been thought of as software that passively reports the status and operation of devices in the network. In the switched virtual network, the network management software takes on a new role as an active participant in operations as well as configuration and reporting. A new middleware component known as the virtual network server (VNS) enforces the policies of operation defined by the network administrator through management software applications. The switches provide the data transport for the users of the network.

Directory Service. One of the software features in the VNS is the directory service. The directory service allows the identification of a device by logical name, MAC address, network protocol address, and ATM address, along with the switch and port that the user is connected to within the virtual network domain. The directory listing could be populated manually or dynamically as addresses are discovered. To

fully realize the benefits of switched virtual networking, automatic configuration is absolutely essential. The directory service allows end nodes to be located and identified.

Security Service. The VNS security service will be used during call setup phases to determine whether users or groups of users were allowed to connect to each other. On a user by user and conversation by conversation basis, the network manager would have control. This communications policy management is analogous to call management on a telephone private branch exchange (PBX) where 900 numbers, long distance, or international calls can be blocked. Users could be grouped together to form policy groups in which rules could be applied to individual users, groups, or even nested groups. Policies could be defined as open or secure, inclusive or exclusive.

A sample default policy can ensure that all communications are specifically defined to the VNS in order to be authorized. Policy groups can be manipulated either through drag and drop graphical user interfaces or programmatically through simple network management protocol (SNMP)commands.

Finally, and most important, the directory service can work in conjunction with the security service to ensure that policies follow the users as they move throughout the network. This feature alone could save time spend maintaining a router access list, as occurs when a user changes location in the traditional network. However, it is important to realize that switched virtual networks ease administrative chores, they do not eliminate them.

Connection Management Service. The VNS connection management service is used to define the path communications would take through the switch fabric. A site may be linked by a relatively high speed ATM link and a parallel but relatively low speed Ethernet link. Network connections with a defined high quality of service (QoS) could traverse the ATM link and lower QoS connections could traverse the Ethernet. This connection management service allows for the transparent rerouting of calls in the event of a network fault. Connection management could also provide ongoing net work monitoring in which individual user conversations could be tapped or traced for easy troubleshooting.

Bandwidth Service. The VNS bandwidth service is used during the call setup when a connection request is made. Video teleconferencing users may require a committed information rate (CIR) of 10 Mbps whereas the terminal emulation users may only require 1 Mbps. This is where ATM end stations and ATM switches negotiate the amount of bandwidth dedicated to a particular virtual circuit using user to network interface (UNI) signaling. Ethernet, Token Ring, and FDDI nodes do not recognize UNI signaling, but the switches they attach to could proxy the signal for the end station, thus allowing a single bandwidth manager for the entire network, not just the ATM portion.

Broadcast Service. The VNS broadcast service uses as its base the concept of the broadcast unknown server (BUS) that is part of the ATM Forum's LAN emulation draft standard. This is how broadcasts are flooded through the network to remain compatible with the operation of many of today's protocols and network operating systems. A degree of intelligence can be assigned to the VNS that would allow

for broadcasts or multicasts based on protocol type or even policy group.

Virtual Routing Service. The VNS virtual routing service is one of the most critical components of a virtual network. Just as traditional networks required traditional routers for interconnection, virtual LANs will require virtual routers for internetworking between virtual LANs. In other words, routing is required, but routers may not be. Some protocols such as TCP/IP actually require a router for users on two different sub networks to speak with each other. In addition, most networks today are logically divided based on network layer protocol addresses with routers acting as the building block between segments.

The difference in operation between a virtual router and a traditional router goes back to the connection oriented vs. connectionless distinction. Routing allows for address resolution between the layer 3 protocol addresses and the layer 2 MAC address just as it happens through the address resolution protocol (ARP) process in TCP/IP networks. The VNS virtual routing service performs the address resolution function, but once the end station addresses are resolved, establishes a virtual connection between the two users. Two users separated by a traditional router would always have the router intervening on every single packet because the router would have resolved the protocol addresses to its own MAC address rather than the actual end station's MAC address. This VNS routing service allows the network to route once for connection setup and switches all successive packets.

Accounting Service. The VNS accounting service is beneficial because it allows the creation of the network bill. Similar to the way a

telephone bill is broken down, the accounting service details connection duration with date and time stamp along with bandwidth consumption details. This is most directly applicable in the WAN. For many managers, WAN usage is never really accounted for on an individual user basis, yet it can consume up to 40 percent of the operations budget.

As usage based WAN service options such as integrated services digital network (ISDN) gain popularity, accounting becomes that much more critical. Interexchange carriers (IXCs), competitive access providers, and the regional Bell operating companies (RBOCs) continue to deliver higher bandwidth links with usage based tariffs. In the future, they could install a 155 Mbps synchronous optical network (SONET) OC3 link and only charge for the actual bandwidth used. Unless managers have tools to control access to and account for usage of WAN links, WAN costs will continue to rise. This service lets IS managers know who is using the WAN.

3.1.6 Virtual Networks vs Virtual LANS

Throughout this discussion, words have been carefully chosen to describe the operation of switched virtual networks. Many of the current vendor offerings on the market have as their goal the construction of a switched virtual LAN. These virtual LANs are interconnected using a traditional router device. However, the router has been viewed as the performance bottleneck. Routers should be deployed when segmentation or separation is the need; switches should be used to deliver more bandwidth.

The virtual LAN (VLAN) concept is merely an interim step along the way torealizing the fully virtual network.

The ATM Forum's draft LAN emulation standard allows ATM devices to internetwork with traditional LAN networks such as Ethernet and Token Ring. However, it seems ironic that it essentially tries to make ATM net works operate like a traditional shared access LAN segment. Although it is required for near term deployment of ATM solutions into existing LAN architectures, its position as an end all solution is questionable. A more logical approach uses ATM as the model that LANs must emulate.

3.2 PUTTING VPNS TO WORK FOR SMALL BUSINESSES AND OFFICES

MODERN BUSINESS PROCESSES DEMAND TIGHT LINKS between mobile users, customers, and third parties on both a temporary basis (project based) and permanent basis. Virtual Private Networks (VPNs) can provide significant business benefits by overcoming the barriers to achieving widely available and secure communication. VPNs provide the appearance of a single network connecting corporate offices, telecommuters, customers, and even competitors, while using separate public and private networks. A company retains control of user access and the privacy and integrity of its data even though the data travel on the public Internet. VPNs can provide as much as 60 percent cost savings over private leased lines and significantly reduce telecommuter dialup charges.

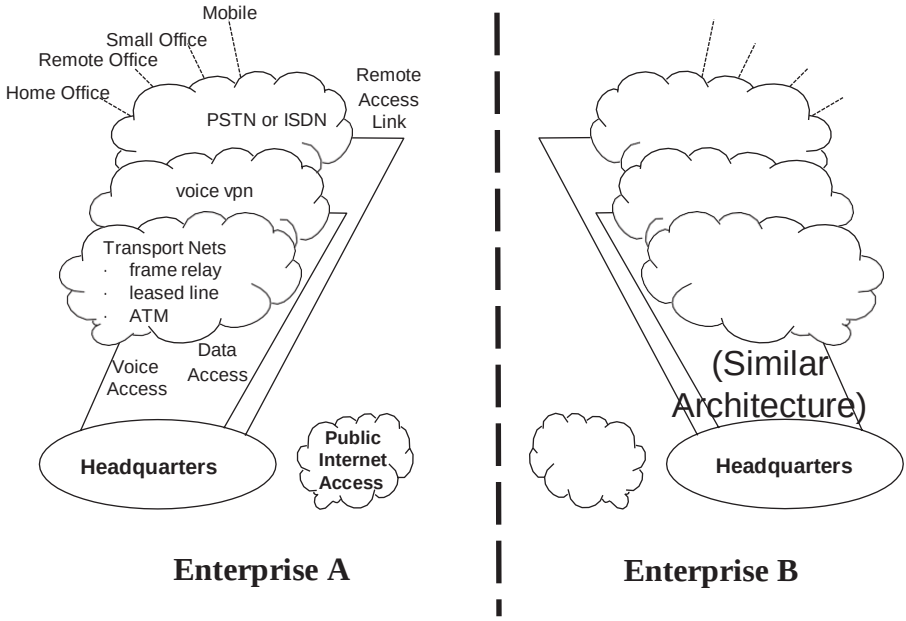
VPNs and their many benefits, however, have traditionally been thedomain of larger organizations. These huge companies enjoy access

to the capital and scale necessary to build VPNs and have the technical staff to maintain them. They are able to use VPNs to enhance and sustain their competitive advantage over their smaller and less technically sophisticated competitors. In practical terms, the benefits of VPNs have been off limits to small and medium sized businesses. And, even larger organizations have had difficulty deploying VPNs in branch offices because they are often too small to justify onsite IT staff.

The barriers to creating and maintaining a VPN include the need to construct and maintain a secure physical infrastructure and administer a wide range of data communications services. The infrastructure challenges include setting up access equipment, firewalls, servers, telecommunications services, and maintaining connections to multiple Internet Service Providers (ISPs) at hundreds or even thousands of enterprise locations.

Administrative challenges include maintenance of servers, synchronization of software upgrades, replication of Web servers, and sophisticated policy management spanning the whole network. Services that must be supported include email, directory, internal and external Web, firewall, FTP, and access control.

Virtual Services Management (VSM) technology and secure VPN transports are making VPNs realistically deployable for smaller organizations and branch offices. VSM solves the service related headaches of multiple points of administration required when setting up multiple sites, users, devices, and Internet Service Providers (ISPs). Through use of low cost, easily managed, and secure VPNs, the benefits of improved business management practices can be realized by even medium and small companies.



Today's enterprise networks.

3.2.1 Emergence of the Virtual Private Network

Today's private networks resemble the network in Figure. Basic connectivity is provided to a wide variety of locations, but the overhead costs are severe. The functionality includes the following services.

3.2.2 Remote Access

Remote access has matured from a "nice to have" option to a business critical requirement to support a mobile workforce and telecommuters.

For example, utility companies are increasing the productivity of their field service workers and eliminating the cost of maintaining distribution centers by applying remote access technologies. Line crews take their vehicles home with them and receive their day's work orders through either telephone or wireless dispatching systems. This setup eliminates the time it takes to report to the service center, pick up the service vehicle, and drive to the first job site. Remote access creates a win win situation for the company, worker, and customer. The utility company realizes increased worker productivity, reduced transportation costs, and reduced building and land costs. The worker eliminates commuting time and expense, while customers obtain faster, more responsive service, and lower rates.

Sales and marketing organizations are especially reliant on remote access capabilities. The use of remote access capabilities and laptop computers enables salespeople to complete contracts and obtain real time technical sales support while being face to face with customers, meeting customer needs and resolving buyer objections through a single sales call and resulting in more successful sales and shorter sales cycles.

3.2.3 Intra corporate Core Connectivity

Business process reengineering programs and application of Enterprise Resource Planning (ERP), such as SAP, succeed by eliminating barriers to communications across departmental boundaries and by replacing slow paperwork procedures with shared electronic databases. These management practices and the associated computer software require reliable, high speed, and secure communications among all employees. The same high level of communications connectivity is required at all of the enter prise's establishments. This setup typically requires that small offices and branch offices be upgraded to the higher standards more commonplace at large headquarters locations. The

payoff for successful ERP implementation is an order of magnitude reduction in cycle times, increased flexibility and responsiveness, and sharp reductions in IT overhead costs.

3.2.4 Closed User Groups with Partners, Customers, and Suppliers

Some of the most dramatic improvements in business processes are obtained by eliminating certain sub processes entirely. The supply chain is one business process where big improvements are being realized. For example, Boeing suppliers are required to participate in its supply network. This enables Boeing to eliminate stores and parts costs entirely by moving those functions back into the supplier's operation. Similar successes have been achieved in sales and marketing. In another example, Saturn customers can step through the entire sales process online. Saturn reduces selling costs and provides prospective customers with full and accurate examination of options and features, independent of high pressure sales people.

Highly technical sales organizations can create lock in relationships with their customers through creation of closed user groups. For example, semiconductor manufacturers provide online engineering design tools so that circuit designers can incorporate the manufacturer's chips directly into finished designs. Closed user groups not only assure product loyalty, they also provide value to circuit designers by reducing cycle times.

3.2.5 Public Internet Access

Essentially all functional areas can benefit from public Internet access. Accounting organizations retrieve forms and advice from federal, state, and local revenue offices. Human resources organizations use the Monster Board for recruiting. Mechanical designers can peruse

online parts catalogs and download CAD/CAM drawings directly into their blue prints. Energy marketers buy and sell natural gas through Internet based trading systems and retrieve weather data from government and private sources. Pension fund managers follow the financial markets and retrieve stock holder information from company Web pages. IT professionals stay ahead of industry developments and product releases by studying computer and software vendors' online product literature. The business benefit of most of this activity is faster and better informed decision making.

3.2.6 Internet Based Customer Interaction

Retail sales and service companies operate on thin operating margins. Their success depends on executing transactions rapidly and at low cost while giving the customer the appearance of custom tailored service this is sometimes referred to as mass customization. Industries such as air lines, utilities, banks, and brokerage, insurance, and mail-order retailers know that market segmentation, customer loyalty, and low transaction costs are the keys to their success (or survival). Of course, the more time customer service representatives spend with customers and the more they can learn about customers, the better the market segmentation and the customer relationship. Unfortunately, this tender loving care costs money and drives up transaction costs.

Well designed Internet based customer interaction systems resolve this dilemma by eliminating customer service staffing costs and simultaneously providing customers with many custom choices. Information provided by the customer during these online sessions flows directly to the enterprise's data warehouse and is used by data mining tools to further refine the market segmentation models. Brokerage and financial services firms are especially effective at using the Internet to drive down small lot trading fees and eliminate the cost of account representatives. For example, a trade of 100 shares that once cost

several hundred dollars can be done on the Internet for $10. As another example, airlines, including United Airlines, provide Web pages where customers can shop for the best price and schedule, and book their travel over the Internet.

3.2.7 Web Presence

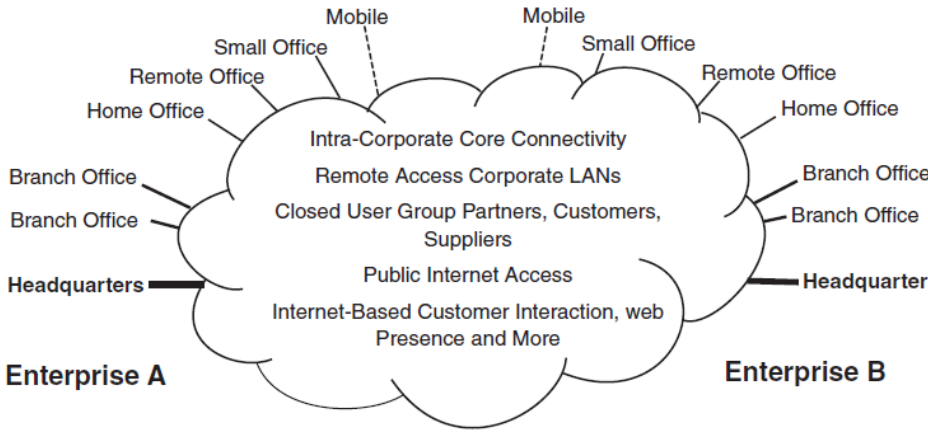
The public Internet is rapidly replacing mass media, including television, radio, and print, as the vehicle for certain product and institutional advertising. While practically all businesses feel compelled to have a Web page, it is essential in many industry segments. Use of Web pages is firmly entrenched in the IT industry itself, financial services, education, and government services. The key item these enterprises share in common is a need for dissemination of large quantities of time sensitive information to millions of people. While these enterprises gain high value from rapid and cheap dissemination of information through Internet Web pages, they also face large risks. Incorrect or false information could destroy the public trust that was built up over decades. Slow information access or unreliable access could create an image of ineptitude or unresponsiveness, damaging institutional loyalty and trust. Failure to safeguard customer data and protect privacy could, at best, destroy trust and, at worst, cause financial ruin. Thus, a Web presence can be effective in reaching the mass market, but security and reliability must be assured.

3.2.8 Getting Real Business Value from Virtual Private Networks

The preceding section describes six ways data communications can be used to produce business value. However, today's data communications networks are failing to deliver the value, because they are too complex and costly. VPNs provide more efficient and secure data communications at a fraction of the cost of today's network architectures. In particular, VPNs reduce the administrative effort and

costs of building and operating private networks. This is particularly true as customers, suppliers, and third parties are added to the network. Figure shows the emerging VPN architecture.

One difference between the VPN architecture and today's private net work architecture is that the VPN architecture is seamless. Users in each enterprise, regardless of whether their location is at headquarters or on a wireless link, obtain the same access and logical view of services, despite being served by a number of ISPs and through different physical media. Another difference between the private data communications network and the VPN is that business users never see the network complexity, and net work administrators are freed from complex network engineering tasks.



Emerging VPN architecture.

3.2.9 Virtual Service Management

Many of today's VPNs have focused only on providing a secure transport, the network "plumbing." But in practical terms, the benefits of VPN have been off limits to smaller businesses and organizations with limited IT staff and resources, because of the technical complexity of setting up and administering a VPN. Virtual Services Management (VSM) is critical to making a VPN easy to administer and manage across multiple locations and services.

The administrative challenge of creating and maintaining a VPN is formidable. A single enterprise often must accommodate headquarters, campuses, branch offices to home offices, and users who want to use a range of applications and services, and have specific accessing privileges and options. In addition, modern management practice requires many additional links to suppliers, customers, and third parties, as well as access to the public Internet with its 100 million computers.

Through a single point of administration anywhere on the network (local or remote), VSM technology simplifies the administrative burden of setting up multiple branch office email, Web, firewall, and other user services; multiple domain and user names; and coordination among multiple ISPs. It also simplifies the administrative burden through automatic synchronization of software upgrades, replication of Web servers, and sophisticated policy management. VSM overcomes the barrier to private network implementation and VPN that could previously be addressed by only a handful of the largest, more technically sophisticated enterprises.

VSM can help resellers by making it easy for them to add services without raising the level of technical support they will need to provide. This can be done with service providers or as a standalone value added feature.

Similarly, service providers can take advantage of VSM and VPNs to provide a value added network feature to their customers. VPN services are typically provided on a monthly fee basis and often require customers to perform the network configuration and route determination for their VPN. Where the customer is doing much of the work already, customers often acquire the lines and build a VPN network using CPE products such as an all in one Internet system (described below). Many enterprises are finding if they partner with their service provider to produce a VPN solution, it can be a very effective way to take

development costs out of the equation.

3.3 SECURE AND RELIABLE NETWORKING TRANSPORT

To provide secure and reliable transport across the network, three mainissues must be resolved:

1. Overall network security
2. Wide area network tunneling
3. Class of service and quality of service

Products and standards are in place to provide overall network security while emerging standards will soon resolve the other two issues.

Four functions are key to overall network security:

1. Authentication - verify the identity of the user
2. Authorization - verify which services the user is allowed to access
3. Accounting - create an audit trail of the user's network activity
4. Encryption- protect data privacy

These four functions are typically provided by access control lists in routers that restrict access to data packets and network segments in both directions. Firewalls provide more sophisticated control of incoming and outgoing packets at the network's edge. Authentication and authorization is provided by services such as PAP or CHAP and by security servers. Proxy application servers and the network operating system provide additional network security. These necessary services and products are now widely deployed in ISPs and private networks.

Wide area network tunneling is a technique that establishes a

secure network connection across the public Internet. Trade press articles sometimes equate VPNs to tunneling. Our view is that tunneling, while an essential ingredient of the VPN solution is but one element of the VPN and that administrative and reliability issues are at least as important to successful VPN adoption. Major networking vendors have advanced proposed tunneling standards such as Point to Point Tunneling Protocol and L2F. Much marketplace confusion has resulted from these competing standards. Happily, it appears that a compromise approach called L2TP will resolve the differences between these competing standards and will soon emerge from the IETF standards setting process.

3.3.1 IMPLEMENTING THE VPN

The key to deploying a VPN is to give the appearance of a seamless net work with identical user services at all locations headquarters, branch offices, home offices, and those of partners, suppliers, and customers. One approach to VPN implementation for small and medium sized organizations is to deploy all in one Internet systems, sometimes called "Internet edge servers," at the network edge between each enterprise site and the local ISP. The all in one Internet system integrates Internet server, firewall, and networking functionality for organizations that want to take greater advantage of the Internet without adding a complex and costly assembly of boxes and IT staff.

VSM capabilities supported by the system can then provide single point administration of VPN services. Figure shows how the three versions of VSM technology in branch, remote, and extranet applications can be used.

A multi branch VPN can be used to connect a company's remotely located, LAN attached offices. An all in one Internet system will be required at each office, in this case. Class of Service policies, such as access privileges and priorities, can be applied as if the branch users were physically located at headquarters. Security can be

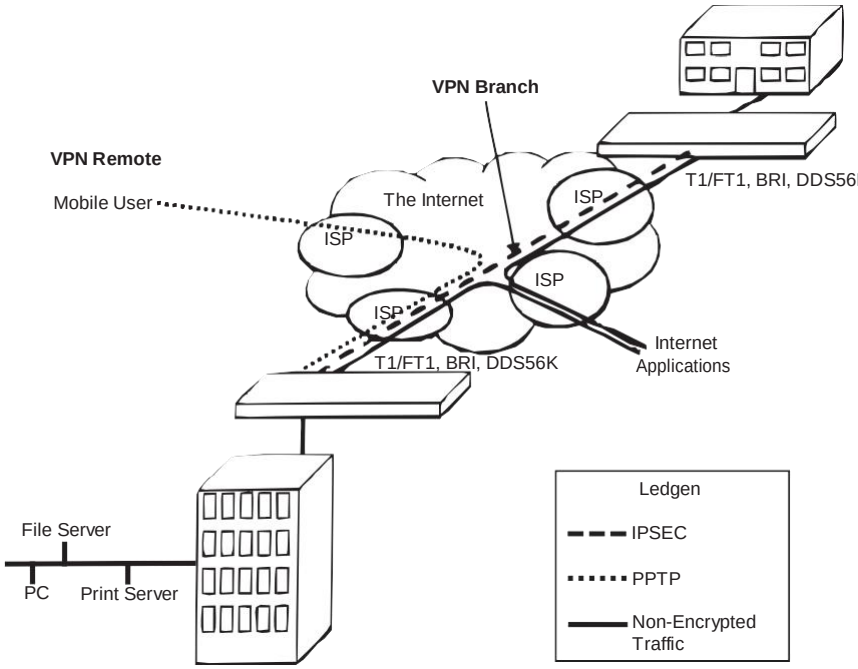
implemented through the emerging industry standard IP Security (IPSec) protocol, which will provide DES encryption, authentication, and key management.

A remote VPN can enable mobile workers and telecommuters to dial into a local ISP to access corporate information and service, making it appears as if they were sitting at their desks in the main office. An all in one Internet system will be required at headquarters and Microsoft's Point to Point Protocol (PPTP), available with MS Windows clients; will be requiredon the remote user's desktop or laptop system. A Point to Point Protocol server in the system can authenticate the remote user, and then open an encrypted path through which traffic flows as if through the LAN.

An extranet VPN opens a corporate network selectively to suppliers, customers, strategic business partners, and users having access to a limited set of information behind the corporate firewall. An extranet VPN implementation differs from branch and remote VPN implementations in that its use is likely to involve temporary virtual networks which may be set up for specific projects and dismantled as the project's end.

It is important that all necessary service management, security, and Quality of Service functions are combined in the system so that multiple systems can be administered as though they are on a single local network. The supported services should include all of the administrative, security, and reliability requirements of the VPN:

Hardware costs can also be minimized because all the necessary administrative, security, and reliable transport functionalities are combined in a single unit. Administrative and operating expenses can be controlled through VSM, which permits management of all sites from a single point minimizing the need for costly data communications experts.



Branch Office

Corporate Central Site

The three versions of VSM technology.

- IP router
- Web server
- firewall
- email
- file transfer (FTP)
- Domain Name Service (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- remote management

3.3.2 SECURE REMOTE ACCESS OVER THE INTERNET

THE COMPONENTS AND RESOURCES OF ONE

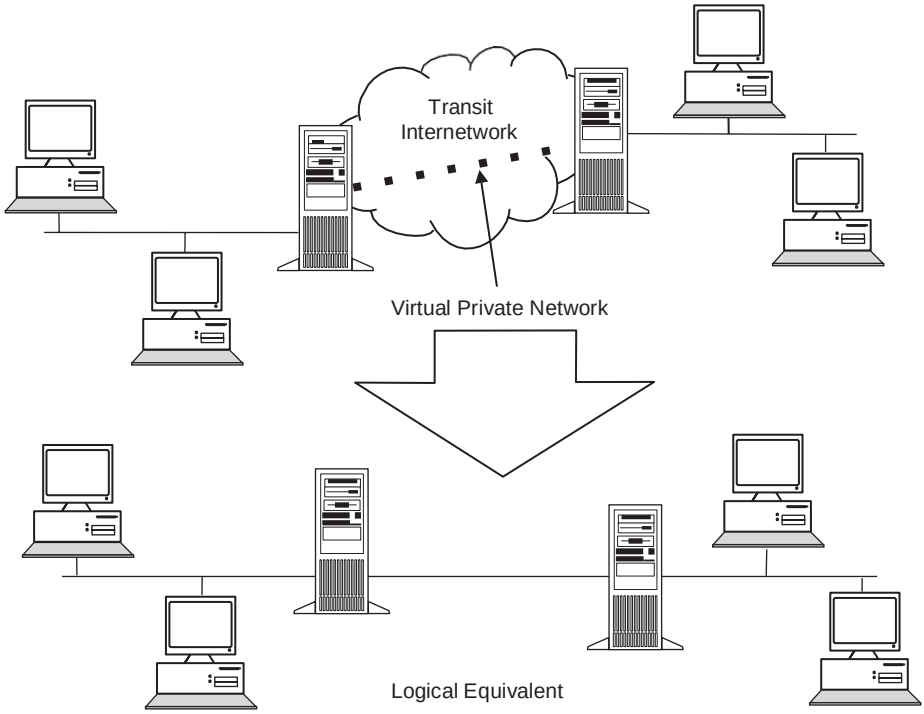
NETWORK OVER ANOTHER NETWORK are connected via a Virtual Private Network (VPN). As shown in Figure, VPNs accomplish this by allowing the user to tunnel through the Internet or another public network in a manner that lets the tunnel participants enjoy the same security and features formerly available only inprivate networks.

Using the routing infrastructure provided by a public internetwork (such as the Internet), VPNs allow telecommuters, remote employees like salespeople, or even branch offices to connect in a secure fashion to an enterprise server located at the edge of the enterprise local area network (LAN). The VPN is a point to point connection between the user's computer and an enterprise server from the user's perspective. It also appears as if the data is being sent over a dedicated private link because the nature of the intermediate internetwork is irrelevant to the user. As previously mentioned, while maintaining secure communications, VPN technology also allows an enterprise to connect to branch offices or to other enterprises (extranets) over a public internetwork (such as the Internet). The VPN connection across the Internet logically operates as a wide area net work (WAN) link between the sites. In both cases, the secure connection across the internetwork appears to the user as a private network communication (despite the fact that this communication occurs over a public internetwork); hence the name Virtual Private Network.

VPN technology is designed to address issues surrounding the current enterprise trend toward increased telecommuting, widely distributed global operations, and highly interdependent partner operations. Here, workers must be able to connect to central resources and communicate with each other. And, enterprises need to efficiently manage inventories for just in time production.

An enterprise must deploy a reliable and scalable remote access solution to provide employees with the ability to connect to enterprise computing resources regardless of their location. Enterprises typically

choose one of the following:



Virtual Private Network.

- an IT department driven solution, where an internal information systems department is charged with buying, installing, and maintaining enterprise modem pools and a private network infrastructure
- value added network (VAN) solutions, where an enterprise pays an outsourced enterprise to buy, install, and maintain modem pools anda Telco infrastructure

The optimum solution in terms of cost, reliability, scalability, flexible administration and management, and demand for connections is provided by neither of these traditional solutions. Therefore, it makes sense to finda middle ground where the enterprise either supplements or replaces its current investments in modem pools and its private network

infrastructure with a less expensive solution based on Internet technology. In this manner, the enterprise can focus on its core competencies with the assurance that accessibility will never be compromised, and that the most economical solution will be deployed. The availability of an Internet solution enables a few Internet connections (via Internet service providers, or ISPs) and deployment of several edge of network VPN server computers to serve the remote networking needs of thousands or even tens of thousands of remote clients and branch offices, as described next.

3.3.3 VPN Common Uses

The next few subsections of this chapter describe in more detail common VPN situations.

3.3.4 Secure Remote User Access over the Internet

While maintaining privacy of information, VPNs provide remote access to enterprise resources over the public Internet. A VPN that is used to connect a remote user to an enterprise intranet is shown in Figure. The user first calls a local ISP Network Access Server (NAS) phone number, rather than making a leased line; long-distance (or 1800) call to an enterprise or outsourced NAS. The VPN software creates a virtual private network between the dialup user and the enterprise VPN server across the Internet using the local connection to the ISP.

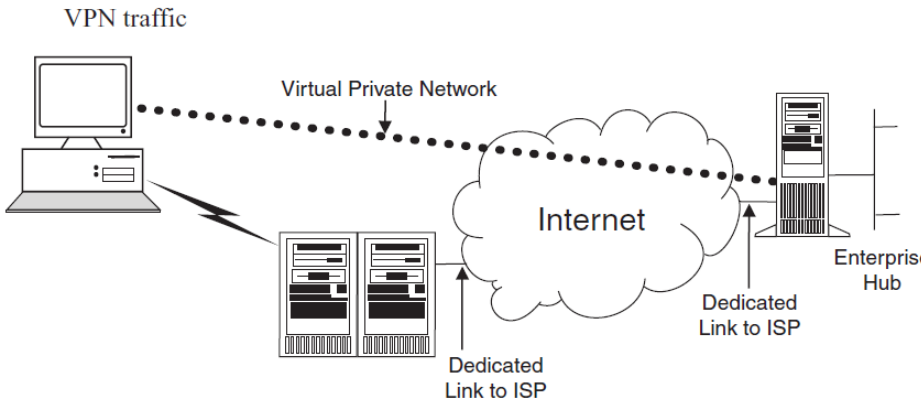
3.3.5 Connecting Networks over the Internet.

To connect local area networks at remote sites, there exist two methods for using VPNs: using dedicated lines to connect a branch office to an enterprise LAN, or a dialup line to connect a branch office to an enterprise LAN.

Using Dedicated Lines to Connect a Branch Office to an

Enterprise LAN. Both the branch office and the enterprise hub routers can use a local dedicated circuit and local ISP to connect to the Internet, rather than using an expensive long haul dedicated circuit between the branch office and the enterprise hub. The local ISP connections and the public Internet are used by the VPN software to create a virtual private network between the branch office router and the enterprise hub router.

Using a DialUp Line to Connect a Branch Office to an Enterprise LAN. The router at the branch office can call the local ISP, rather than having a router at the branch office make a leased line, long distance or (1800) call to an enterprise or outsourced NAS. Also, in order to create a VPN between the branch office router and the enterprise hub router across the Internet, the VPN soft ware uses the connection to the local ISP as shown in figure

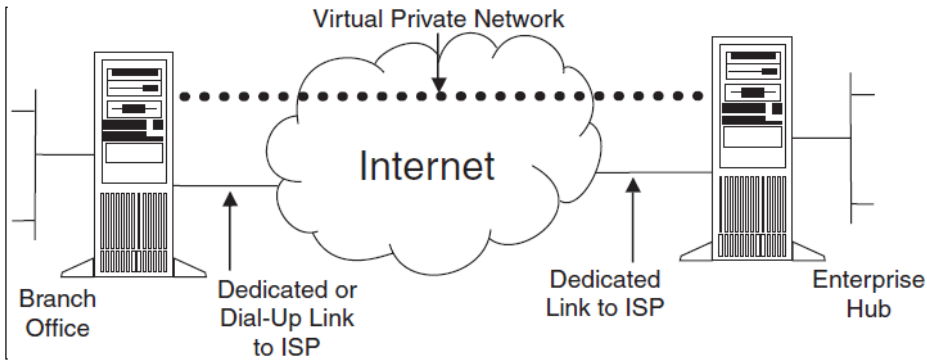


Using a VPN to connect a remote client to a private LAN.

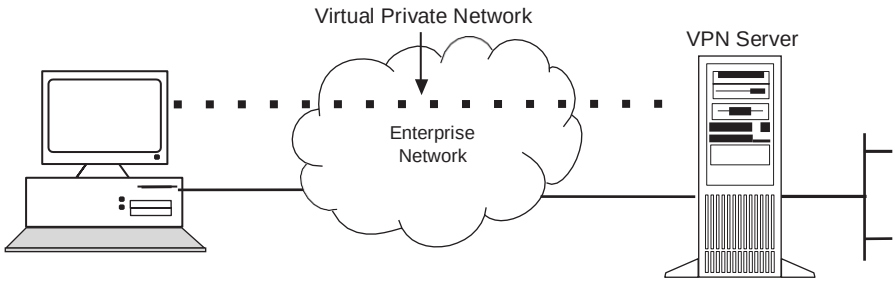
The facilities that connect the branch office and enterprise offices to the Internet are local in both cases. To make a connection, both client/server, and server/server VPN cost savings are largely predicated on the use of a local access phone number. It is recommended that the enterprise hub router that acts as a VPN server be connected to a local ISP with a dedicated line. This VPN server must be listening 24 hours per day for incoming VPN traffic.

3.3.6 Connecting Computers over an Intranet

The departmental data is so sensitive that the department's LAN is physically disconnected from the rest of the enterprise internetwork in some enterprise internetworks. All of this creates information accessibility problems for those users not physically connected to the separate LAN, although the department's confidential information is protected.



Using a VPN to connect two remote sites.



Secured or Hidden Network

Using a VPN to Connect to two computers on the same LAN.

VPNs allow the department's LAN to be separated by a VPN server but physically connected to the enterprise internetwork. One should note that the VPN server is not acting as a router between the enter prise internetwork and the department LAN. A router would interconnect the two networks, thus allowing everyone access to the sensitive LAN. The network administrator can ensure that only those

users on the enterprise internetwork who have appropriate credentials (based on a need to know policy within the enterprise) can establish a VPN with the VPN server and gain access to the protected resources of the department by using a VPN. Additionally, all communication across the VPN can be encrypted for data confidentiality. Thus, the department LAN cannot be viewed by those users who do not have the proper credentials.

3.3.7 BASIC VPN REQUIREMENTS

Normally, an enterprise desires to facilitate controlled access to enterprise resources and information when deploying a remote networking solution. In order to easily connect to enterprise local area network (LAN) resources, the solution must allow freedom for authorized remote clients. And, in order to share resources and information (LAN to LAN connections), the solution must also allow remote offices to connect to each other. Finally, as the data traverses the public Internet, the solution must ensure the privacy and integrity of data. Also, in the case of sensitive data traversing an enterprise internetwork, the same concerns apply. A VPN solution should therefore provide all of the following at a minimum:

- *Address management:* the solution must assign a client's address on the private net, and must ensure that private addresses are kept private
- *Data encryption:* data carried on the public network must be rendered unreadable to unauthorized clients on the network
- *Key management:* the solution must generate and refresh encryption keys for the client and server
- *Multiprotocol support:* the solution must be able to handle common protocols used in the public network; these include Internet Protocol (IP), Internet Packet Exchange (IPX), etc.

- *User authentication:* the solution must verify a user's identity and restrict VPN access to authorized users; in addition, the solution must provide audit and accounting records to show who accessed what information and when

Furthermore, all of these basic requirements are met by an Internet VPN solution based on the Point to Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP). The solution also takes advantage of the broad availability of the worldwide Internet. Other solutions meet some of these requirements, but remain useful for specific situations, including the new IP Security Protocol (IPSec).

3.3.8 Point to Point Tunneling Protocol (PPTP)

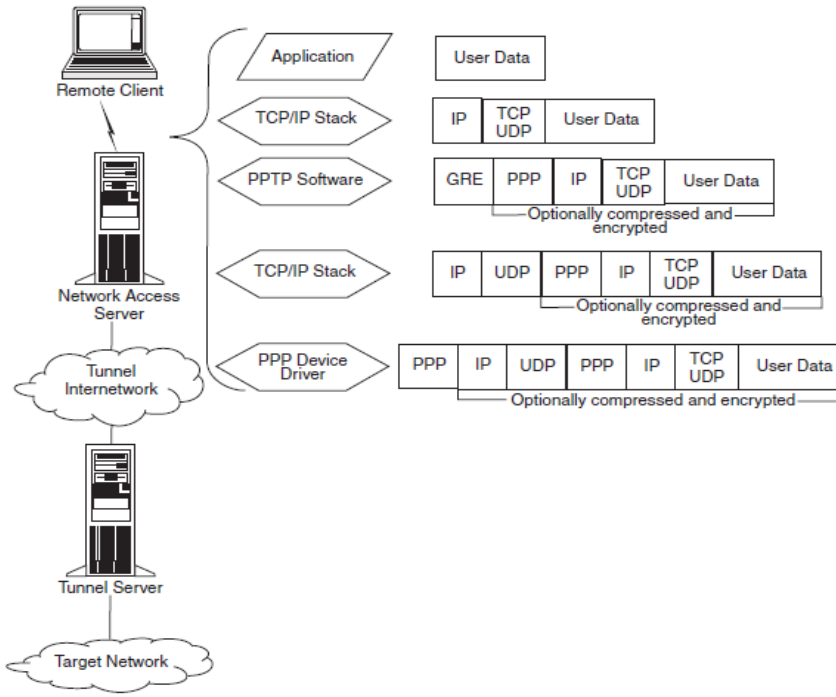
PPTP is a Layer 2 protocol that encapsulates PPP frames in IP datagram for transmission over an IP internetwork, such as the Internet. PPTP can also be used in private LAN to LAN networking.

PPTP is documented in the draft RFC, "Point to Point Tunneling Proto col."[1] This draft was submitted to the IETF in June 1996 by the member enterprises of the PPTP Forum, including Microsoft Corporation, Ascend Communications, 3Com/Primary Access, ECI Telematics, and U.S. Robotics (now 3Com).

The Point to Point Tunneling Protocol (PPTP) uses Generic Routing Encapsulation (GRE) encapsulated Point to Point Protocol (PPP) frames for tunneled data and a TCP connection for tunnel maintenance. The payloads of the encapsulated PPP frames can be compressed as well as encrypted. How a PPTP packet is assembled prior to transmission is shown in Figure. The illustration shows a dialup client creating a tunnel across an internetwork. The encapsulation for a dialup client (PPP device driver) is shown in the final frame layout.

3.3.9 Layer 2 Forwarding (L2F)

L2F (a technology proposed by Cisco Systems, Inc.) is a transmission protocol that allows dialup access servers to frame dialup traffic in PPP and transmit it over WAN links to an L2F server (a router). The L2F server then unwraps the packets and injects them into the network. Unlike PPTP and L2TP, L2F has no defined client.



Construction of a PPTP packet.

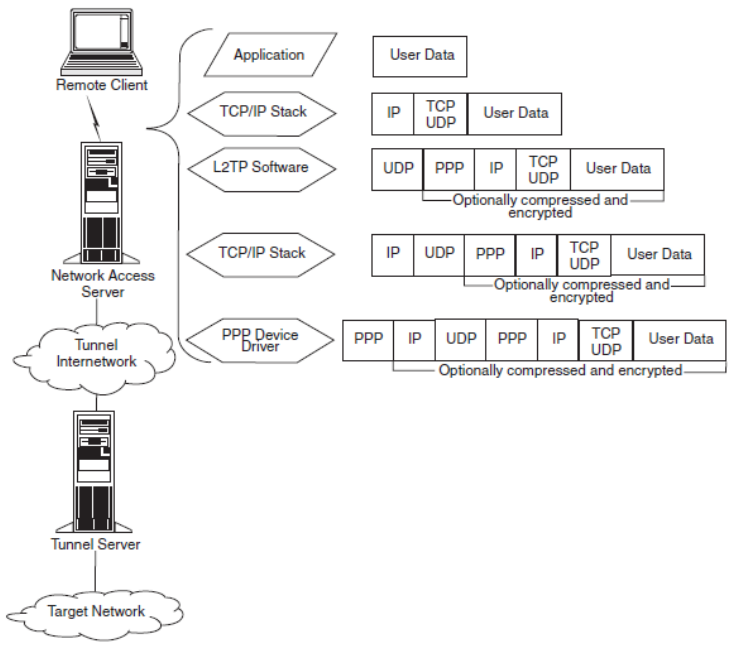
3.3.10 Layer 2 Tunneling Protocol (L2TP)

A combination of PPTP and L2F makes up L2TP. In other words, the best features of PPTP and L2F are incorporated into L2TP.

L2TP is a network protocol that encapsulates PPP frames to be sent over Asynchronous Transfer Mode (ATM), IP, X.25, or frame relay networks. L2TP can be used as a tunneling protocol over the Internet

when configured to use IP as its datagram transport. Without an IP transport layer, L2TP can also be used directly over various WAN media (such as Frame Relay). L2TP is documented in the draft RFC, Layer 2 Tunneling Protocol "L2TP" (draftietfpppextl2tp09.txt). This draft document was submitted to the IETF.

For tunnel maintenance, L2TP over IP internetworks uses UDP and a series of L2TP messages. As the tunneled data, L2TP also uses UDP to send L2TPencapsulated PPP frames. The payloads of encapsulated PPP frames can be compressed as well as encrypted. How an L2TP packet is assembled prior to transmission is shown in Figure . A dialup client creating a tunnel across an internetwork is shown in the Figure. The encapsulation for a dialup client (PPP device driver) is shown in the final frame layout. L2TP over IP is assumed in the encapsulation.



Construction of an L2TP packet

3.3.11 L2TP Compared to PPTP. PPP is used to provide an initial

envelope for the data for both PPTP and L2TP. Then, it appends additional headers for transport through the internetwork. The two protocols are very similar. There are differences between PPTP and L2TP, however. For example,

- L2TP provides for header compression. When header compression is enabled, L2TP operates with four bytes of overhead, as compared to six bytes for PPTP.
- L2TP provides for tunnel authentication, while PPTP does not. However, when either protocol is used over IPSec, tunnel authentication is provided by IPSec so that Layer 2 tunnel authentication is not necessary.
- PPTP can only support a single tunnel between endpoints. L2TP allows for the use of multiple tunnels between endpoints. With L2TP, one can create different tunnels for different qualities of service.
- PPTP requires that the internetwork be an IP internetwork. L2TP requires only that the tunnel media provide packet oriented point to point connectivity. L2TP can be used over IP (using UDP), Frame Relay permanent virtual circuits (PVCs), X.25 virtual circuits (VCs), or ATM VCs.

3.4 INTERNET PROTOCOL SECURITY (IPSEC) TUNNEL MODE

The secured transfer of information across an IP internetwork is supported by IPSec (a Layer 3 protocol standard). Nevertheless, in the context of tunneling protocols, one aspect of IPSec is discussed here. IPSec defines the packet format for an IP over an IP tunnel mode (generally referred to as IPSec Tunnel Mode), in addition to its definition of encryption mechanisms for IP traffic. An IPSec tunnel consists of a tunnel server and tunnel client. These are both configured to use a negotiated encryption mechanism and IPSec tunneling.

For secure transfer across a private or public IP internetwork,

IPSec Tunnel Mode uses the negotiated security method (if any) to encapsulate and encrypt entire IP packets. The encrypted payload is then encapsulated again with a plaintext IP header. It is then sent on the internetwork for delivery to the tunnel server. The tunnel server processes and discards the plain text IP header and then decrypts its contents to retrieve the original payloadIP packet. Upon receipt of this datagram, the payload IP packet is then processed normally and routed to its destination on the target network. The following features and limitations are contained within the IPSec Tunnel Mode:

- It is controlled by a security policy: a set of filter matching rules. This security policy establishes the encryption and tunneling mechanisms available in order of preference and the authentication methods available, also in order of preference. As soon as there is traffic, the two machines perform mutual authentication, and then negotiate the encryption methods to be used. Thereafter, all traffic is encrypted using the negotiated encryption mechanism and then wrapped in a tunnel header.
- It functions at the bottom of the IP stack; therefore, applications and higher level protocols inherit its behavior.
- It supports IP traffic only.

The remainder of this article discusses VPNs and the use of these technologies by enterprises to do secure remote access (e.g., by traveling employees and sales reps) over the Internet in greater detail.

3.4.1 EASY TO MANAGE AND USE

While squeezing the maximum possible from budget and support staffs, today's enterprises are asking their information technology groups (ITGs) to deliver an increasing array of communication and networking services. It appears that the situation is no different at Microsoft Corporation (Redmond, Washington). The Microsoft ITG

needed to provide secure, Internet based remote access for its more than 35,000 mobile sales personnel, telecommuters, and consultants around the world.

Microsoft's ITG is currently using and deploying a custom Windows based remote dialup and virtual private networking (VPN) solution by using Windows based clients and enhanced Windows 2000® RAS (Remote Access Server) technology available in the Windows 2000 Option Pack (formerly named Windows NT 5.0). Users are given quick, easy, and low cost network access. Additional user services are provided with new Windows based network services from UUNet Technologies, Inc.[3]

3.4.2 Integrated RASVPN Clients

According to Microsoft, its ITG has learned that the widespread adoption and use of technology largely depends on how easy and transparent the experience is for the end user. Likewise, Microsoft's ITG has learned not to deploy technologies for which complexity results in an increased support burden on its limited support staff. Microsoft's ITG provided a single client interface with central management to simultaneously make the remote access solution easy to use and manage.

3.4.2.1 Single Client. A single client is used for both the direct dial up and virtual private network connections. Users utilize the same client interface for secure transparent access, whether dialing directly to the enterprise network or connecting via a VPN, by using Windows integrated dialup net working technology (DUN) and Microsoft Connection Manager. In fact, users do not need to concern themselves with which method is employed.

3.4.2.2 Central Management. Central management is used for remote dialup and VPN access phone numbers. According to Microsoft, its ITG has found that one of the most common support problems traveling users face is deter mining and managing local access phone numbers. This problem translates into one of the principal reasons for support calls to Microsoft's user support centers. Using the Connection Manager Administration Kit (CMAK) wizard (which is part of Microsoft's remote access solution), Microsoft's ITG preloads each client PC with an electronic phone book that includes every dialup remote access phone number for Microsoft's net work. The Windows solution also allows phone books to be centrally integrated and managed from a single remote location, and clients to be updated automatically.

3.4.3 WINDOWS COMMUNICATION PLATFORM

In order to provide a flexible and comprehensive network solution, the open extensibility of the Windows 2000 allows Microsoft's ITG to preserve its current hardware network investments while partnering with UUnet Technologies, Inc. According to Microsoft, the Windows platform enabled its ITG to integrate the best of breed network services and applications to best meet its client and network administration needs.

3.4.3.1 High Speed Internet Access on the Road

Microsoft employees can also connect to high speed Internet access by plugging into public IPORT[4] jacks in hotels, airports, cafes, and remote locations. The Microsoft ITG integrates the IPORT[5] pay per use Internet access features into its custom remote access solution. According to Microsoft, this high bandwidth, easily available connection helps Microsoft employees be more productive and have a better online experience while on the road.

3.4.4 Secure Internet Access and VPN

Microsoft's ITG, like its counterparts at every enterprise, must ensure that the edge of its network is secure while still providing all employees with the freedom needed to access information worldwide. Microsoft's ITG has also deployed Microsoft Proxy Server to securely separate the LAN from the Internet to meet this need.

To ensure that no intruders compromise the edge of network, the Microsoft Proxy Server firewall capabilities protect Microsoft's network from unauthorized access from the Internet by providing network address translation and dynamic IPlevel filtering. Microsoft's ITG uses the powerful caching services in Microsoft Proxy Server to expedite the delivery of information at the same time.

The Proxy Server is able to service subsequent user requests of already requested information without having to generate additional network traffic by reusing relevant cached information. In addition, in order to operate at peak efficiency with the utmost security, ITG uses Microsoft Proxy Server to enable the Microsoft intranet and remote employees.

3.4.5 RAS Reporting and Internal Usage Chargeback (Billing)

Microsoft pays a substantial amount for remote access fees due to the need to maintain private leased lines and dedicated 800 numbers like many large enterprises with a multitude of branch offices and remote employees. In addition, according to Microsoft, the sheer number of LAN entry points and autonomy afforded its international divisions made centralized accounting and retail reporting for remote access use and roaming users important.

Microsoft's ITG is deploying a VPN solution — bolstered with centralized accounting and reporting of enterprise wide remote access

and VPN use — by using Windows 2000, integrated user domain directory, and RADIUS services. As part of this solution, Microsoft is also deploying TRU RADIUS Accountant™ for Windows 2000 from TelcoResearch.[6]

Furthermore, Microsoft's ITG is also able to generate detailed reporting of remote access and VPN network use for internal cost accounting purposes while using familiar Windows 2000 management tools by using Telco Research's product. In addition, Microsoft's ITG is able to quickly and easily deploy a turnkey reporting solution built on the intrinsic communication services of Windows 2000 in this manner. According to Microsoft, while maintaining the flexibility to accommodate future change, they receive better security as a result, reduced implementation costs, and enhanced reporting to improve remote access management and charge back service.

3.4.6 VIP Services: Economical Internet Access and VPN

By working with UUnet Technologies, Inc. (the largest Internet service provider in the world), the Microsoft ITG supplemented its private data network infrastructure and RAS with VPN services. Microsoft's VPN solution is integrated with the UUnet Radius Proxy servers through the Windows 2000 native support for RADIUS under this relationship.

Through the Windows 2000 Remote Access Service integrated RADIUS support, Microsoft's ITG made reliable and secure local access to UUnet Technologies IP network available to all Microsoft mobile employees. This resulted in the delivery of high quality VPN services over the UUnet Technologies, Inc. infrastructure at a reduced cost. The ITG conservatively estimates that this use of VPN service as an alternative to traditional remote access will save Microsoft more than $7 million per year in remote access fees alone. Additional savings are expected from the elimination of call requests for RAS phone numbers

and greatly reduced remote access con figuration support.

The ITG utilized the integrated support for RADIUS based authentication available from the Windows Directory in Windows 2000. This allowed them to retain all existing authentication rights for both Internet and LAN access, avoiding change or redundant replication of directory, and provided for enhanced network security.

According to Microsoft, their ITG was able to instantly extend network access to its more than 50,000 employees in more than 100 countries through its relationship with UUnet Technologies. So that Microsoft employees can access information locally anywhere with reliability guarantees and the support of UUnet, UUnet Technologies' transcontinental backbone provides access throughout North America, Europe, and the Asia–Pacific region.

PLANNING FOR THE FUTURE

Finally, Microsoft's ITG wanted to ensure that its current investment in the remote access infrastructure would not only be able to meet today's needs, but also enable it to make the most of opportunities provided by the digital convergence of network aware applications in the near future. Evidence of an increased need for higher degrees of client/server network application integration is found in the momentum of Windows 2000 as a platform for IP telephony, media streaming technologies, and the migration to PBX systems based on Windows 2000.

The flexibility needed to economically address current and future needs of Microsoft's ITG is provided through the use of Windows 2000 as the backbone of the remote access solution. Through partnerships with multiple service providers such as UUnet Technologies, the selection of a Windows based solution allows ITG the freedom to both centrally manage and incrementally extend the Microsoft direct dial and VPN infrastructure at a controlled pace and in an open manner.

In order to connect Microsoft subsidiaries, branch offices, and extranet partners securely to the enterprise network over private and

public net works, Windows 2000 Routing, RAS, and VPN services — along with tight integration with Microsoft Proxy Server — are already enabling Microsoft's ITG to seamlessly extend its RAS–VPN infrastructure. Furthermore, to meet Microsoft's enterprise needs into the future, the broad application support enjoyed by the Windows communication platform ensures that ITG will continue to have access to a host of rich application services made available by developers and service providers, such as ATCOM, Inc., Telco Research, and UUnet Technologies, Inc.

3.5 IPSec VPNS

VPNS ARE MAKING A HUGE IMPACT ON THE WAY COMMUNICATIONS ARE VIEWED. They are also providing ample fodder for administrators and managers to have seemingly endless discussions about various applications. On one side are the possible money savings, and the other are implementation issues. There are several areas of serious concern:

- performance
- interoperability
- scalability
- flexibility

3.5.1 Performance

Performance of data flow is typically the most common concern, and IPSec is very processor intensive. The performance costs of IPSec are the encryption being performed, integrity checking, packet handling based on policies, and forwarding, all of which become apparent in the form of latency and reduced throughput. IPSec VPNs over the Internet increase the latency in the communication that conspires with the processing costs to discourage VPN as a solution for transport sensitive

applications. Process time for authentication, key management, and integrity verification will produce delay issues with SA establishment, authentication, and IPSec SA maintenance. Each of these results in poor initialization response and, ultimately, disgruntled users.

The application of existing hardware encryption technology to IPSec vendor products has allowed these solutions to be considered more closely by prospective clients wishing to seize the monetary savings associated with the technology. The creation of a key and its subsequent use in the encryption process can be offloaded onto a dedicated processor that is designed specifically for these operations. Until the application of hard ware encryption for IPSec, all data was managed through software computation that was also responsible for many other operations that may be running on the gateway.

Hardware encryption has released IPSec VPN technology into the realm of viable communication solutions. Unfortunately, the client operating system participating in a VPN is still responsible for the IPSec process. Publicly available mobile systems that provide hardware based encryption for IPSec communications are becoming available, but are sometime away from being standard issue for remote users.

3.5.2 Interoperability

Interoperability is a current issue that will soon become antiquated as vendors recognize the need to become fully IPSec compliant — or consumers will not implement their product based simply on its incompatibility. Shared secret and ISAKMP key management protocol are typically allowing multivendor interoperability. As Certificate Authorities and the technology that supports them become fully adopted technology, they will only add to the cross platform integration. However, complex and large VPNs will not be manageable using different vendor products in the near future.

Given the complexity, recentness of the IPSec standard and the various interpretations of that standard, time to complete interoperability seem great.

3.5.3 Scalability

Scalability is obtained by the addition of equipment and bandwidth. Some vendors have created products focused on remote access for roaming users, while others have concentrated on network to network connectivity without much attention to remote users. The current ability to scale the solution will be directly related to the service required. The standard supporting the technology allows for great flexibility in the addition of services. It will be more common to find limitations in equipment configurations than in the standard as it pertains to growth capabilities. Scalability ushers in a wave of varying issues, including:

- authentication
- management
- performance

Authentication can be provided by a number of processes, although the primary focus has been on RADIUS, Certificates, and forms of two factor authentication. Each of these can be applied to several supporting databases. RADIUS is supported by nearly every common authenticating system from Microsoft Windows NT to Net Ware's NDS. Authentication, when implemented properly, should not become a scalability issue for many implementations, because the goal is to integrate the process with existing or planned enterprise authenticating services.

A more interesting aspect of IPSec vendor implementations and the scalability issues that might arise is management. As detailed earlier, certain implementations do not scale, due to the shear physics of shared

secrets and manual key management. In the event of the addition of equipment or increased bandwidth to support remote applications, the management will need to take multiplicity into consideration. Currently, VPN management of remote users and networks leaves a great deal to be desired. As vendors and organizations become more acquainted with what can be accomplished, sophisticated management capabilities will become increasingly available.

Performance is an obvious issue when considering the increase of an implementation. Typically, performance is the driving reason, followed by support for increased numbers. Both of these issues are volatile and inter related with the hardware technology driving the implementation. Performance capabilities can be controlled by the limitation of supported SAs on a particular system a direct limitation in scalability. A type of requested encryption might not be available on the encryption processor currently available. Forcing the calculation of encryption onto the operating system ultimately limits the performance. A limitation may resonate in the form of added equipment to accomplish the link between the IPSec equipment and the authenticating database. When users authenticate, the granularity of control over the capabilities of that user may be directly related to the form of authentication. The desired form of authentication may have limitations in various environments due to restrictions in various types of authenticating databases. Upgrade issues, service pack variations, user limitations, and protocol requirements also combine to limit growth of the solution.

3.5.4 THE MARKET FOR VPN

Several distinct qualities of VPN are driving the investigation by many organizations to implement VPN as a business interchange technology. VPNs attempt to resolve a variety of current technological limitations that represent themselves as costs in equipment and support or solutions where none had existed prior. Three areas that can be

improved by VPNs are:

- remote user access and remote office connectivity
- extranet partner connectivity
- internal departmental security

3.5.4.1 Remote Access

Providing remote users access via a dialup connection can become a costly service for any organization to provide. Organizations must consider costs for:

- telephone lines
- terminating equipment
- long distance
- calling card
- 800/877 number support

Telephone connections must be increased to support the number of proposed simultaneous users that will be dialing in for connectivity to the net work. Another cost that is rolled up into the telephone line charge is the possible need for equipment to allow the addition of telephone lines to an existing system. Terminating equipment, such as modem pools, can become expenses that are immediate savings once VPN is utilized. Long distance charges, calling cards that are supplied to roaming users, and toll free lines require initial capital and continuous financial support. In reality, an organization employing conventional remote access services is nothing more than a service provider for their employees. Taking this into consideration, many organizations tend to overlook the use of the Internet connection by the remote users. As the number of simultaneous users access the network, the more bandwidth is utilized for the existing Internet service.

The cost savings are realized by redirecting funds, originally to

support telephone communications, in an Internet service provider (ISP) and its ability to support a greater area of access points and technology. This allows an organization to eliminate support for all direct connectivity and focus on a single connection and technology for all data exchange — ultimately saving money. With the company access point becoming a single point of entry, access controls, authenticating mechanisms, security policies, and system redundancy is focused and common among all types of access regardless of the originator's communication technology.

The advent of high speed Internet connectivity by means of cable modems and ADSL (Asynchronous Digital Subscriber Line) is an example of how VPN becomes an enabler to facilitate the need for high speed, individual remote access where none existed before. Existing remote access technologies are generally limited to 128K ISDN (Integrated Services Digital Network), or more typically, 56K modem access. Given the inherent properties of the Internet and IPSec functioning at the network layer, the communication technology utilized to access the Internet only needs to be supported at the immediate connection point to establish an IP session with the ISP. Using the Internet as a backbone for encrypted communications allows for equal IP functionality with increased performance and security over conventional remote access technology.

Currently, cable modem and ADSL services are expanding from the home user market into the business industry for remote office support. A typical remote office will have a small frame relay connection to the home office. Any Internet traffic from the remote office is usually forwarded to the home office's Internet connection, where access controls can be centrally managed and Internet connection costs are eliminated at the remote office. However, as the number of remote offices and the distances increase, so does the financial investment. Each frame relay connection, PVC (Permanent Virtual

Circuit), has costs associated with it. Committed Information Rate (CIR), port speed (e.g., 128K), and sometimes a connection fee add to the overall investment. A PVC is required for any connection; so as remote offices demand direct communication to their peers, a PVC will need to be added to support this decentralized communication. Currently within the United States, the cost of frame relay is very low and typically outweighs the cost of an ISP and Internet connectivity. As the distance increases and moves beyond the United States, the costs can increase exponentially and will typically call for more than one telecommunications vendor. With VPN technology, a local connection to the Internet can be established. Adding connectivity to peers is accomplished by con figuration modifications; this allows the customer to control communications without the inclusion of the carrier in the transformation.

The current stability of remote, tier three and lower ISPs is an unknown variable. The arguable service associated with multiple and international ISP connectivity has become the Achilles' heel for VPN acceptance for business critical and time critical services. As the reach of tier one and tier two ISPs increases, they will be able to provide contiguous connectivity over the Internet to remote locations using an arsenal of available technologies.

3.5.4.2 Extranet Access

The single, most advantageous characteristic of VPNs is to provide protected and controlled communication with partnering organizations. Years ago, prior to VPN becoming a catchword, corporations were beginning to feel the need for dedicated Internet access. The dedicated access is becoming utilized for business purposes, whereas before it was viewed as a service for employees and research requirements.

The Internet provides the ultimate bridge between networks that

was relatively nonexistent before VPN technology. Preceding VPNs, a corporation needing to access a partner's site was typically provided a frame relay connection to a common frame relay cloud where all the partners claimed access. Other options were ISDN and dial on demand routing. As this requirement grows, several limitations begin to surface. Security issues, partner support, controlling access, disallowing unwanted interchange between partners, and connectivity support for partners without supported access technologies all conspire to expose the huge advantages of VPNs over the Internet. Utilizing VPNs, an organization can maintain a high granularity of control over the connectivity per partner or per user on a partner network.

Internal Protection

As firewalls became more predominant as protection against the Internet, they were increasingly being utilized for internal segmentation of departmental entities. The need for protecting vital departments within an organization originally spawned this concept of using firewalls internally. As the number of departments increase, the management, complexity, and cost of the firewalls increase as well. Also, any attacker with access to the protected network can easily obtain sensitive information due to the fact that the firewall applies only perimeter security.

VLANs (Virtual Local Area Networks) with access control lists became a minimized replacement for conventional firewalls. However, the same security issue remained, in that the perimeter security was controlled and left the internal network open for attack.

As IPSec became accepted as a viable secure communication technology and applied in MAC environments, it also became the replacement for other protection technologies. Combined with strategically placed fire walls, VPN over internal networks allows secure connectivity between hosts. IPSec encryption, authentication, and access control provide

protection for data between departments and within a department.

3.5.5 CONSIDERATION FOR VPN IMPLEMENTATION

The benefits of VPN technology can be realized in varying degrees depending on the application and the requirements it has been applied to. Considering the incredible growth in technology, the advantages will only increase. Nevertheless, the understandable concerns with performance, reliability, scalability, and implementation issues must be investigated.

3.5.5.1 System Requirements

The first step is determining the foreseeable amount of traffic and its patterns to ascertain the adjacent system requirements or augmentations. In the event that existing equipment is providing all or a portion of the service the VPN is replacing, the costs can be compared to discover initial savings in the framework of money, performance, or functionality.

3.5.5.2 Security Policy

It will be necessary to determine if the VPN technology and how it is planned to be implemented meets the current security policy. In case the security policy does not address the area of remote access, or in the event a policy or remote access does not exist, a policy must address the security requirements of the organization and its relationship with the service provided by VPN technology.

3.5.5.3 Application Performance

As previously discussed, performance is the primary reason VPN technology is not the solution for many organizations. It will be

necessary to determine the speed at which an application can execute the essential processes. This is related to the type of data within the VPN. Live traffic or user sessions are incredibly sensitive to any latency in the communication. Pilot tests and load simulation should be considered strongly prior to large scale VPN deployment or replacement of exiting services and equipment.

Data replication or transient activity that is not associated with human or application time sensitivity is a candidate for VPN connectivity. The application's resistance to latency must be measured to determine the minimum requirements for the VPN. This is not to convey that VPNs are only good for replication traffic and cannot support user applications. It is necessary to determine the application needs and verify the requirements to properly gauge the performance provisioning of the VPN. The performance "window" will allow the proper selection of equipment to meet the needs of the proposed solution; otherwise, the equipment and application may present poor results compared to the expected or planned results. Or, more importantly, the acquired equipment is underworked or does not scale in the direction needed for a particular organization's growth path. Each of these results in poor investment realization and make it much more difficult to persuade management to use VPN again.

3.5.5.4 Training

User and administrator training are an important part of the implementation process. It is necessary to evaluate a vendor's product from the point of the users, as well as evaluating the other attributes of the product. In the event the user experience is poor, it will reach management and ultimately weigh heavily on the administrators and security practitioners. It is necessary to understand the user intervention that is required in the everyday process of application use. Comprehending the user knowledge requirements will allow for the

creation of a training curriculum that best represents what the users are required to accomplish to operate the VPNas per the security policy.

3.5.6 FUTURE OF IPSec VPNs

Like it or not, VPN is here to stay. IP version 6 (IPv6) has the IPSec entrenched in its very foundation; and as the Internet grows, Ipv6 will become more prevalent. The current technological direction of typical net works will become the next goals for IPSec; specifically, Quality of Service (QoS). ATM was practically invented to accommodate the vast array of communication technologies at high speeds; but to do it efficiently, it must control who gets in and out of the network.

Ethernet Type of Service (ToS) (802.1p) allows for three bits of data in the frame to be used to add ToS information and then be mapped into ATM cells. IP version 4, currently applied, has support for a ToS field in the IP Header similar to Ethernet 802.1p; it provides three bits for extended information. Currently, techniques are being applied to map QoS information from one medium to another. This is very exciting for service organizations that will be able sell end to end QoS. As the IPSec standard grows and current TCP/IP applications and networks begin to support the existing IP ToS field, IPSec will quickly conform to the requirements.

The IETF and other participants, in the form of RFCs, are continually addressing the issues that currently exist with IPSec. Packet sizes are typically increased due to the added headers and sometimes trailer information associated with IPSec. The result is increased possibility of packet fragmentation. IPSec addresses fragmentation and packet loss; the over head of these processes are the largest concern.

IPSec can only be applied to the TCP/IP protocol. Therefore, multiprotocol networks and environments that employ IPX/SPX, NetBEUI, and others will not take direct advantage of the IPSec VPN.

To allow non TCP/IP protocols to communicate over an IPSec VPN, an IP gateway must be implemented to encapsulate the original protocol into an IP packet and then be forwarded to the IPSec gateway. IP gateways have been in use for some time and are proven technology. For several organizations that cannot eliminate non TCP/IP protocols and wish to implement IPSec as the VPN of choice, a protocol gateway is imminent.

As is obvious, performance is crucial to IPSec VPN capabilities and cost. As encryption algorithms become increasingly sophisticated and hard ware support for those algorithms become readily available, this currentlimitation will be surpassed.

Another perceived limitation of IPSec is the encryption export and import restrictions of encryption. There are countries that the United States places restrictions on to hinder the ability of those countries to encrypt possibly harmful information into the United States. In 1996, the International Traffic in Arms Regulation (ITAR) governing the export of cryptography was reconditioned. Responsibility for cryptography exports was transferred to the Department of Commerce from the Department of State. However, the Department of Justice is now part of the export review process. In addition, the National Security Agency (NSA) remains the final arbiter of whether to grant encryption products export licenses.

The NSA staff is assigned to the Commerce Department and many other federal agencies that deal with encryption policy and standards. This includes the State Department, Justice Department, National Institute for Standards and Technology (NIST), and the Federal Communications Commission. As one can imagine, the laws governing the export of encryption are complicated and are under constant revision. Several countries are completely denied access to encrypted communications to the United States; other countries have limitations due to government relationships and political posture. The

current list of (as of this writing) embargoed countries include:

- Syria
- Iran
- Iraq
- North Korea
- Libya
- Cuba
- Sudan
- Serbia

As one reads the list of countries, it is easy to determine why the United States is reluctant to allow encrypted communications with these countries. Past wars, conflict of interests, and terrorism are the primary ingredients to become exiled by the United States.

Similar rosters exist for other countries that have the United States listed as "unfriendly," due to their perception of communication with the United States.

As one can certainly see, the concept of encryption export and import laws is vague, complex, and constantly in litigation. In the event a VPN is required for international communication, it will be necessary to obtain the latest information available to properly implement the communication as per the current laws.

3.6 INTEGRATING DATA CENTERS WITH INTRANETS

NEARLY ALL ENTERPRISES THAT HAVE MAINFRAMES or large, networked AS/400s now have an intranet. Most, in addition, already have a presence on the Internet in the form of a home page, and many are actively exploring the possibilities of using the Internet for electronic commerce, customer support, and as an ultra cost effective means of global remote access. In parallel, intranet to intranet communication via extranets is being viewed as the means of

streamlining and expediting enterprise transactions. Very few enterprises at present have tightly integrated their intra nets with their data centers. This is despite the fact that up to 70 percent of the vital data, and many of the mission critical applications required by these enterprises, are still likely to reside on their mainframes or AS/400s. That is akin to baking an apple pie with no apple filling.

Integrating an intranet with a data center is not simply a matter of implementing TCP/IP on a mainframe or AS/400 along with a Web server. Many of the host resident, mission critical applications still required were developed, typically 15 years ago, such that they only work in Systems Network Architecture mode. The nearest that one can come to making these applications TCP/IP compatible is to use them in conjunction with a host resident or "Off Board" tn3270(E) (or tn5250, in the case of AS/400s) server which will perform standards based SNA to TCP/IP protocol conversion. Otherwise, the applications will have to be rewritten to work in TCP/IP mode. This is not feasible since the cost and effort of doing so for the $20 trillion installed base of SNA mission critical applications would make all the tribulations associated with the Y2K challenge appear trivial.

While some of the data center resident data could be accessed using an Open Database Connectivity type scheme, this is certainly not true for all of the data center resources. Some data, especially if stored on "flat files" or non relational databases (such as IBM's still widely used Information Management System), can only be accessed via SNA applications. In other instances, the data make sense only when combined with the "business logic" embedded within an SNA mission critical application. In addition to these crucial SNA applications, there is inevitably a large installed base of SNA only "legacy" devices such as IBM 4700 Financial Systems, automated teller machines, and control units that still need to be supported. Thus, there is a need for explicit SNA related technologies in order to get the most from your host

intranet.

The good news is that highly proven and stable technology from more than 40 credible vendors including IBM, Cisco, Attachmate, Open Connect Systems, Wall Data, Eicon, Novell, WRQ, Farabi, Client/Server Technology, Sterling Software, Blue Lobster, etc., is now readily available to facilitate data center to intranet integration in a seamless and synergistic manner. Enterprises around the world such as GM, FedEx, Ohio State University, Royal Jordanian Airlines, Nestles, The Chickering Group, National Van Lines, the State of Idaho, Al Rajhi Banking & Investment Corp. (Saudi Ara bia's largest bank), and Gazprom (a $30 billion natural gas company in Rus sia) are already gainfully using this intranet to data center integration technology on a daily basis for business critical production use. Al Rajhi Bank, for example, uses browser based access to SNA to provide home banking, while GM, National Van Lines, Royal Jordanian Airlines, and The Chickering Group use it to permit agents to access applications or databases resident on mainframes or AS/400s over the Internet.

3.6.1 INTRANET TO DATA CENTER INTEGRATION TECHNOLOGIES

To be viable, integration technologies need to be able to accommodate an extremely broad and disparate population of client equipment and functionality including PCs, UNIX workstations, coax attached 3270/5250 terminals, printers, minicomputers, SNA applications that communicate program to program using LU 6.2 or LULU Session Type 0based protocols, SNA only devices, SNALAN gateways (e.g., NetWare for SAA), and legacy control units. The PCs, workstations, and printers may work in either SNA or TCP/IP mode. Consequently, you will need SNA Access technologies to deal with TCP/IP clients, particularly PCs and workstations, and SNA Transport technologies to deal with SNA only clients. The most pertinent

technologies are:

- SNA Access technologies that permit non SNA clients to gain access to SNA applications

— *ip3270/ip5250* — the use of existing PC/workstation SNA emulators (e.g., Attachmate EXTRA! Personal Client) and existing SNALAN gateways (e.g., Microsoft's SNA server) with proprietary encapsulation schemes for conveying a 3270/5250 data stream within TCP/IP

— *tn3270(E)/tn5250* — IETF standard that enables TCP/IP clients (e.g., Attachmate EXTRA! Personal Client) to access SNA applications via tn3270(E) (e.g., IBM 2216) or tn5250 servers

- *Browser based Access with 3270/5250toHTML Conversion* — thin client solution where a server resident SNAWeb gateway performs 3270/5250 data stream to HTML conversion replete with some amount of user interface rejuvenation so that SNA applications can be accessed directly from a browser.
- *Browser invoked Java or ActiveX applets* — dynamically download able applets, which can optionally be cached on a PC/workstation hard disk, that provide 3270/5250 emulation either directly or in conjunction with an intermediate SNA Web gateway
- *Browser invoked applets as "4" above,* but with user interface reju venation
- *Application specific web to data center gateways,* e.g., IBM's CICS Web Interface or Interlink's ActiveCICX
- *Programmatic (or Middleware) Servers,* e.g., IBM's MQSeries, Blue Stone's Sapphire/Web, or Blue Lobster's Stingray SDK SNA end to end transport
- *Data Link Switching — ubiquitous, standardsbased encapsulation scheme performed by bridge/routers that permits any kind of SNA/APPN traffic, independent of session type, to be transported*

end toend across a TCP/IP WAN. Desktop DLSw (DDLSw) is also available where SNA traffic can be encapsulated within TPC/IP at the source PC

- *High Performance RoutingoverIP — alternative to the DLSw champi oned by IBM, whereby SNAoriented routing is performed across IP*
- *AnyNet* — IBM protocol conversion technology, integrated within IBM server software including Comm. Server/NT and OS/390 as well as within some SNA/3270 emulation packages, that converts SNA message units into corresponding TCP/IP packets

The three transport technologies ensure that the still large installed base of SNA devices and control units are able to communicate with main frame or AS/400resident SNA/APPN applications across an intranet using SNA on an end to end basis. Of the three, standards based DLSw, which is available on nearly all major brands of bridge/routers, is by far the most widely used and the most strategic. AnyNet, in marked contrast, is not available on bridge/routers or within SNA devices such as 3174s, 4700s, etc. Consequently, it cannot be used easily as a universal scheme for supporting any and all SNA devices and control units as can DLSw. Thus, AnyNet is not as strategic or useful as DLSw. High Performance Routing (HPR) is IBM's follow on architecture to APPN and SNA. HPRoverIP, now available on IBM 2216 and CS/NT, has irrefutable advantages over DLSw: it can support native, data center to data center SNA/APPN routing over TCP/IP; SNA LU 6.2 Class of Service (COS)based path selection; and traffic prioritization. If and when this technology is more readily available, corporations that require SNA/APPN routing to obtain optimum traffic routing in multi data center networks, or those that have LU 6.2based applications thatrely on COS, may want to consider HPRoverIP as an alternative to DLSw.

DLSw's ability to support any and all types of SNA/APPN traffic

effortlessly could be easily abused when trying to integrate intranets with data centers. DLSw could be used all by itself to realize the integration by grafting the existing SNA/APPN network, totally unchanged, onto the intranet through the extensive deployment of DLSw all around the periphery of the intranet. This brute force, "no SNA reengineering whatsoever" approach has been used in the past to integrate SNA networks into TCP/IP networks. With this type of DLSw only network you would find SNALAN gateways being used downstream of the intranet, and then DLSw being used to trans port the SNA output of these gateways across the intranet. While such net works indubitably work, there are other strategic techniques such as a 3270toHTML and applet based 3270/5250 emulation that should typically be used in conjunction with DLSw to achieve the necessary integration. Figure summarizes how the various SNA Transport and SNA Access integration techniques can be gainfully synthesized to integrate data centers with intranets.

3.7 IMPLEMENTING AND SUPPORTINGEXTRANETS

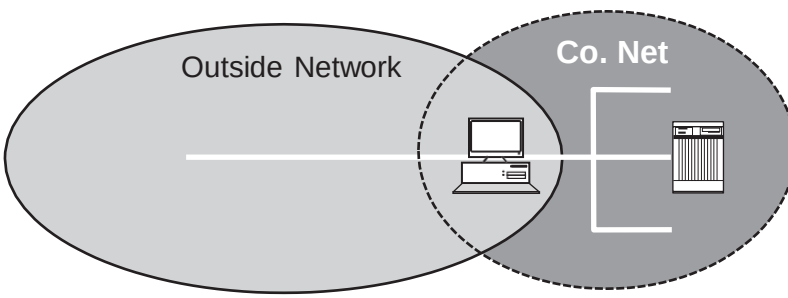
EXTRANETS HAVE BEEN AROUND as long as the first rudimentary LAN to LAN networks began connecting two different business entities together to form WANs. In its basic form, an extranet is the interconnection of two previous separate LANs or WANs with origins from different business entities. This term emerged to differentiate between the previous definitions of external "Internet" connection and a company's internal intranet. Figure depicts an extranet as a Venn diagram, where the intersection of two (or more) nets forms the extranet. The network in this intersection was previously part of the "intranet" and has now been made accessible to external parties.

Under this design, one of the simplest definitions comes from

R.H. Baker,[1] "An extranet is an intranet that is open to selective access by outside parties." The critical security concept of the extranet is the new net work area that was previously excluded from external access now being made available to some external party or group. The critical security issue evolves from the potential vulnerability of allowing more than the intended party, or allowing more access than was intended originally for the extra net. These critical areas will be addressed in this article, from basic extranet setup to more complex methods and some of the ongoing support issues.

The rapid adoption of the extranet will change how a business looks at its security practices, as the old paradigm of a hard outer security shell for a business LAN environment has now been disassembled or breached with a hole to support the need for extranets. In many cases, the age-old firewall will remain in place, but it will have to be modified to allow this "hole" for the extranet to enable access to some degree to internal resources that have now been deemed part of the extranet.

Recognizing the growth of extranets as a common part of doing business today is important, and therefore the business enterprise must be ready with architectures, policy, and approaches to handle the introduction of extranets into its environment. A few of the considerations are the requirements versus security balance, policy considerations, risk assessments, and implementation and maintenance costs.



Extranet Venn diagram.

Recognizing the growth of extranets as a common part of doing business today is important, and therefore the business enterprise must be ready with architectures, policy, and approaches to handle the introduction of extranets into its environment. A few of the considerations are the requirements versus security balance, policy considerations, risk assessments, and implementation and maintenance costs.

From requirements versus security balance standpoint, the issue is the initial claim by business that extranets are an immediate need and absolutely must be established "if we are to remain competitive." But from a security standpoint, such a drastic change to the environment, which may not have had any form of an extranet in place, may well be throwing their financial data assets out the door with the first implementation of an extranet. Therefore, care must be taken from a security perspective and put in balance with the claimed business need for an extranet implementation.

One of the first areas of review and (possibly) update is the inner company's security policy. This policy most likely was not written with extra nets in mind and thus may need modification if a common security philosophy is to be established regarding how a company can securely implement extranets. However, the policy review does not stop with one company's review of its own policy, but also includes connecting the company or companies on the outside. In the case of strategic business relationships that will be ongoing, it is important that both parties fully understand each other's responsibilities for the extranet, what traffic they will and will not pass over the joined link — what degree of access, and by whom, will occur over this link.

Part of any company's policy on extranets must include an initial

requirement for a security risk assessment, the main question being: what additional levels of risk or network vulnerability will be introduced with the implementation of the proposed extranet? As well as vulnerability assessment, a performance assessment should be conducted to assist in the design of the extranet to ensure that the proposed architecture not only addresses the security risk, but that it also will meet performance expectations. Some of the questions to be asked in a combined security and performance assessment should be:

- data classification/value of data
- data location(s) in the network
- internal users' access requirements to extranet components (internal access design)
- data accessibility by time of day (for estimating support costs)
- protocol, access services used to enter extranet (network design implications)
- degree of exposure by transmission mechanism (Internet, private net, wireless transmission)
- end user environment (dialup, Internet)
- number of users, total/expectation for concurrent users access (line sizing)
- growth rate of user base (for estimating administrative costs)
- CONUS (continental U.S.), international access (encryption implications)

The risk and performance assessment would, of course, be followed by a risk mitigation plan, which comes in the form of selecting an acceptable extranet architecture and identifying the costs. The cost aspect of this plan is, of course, one of the critical drivers in the business decision to implement an extranet. Is the cost of implementing and maintaining the extranet (in a secure manner) less than the benefit gained by putting the extranet in place? This cost must include the costs

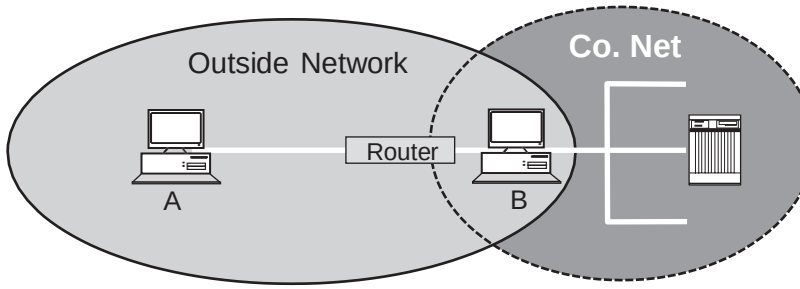
associated with implementing it securely; otherwise, the full costs will not be realistically reflected.

Finally, the company implementing the extranet must have a clear set of architectures that best mitigate the identified vulnerabilities, at the least cost, without introducing an unacceptable degree of risk into its computing environment. The following section reviews various extranet architectures, each with differing costs and degrees of risk to the environment.

3.7.1 EXTRANET ARCHITECTURES

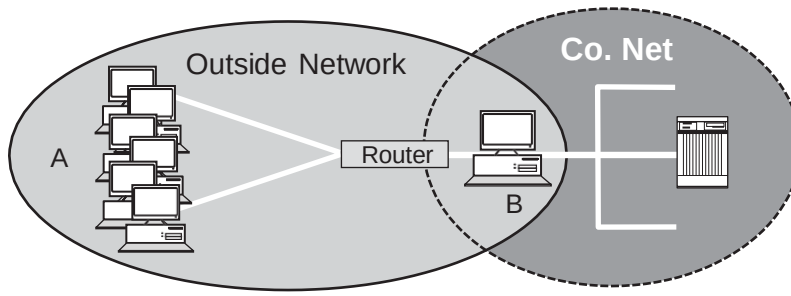
3.7.1.1 Router Based Extranet Architecture

The earliest extranet implementations were created with network routers that have the capability to be programmed with rudimentary "access control lists" or rules. These rules were implemented based solely on TCP/IP addresses. A rule could be written to allow External User A access to a given computer B, where B may have been previously unreachable due to some form of private enterprise network firewall (and in the early days, this firewall may have been a router also). Figure depicts this very basic extranet. A more realistic rule can be written where all computers in an "outside network" are allowed to access computer B in a company net work, thus forming an extranet. This is depicted in Figure.

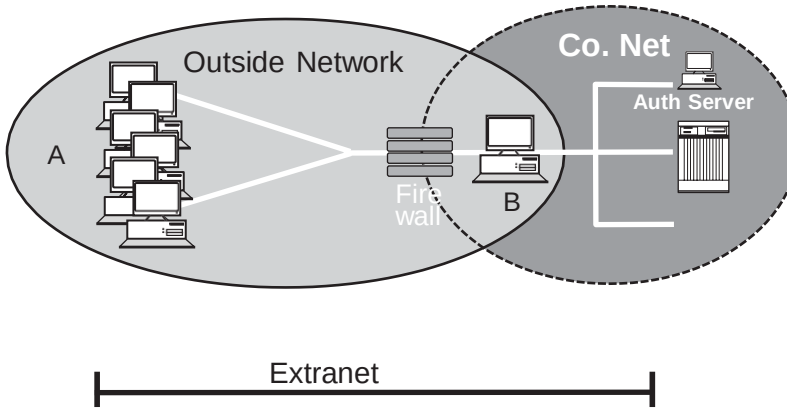


Basic extranet with router

As network security architectures matured, routers as the sole network access control device were replaced by more specific security mechanisms. Routers were originally intended as network devices and not as security mechanisms and lost functionality as more and more security rules were placed in them. Additionally, the security rules that were put into them were based on TCP/IP addresses, which were found to be subject to spoofing/masquerading and thus deemed ineffective in positively identifying the real external device being granted access. Therefore, routers alone do not provide an entirely secure extranet implementation; but when used in conjunction with one of the following extranet architectures, routers can be a component to add some degree of security, but only when used in conjunction with other network security devices.



More realistic extranet



Extranet using an application layer gateway firewall.

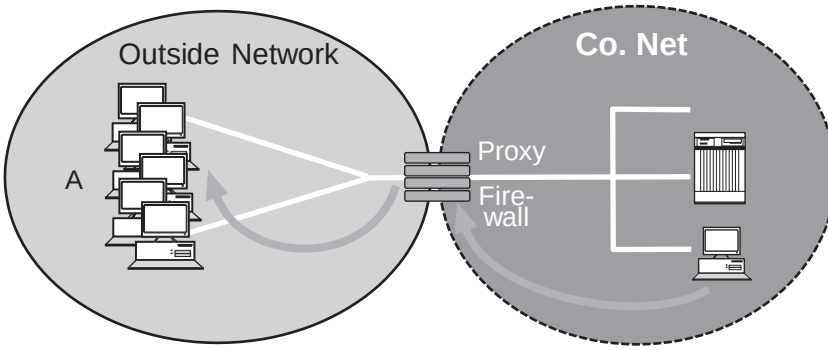
Application Gateway Firewalls

As network security architectures matured, the introduction of application layer gateway firewalls, software tools on dedicated machines, usually dual homed (two network interfaces, one internal, one external), became the more accepted external protection tool. These software tools have the ability to not only perform router type functions with access control rules, but also provide user authentication services on a per user basis. This user authentication can take the form of an internal user authentication list, or an external authentication call to token based authentication services, such as the ACE Secure ID™ system. Figure depicts this type of architecture setup to support an extranet using an a application layer gateway firewall to enable authenticated users inward access to an enterprise in a controlled manner.

In addition to supporting access control by IP address and user, some gateways have the further capability to restrict access by specific TCP/IP service port, such as Port 80, HTTP, so the extranet users can only access the internal resource on the specific application port and not expose the internal machine to any greater vulnerability than necessary.

Follow on application layer gateway implementations have since emerged to provide varying additional degrees of extranet connectivity and security. One such method is the implementation of a proxy

mechanism from an outside network to a portion of an internal company network. Normally, a proxy performs control and address translation for access from an intranet to the external Internet. These types of proxies normally reside on the firewall, and all user access to the Internet is directed through the proxy. The proxy has the ability to exert access control over who in the intranet is allowed external access, as well as where they can go on the Internet. The proxy also provides address translation such that the access packet going



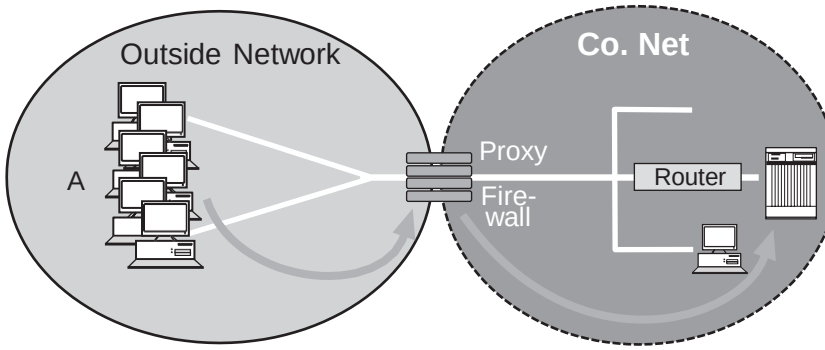
Outbound proxy architecture.

to the Internet is stripped of the user's original internal address, and only the external gateway address of the enterprise is seen on the packet as it traverses the Internet. Figure depicts these proxy functions.

The proxy provides both security and network address functions, although the entire process can be used in its reverse to provide an extranet architecture because of its ability to provide access rules over who can use the proxy, where these proxy users are allowed to go, and what resources they can access. Figure depicts a *reverse proxy* extranet architecture.

Today, most proxies are set up for HTTP or HTTPS access, although application layer gateway proxies exist for most popular Internet access services (Telnet, FTP, SQL, etc.). One of the major issues with proxy servers, however, is the amount of cycle time or

machine overhead it takes to manage many concurrent proxy sessions through a single gateway. With highly scalable hardware and optimized proxy software, it can be carried

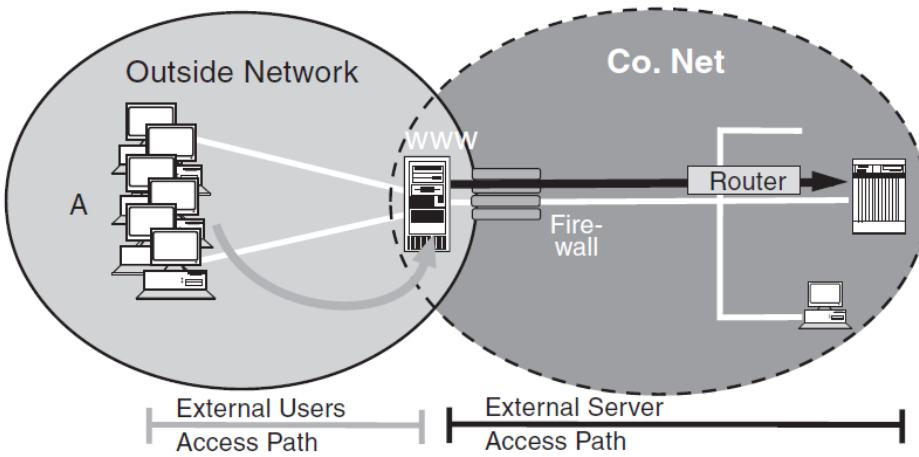


Reverse proxy extranet architecture

to potentially handle high user demands, but the system architecture must be specifically designed for high loads to be able to meet user response expectations while still providing the security of an authenticated proxy architecture. On the inward proxy depicted in Figure, the proxy can be configured to only allow access to a single internal resource on a given TCP/IP port. Further protection can be added to this reverse proxy architecture by putting the target internal resource behind a router with specific access control rules, limiting the portion on the company intranet that inbound proxies can reach, which can ensure limited access on the intra net; should the internal machine ever be compromised, it cannot be used as a "jumping off point" into the rest of company intranet.

A somewhat *hybrid* architecture extranet, where some firewall controls are put in place but the external user is not granted direct inward access to an enterprise's internal domain, has been evolving and put in place as a more popular extranet implementation. In this

architecture, the external user is granted access to an external resource (something outside of the enterprise firewall), but still on the property of the enterprise. Then, this external resource is granted access to one or more internal resources through the enterprise firewall. This architecture is based on minimizing the full external access to the intranet, but still makes intranet based data available to external users. The most popular implementation is to place an authenticating Web server outside the firewall and program it to make the data queries to an internal resource on the enterprise intranet, over a specific port and via a specific firewall rule, allowing only that one external resource to have access to the one internal resource, thus reducing the external exposure of the intranet. Figure depicts this type of extranet.



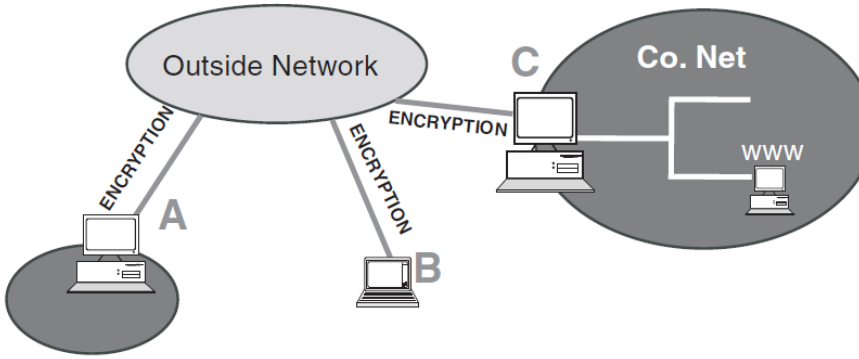
Extranet with authenticating Web server.

Issues with this type of architecture include reliance on a single user interface that can be safely placed outside the enterprise firewall, which makes it vulnerable to attack. Additionally, there is the issue of whether tight enough access rules can be placed on the access method between the external user interface resource (the Web server, in this example)

and the internal resources that it needs access to on the protected enterprise intra net. If these two issues can be safely addressed, then this form of extranet can be very useful for an enterprise extranet with a high volume or varied user base and a large intranet based data repository.

The user front end has been deployed as a Web server, usually SSL enabled to ensure data integrity and protection by encrypting the data as it passes over an external SSL link. Access to this external server is also associated with some form of user authentication, either a static ID or password over the SSL link, and more recently with client digital certificates where each individual accessing the SSL enabled site is issued his own unique digital certificate from an acknowledged certificate authority, thereby validating his identity. Each client maintains its own digital certificate, with the Web server having some record of the public key portion of the client's digital certificate, either directly in the Web server internally, or accessible from a standalone directory server (usually LDAP reachable).

The most recent entrant in the extranet architecture arena is the Virtual Private Network (VPN). This architecture is based on a *software tunnel* established between some external entity, either client or external net work, and a gateway VPN server. Figure depicts both types of VPN architectures. External Network A has a VPN server at its border which encrypts all traffic targeted for Company Network C; this is a gateway to gateway VPN. Or, External Client B may have client VPN software on his workstation which would enable him to establish a single VPN tunnel from his workstation over the external network to Company C's VPN server.



VPN architectures

Although both server to server VPN and client to server VPN architectures are offered in the industry today, it is this author's experience that the more popular extranet architect is the client to server VPN architecture, as it offers the most flexibility for the most diverse audience of external users. This flexibility does add to the complexity of the implementation, as it can involve a potentially large number of external desktops, all with differing configurations. The benefits of VPNs include the ability to safely traverse external public networks with some assurance of data integrity and authentication as part of the VPN implementation. This architecture shows the most promise to meet the needs of extranets and cost savings for a world hungry for connectivity over public/external networks, although it still has some growing pains to go through to reach full product maturity.

An emerging standard for VPNs is coming out of the ITEF IPSec implementation, which draws a roadmap for the next generation TCP/IP security protocol. Under this protocol, standards are being drafted that will enable differing devices to securely communicate under an agreed upon security protocol, including key exchange for encryption and standardized authentication. Today, there are IPSec compliant products on the market; however, the standard is still evolving and tests are being conducted to evaluate differing vendor compatibilities with each under

the IPSec standard. One of the leading initiatives to evaluate this compliance is the Automotive Network Exchange (ANX) test, which is intended to establish a large extranet environment between the core automotive manufacturers and their vendors.

In the meantime, there are a wide variety of VPN product vendors on the market some touting IPSec compliance and others, with proprietary implementations with IPSec in their future product roadmaps, choosing to wait until the standard stabilizes. The recommendation is to either select a vendor offering IPSec if it has some degree of maturity within its own product line, or one that is planning on adopting the standard; IPSec appears to be a viable standard once it fully matures.

Regardless of what VPN solution is being considered for implementing secure extranets, a few technical considerations must be understood and planned for before selecting and implementing a VPN extranet architecture.

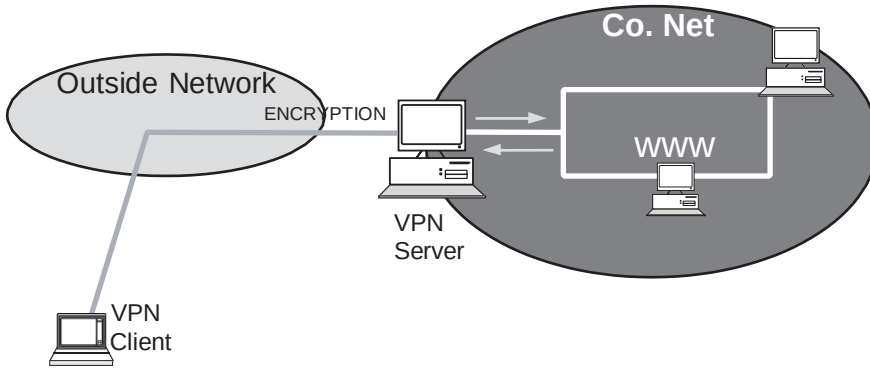
Scalability. Similar to proxy servers, VPN servers incur a fair amount of processing overhead that consumes processing resources as high levels of concurrent VPN sessions pass through a single server. It is important to attempt to estimate one's projected user base and current access to appropriately size a VPN server. Some servers are on established lower level processors for smaller environments and should not be implemented where high concurrent access rates are expected, although there is some benefit to physical load balancing spreading the access among multiple servers. However, there is also concern about implementing too many servers to manage easily. A balance between installing a single large server and creating a single point of failure versus implementing many smaller servers creates an administrative nightmare.

Multi homed Intranets and Address Translation. In large intranet environments, many operate under a *split DNS* (domain naming structure) where intranet addresses are not "advertised" to the external networks, and external addresses are kept external so as not to flood the internal net work. Additionally, many larger intranet environments have multiple gate ways to external networks. If one of the gateways is established with a VPN gateway and an external client makes a connection to the internal intranet, it is important that the tunnel comes in through the appropriate VPN gate way, but also that the return traffic goes back out through that same gate way so that it gets re encrypted and properly returned to the external VPN client. Figure depicts the correct traffic patterns for a multi homed intranet with a single VPN gateway and an external VPN client.

VPN Based Access Control. Many forms of gateway VPN servers offer the ability to restrict user access to a company intranet based on access groupings. This is especially important when intranets are being established for a diverse set of external users and it is important to minimize user access to the intranet. This type of access control is, of course, critical in establishing secure extranets, which further highlights the importance of understanding VPN access control capabilities.

User Authentication. Multiple options exist for user authentication, although the recommended option is to select a high level authentication method (e.g., onetime passwords) or a time synchronized password method. Under the IPSec standard, client side digital certificates are evolving as a standard for high level authentication. Unfortunately, initial implementations of client side digital certificates for user authentication are entirely software based, eliminating the second factor authentication, the something the user physically has" in their possession. The return to true two factor authentication under digital certificates will not really occur until physical smart cards

become part of the authentication architecture. (Smart cards are credit card type tokens that have a physically embedded chip which can be read electronically and written to, either with a portion of the client's digital certificate or the encryption algorithm used to unlock the digital certificate.)



Traffic patterns for multi homed intranet with a single VPN gateway and an external VPN client.

IPSec Interoperability. Ultimately, the IPSec standard will stabilize, and all vendors following the established standard will allow different vendors' VPN products to interoperate. Under this environment, a company can implement a vendor's VPN server, and their acknowledged clients can purchase and use an IPSec compliant client to gain access to the company intranet once they are authorized.