The Registry®

Excellence in Information
Consulting Services

189 Wells Avenue
Newton, MA 02159
888/377-9119   617/527-6886
FAX 617/527-0073

RAISING THE BAR ON

VIRTUAL PRIVATE DATA NETWORK SOLUTIONS

JULY 8, 1997

PREPARED BY: THE REGISTRY, INC.

NETWORK INDUSTRY PRACTICE

18-02

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY 1

2. REQUIREMENTS THAT DRIVE VIRTUAL PRIVATE DATA NETWORKING 3

3. VIRTUAL PRIVATE DATA NETWORKS - WHAT ARE THEY AND WHAT DO THEY GIVE ME? 5

4. THE FIVE CORE CRITERIA FOR VPDN SOLUTION EVALUATION 7

I. BENCHMARKING PERFORMANCE AND AVAILABILITY 8
II. SCALABILITY - THE KEY CRITERIA FOR AVOIDING GROWING PAINS 10
III. ENSURING HIGH CUSTOMER SATISFACTION 13
IV. KEEPING THE CORPORATE INFORMATION VAULT SAFE 15
V. IMPLEMENTING A NON-PROPRIETARY VPDN 19

5. WHY TECHNOLOGICAL INNOVATION MATTERS FOR YOUR BUSINESS 21

6. ENSURING YOU HAVE THE BEST SOLUTION 22

TABLE OF FIGURES

Figure 1: Why Users Outsource....................................4

Figure 2: Cost of Ownership by Category....................................5

Figure 3: Accessing Public and Private Resources....................................7

Figure 4: NSP Backbone/Internet Building Block....................................11

Figure 5: The Network Security Perimeter Demarc....................................16

Figure 6: Secure Tunnels through Untrusted Network(s)....................................17

Figure 7: Integrated Security Model....................................18

1. EXECUTIVE SUMMARY

The industry shift to a network-centric applications model is fundamentally transforming the manner in which many products and services are delivered. A key pre-requisite to this delivery, however, is the meeting of most if not all of the following connectivity requirements:

- efficient and reliable "on-line" interaction with customers, partners, and suppliers who are themselves network-connected and require effective interoperation with their unique protocols, applications, and management systems;
- a secure networked environment across which electronic commerce can be effectively implemented;
- ease of network access for an increasingly mobile workforce who need to either effect sales or deliver service at a location remote from the corporate offices; and
- performance scalability that can continue to meet the growth in capacity demand generated by both current and next generation business applications that are increasingly incorporating multimedia content.

In order to meet these requirements, CIOs are becoming more aggressive in both their evaluation and implementation of alternative network implementation and support models. The combination of the need to more effectively manage network cost of ownership and of the compelling need to begin offering electronic commerce services on the Internet is driving many of today's CIOs to evaluate the use of strategic partners who can deliver solutions in both of these crucial areas.

Virtual Private Data Networks (VPDNs) offer a more cost-effective solution to the CIO for solving these connectivity requirements. VPDNs are private data networks that utilize secure tunneling across the wide area network and typically leverage the public Internet to deliver data services for intra- and inter-company communication. Industry research estimates that operational cost savings of up to 60% over equivalent private networks can be realized.

VPDNs are offered and managed by Internet Service Providers (ISPs). Given the number of vendor choices and breadth of service offerings, it is in the CIO's best interest to benchmark ISP VPDN solutions. A core set of selection criteria can be used that ensures high user satisfaction and secure business-to-business relationships, regardless of the permitted user's accessing location. These criteria are:

- **Performance and availability** – how rapidly can the ISP respond to connection requests and ensure the necessary bandwidth throughout the connection.
- **Scalability** – how flexible is the ISP's infrastructure in meeting your anticipated users' and business growth requirements.
- **Service level management** – does the ISP support or plan to support Service Level management that addresses your users' demands for Service Level Agreements (SLAs).
- **Security** – what steps has the ISP taken to ensure safe, secure business-to-business connectivity that prevents planned or unintentional damage to your corporate data resources.
- **Standards** – ISP support of relevant IETF and industry standards that ensure the greatest degree of network application interoperability as well as client hardware and software investment protection.

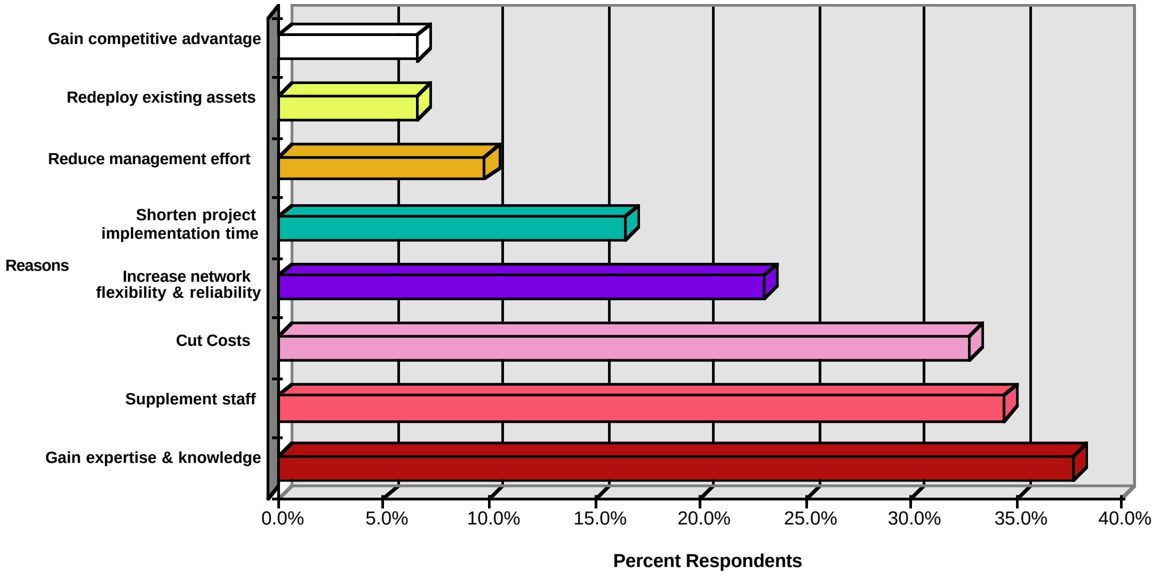
Clearly, the ability of an ISP to deliver solutions that either meet or exceed the above criteria is a direct function of the hardware and software products used to implement a provider's network. Recently, The Registry, Inc. conducted a functional assessment of Ascend Communications' product line relative to its support of these key criteria. Given the functionality, performance and security instrumentation of these products, the Registry firmly believes that they offer extremely strong alternatives to both users and service providers who are looking for a VPDN solution that is more than a simple sum of piecemeal parts. The actual criteria we used to evaluate the Ascend product line along with relevant product details are provided in the following sections.

2. Requirements that Drive Virtual Private Data Networking

As businesses expand and identify new business opportunities, the CIO is constantly challenged by the burgeoning, unique connectivity requirements imposed by:

- the need to interact "on-line" with customers, partners, and suppliers who are themselves connected to networks running unique protocols, applications, and management systems;
- a business decision to reach new markets by implementing electronic commerce for competitive advantage;
- an increasingly mobile workforce who requires dial-up access to the corporate intranet or databases as they work from home or while traveling; and,
- the proliferation of new web-based and multimedia applications appearing on the network.

This is all occurring as CIO's are tasked to do more with less, even though costs continue to rise implementing and maintaining the classic internetwork model. Research conducted by Dataquest (summarized in Figure 1) also shows that for those organizations who have chosen outsourcing as an alternative route to address these IS challenges, over 30% did so to reduce costs, nearly 35% to augment staff expertise, and over 35% did so to elevate the IS staff's support capabilities.

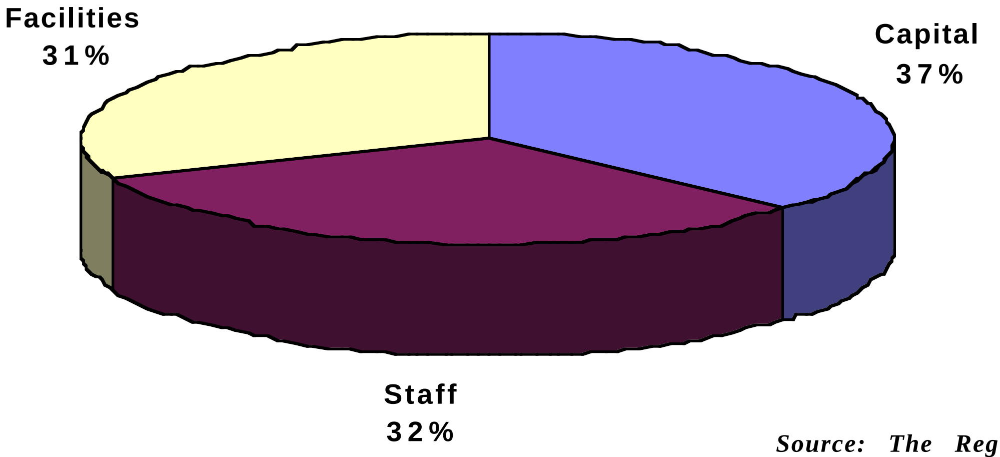


Source: Dataqu

Figure 1: Why Users Outsource

Results of numerous network Cost of Ownership studies conducted by The Registry, Inc. confirm the high costs associated with traditional in-house management of the network with respect to three cost categories – Capital, Personnel, and Facilities.

Technical support staff salaries and benefits, for example, can account for over one third of the costs, averaging **$63,000** per support person to support an average of **150** desktops per person or **$420** support dollars per desktop. Facilities costs represent recurring operational costs for resources such as wide area circuits, dial-up services and network product maintenance. Figure 2 summarizes the study results by cost category and shows that combined Staff and Facilities costs constitute **nearly two thirds** of annual cost of ownership.



Source: The Registry,

Figure 2: Cost of Ownership by Category

The combination of the need to more effectively manage network cost of ownership and of the compelling need to begin offering electronic commerce services on the Internet is driving many of today’s CIOs to evaluate the use of strategic partners who can deliver solutions in both of these crucial areas.

3. Virtual Private Data Networks - What are They and What do they Give Me?

Classically, most businesses have used high-speed leased lines or dial-up access over the Public Switched Telephone Network (PSTN) to satisfy their off-premises data, voice, and video networked communication requirements. Given the explosive growth of the public Internet, however, a more cost-effective solution is now available to address these needs – *Virtual Private Data Networks* or *VPDNs*.

Modeled after today’s private enterprise networks, a VPDN is a private data network that uses a *public* (i.e. the Internet) rather than a private (e.g. private leased lines) data network to carry traffic over the wide area network. VPDN enables businesses to implement enterprise-wide communications with the same capabilities as a private network, but at a significantly reduced operational cost, thus providing an important solution for managing cost of network ownership. In addition, given that VPDNs are offered and managed by Internet Service Providers (ISPs), they also offer a means for users to take that important first step towards Internet-based electronic commerce services.

According to a study by Forrester Research, organizations with VPDNs are able to **save up to 60% of the operational cost** of equivalent private networks by:

- eliminating long distance leased line connections among facilities;
- eliminating long distance calls for dial-up access to the corporate network; and,
- requiring less equipment such as separate modem banks, terminal adapters, remote access servers and so forth when a single solution is implemented for both enterprise networking and Internet access.

Moreover, a VPDN leverages the infrastructure of the public Internet since it provides nearly worldwide local access through ISPs, supplies more reliable connectivity via local line connections that are less susceptible to line noise compared to long distance access, and includes built-in mesh redundancy and fault tolerance for end-to-end network reliability.

VPDN's are a flexible alternative to private networks given the Internet's worldwide presence. Users can quickly connect to and disconnect from the VPDN regardless of their accessing location, businesses can easily permit VPDN access by customers, suppliers or partners, and a range of data rates are available to accommodate users' needs from analog modem (e.g. 28.8 kilobits/second) to T1/E1 speeds (1.544/2.048 megabits/second) to the more recent Digital Subscriber Line (DSL) technology that supports up to several megabit per second data rates. Most importantly, VPDN's enable user access to both public and private resources using a single network connection that can support both private and public business services (Figure 3).

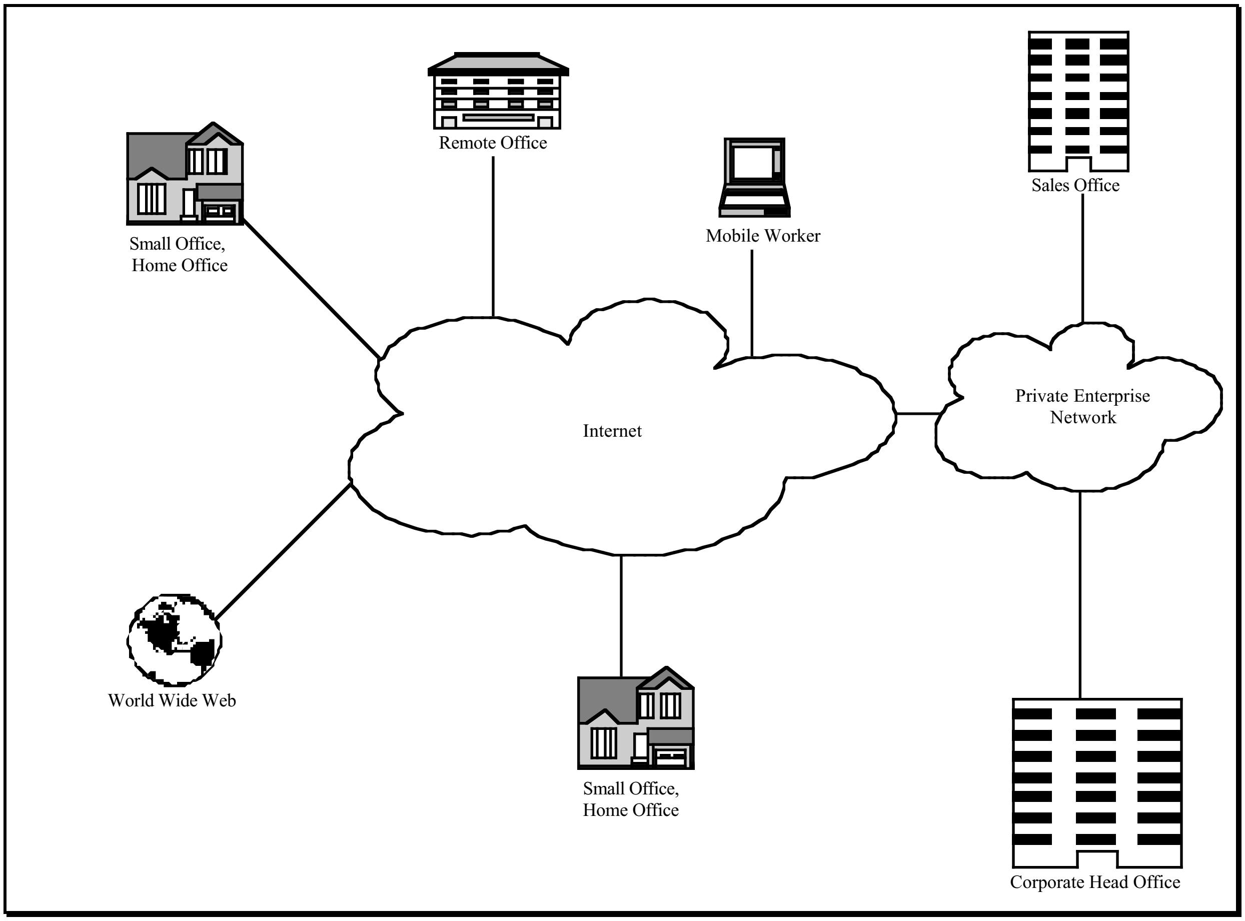


Figure 3: Accessing Public and Private Resources

4. THE FIVE CORE CRITERIA FOR VPDN SOLUTION EVALUATION

Implementing this new VPDN model requires careful selection of an ISP to ensure high performance connectivity and high quality availability for existing and future services. This process is akin to the selection of carriers for Virtual Private Voice Networks (VPVNs) in the mid to late 1980s.

In order for the VPDN to be declared a success, the VPDN infrastructure must meet a set of criteria to ensure high user satisfaction and secure business-to-business relationships, regardless of the permitted user's accessing location. That means the network must be built, end-to-end, using five core criteria as the foundation of VPDN planning efforts: performance and availability, scalability, service level management, security, and standards.

In the next few sections, we will expand on what each of these criteria really mean as well as relate how the Ascend product line addresses them. The latter is being provided as a result of a functional assessment conducted by The Registry of Ascend Communications' products that are most relevant to VPDN support. These products include the Ascend MAX™, GRF™, Pipeline®, Security, and Network Management product families, as well as other members of the vendor's product portfolio. Collectively, this product set offers users a fairly complete foundation for establishing a secure virtual private network.

I. Benchmarking Performance and Availability

Any discussion about Internet access and performance is likely to bring to mind recent network outages experienced by over 6.5 million users. In these incidents, the lack of up front planning and a less than scaleable equipment infrastructure resulted in high rates of denial of service for many mission critical users. These incidents clearly illustrate the high expectations that users now have for Internet access along with the significant business, legal and public relations ramifications if this access becomes unavailable for any extended period.

Implications that affect VPDN criteria concern a provider's ability to maintain non-blocking, consistent performance to the subscriber despite an ongoing growth rate in excess of 90% in the number of subscribers. According to a recent survey conducted by *Boardwatch* magazine, the average ISP adds over 140 new customers a month, all of whom expect to gain the best possible network performance from their 28.8kbps modems and/or ISDN connections.

Two key factors affect the effective performance that the Internet users see. The first and most obvious is the maximum speed with which that user can connect to the network. In many cases, however, particularly given the recent denial of service outages, the ability to connect is not always a given.

Many factors, including the ability of an ISP partner to quickly expand the number of available dial-up ports in order to scale with demand, effective bandwidth impedance matching between dial-in ports and Internet access trunks, and the ability of the ISP to effectively load share raw transmission and Web server capacity on demand, all serve to separate the partners of choice from the also-rans. It is this class of criteria that the senior manager should use in measuring and selecting the partner of choice that makes the most sense for his or her business.

The Registry believes that Ascend Communications is highly differentiated in its ability to meet these rapid provisioning requirements. Today, Ascend is relatively unique amongst the major vendors in its ability to enable a service provider to rapidly provision additional circuits either on an incremental low-end or mid-range product basis, or to front load the required capacity through use of a single high-density box – its MAX TNT product (which can support over 2,016 modem calls, and 4,032 ISDN or Frame Relay calls in a single eight foot rack). The MAX TNT is not only fully software compatible with the other members of the MAX product line, it also offers proven interoperability in multivendor networks.

This scalability effectively complements the transmission technology diversity that the vendor supports – analog (both V.34 and asynchronous 56 Kbps service), Basic and Primary Rate ISDN, T1, T3, Frame Relay, and Digital Subscriber Line (DSL). Ascend has a proven track record of flexible dial-up and transmission service support that will result in continued competitive advantage in an increasingly cost and performance-sensitive market.

II. Scalability - The key criteria for Avoiding Growing Pains

Regardless of whether a user is considering augmenting an existing VPDN or starting from scratch, users will need to pre-determine if a service provider's infrastructure is capable of supporting anticipated speed and port growth requirements of the business. Figure 4 represents a comprehensive network service provider model that enables built-in flexibility to meet the expected increases in the number of users and applications as well as to accommodate diverse work models.

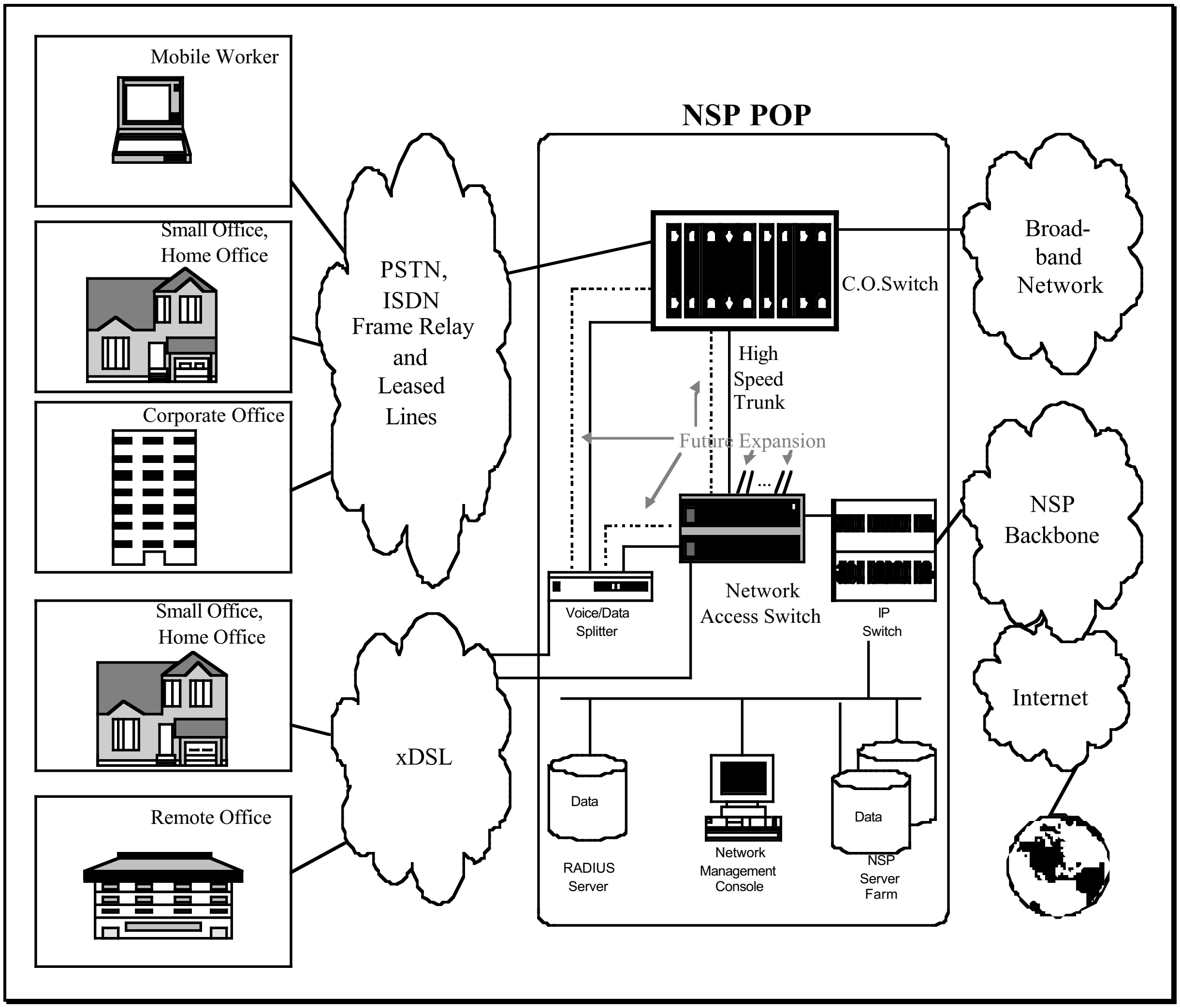


Figure 4: NSP Backbone/Internet Building Block

The key requirement represented in Figure 4 is the provider's ability to easily and effectively keep up with nearly exponentially increasing service demand without compromising service pricing, performance, access flexibility, and functionality. The ability to meet this requirement in all dimensions on a sustained basis is by no means a trivial proposition. It requires that the provider has invested in strategic vendors that offer products that are distinguished by the breadth and depth of protocol support they provide; media and transmission service flexibility; transmission service support excellence; effective and efficient management services; and a strong customer base that results in improved product quality and service excellence.

These dimensions of scalability are crucial decision factors because they directly enable a user to effectively manage his or her cost of network ownership supporting effective cost containment for both support and facilities costs. In addition, they constitute effective enablers for electronic commerce because they allow a user to get started today with the knowledge that the provider's network infrastructure will grow with them into the future and support a breadth of services that are likely not even envisioned today.

An additional important consideration lies in ensuring that an effective capacity match exists between the incoming service circuits and the trunks that connect the provider to the worldwide Internet. This dictates the product requirement for high-speed channel throughput between access server and backbone router that can be effectively supported by the packet forwarding rates in each product.

While this consideration is certainly important in the case of access servers, it becomes particularly crucial in the case of service provider backbone routers that support the crucial linkage between the provider's POP and the Internet backbone. In this case, the backbone router must support a combination of multiple high speed trunks and provide the internal packet forwarding capacity that can sustain each of them on a non-blocking basis. While this is not practical for every conceivable type of workload, a small number of vendors have been able to produce a class of product that effectively addresses most of the mainstream requirements.

Ascend Communications' GRF meets these infrastructure requirements to improve the scalability of the backbone as IP traffic increases. The GRF is a high performance IP switch that combines Layer-3 switching with intelligent IP forwarding cards. The GRF performs routing (Layer-3) decisions at a maximum advertised forwarding rate of 10 million packets per second, and performs hardware look-ups in less than 2.5 microseconds – on routing tables that contain as many as 150,000 routes. The high end GRF chassis can support up to 16 media cards with 1 gigabit of dedicated bandwidth per card, enabling it to scale linearly.

In addition, the GRF supports a wide range of media – 10/100Base-T Ethernet, FDDI, CDDI, HSSI, ATM OC-3c, HIPPI, IP/SONET OC-3c and ATM OC-12c. Ascend has wisely chosen to eschew the custom IP switching boutique protocols in favor of supporting only open IP standards that are complemented by high product performance. Consequently, we see Ascend as being uniquely positioned over its competition relative to the range of standards-based backbone performance that it offers to the service provider.

III. Ensuring High Customer Satisfaction

The evolution of electronic commerce speaks to the need to production quality service within a VPDN. Production quality service (and its delivery) has rapidly become a key issue with which many senior network managers have been tasked to address. It is most often raised in the form of quantified *service level requirements* that are defined in terms of service performance, reliability, availability, security or some combination thereof.

Given the combination of technology push coupled with business opportunity pull associated with network-based electronic commerce, many network managers are now experiencing a rapidly increasing demand from their end users to both define and be measured upon Service Level Agreements (SLAs) similar to what have existed within networked mainframe environments for years. What has driven the recent interest in SLAs is the fact that the service quality defined by the SLA constitutes the investment return associated with network cost of ownership.

While SLA definition was relatively straightforward and widely implemented for mainframe networking, defining similar SLAs for production internetworks has proven to be anything but straightforward; a similar, if not greater, challenge can be expected for VPDNs. Providers who offer superior Internet service capability, particularly those who excel in implementing products that provide superior scalability features referenced in the previous section, will most likely be the leaders in offering effective SLAs that will most likely initially focus key network availability, reliability and security metrics.

Users are strongly urged to not consider a provider partner who does not either already support or have a well thought out plan for Service Level management. The reason is that it is only through rigorous provider Service Level management that a business will be able to reap the business benefits that come from being an early mainstream implementer of electronic commerce services.

While SLAs are unquestionably the direction of the future, their short term implementation, particularly in terms of guaranteeing end-to-end application performance, is likely to occur in small, measurable steps. For many providers, the best that will be possible in the short term is to implement the best possible non-blocking service infrastructure that will deliver the deterministic performance that has been classically associated with an environment that does commit to service levels.

This is another reason why The Registry feels that Ascend Communications is very well positioned to support both service providers and end users. Through its multi-device, multivendor network management product, NetClarity®, Ascend can provide performance level support throughout the network, in addition to supporting broad connectivity. This network management system monitors the performance of the network's physical interfaces and access devices (Layer-1), switching devices (Layer-2), and routers (Layer-3) to deliver a comprehensive view of the network's performance as well as enable capacity planning. These management capabilities effectively position Ascend to offer longer term end-to-end class of service provisioning, as well as provide shorter term quality of service guarantees.

IV. KEEPING THE CORPORATE INFORMATION VAULT SAFE

Given the public nature of the Internet, a legitimate concern for businesses contemplating the implementation of a VPDN and an e-commerce business model is the threat of a security break-in to the corporate data warehouse (i.e. the corporate intranet or corporate data center). The reality is that you need to assume this possibility as part of your VPDN planning efforts.

All of the cost and associated benefits of a VPDN solution are moot if there is not a strong security infrastructure in place. Security is what puts the "private" in virtual private networks. As a first step, it is necessary to address the very real security concerns associated with untrusted members of the VPDN having access to confidential company information, or compromising system integrity. Figure 5 illustrates the demarcation point or the *Network Perimeter* between the untrusted and trusted members of a Corporate network.

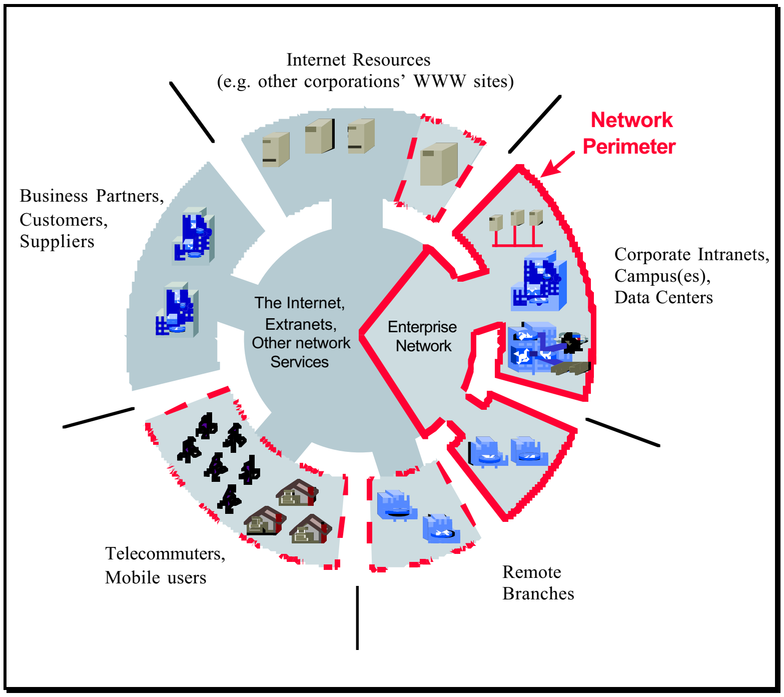


Figure 5: The Network Security Perimeter Demarc

To allow access via untrusted networks through the Network Perimeter to the corporate intranet or corporate data center, it is necessary to build secure tunnels through these untrusted networks, as shown in Figure 6.

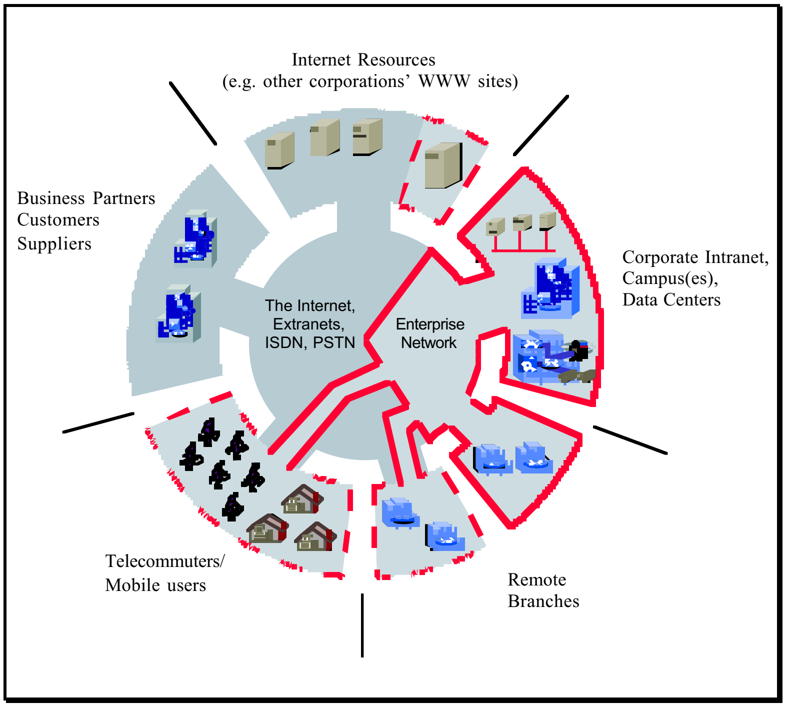


Figure 6: Secure Tunnels through Untrusted Network(s)

The process of supporting trusted users across the corporate network by establishing Secure Tunnels through untrusted networks is referred to as *Establishing Membership.* The process of establishing membership consists of three stages. First, the network must establish that the user is who they say they are using some means of strong authentication. Then, each party must obtain secret encryption keys so that any data sent over the network can be kept private. And finally, so as to avoid unnecessarily complex routing gateways, the remote workstation or branch router must join the corporate routing scheme so that the secure tunnel appears to the rest of the network and the remote device(s) as a simple direct network connection.

Note that this process of establishing membership is not related to user privilege or authorization; we have only established that the remote user(s) can be trusted to be who they say they are, that communications will be private and that the underlying complexity of the untrusted IP network is invisible to the rest of the corporate network. We have not yet established what the user is allowed to do. This is important, because it means that the administration of user privileges can be largely independent of the means by which the user has accessed the network. The same authorization mechanism can be used for users on the corporate LAN as for those connected via the un-trusted network. This approach provides a simple hybrid network security model which can be applied to all users, irrespective of where they are located on the hybrid network (Figure 7).

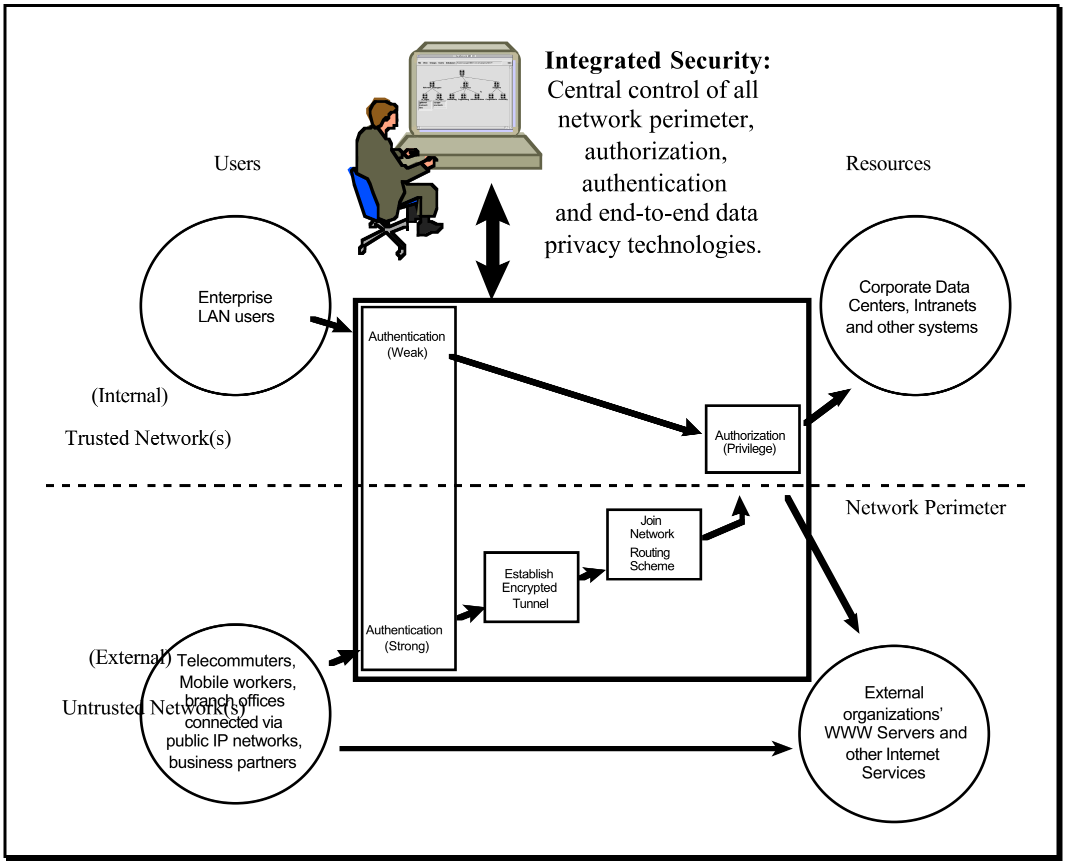

Integrated Security:
Central control of all network perimeter, authorization, authentication and end-to-end data privacy technologies.
Users
Resources
Enterprise LAN users
(Internal)
Trusted Network(s)
Authentication (Weak)
Authorization (Privilege)
Corporate Data Centers, Intranets and other systems
Network Perimeter
Join Network Routing Scheme
Establish Encrypted Tunnel
Authentication (Strong)
(External)
Untrusted Network(s)
Telecommuters, Mobile workers, branch offices connected via public IP networks, business partners
External organizations' WWW Servers and other Internet Services

Figure 7: Integrated Security Model

While no vendor today has fully implemented this distributed security model, Ascend Communications has, in the view of The Registry, implemented a strong start with its Secure Access product family which is supported across most of the members of its Pipeline branch/remote office, customer premise and MAX remote access products. Ascend's security solution integrates all of the major security components into each product: a user and security management system, dynamic firewall, and tunneling support as well as payload encryption support.

The fact that a consistent, flexible and dynamic security system has been uniformly implemented at both the remote office end and service provider ends of the connection constitutes a strong functional differentiator for the vendor vis-a-vis its competition, which generally offers strong firewall services only for router products. The integrated focus at both ends should provide a stronger comfort factor for users who have business requirements to implement Intranets over VPDNs, but have been hesitant to do so due to network security concerns.

V. Implementing A Non-Proprietary VPDN

Interoperability is a key requirement for establishing a VPDN in this early stage of deployment. While there are a number of standard tunneling and security protocols, there remain proprietary protocols and proposed industry standards that have not yet been cleared.

Rather than creating a single-vendor VPDN solution, which would impose limits on future equipment selection and threaten ubiquitous client interoperability, the VPDN-provider needs to select products that have been tested and proven to conform to the applicable standards, and to choose vendors based on their commitment to open standards and easy upgrade paths. Similarly, the CIO wishing to implement a VPDN solution should be aware that successful implementation will require a provider that can supply an open, standards-based VPDN.

Ascend Communications, unlike some of its competitors in the networking equipment industry, has maintained a commitment to support open standards in its remote access and IP switching/routing equipment, as well as in its security and network management software. Its products support the proposed industry standard Layer-2 Tunneling Protocol (L2TP), and IPsec, the IP security standard that combines several technologies to provide robust encryption.

5. WHY TECHNOLOGICAL INNOVATION MATTERS FOR YOUR BUSINESS

Building a high performance, extremely robust and secure VPDN infrastructure that is accessible at any hour from any location requires the latest in remote networking and Internet access technology. Innovation brings:

- Bandwidth optimization techniques which enable transparent network connects and disconnects, lessening the chances of customers receiving a busy signal when calling for order status, for example.

- Digital Subscriber Line (DSL) technology which uses advanced digital signal processing to enable the use of existing twisted pair wiring for higher speed, more reliable dial-in connections. Not only does this protect the existing cabling infrastructure investments, but it also provides increased flexibility to support the changing work model (e.g. home offices).

- The collapsing of multiple, disparate, technology-dependent equipment platforms into single integrated platforms that provide room for growth and simpler technology upgrades (e.g. ISDN, 56 Kbps), resulting in less disruption to customers' operations and management procedures, and reducing the overall cost of ownership.

- Innovative dynamic firewall technology for a network-wide security system that protects corporate information resources from unauthorized intrusion throughout the network – whether the break occurs via the Internet or through other forms of open remote access. For example, during file transfer protocol (FTP) transactions, dynamic firewall technology only opens the required access ports, then automatically closes the ports at the end of the session. In contrast, static packet filtering opens all access ports for every data transfer, providing an opportunity for hackers to probe the network for the duration of the session, leaving the corporate assets exposed. Such technological innovations enable the construction of architecturally sound VPDN infrastructures that will support and help drive your business strategy rather than dictate it.

6. Ensuring You Have the Best Solution

Conducting business electronically over the public Internet offers unprecedented opportunities for new business ventures and service offerings as well as communication flexibility to accommodate changing workflow processes. The phenomenal success and simplicity of the worldwide web has been a significant driving force behind businesses seeking the Internet as an alternative approach to traditional marketing and communication channels. In fact, IDC reports that Internet-based commerce will grow from over $5B in 1996 to $100B by 2000. The challenges this new order brings to the IS organization has caused a re-evaluation of classic internetworking processes and practices in an effort to more closely align the network infrastructure with the business needs while better optimizing expensive personnel and facilities resources.

Virtual Private Data Networking is quickly evolving to be the answer to these challenges. Its implementation, however, requires careful up-front planning to ensure the end result is what you and the business expect. Working in partnership with an ISP who is experienced in planning, designing, implementing and managing a VPDN will enable more efficient allocation of your IS resources and go a long way toward building the optimal VPDN.

To effect this, selection of the best provider should focus on the ISP's ability to provide:

- a scaleable, high performance network infrastructure that provides on-demand, non-blocking access to the network;
- strict security functionality that prevents planned or unintentional damage to corporate databases and systems;
- superior Internet service capability, including rigorous Service Level management; and,
- an infrastructure that is designed with built-in flexibility to support proven technology innovation in anticipation of its customers' changing business models and strategies.

Given the functionality, performance and security instrumentation of Ascend Communications product line, the Registry believes that the vendor currently offers strong solutions to both users and service providers who are looking for a VPDN solution that is more than a simple sum of piecemeal parts.