Ascend

WHITE PAPER

MultiVPN for the Enterprise

Breaking Down the Barriers to VPNs



Table of Contents

1. Executive Summary 1

2. MultiVPN: A Complete Solution for the Enterprise 3

Compatibility 3

Security 4

Availability 4

Manageability 5

3. Ascend's MultiVPN Product Line 6

Pipeline WAN Routers 6

MAX WAN Access Switches 7

SecureConnect Firewall 7

Ascend's RADIUS Database 8

Navis Network Management System 8

4. Conclusion 9

Appendix: MultiVPN: A Comprehensive Approach to VPNs 10

Virtual Private Remote Networking (VPRN) 11

Virtual Private Trunking (VPT) 11

Virtual IP Routing (VIPR) 12

©1998 Ascend Communications, Inc.

1. Executive Summary

Virtual Private Networks (VPNs) which utilize public network services, such as the Internet, offer a number of substantial benefits to enterprise organizations. VPNs cost about half as much to operate as an equivalent private network. With resiliency and redundancy built into the next generation public network, VPNs are capable of providing the same level of reliability as most private networks. The power of the next-generation public network gives users unprecedented possibilities for enterprise networking, including VPNs and integrated voice/data/fax communications. VPNs give the enterprise a worldwide presence for communicating with employees, customers, suppliers and business partners. VPNs add flexibility and capability to enterprise networking, especially with the powerful any-to-many nature of public network services such as the Internet. And VPNs dramatically reduce the management burden, with much of the remote user support being handled by a knowledgeable service provider. Indeed, VPNs are the future of enterprise networking.

Ascend is making the future of VPNs a reality today. Already one of the leaders in VPN solutions, Ascend is the first vendor to break down the remaining barriers to widespread VPN adoption with a strategy to match enterprise-wide needs with carrier-class VPN infrastructure enhancements. The Ascend MultiVPN™ enabling strategy, with its visionary provider/subscriber approach and broad interpretation of VPNs, has three equally important dimensions:

- Creating the industry's first comprehensive set of fundamental VPN architectures
- Addressing the concerns organizations have regarding enterprise-wide VPNs
- Satisfying the special needs of service providers responsible for the infrastructure

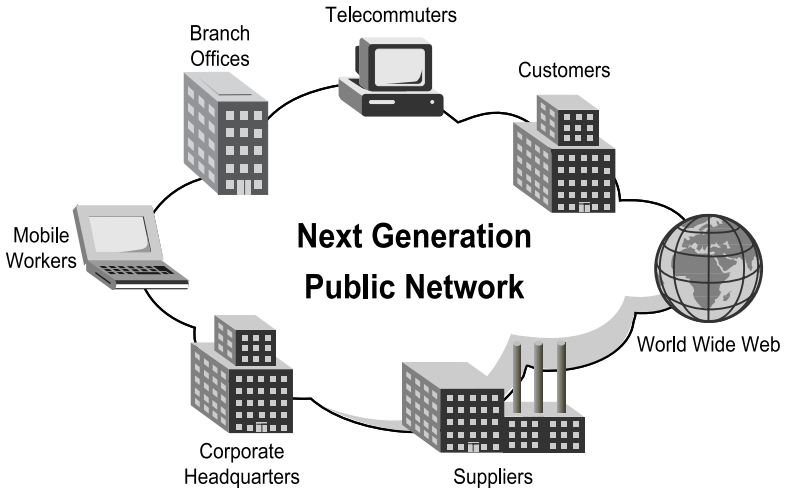


Figure 1 – The Ascend MultiVPN strategy makes VPNs suitable for all networking applications—from simple remote LAN access to sophisticated enterprise-wide internetworking.

Some vendors believe tunneling in the Internet alone defines a VPN, and The Ascend MultiVPN solution supports tunneling in the form of Virtual Private Remote Networking (VPRN) as the appropriate solution for Internet-based remote LAN access. But MultiVPN transcends basic tunneling with two additional and powerful ways of constructing VPNs: Virtual Private Trunking (VPT) and Virtual IP Routing (VIPR). VPT delivers the performance and reliability of a leased line, the lifeblood of today's private networks, with direct access to public Frame Relay and ATM services. VIPR extends private routing environments into the public IP network seamlessly and securely. The capability and flexibility afforded by all three MultiVPN architectures enables—for the first time—production, enterprise-wide VPN deployment.

Many other vendors believe that "point products," such as a firewall or some encryption, create a VPN. The Ascend MultiVPN solution puts the "private" in virtual private network through an integrated combination of state-of-the-art dynamic firewall protection and IP Security (IPSec) encryption and authentication. But MultiVPN goes beyond security needs by addressing three other primary enterprise concerns: compatibility, availability and manageability. With

©1998 Ascend Communications, Inc.

Ascend in the infrastructure, enterprise users get compatibility through a choice of MultiVPN's VPRN, VPT and VIPR architectures. They get availability in two ways: Quality of Service (QoS) and Service Level Agreement (SLA) guarantees. And with Ascend Customer Network Management (CNM), the enterprise can manage the complete VPN, including its private portion of the public network.

No vendor has satisfied the demanding needs of service providers—until now. Strategic partnerships with the world's leading service providers give Ascend a valuable perspective on their top three VPN needs: high availability, service management and customer network management. MultiVPN integrates these three capabilities, and more, into Ascend's carrier-class switching, routing and access systems. The high performance and inherent redundancy of Ascend's multiservice platforms allow service providers to deliver QoS and SLA availability guarantees with confidence. Service management affords optimal network utilization at minimal cost for maximum efficiency. And Customer Network Management—a service offering in itself—lets service providers share VPN-specific network information with their enterprise subscriber customers 24 hours a day.

Individually, MultiVPN's three dimensions enhance the state-of-the-art technology available for VPNs. Collectively, they eliminate all of the obstacles remaining to the cost-effective deployment (by service *providers*) and cost-saving utilization (by business *subscribers*) of the public network infrastructure for private enterprise-wide VPNs. The section that follows outlines MultiVPN's comprehensive approach to VPNs in the context of the four enterprise concerns: compatibility, security, availability and manageability. The next section summarizes Ascend's product offering, which consists of internetworking equipment, security systems and management capabilities. A final section provides a brief conclusion.

The Ascend Advantage

Ascend's comprehensive MultiVPN offering has "raised the bar" in the burgeoning VPN marketplace. Ascend's VPN leadership derives from the company's many strengths and achievements:

- Broadest experience in the deployment, utilization and management of public networking solutions with nearly 5 million ports installed
- Most comprehensive family of field-proven VPN products with industry-leading features and international certification for worldwide interoperability
- Highest degree of integration, including built-in firewall and IPSec protections, to simplify installation, operation and management
- Greatest flexibility with a choice of VPN architectures, equipment configurations, security provisions, performance guarantees and management techniques
- Quality of Service (QoS) and Service Level Agreement (SLA) assurances from MultiVPN service providers that guarantee all three dimensions of availability: throughput, latency and uptime
- Customer Network Management (CNM) that lets service providers and their enterprise subscribers jointly, completely and securely manage the end-to-end VPN
- Delivery of "multimedia" VPNs that integrate voice, fax, video and data communications, including the any-to-many capability of IP multicast

©1998 Ascend Communications, Inc.

2. MultiVPN: A Complete Solution for the Enterprise

Organizations, large and small and in both the public and private sectors, are intrigued by virtual private networks. They realize VPNs are the future of enterprise networking as private networks get too complex—and expensive—for most organizations to justify. An Ascend MultiVPN can integrate private enterprise, semi-private extranet and public Internet access—all over a single connection for each site or user—with less cost, and more reliability, flexibility and capability than a private network.

But despite the many advantages, organizations continue to have four fundamental concerns about utilizing VPNs in most enterprise applications: compatibility, security, availability and manageability. Ascend's MultiVPN strategy is the first to attack all four issues head-on, giving enterprises all the benefits of VPNs without sacrificing or even jeopardizing any of the control organizations have grown to expect in a private network. With Ascend's MultiVPN, organizations get complete freedom of choice and unparalleled versatility in the configuration, operation and management of their enterprise-wide VPNs.

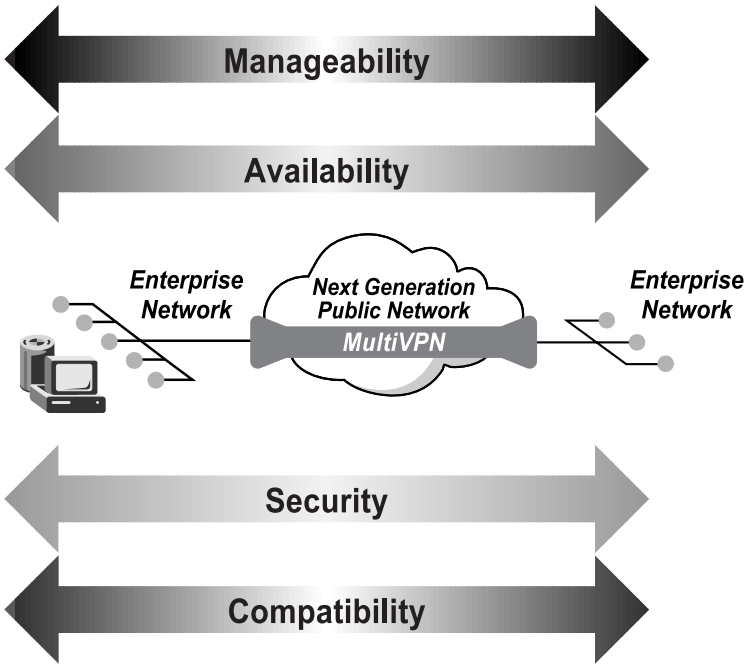


Figure 2 – Ascend's MultiVPN strategy overcomes all user concerns preventing enterprise-wide adoption of virtual private networks.

Compatibility

Compatibility cannot be taken for granted with a VPN. While an increasing percentage of enterprise applications utilize the Internet protocol (IP), most still employ other protocols, such as IPX (Novell NetWare) and SNA (IBM). And even when IP is used, the address scheme is normally "private" (unregistered addresses), making it incompatible with the Internet. MultiVPN maximizes enterprise application compatibility with a choice of:

- Virtual Private Remote Networking (VPRN) to supply multiprotocol tunneling for a wide range of enterprise applications, especially remote access by individual users. MultiVPN supports all three leading tunneling technologies: the Point-to-Point Tunneling Protocol (PPTP), created in a strategic partnership between Ascend and Microsoft, and now a standard feature of Windows; the Layer 2 Tunneling Protocol (L2TP), an industry standard based on PPTP; and Ascend Tunnel Management Protocol (ATMP), an enhanced implementation of standard Generic Routing Encapsulation (GRE).

©1998 Ascend Communications, Inc.

- *Virtual Private Trunking* (VPT) to give direct access to the advanced capabilities of Frame Relay and Asynchronous Transfer Mode (ATM) services in a MultiVPN-based public network infrastructure. VPT goes beyond traditional switched and permanent virtual circuits to provide the functional equivalent of protocol-independent leased lines, and maintains interoperability with RFC1490 for Frame Relay networks that combine LAN and SNA traffic.

- *Virtual IP Routing* (VIPR) to extend private route tables and address spaces from the enterprise into the MultiVPN service provider's routed/switched network. Essentially, VIPR is a logical partition of a physical router or switch based on the emerging Multi-Protocol Label Switching (MPLS) standard. VIPR preserves private IP address schemes, making it ideal for branch office internetworking, and works with any IP encapsulation technique, such as Data Link Switching (DLSw).

Compatibility with the past and present is only part of the issue. For VPNs to provide an enduring solution, they must be compatible with emerging technologies. Ascend already supports many of these future possibilities, including Voice over IP (VoIP) using the H.323 standard, Internet faxing, and IP multicast for any-to-many communications.

Security

At a minimum, every node in a VPN should have a firewall. Why? Because *if you don't have security everywhere, you don't have security anywhere*. Just as a chain is only as strong as its weakest link, so too is a VPN security system. Any "unlocked door" makes resources throughout the enterprise vulnerable. A firewall passes only authorized traffic for only trusted users, and blocks everything else. The biggest single limitation of most firewalls, however, is that securing every single connection becomes cost-prohibitive, thus negating the cost-saving advantages of a VPN! Ascend makes VPN-wide security affordable with a combination of MultiVPN and Ascend's suite of network security products.

The three MultiVPN architectures provide various levels of security to complement the SecureConnect™ firewall:

- *Virtual Private Remote Networking* integrates IPSec packet encryption and digital signatures to add confidentiality, integrity and authenticity to Internet-based VPNs (Ascend's implementation of IPSec supports DES/3DES encryption, MD-5/SHA-1 authentication headers and the Internet Key Management Protocol)

- *Virtual Private Trunking* adds a full layer of security through logical segmentation of physical resources in the public network, effectively isolating a VPN's traffic

- *Virtual IP Routing* utilizes private route tables and closed user groups to preserve privacy in a public IP network

Ascend also supports many additional security mechanisms in the public network infrastructure, including the password and challenge-handshake authentication protocols (PAP and CHAP), single- and two-factor token authentication systems, Calling Line ID (CLID), Dialed Number Information String (DNIS) and more.

Ascend's enhanced implementation of RADIUS (the Remote Authentication Dial-In User Service) supports proxy capabilities to facilitate centralized control of security provisions. MultiVPN solutions are compatible with existing addressing mechanisms, including Novell Directory Services (NDS), Windows NT, the Lightweight Directory Access Protocol (LDAP), X.500, the Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT), and others. Support is planned for the Directory Enabled Network (DEN) initiative.

Availability

For the enterprise to depend on a VPN, the public network must deliver the reliability and performance of a private network. Ascend MultiVPN infrastructure access, routing and switching platforms have features that make a service provider's public data network perform as well as the Public Switched Telephone Network (PSTN), with guarantees for all three dimensions of availability: throughput; latency and latency variations; and uptime. ATM's ability to deliver circuit-like constant bit rate (CBR) is well known. But Ascend extends ATM-like QoS capabilities to both Frame Relay and IP. Ascend also adds the ability to deliver and confirm SLAs. Together, QoS and SLA guarantees offer the full range of availability to fit any need and budget.

©1998 Ascend Communications, Inc.

Manageability

Organizations have always wanted to manage their enterprise networks end-to-end, including their "private portion" of the intervening public network. Surprisingly, this seamless provider/subscriber capability has remained elusive, until now, with the advent of the Ascend Navis™ network management system for MultiVPN.

Today with private networks, the service provider manages its public network up to the edge of the enterprise; enterprise subscribers can manage only to the edge of the service provider's WAN. Navis eliminates this traditional edge-to-edge "separation of powers" with advanced capabilities that permit provider/subscriber management of the combined private/public VPN. Through the familiar Web browser interface, Ascend's advanced CNM system gives the enterprise subscriber a window into the service provider's infrastructure to view, monitor, reconfigure, troubleshoot and otherwise manage its entire VPN, including its private portion of the public network.

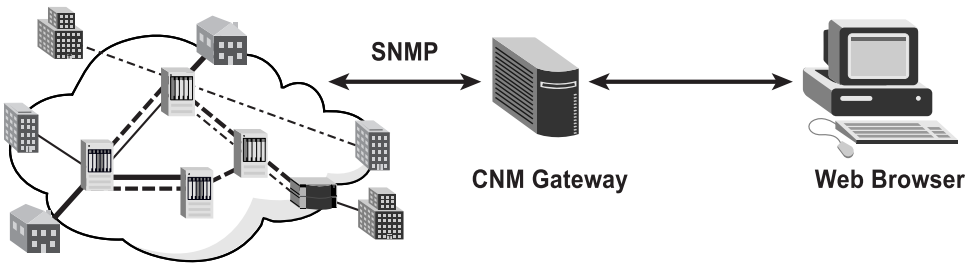


Figure 3 – The Ascend Navis CNM gateway combines unprecedented VPN management capabilities with the simplicity of browser-based access.

The table below summarizes Ascend's solution by portraying MultiVPN options in the context of enterprise VPN concerns.

MultiVPN for the Enterprise	Virtual Private Remote Networking (VPRN)	Virtual Private Trunking (VPT)	Virtual IP Routing (VIPR)
Compatibility	Multiprotocol Tunneling	Protocol Independence	IP or Protocols Encapsulated in IP
Security	Integral Firewall with IPSec Encryption and Multi-factor Authentication	Integral Firewall and Traffic Isolation	Integral Firewall and Closed User Groups
Availability	Internet-dependent	Full QoS and SLA Guarantees	Full QoS and SLA Guarantees
Manageability	RADIUS	Customer Network Management (CNM)	Router Management

©1998 Ascend Communications, Inc.

MultiVPN's Provider/Subscriber Approach

Only Ascend MultiVPN addresses the four primary enterprise concerns in a way that makes it possible for service providers to deliver a total VPN solution to their business subscribers. By making VPNs a win/win arrangement between providers and subscribers, Ascend eliminates any remaining obstacles to the widespread deployment and utilization of VPN-capable public network services. With MultiVPN, providers are able to take advantage of Ascend's capable, scalable and affordable infrastructure offering, then pass along the many economies of scale and other cost-saving efficiencies for the immediate benefit of their business subscribers.

3. Ascend's MultiVPN Product Line

The Ascend MultiVPN product line includes internetworking equipment (Pipeline® and MAX™ families), security systems (SecureConnect™ and RADIUS) and management capabilities (the Navis™ network management system with CNM). Each element is highlighted here. Detailed information on these and other Ascend products is available at Ascend's Web site (www.ascend.com).

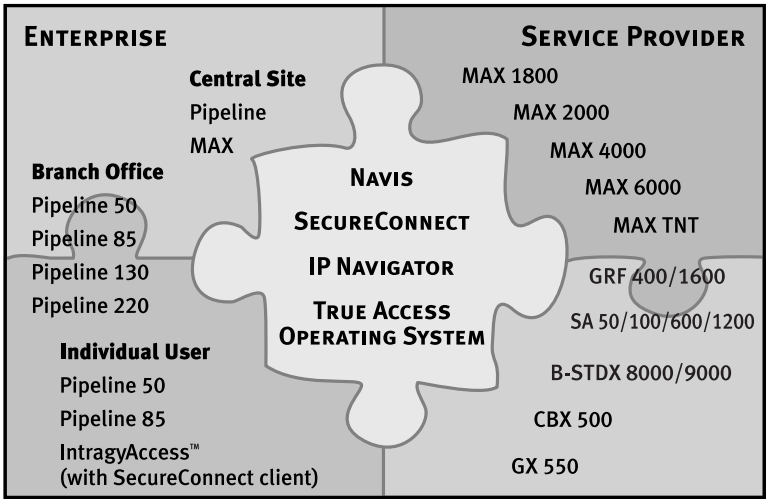


Figure 4 – Ascend's VPN product line is a fully integrated solution with customer premises equipment, infrastructure access, IP routing/switching, core switching, security and management, that together constitute the industry's most comprehensive VPN offering.

Pipeline WAN Routers

The award-winning Ascend Pipeline family provides the industry's widest assortment of VPN-capable routers for branch offices, small office/home office (SOHO) environments, and full-or part-time telecommuters. VPNs benefit substantially from the Pipeline routers superb price/performance and low cost of ownership, especially from its ease of management.

Ascend's Pipeline family includes several models to fit applications ranging from single-user home offices to multi-user branch offices of virtually any size. The SOHO models are complete data/voice/fax communications solutions with two analog POTS (Plain Old Telephone Service) ports to connect telephones, answering machines and fax machines.

©1998 Ascend Communications, Inc.

Ascend's flagship SOHO router is the Pipeline 75, which offers the industry's most extensive feature set. The Pipeline 85 adds a 4-port Ethernet hub.

Data-only models of the Pipeline are available in switched (ISDN or SW56) and leased line (T1/Fractional T1, DDS56 or xDSL) versions, each with support for Frame Relay. The award-winning Pipeline 50, ideal for smaller branch offices, is Ascend's most popular ISDN remote access router. The Pipeline 130 offers both leased line and switched WAN ports for situations that require dial-up bandwidth on demand for backup and overflow needs. The Pipeline 220 adds a second Ethernet LAN port on the Internet side of the optional SecureConnect firewall.

MAX WAN Access Switches

For larger sites in a hybrid private/virtual private network, The Ascend MAX WAN Access Switch offers a total solution. The industry-leading MAX combines capabilities for both PSTN (private network) and VPN services, and is available in a variety of models that can support as few as two to over 2,000 concurrent sessions cost-effectively. All models offer the capability, scalability and versatility enterprises need during the migration from private to virtual private networks.

Every member of the MAX family offers the same proven and robust True Access™ Operating System (TAOS) feature set that has made the MAX the number one choice for Internet access. Specific features include:

- Integral firewall, IPSec and tunneling capabilities
- Multi-port WAN capabilities supporting a wide range of PSTN and public data network services, including T1/E1, ISDN PRI/BRI, xDSL, DS-3, analog modems, cellular, Frame Relay and X.25
- High-speed channelized trunk lines to consolidate traffic cost-effectively from all sites and users in the VPN
- Dynamic bandwidth management (DBA, MP, MP+ and BACP) for enhanced performance
- Call detail reporting to track usage by all users
- Resiliency with dual power supplies and hot-swappable interface cards
- Certification for operation with carrier services worldwide

Across the board, MAX products supply their rich functionality and high performance for the industry's lowest cost of ownership, which explains why MAX systems are used for over half of all digital access concentrator ports installed by corporations, carriers and network/Internet service providers.

SecureConnect Firewall

Ascend SecureConnect combines an ICSA-certified dynamic firewall protection with IP Security (IPSec) packet encryption and authentication. SecureConnect is an integrated feature for the Ascend Pipeline family (Pipeline 50-220) and is an integrated option for the MAX WAN access switch, and is available in a software-only Intragy™ Personal Edition for PCs with ordinary modems.

SecureConnect overcomes the biggest single limitation of most firewalls, which is securing every single connection affordably enough to preserve cost-saving advantages of a VPN. Additional features of SecureConnect include:

- State-of-the-art dynamic stateful inspection for maximum protection
- Strict enforcement of "that which is not expressly permitted is denied"
- Certification by the International Computer Security Association (ICSA)
- An optional unprotected "de-militarized zone" (DMZ) LAN interface, on the Internet side of the firewall, for Web and other public servers

©1998 Ascend Communications, Inc.

Ascend's RADIUS Database

Ascend's enhanced implementation of RADIUS (Remote Authentication Dial-In User Service) handles the three A's of remote networking administration—authentication, authorization and accounting—with individual profiles for all VPN members. RADIUS employs a client/server architecture with the RADIUS database itself as the server and network access switches as its clients. Proxy capability gives a RADIUS server at the service provider's point of presence (POP) the ability to query the enterprise organization's RADIUS server to access VPN member profiles. In this way the enterprise maintains complete control over access to its VPN resources, while allowing the security provisions to be enforced at service provider POPs. This ability to handle distributed management with centralized control makes RADIUS ideal for VPNs of any architecture.

Navis Network Management System

The Ascend Navis Customer Network Management (CNM) solution grants network managers controlled access to the public network infrastructure, thereby empowering the enterprise to manage its complete MultiVPN. Navis CNM provides real-time, 24 hour access to the public network's configuration, operation, performance and fault status—all through the familiar Web browser interface for maximum productivity. Specific CNM capabilities include:

- Auto-discovery and dynamic mapping of the network topology with both physical and logical groupings of equipment and links
- Real-time network monitoring of physical and logical WAN links and traffic conditions, with fault alert/alarm generation based on user-defined thresholds
- Monitoring that offers a way to assess actual throughput on WAN lines to help control delivery of contracted QoS and SLAs
- Capacity planning and performance trending through collection and analysis of traffic statistics that show both the level and patterns of usage by all users/sites
- Base-lining of normal operating conditions to help determine overall network "health" and for capacity planning needs
- Integrated, statistical accounting to track network traffic by user/department/site for billing, accounting, auditing or other purposes
- Remote configuration management for bringing new locations on-line, as well as coordinating network-wide updates and changes
- A means of comparing actual vs. intended equipment configurations
- Traditional device-oriented fault detection and diagnostics for pinpointing and troubleshooting specific equipment problems
- A trace function that tracks traffic through the network, to help isolate bottlenecks and other problems
- A way to examine the WAN's Physical and Data Link layers, as well as assess actual throughput of dial-up and dedicated WAN links

©1998 Ascend Communications, Inc.

4. Conclusion

The Ascend MultiVPN strategy fulfills the promise of VPNs by making “the network of the future” a reality today for the full range of enterprise-wide networking needs. Ascend is the first vendor to adopt a visionary provider/subscriber approach to VPNs and to deliver a solution for the enterprise that offers a comprehensive choice of VPN architectures. MultiVPN makes virtual private networking a commercial reality by overcoming the obstacles to pervasive deployment by providers, as well as to widespread adoption by enterprise subscribers. Finally, Ascend is the only vendor offering the full spectrum of products and features necessary to meet the demanding needs of providers and subscribers alike. MultiVPN from Ascend. It’s a whole new way of networking.

MultiVPN Benefits for the Enterprise

- Lower costs—from 30 to 80%, according to industry analysts—for data networking and voice/video/fax telecommunications
- Achieve high reliability through the carrier-class redundancy and resiliency of the MultiVPN-based public network infrastructure
- Extend reach and gain worldwide access to all enterprise sites, other organizations and public information resources
- Build new, secure communication relationships with buyers and suppliers
- Leverage enhanced and expanded services that are unavailable in the PSTN, such as multicast and ubiquitous interoperability
- Increase flexibility with full freedom of choice regarding fundamental VPN architectures, security provisions, QoS and SLA performance assurances, and outsourcing options
- Simplify operations with a single per-site connection to the enterprise network, an extranet and the Internet
- Gain greater control of the VPN with Customer Network Management

©1998 Ascend Communications, Inc.

Appendix: MultiVPN: A Comprehensive Approach to VPNs

MultiVPN affords the industry's most comprehensive choice of fundamental architectures for enterprise-wide VPNs. No other vendor offers such a complete solution with these three powerful options:

- Virtual Private Remote Networking (VPRN) with multiprotocol tunneling for remote LAN access by client PCs
- Virtual Private Trunking (VPT) to establish the equivalent of leased lines among major facilities
- Virtual IP Routing (VIPR) to internetwork branch offices or establish extranets with closed user groups

Each MultiVPN option, supported by Ascend's many service provider partners worldwide, provides the physical and/or logical paths through the public network that replace the many long-distance leased or switched links in a private network. All three options can be employed individually or in combination, providing the many benefits of unparalleled flexibility and complete freedom of choice in the configuration, operation and management of enterprise-wide VPNs.

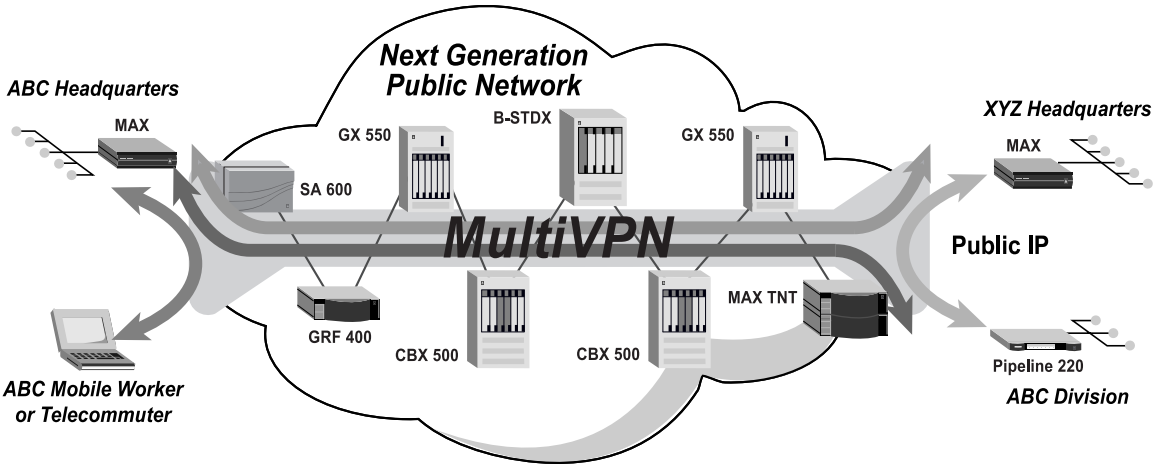


Figure 5 –Three MultiVPN architectures provide the industry's most comprehensive and flexible foundation for configuring, operating and managing VPNs.

©1998 Ascend Communications, Inc.

Virtual Private Remote Networking (VPRN)

VPRN multiprotocol tunneling is the best choice for transporting private client/server traffic over public IP networks like the Internet. Ascend's VPRN—via both the MAX family of WAN Access Switches and the Pipeline family of remote access routers—adds QoS and SLA assurances to IP, and supports the leading tunneling technologies to give users complete freedom of choice:

- Point-to-Point Tunneling Protocol (PPTP), created in a strategic partnership between Ascend and Microsoft, and now a standard feature of Windows
- Layer-2 Tunneling Protocol (L2TP), an industry standard based on PPTP

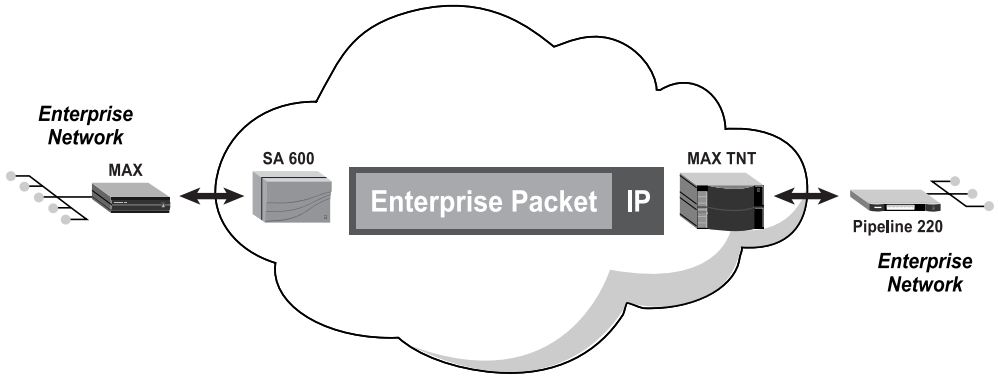


Figure 6 – Virtual Private Remote Networking with multiprotocol tunneling allows the Internet to be used for remote LAN access by client PCs.

Virtual Private Trunking (VPT)

VPT makes the powerful capabilities of Ascend's core Frame Relay and ATM multiservice switches (B-STDX, CBX 500 and GX 550) available directly to the enterprise VPN. VPT goes beyond traditional permanent and switched virtual circuits to provision trunk lines and/or bandwidth in a way that both optimizes resource utilization and guarantees performance. Dedicated bandwidth in the form of reserved lines or capacity might be used to link major enterprise facilities, while bandwidth on demand would more efficiently internetwork numerous branch offices. Ascend permits use of the full spectrum of underlying Frame Relay and ATM traffic profiles, with their respective price/performance attributes, for tuning VPN configurations to customer requirements. Organizations concerned about using the public network for private enterprise applications will find trunking's inherent security and performance particularly appealing.

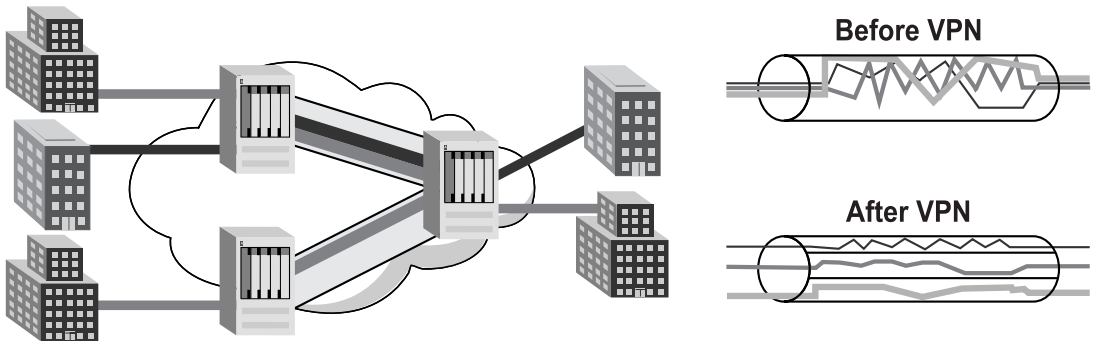


Figure 7 – Virtual Private Trunking makes the power of the public Frame Relay/ATM infrastructure available directly to the enterprise-wide virtual private network.

©1998 Ascend Communications, Inc.

Virtual IP Routing (VIPR)

VIPR extends private route tables and address spaces from the enterprise into the service provider's routing/switching infrastructure. Essentially, a virtual IP router is a logical partition of a physical IP router or switch in the infrastructure. Ascend offers VIPR via IP Navigator, which adds IP switching to Ascend's core Frame Relay and ATM multiservice switches, and soon in the MAX WAN Access Switch family. Of particular appeal to the enterprise is VIPR's ability to create individual broadcast domains and use private (unregistered) IP addresses, which are the norm in large organizations. Each virtual router is configured and managed like a physical router, with a separate and secure route table and closed user group, making VPN implementation and operation integrate seamlessly with existing systems and procedures. Ascend is unique in being able to deliver this additional level of privacy within the public network infrastructure. Finally, Ascend's virtual routers are able to dedicate physical network elements, such as WAN interfaces and bandwidth for QoS and SLA assurances, to a particular VPN, which is attractive to organizations with demanding applications.

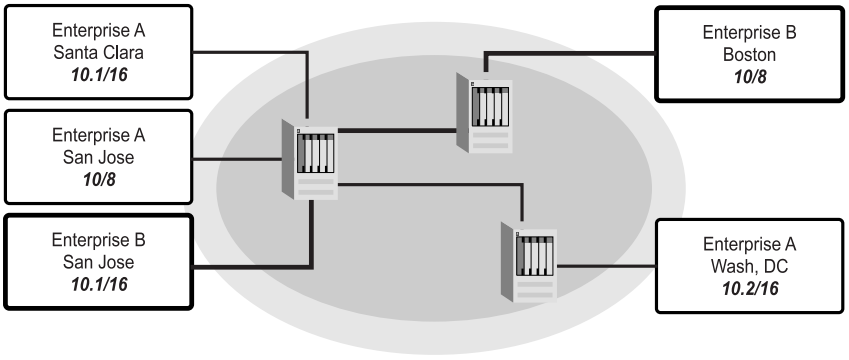


Figure 8 – Virtual IP Routing makes configuring and managing a VPN as straightforward as configuring and managing a router-based private network.

©1998 Ascend Communications, Inc.

Ascend's MultiVPN approach allows combinations and permutations of all three architectures in a single VPN. An enterprise-wide VPN, for example, might use VPRN tunneling for remote access by individual telecommuters, along with Virtual IP Routing to interconnect all multiuser sites. For sites that have NetWare servers with IPX, tunneling can be combined with Virtual IP Routing. Frame Relay and ATM trunks are more suitable for the largest sites in the enterprise, such as the headquarters and major divisions. The service provider will need to interface the various networks to one another, but having done so, the VPN operates transparently to all users and sites thereafter.

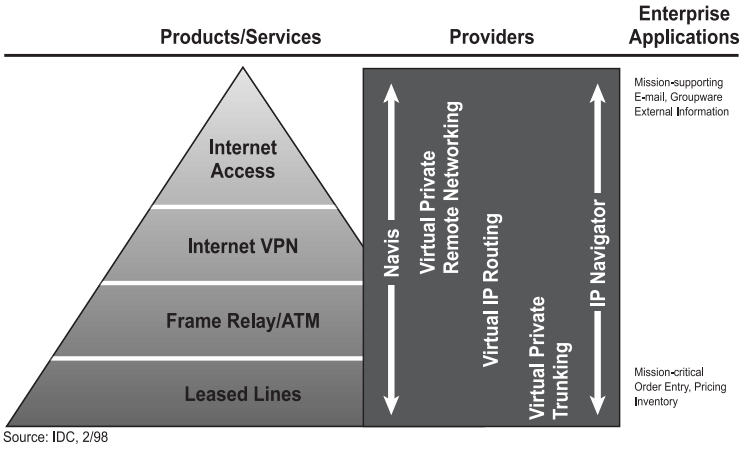


Figure 9 – Ascend's MultiVPN provides a continuum of service options across the full spectrum of enterprise networking applications.

©1998 Ascend Communications, Inc.



Where Network Solutions Never End™

Worldwide and North American Headquarters
Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
TEL: 510.769.6001
FAX: 510.747.2300
E-mail: info@ascend.com
Toll Free: 800.621.9578
FAX Server: 415.688.4343
Web Page: http://www.ascend.com

European Headquarters
Rudolph-Diesel-Strasse 16
D-64331 Weiterstadt
Germany
Tel: +49.6150.1094.10
Fax: +49.6150.1094.94

Asia-Pacific Headquarters
Suite 1908
Bank of America Tower
12 Harcourt Road
Hong Kong
Tel: +852.2844.7600
Fax: +852.2810.0298

Japan Headquarters
Level 19 Shinjuku Daiichi-Seimei Bldg.
2-7-1 Nishi-Shinjuku
Shinjuku-ku, Tokyo 163-07, Japan
Tel: +81.3.5325.7397
Fax: +81.3.5325.7399
Web Site: http://www.ascend.co.jp

Latin, South America and the Caribbean Headquarters
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, United States
TEL: 510.769.6001
FAX: 510.747.2300

Ascend and the Ascend logo are registered trademarks and all Ascend product names are trademarks of Ascend Communications, Inc. Other brand and product names are trademarks of their respective holders.

05-58
9/98

©1998 Ascend Communications, Inc.