RESOURCE GUIDE

Ascend

RESOURCE GUIDE

BUILDING THE ENTERPRISE
NETWORK OF THE FUTURE



ASCEND

Building the Enterprise Network of the Future

A Resource Guide for Information Technology and Network Managers



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.

Building the Enterprise Network of the Future

Table of Contents

1. Executive Summary 1

2. The Future of Enterprise Networking 4
- Today's "Typical" Enterprise-wide Network 4
- Circuit Switched LANs 5
- The Public Data Network-based Enterprise Network of the Future 6
- Three Steps to a PDN-based Enterprise 11

3. IP: The Strategic Protocol 12
- The IP Advantage 13
- The Virtual Private Network 15

4. IP Options for Non-IP Networks 18
  - IBM's SNA 18
  - Novell's NetWare 20
  - Windows NT 20
  - Other Non-IP Network Environments 20
- Private IP 20
- Scenarios for Today's Enterprise Networks 21
  - Scenario #1: A Large Manufacturer 21
  - Scenario #2: A Regional Consortium of Hospitals 22
  - Scenario #3: An Insurance Company 23
  - Scenario #4: A Small International Distributor 24
- Putting It All Together 25

5. "How-To" Checklists 26
- Network Management Tools Checklist 26
- Network Access Switch Checklist 27
- Remote Office Router Checklist 28
- SOHO Router Checklist 29
- Bandwidth Manager Checklist 30

Appendix 31
- Ascend Product Line Overview 31
- Additional Resources 32

© 1997 Ascend Communications, Inc.

1. Executive Summary

Change is not new to enterprise networks, which have evolved over the decades to accommodate new technologies, new applications and new Wide Area Network (WAN) services. By definition, a WAN is a communications network that connects geographically remote Local Area Networks over local and/or long distance telephone services. The enterprise network constitutes the nationwide or worldwide network connecting all of an organization's sites and users. But now, intranets and extranets are an integral part of the enterprise, even though "legacy" applications remain vital to running the business. Applications like e-mail and file transfer have become mission critical and have brought the WAN right to the end-user. Remote office personnel are dependent on distributed resources for their daily activities. Workers are untethered and mobile. Telecommuting is commonplace. Organizations are expanding and partnering internationally. Multimedia, collaborative work and other new forms of communications are imminent.

To meet these changing needs, a new model for enterprise networking is emerging. The new model recognizes that now is the time for organizations to:

- Benefit from the long-awaited single protocol enterprise backbone
- Make the WAN just as manageable as the LAN
- Take advantage of public data network services
- Integrate security into the basic network infrastructure
- Leverage the vast capabilities and worldwide presence of the Internet
- Step into the future of enterprise networking

New technologies and new WAN services have combined to create a major new opportunity for enterprise networks. To date, most corporations have down-played the WAN as an integral part of the enterprise, preferring instead to use it strictly for providing circuit switched connectivity between sites. But this use of the WAN imposes limitations while, at the same time, increases operational and management expenses.

With the advent of high-speed, public data networks in the wide area, corporations now have an alternative to complex and costly private circuit-switched networks. Public WANs can be seamlessly integrated into enterprise networks and this resource guide is intended to help organizations take advantage of this new and exciting opportunity.

The evolving model for enterprise networking is being driven by the Internet — an unparalleled phenomenon in the history of computer networking. Long the domain of academia and government agencies, the Internet has now been commandeered by businesses and homes around the globe. The World Wide Web makes the PC a portal to a wealth of information that would take several lifetimes to read, but only a few moments to search. In effect, the Internet is creating a "data dialtone" that permits connectivity anywhere, anytime, on demand. Organizations are now asking for a similar model for the enterprise network.

© 1997 Ascend Communications, Inc.

The Enterprise Network of the Future

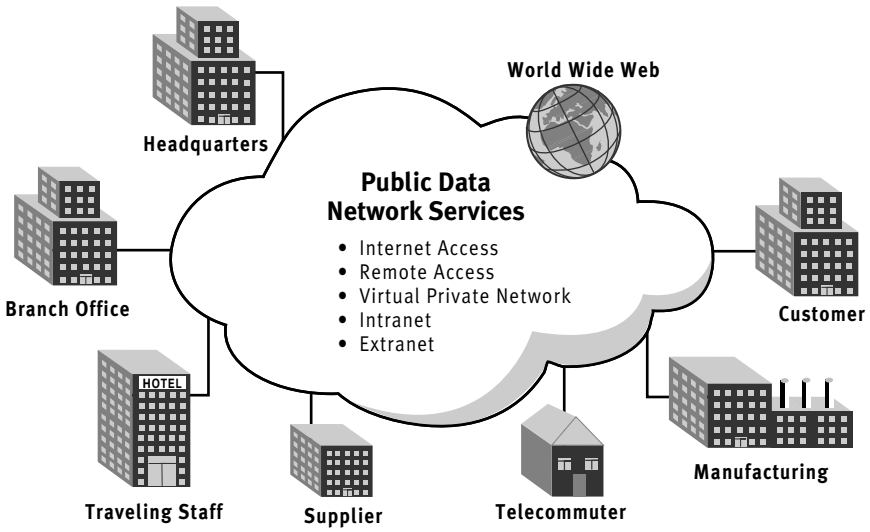


Figure 1 — The enterprise network of the future must be far more capable, flexible and affordable. The enterprise network of the future needs to leverage the public data services to meet the challenges that lie ahead.

However, the current infrastructure is inappropriate for the enormity of the Internet. With this model, data is transmitted over the voice-oriented Public Switched Telephone Network (PSTN), which simply cannot handle such huge volumes of data. Instead, organizations require a WAN optimized for high-speed data communications. The two most popular technologies for supporting these data rates are Frame Relay and Asynchronous Transfer Mode (ATM). Users can still access the Internet using PSTN-based services, but the Internet's backbone is built using high-speed, data-capable Frame Relay and ATM. Although these backbone technologies are not available everywhere, the Internet is the first worldwide, high-speed Public Data Network (PDN).

Consider the potential of using a PDN, rather than the PSTN, at the core of the enterprise network. There would be no more cross-country private lines to manage at the core. No more redundant mesh topologies to worry about. No more relentless reconfiguration of the point-to-point nature of the private network infrastructure. In its place will be a Virtual Private Network, or VPN. The VPN makes use of the Internet as the wide-area backbone. According to a study by Forrester Research, Internet-based VPNs offer a savings of up to 60% over equivalent private networks. And with this savings your organization has a worldwide enterprise network that is just as dependable and secure as before, plus is more capable and manageable with much greater flexibility.

Over time, there will be other PDN alternatives available worldwide. Frame Relay is fairly ubiquitous in the U.S. as is x25 in Europe, and ATM access is now being offered in many metropolitan areas. Eventually, this "New Public Network" infrastructure will give organizations a choice of local data dialtone options to the Internet or their own virtual private network. Then data networking will be just as convenient, dependable and affordable as voice networking has been for years.

© 1997 Ascend Communications, Inc.

This resource guide is designed to help any organization optimize its enterprise network using existing public data networking services and off-the-shelf technology. The material is suitable for chief information officers, vice-presidents of MIS, Information Technology (IT) managers and network managers. The content is organized into four remaining chapters. Chapter 2, *The Future of Enterprise Networking*, compares today's typical enterprise network with the enterprise network of the future. Chapter 3, *IP: The Strategic Protocol*, outlines the many enterprise capabilities and advantages of the Internet Protocol. Chapter 4, *IP Options for Non-IP Networks*, presents alternatives for adding IP compatibility to existing systems. The final chapter, Chapter 5, contains useful "*How-To Checklists*". There are also two appendices: *Additional Resources*, which lists relevant standards and other useful materials; and *Ascend Product Line Overview*, which provides an introduction to Ascend's enterprise networking product line.

© 1997 Ascend Communications, Inc.

2. The Future of Enterprise Networking

Enterprise networks are constantly changing, and many are about to undergo some long-awaited improvements as a new model of enterprise networking emerges. Before exploring the future, though, it is to helpful to take a look at the present: today's "typical" enterprise-wide network. Naturally, your organization's existing network will vary somewhat from the typical one portrayed here, but the fundamental structure should be familiar.

Today's "Typical" Enterprise-wide Network

Most enterprise networks today have a site-to-site or LAN-to-LAN orientation. The applications involve a mix of host/terminal and client/server traffic. Many protocols are used; the dominant ones are IBM's Systems Network Architecture (SNA), Novell's Internetwork Packet Exchange (IPX), NetBIOS/NetBEUI and, increasingly, the Internet Protocol (IP).

Because bandwidth in the LAN costs relatively little, the various protocols can operate quite affordably in parallel, even when on separate building or campus backbones. In the WAN, however, bandwidth is much more expensive.

The Public Switched Telephone Network (PSTN) — the most common WAN solution for today's enterprise networks — establishes end-to-end circuits. Circuits are used because they are the most efficient way to accommodate voice communications. For this reason, most organizations find it less expensive to use the PSTN for internal voice communications rather than keep this traffic load on the private enterprise network.

Data comes in packets and these packets must be mapped to the PSTN's circuits. In an effort to achieve more efficient use of circuits —and thereby help reduce the cost of operating enterprise networks — a variety of solutions now exist for integrating multiple protocols and/or applications. All make it possible to perpetuate parallel backbones across the WAN. The popular options include:

- Gateways that convert one protocol to another
- Encapsulation that embeds one protocol within another
- Multiprotocol routers or protocol-independent bridges
- Multiplexers that combine data streams from multiple routers and controllers
- Inverse multiplexers for achieving higher aggregate throughput, as well as for adding dial-up backup and overflow bandwidth

Already, many organizations have moved away from a purely PSTN-based WAN. An older packet-oriented public data network, X.25, has been used for years in predominantly

operate. While the PSTN's 56 and 64 Kbps channels are great for voice, they offer relatively low data bandwidth for the cost. Either packets of data traffic sit in a queue waiting to be sent or the PSTN circuit sits idle awaiting traffic. Second, the PSTN's circuit-oriented, point-to-point nature reduces the scalability and versatility of packet-oriented enterprise data networks. Frame Relay and ATM — any-to-any public data networks — do not suffer from this limitation.

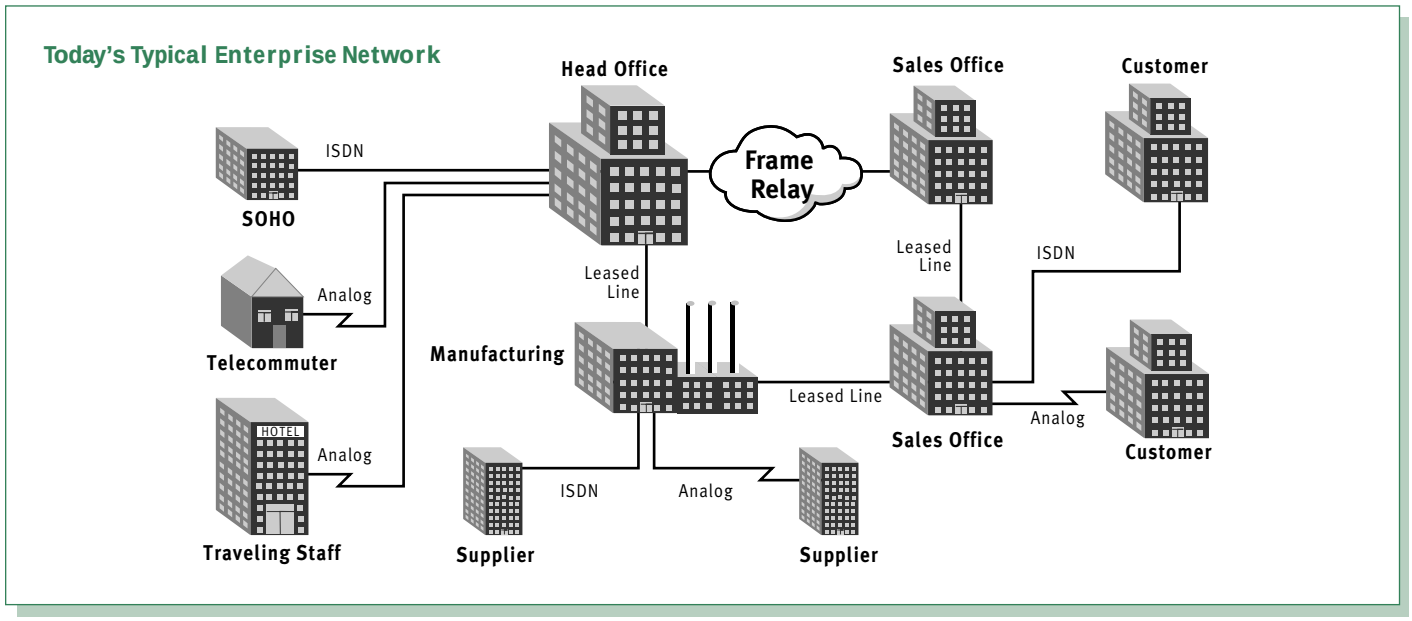


Figure 2 — Most of today's private enterprise networks employ the public voice network infrastructure for wide-area data communications.

Circuit-switched LANs

The biggest limitation of using circuit-switched WANs for data communications is effectively managing them end-to-end. LAN management tools cannot distinguish between analog and digital dial-up or T1 and Frame Relay. This means that the first two layers of the WAN — the physical and data link layers — are invisible. This might not be a problem if the carrier(s) provided the necessary management tools, but many do not. Fortunately, the PSTN is dependable. However, when something does go wrong, the network support staff is forced to operate partially or totally in the blind.

LAN tools can "isolate" a "problem" to a router across the WAN. The router can be reconfigured remotely, and the symptoms may go away. But how can you be certain that the problem was not in the carrier's network infrastructure all along? All the "fix" may have done was buy time for the carrier to detect and correct the real problem. And when the same "problem" occurs again, what "fix" is going to correct it — for real — this time?

Further complicating the enterprise network management effort is the presence of multiple protocols in the WAN backbone. The popular protocol integration techniques create an additional dimension of network complexity. The support staff must now maintain expertise in all of the individual protocols, as well as in the common equipment used for WAN integration. Of course, each element has its own LAN-oriented management system accompanied by a different set of conventions and tools, adding yet another layer of complexity to managing and securing the enterprise network.

© 1997 Ascend Communications, Inc.

Meanwhile, a number of business, technology and social trends have conspired to make the circuit-switched WAN model increasingly unsuitable for the future of enterprise networking (see sidebar titled **Driving Forces for a New Network Model**). The net result is a fundamental enterprise architecture that is expensive, inflexible and unmanageable. Users complain about the limitations. Executives sometimes question the very capabilities of the IT department. It seems that no one is genuinely satisfied with the current enterprise network model.

Driving Forces for a New Network Model

- ***Reliance on networked resources already make enterprise networks vital to daily business operations.*** *The ultimate goal of network-centric computing remains convergence on a strategic enterprise-wide protocol for maximum accessibility at minimal cost. Most organizations will achieve this goal by the year 2000.*
- ***The workforce will continue becoming increasingly dispersed and mobile.*** *For example, a single function can exist in multiple locations; such a "virtual department" is often used for call processing centers that interact with customers spread around the globe. There is also a growing need for flexible work-at-home arrangements for both part- and full-time telecommuters.*
- ***New applications will continue to emerge****, especially those involving bandwidth-intensive multimedia and collaborative work. And the combination of new and existing applications is applying pressure to unify and simplify the user interface for enhanced productivity.*
- ***Many mission-critical business applications will become dependent on the Internet.*** *Indeed, the ubiquity of the Internet and its IP-based applications create numerous opportunities for commercial users, such as promoting products and services, supporting customers and interacting with suppliers.*
- ***The escalating costs of operating and managing PSTN-based private networks****, especially with the relentless need for more bandwidth by more users around the globe, will lead many organizations to use VPNs that carry internal data traffic via the Internet or other public data network.*
- ***Deregulation will lead to partnerships between Internet Service Providers (ISPs) and carriers*** *for re-engineering public networks to handle voice, video and data traffic more efficiently and economically. Relationships between equipment vendors and service providers will afford additional cost-saving opportunities. New forms of access, including Frame Relay, ATM and Digital Subscriber Lines (xDSL), will emerge to leverage the new public network infrastructure.*

The Public Data Network-based Enterprise Network of the Future

What if you could design your organization's enterprise network from scratch? Imagine having no existing network infrastructure that requires "backwards compatibility" and no externally-imposed restrictions or limitations. You would enjoy total freedom to design the perfect enterprise network.

Of course, no IT manager has the luxury of creating an entire network from scratch. But all regularly evolve their networks toward something better and every such endeavor should be guided by a clear vision. Evolution in affordable and manageable steps, guided by the vision, can carry the organization toward and ultimately to the enterprise network of the future.

© 1997 Ascend Communications, Inc.

The Enterprise Network of the Future

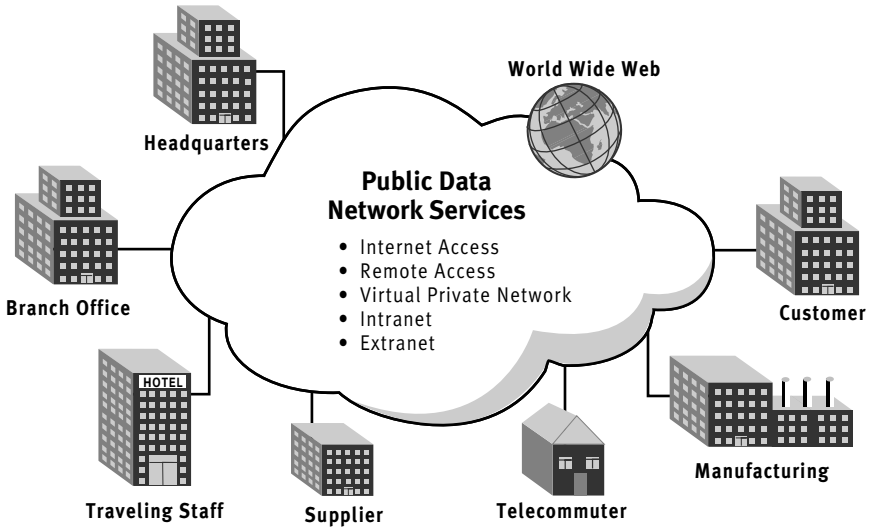


Figure 3 — The enterprise network of the future will use PDNs, just as voice communications (not shown) use the Public Switched Telephone Network today. Organizations will achieve a manageable, dependable, flexible and secure solution at a fraction of the cost of maintaining a private network.

The distinguishing characteristic of the enterprise network of the future is its use of *PDN* services which makes it a *VPN*. These two terms warrant definition. A PDN is a data-oriented WAN operated by network service providers, such as Internet Service Providers and telecommunications carriers. As a packet-based, frame-based or cell-based network, the PDN WAN is optimal for data communications. A VPN (or as some call it, a Virtual Private Data Network) is a private network that uses PDN services, in whole or in part (see sidebar titled **VPNs** for a more thorough explanation). Together, the PDN and VPN create a new model for enterprise networks.

PDN-based enterprise VPNs provide two important advantages. First, the PDN is designed and built for data, rather than for voice, and is therefore more efficient and affordable. Second, being network service provider-operated, the PDN provides maximum dependability and flexibility — also at minimal cost — just as today's PSTN does for voice communications. All sites and users access the PDN with an inexpensive local fixed or switched service, possibly via the PSTN. Bandwidth through the backbone is generous and can easily and dynamically be added or redirected on demand. Industry analysts estimate that these as well as other PDN-related advantages enable VPNs to offer savings of up to 60% over equivalent PSTN-based private networks.

© 1997 Ascend Communications, Inc.

Virtual Private Networks

- *A private network, or a segment of it, that uses Public Data Network (PDN) services for internal communications is considered a Virtual Private Network, or VPN. Because the organization shares the PDN infrastructure with others, the network is not truly private. But because all users enjoy reliable and secure communications at desired levels of performance, the network is virtually private — hence the phrase Virtual Private Network.*
- *Companies will use PDN-based VPNs for data communications for the same reasons they use the PSTN for most voice, fax and video communications: it costs less. "Renting" data bandwidth in a data-optimized PDN is more flexible and cost-effective than "building" it in the voice-oriented PSTN. Flexibility and affordability are the two most important advantages cited by IT managers of Virtual Private Network. According to a study by Forrester Research, VPNs offer a savings of up to 60% over equivalent private networks.*
- *Today, the Internet is the most widely accessible high-speed public data network suitable for enterprise VPNs. It is important to note that access to the Internet PDN is, at least for now, normally via the PSTN; for example, an ISDN or T1/E1 line to an Internet Service Provider's point of presence. Over time, there will be less dependence on the PSTN at the edge, and more PDN options — particularly Frame Relay and ATM — will become available directly worldwide.*
- *Once the PSTN also converts to ATM in its backbone, voice and data may once again share the same public network infrastructure — the New Public Network — but this time with a technology that was conceived for this purpose.*

The enterprise network of the future has a few other notable characteristics:

- It is designed end-to-end for data communications, which improves LAN/WAN synergy for nearly seamless integration.
- Despite many predictions of the demise of the mainframe, it continues to handle a mix of host/terminal and client/server applications.
- It supports IP and the Internet, which provides a substantial price/performance advantage (see sidebar titled **Advantages of a Single Protocol Enterprise Backbone**). The Internet Protocol can become a common denominator among all internal sites and users on an intranet, as well as all customers, suppliers and business partners on extranets. Even though the enterprise backbone is IP, techniques are available that let existing applications use other protocols, such as IPX, NetBIOS/NetBEUI and SNA.
- Access at the very edge of the network offers compatibility with the full spectrum of existing PSTN and new data-oriented WAN options. The PSTN and PDN can even work together. For example, using ISDN (a PSTN service) to access a Frame Relay network or the Internet.
- High-speed channelized digital links from major sites to the WAN, whether using the PSTN or a PDN, eliminate the need to use troublesome modem banks for providing dial-in access.

© 1997 Ascend Communications, Inc.

Advantages of a Single Protocol Enterprise Backbone

- ***Dramatically simplifies enterprise-wide management and support****, which lowers the cost of operations and improves overall network up-time. Keeping current with one protocol is challenging enough; maintaining genuine expertise for several is very difficult — and expensive.*
- ***Saves additional money through economies of scale*** *that can consolidate or eliminate some equipment and WAN lines.*
- ***Facilitates more comprehensive security provisions*** *to protect internal resources.*
- ***Enhances overall flexibility and scalability*** *to accommodate change and growth more cost-effectively.*
- ***Permits all applications to share a common programming interface****, simplifying design, development and deployment.*
- ***Improves user productivity*** *with seamless access to both internal (intranet) and external (Internet and extranet) resources when IP is the single protocol.*

Another significant advantage of the enterprise network of the future is that the transition involves manageable and affordable steps that present little risk. This is possible for several reasons:

- It employs only proven, off-the-shelf technologies. The new enterprise network requires no major breakthroughs or revolutionary new technology for you.
- It protects investment by building on existing systems and applications.
- It accommodates parallel networks during the transition from the multi-protocol LAN backbone to a single protocol WAN backbone. For example, existing leased lines can carry an increasing percentage of IP traffic until the 100% cut-over point is reached, at which time the Internet could be considered for use as a PDN.
- It supports both major WAN alternatives: the PSTN and the PDN.
- It permits any combination of private network and virtual private network segments in the end-to-end enterprise. For example, by leveraging the Internet's ubiquitous presence, new sites can be added as members of an Internet-based VPN subnetwork that is part of the overall enterprise network.
- It allows LANs to remain heterogeneous. Because achieving the backbone-oriented benefits involve changes only in the WAN, there is no need to do anything with the multitude of client users. For example, most network operating system (NOS) applications, such as sharing files and printers, do not really require the sophistication of TCP/IP. To link local users to the enterprise back bone, the two most popular NOSs, NetWare and Windows NT, are available with special gateway software.

Perhaps the most significant advantage of the Public Data Network-based enterprise network of the future is its substantially lower cost of ownership. Nearly 80% of the cost of operating today's enterprise network involves administrative and WAN charges, according to the *Cost of Remote Network Ownership* study published by Strategic Networks Consulting. The PDN-based enterprise network of the future addresses both areas with a VPN-oriented architecture that can take advantage of more affordable PDN services. Consolidating protocols onto a purely IP backbone also reduces administrative costs and permits use of the worldwide Internet as the PDN.

© 1997 Ascend Communications, Inc.

Today's Network Costs

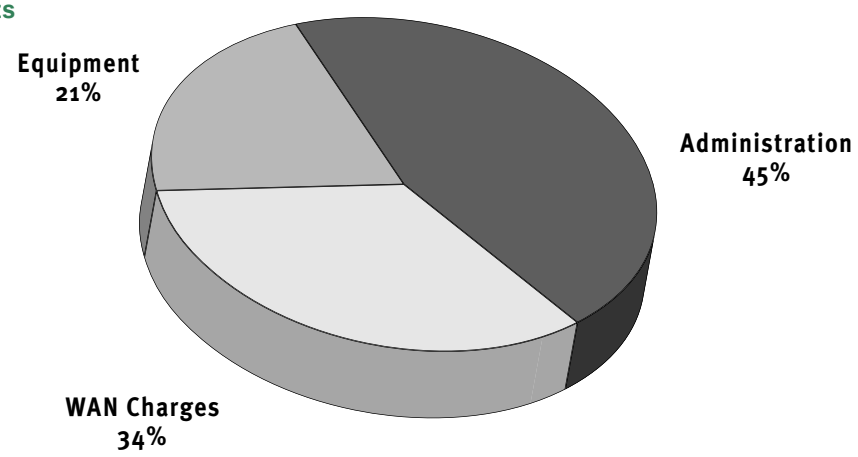


Figure 4 — The PDN-based enterprise network of the future offers substantial savings by focusing on the two principal costs that consume today's networking budgets: administration and WAN charges.

Typical vs. Future Enterprise Network

The following table summarizes the major differences between today's typical enterprise network and the enterprise network of the future.

	Today's Typical Enterprise Network	The Enterprise Network of the Future
Model	Circuit-switched-based	Public Data Network-based
Architecture	Private network based on PSTN WAN services	Virtual Private Network
Manageability	Complex, lacking necessary tools	Substantially simplified
Availability	Very good, but inflexible	Very good, very flexible
Performance	Satisfactory, but at a premium price	Bandwidth used and paid for on demand
Internet integration	Separate connection(s)	Inherent
Connectivity	Internal only — external via the Internet or separate links	Both internal (intranet) and external (Internet, extranet)
Security	Excellent with minimal provisions (authentication and authorization)	Excellent with appropriate provisions (IPSec and firewalls)
Scalability	Limited — PSTN's circuit-orientation complicates expansion	Highly scalable — data-oriented PDN services scale readily and affordably
Overall cost of ownership	Expensive to build and operate	Potential savings of up to 60% over equivalent private network

© 1997 Ascend Communications, Inc.

Three Steps to a PDN-based Enterprise

To go from today's typical circuit-switched-based enterprise to the PDN-based enterprise network of the future involves three basic steps. In order of importance, they are:

- **Convergence on a single protocol as soon as practical.** Chapter 3 analyzes why IP should be that single protocol; Chapter 4 outlines many of the IP options now available for enterprise systems and networks.
- **Use of only WAN-manageable solutions.** (Chapter 5 contains checklists of what to look for in a network management system, along with several other checklists highlighting desirable features for different types of network access systems).
- **Use of public data networks.** PDNs reduce costs and increase manageability by minimizing network complexity. The *Virtual Private Network* section in Chapter 3 discusses using the Internet as a PDN.

Taking any of these steps is bound to strengthen your enterprise network; taking all three brings your enterprise network into the future.

© 1997 Ascend Communications, Inc.

3. IP: The Strategic Protocol

IT managers have long been unanimous in their belief that having a single protocol is the best way to operate an enterprise network. Now the question is: which protocol, as well as when and how to implement it? The first question is now easily answered: the best enterprise protocol is IP, the Internet Protocol.

IP has been a contender for the sole enterprise protocol for over 10 years, but recent events have made it the compelling choice. The most significant of these events is the unprecedented popularity of the Internet, particularly its World Wide Web browser application. The next most powerful "vote of confidence" has been the widespread adoption of intranets, which are private enterprise Internet applications. Similarly, extranets, or private Internet applications between organizations, have just recently become the de facto standard for inter-enterprise communications.

IP moved irrevocably to preferred protocol status when both IBM and Novell embraced it. IBM now has solid TCP/IP stacks and applications across its entire line of computers. According to IBM's own estimates, over half of all mainframe and midrange shops use TCP/IP in the data center alongside SNA and APPN, and most hosts now ship with TCP/IP capabilities. Novell has also made a strong commitment to TCP/IP with its IntranetWare offering and plans to integrate the protocol with standard NetWare.

Forrester Research estimates that TCP/IP is already the dominant protocol, accounting for more than half of all traffic, in over one-third of Fortune 1000 companies. By 1999, Forrester believes TCP/IP will be dominant at some 80% of the Fortune 1000. IP is so clearly destined for pervasiveness in the enterprise, that IT managers may as well consider it the "Inevitable Protocol." With such overwhelming support for IP, there are no longer any major obstacles to realizing the many benefits of a single-protocol enterprise backbone.

Potential Internet Applications for Businesses

Is your organization using the Internet only for Web-based marketing? If so, consider just a few of the Internet's other potential enterprise applications:

- *Supporting customers via the Web*
- *Exchanging internal and external e-mail*
- *Performing market and engineering research*
- *Receiving news and other timely information*
- *Training and distance-learning with IP multicast*
- *Sending faxes long distance and internationally with local calls*
- *Buying and selling products with new forms of electronic commerce or conventional Electronic Document Interchange (EDI) technology*
- *Multicast collaboration with strategic partners and outside project teams*
- *Implementing an Internet-based virtual private intranet or extranet*

© 1997 Ascend Communications, Inc.

The IP Advantage

TCP/IP was designed for large-scale networking. Indeed, it was conceived with the potential to network the world and is well on its way to achieving that goal. As a result, the protocol satisfies the demanding needs of enterprise networks. TCP/IP and its comprehensive array of client/server and host/terminal applications are:

- **Fully open and standards-based**, providing the best available multivendor interoperability in the industry
- **Supported on virtually all platforms**, creating a common denominator across systems ranging in size from the PC to the mainframe
- **Proven in large networks**, including the Internet, the world's largest network
- **Affordable**, often bundled at no charge with the operating system

Familiarity with TCP/IP is exceptionally high, as well. It seems that almost everyone, including users and support personnel, understand TCP/IP. Most of the support staff, trained in universities on the protocol, are quite proficient with it. Training resources, including books, classes and articles are widespread and affordable, even over the Internet itself. And additional expertise, from ISPs, consultants and integrators, is readily available.

Support personnel also appreciate TCP/IP's comprehensive management and security options:

- Industry standard protocols, applications, Management Information Bases (MIBs) and agents
- Simple Network Management Protocol (SNMP) agents are available on virtually every end node and network node
- Familiar user-friendly console applications, including those that either now or will use a Web browser interface
- Remote Authentication Dial-In User Service (RADIUS) database for maintaining authentication, authorization and accounting information on network users
- Dynamic stateful firewall protection, often available as an integrated option for network access equipment
- IPSec encryption

© 1997 Ascend Communications, Inc.

IPSec Encryption

The IP Security series of standards (RFCs 1825-1829), or simply IPSec, provides data authentication, integrity and confidentiality to protect information transmitted in a private or Virtual Private Network. There are two aspects to IPSec: the Authentication Header (AH) and the Encapsulating Security Payload (ESP), which can be employed individually or in combination. AH adds a digital signature to the header using the Message Digest (MD) or the Secure Hash Algorithm (SHA). AH authenticates the packet and assures data integrity by enabling detection of any alteration during transmission. ESP encrypts and de-encrypts either the data or the entire packet using the Data Encryption Standard (DES) or Triple DES (3DES). ESP keeps transmitted data strictly confidential, and can provide adequate user authentication and data integrity for most applications. Both AH and ESP employ digital "keys" at each end of the connection. AH key lengths range from 128 bits (MD5) to 160 bits (SHA-1); ESP key lengths range from 56 bits (DES) to 168 bits (3DES). Both sets are administered using Oakley to generate keys and the Internet Security Association Key Management Protocol to exchange keys, which together are referred to as ISAKMP/Oakley, or more simply, the Internet Key Management Protocol (IKMP).

While TCP/IP is eminently qualified for enterprise networks today, it is constantly being enhanced. Many imminent applications and capabilities will further accelerate the adoption of IP by businesses, both large and small. Here is just a sampling of some of the more promising enhancements coming soon:

- IP multicast for collaborative work and other applications: Microsoft's NetMeeting and Netscape's LiveMedia offer both document sharing and full videoconferencing capabilities; additional applications for multicast include distance-learning and audio/visual "broadcasts"
- IP telephony and multimedia applications for voice/video mail, or "v-mail" as well as for real-time conversations; gateways are also planned for interfacing IP-based networks to the PSTN
- Electronic commerce for selling and purchasing products and services on-line
- Internet faxing to supplement and eventually replace PSTN-based faxing. Users will be able to send faxes long distance, even internationally, with a local connection to the Internet
- Quality of Service (QoS) to guarantee priority and minimum delay to business-critical applications
- Mobile IP for traveling workers, including support for cellular access
- Next-generation IPV6 (version 6) that eliminates the address limitations of IPV4 among other enhancements

IP Multicast

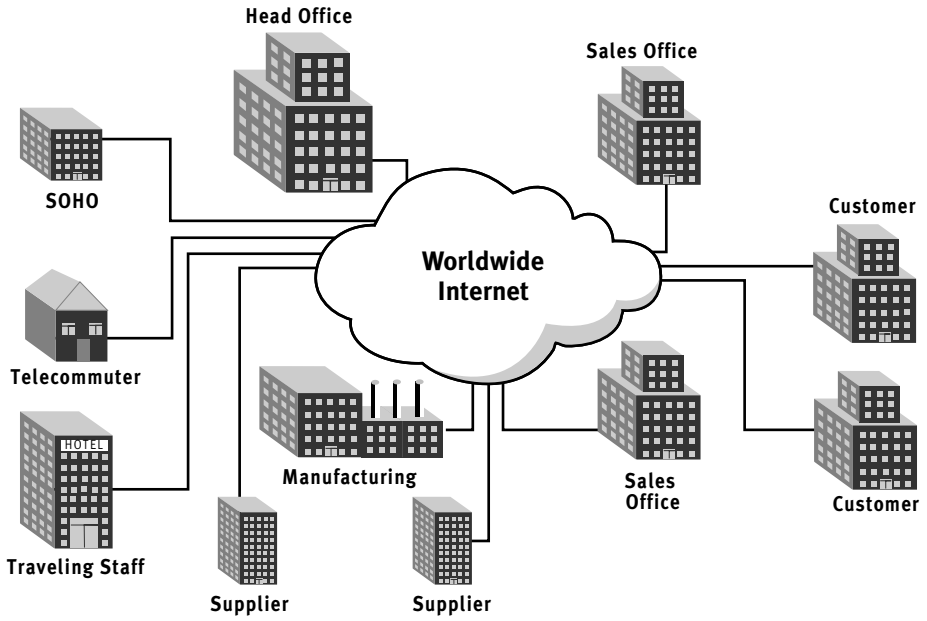
Multicast capabilities will dramatically expand the applications potential of an IP-based enterprise network. IP multicast employs the equivalent of "group addresses" administered by the Internet Group Management Protocol (IGMP). Users wanting to participate in a multicast session register with the nearest multicast-capable router as a member of that session. The router then directs the multicast traffic to the unique IP address(es) of its member participant(s). These "edge" routers must, in turn, register with other routers all the way back to the multicast source using either the Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM). DVMRP and PIM allow multicast traffic to reach all participants without duplication of packets on the mesh topology of an IP backbone. The optimal way to handle IP multicast in the global Internet is a topic of intense scrutiny at this time. The Internet's Multicast Backbone (MBone) has proven itself quite capable, but currently only covers a portion of the world.

© 1997 Ascend Communications, Inc.

The Virtual Private Network

VPNs based on public data network services offer such substantial advantages (see sidebar titled **VPN Benefits**), that they are the next logical step in the evolution of enterprise networking. This section describes a VPN that uses the Internet as its PDN. ATM or Frame Relay could also be used, but the Internet is the only *worldwide, high-speed* PDN today (many network service providers use Frame Relay and ATM as part of their network to deliver Internet services). The Internet may be the perfect PDN for a VPN, but there is a catch: the Internet employs the Internet Protocol exclusively. Its global infrastructure cannot carry native SNA, IPX, NetBIOS/NetBEUI or any other non-IP protocol directly. But it can carry all of this traffic — and more — through a variety of other means covered in the next chapter: *IP Options for Non-IP Networks*.

Internet-based VPN



The primary concern of IT managers regarding Internet-based VPNs involves security. Organizations have become accustomed to the inherent privacy afforded by PSTN-based private networks, and may consider the Internet to be "too" public for internal communications. To put the "private" in Virtual Private Networks, a wide variety of security provisions are available that make the Internet even more secure than the PSTN. Working with your Internet Service Provider(s), you can choose the level of protection you need from the following options (relevant standards, where applicable, are listed):

- **User authentication** affords the minimum level of protection (Password Authorization Protocol and Challenge Handshake Authentication Protocol)
- **Token cards** offer virtually "bulletproof" authentication with single-use passwords

© 1997 Ascend Communications, Inc.

- **Authorization** grants authenticated users permitted access only (RADIUS)
- **Packet authentication** adds data integrity (IPSec's Authentication Header)
- **Encryption** keeps data strictly confidential during transit through the Internet (IPSec's Encapsulating Security Payload)
- **Network Address Translation** and encrypted tunneling prevent internal client, server and host addresses from being "discovered" on the Internet
- **Firewalls** isolate private resources from public ones, such as an organization's World-Wide Web server

VPN Benefits

Organizations with VPNs are able to save up to 60% over equivalent private networks, according to a study by Forrester Research. VPNs save money because they:

- *Eliminate long-distance leased lines among major facilities, including those needed for alternate "mesh" paths*
- *Eliminate long-distance, switched calls via the PSTN for analog modems and ISDN access equipment*
- *Allow companies to pay only for actual usage with no idle line capacity*
- *Require less equipment. A single solution provides both Internet and VPN access, eliminating the need for separate modem banks, terminal adapters, remote access servers, and so on. The consolidation also permits utilization of cost-effective, high-speed trunk lines.*
- *Minimize end-user network design and management responsibilities*

VPNs leverage the Internet infrastructure's power to provide a more capable and dependable alternative to private networks:

- *ISPs in nearly every city create a worldwide presence*
- *Mesh redundancy and fault tolerance afford end-to-end reliability*
- *User familiarity simplifies training needs*

The Internet's ubiquity also makes VPNs more flexible than private networks. With VPNs, end-user organizations can:

- *Add and delete connections instantaneously*
- *Provide permanent, periodic or temporary connectivity as needed*
- *Integrate third-party users, such as customers and suppliers, almost effortlessly*
- *Select optimal data rates ranging from analog modem to T1/E1 speeds and beyond with Digital Subscriber Line technology*

Because VPNs offer a more affordable, capable, dependable and flexible alternative to private networks, nearly all organizations surveyed by the International Data Corporation and other industry analysts have plans to leverage the Internet for internal data networking needs. VPNs are indeed the next step in business communications.

© 1997 Ascend Communications, Inc.

Another concern about Internet-based VPNs for mission-critical business applications derives mostly from some misconceptions regarding the Internet's availability. Availability encompasses both up-time and throughput, and private networks offer assured levels of service in both dimensions. The Internet offers few guarantees today. But despite the occasional *local* outage hyped in headlines, the Internet is actually *more* dependable than most private networks. This is because the Internet has substantial end-to-end redundancy and resiliency. Its elaborate design, which would be prohibitively expensive in private networks, serves to prevent Internet-wide catastrophes. If there is any short-term trade-off with an Internet-based VPN, it is throughput, not up-time. Although QoS will not be available worldwide for another few years, most larger ISPs can deliver service level assurances today over Frame Relay or ATM segments of their backbone.

Already, nearly three-fourths of IT managers surveyed in a Forrester Research study have overcome their security and availability concerns sufficiently to respond favorably to the question: Could the Internet replace other WAN technologies? Just as IP is inevitable, so too are PDN-based VPNs. Today's Internet is suitable for intranets, extranets and even some "legacy" applications (see sidebar titled **Identifying VPN Candidates**). Frame Relay and ATM are also available now in many parts of the world. Whatever PDN option(s) you choose, now is the time to start planning your own VPN. (For detailed information about VPNs, consult Ascend's resource guide: *The Virtual Private Network*.)

Identifying VPN Candidates

VPNs are suitable for a wide range of commercial data networking needs. An Internet-based VPN can:

- *Replace existing private network segments or subnets*
- *Supplement private networks by offloading certain applications or meeting backup/overflow needs*
- *Handle new applications without disturbing the existing private network*
- *Add new locations, especially international sites*

Conditions that favor use of a VPN:

- *Numerous locations, including both individual users and remote office sites*
- *Widespread users/sites involving long distances, especially worldwide locations*

Four applications — remote access, enterprise-wide intranets, extranets and multicast-based collaborative work—are particularly well-suited for Internet-based VPNs. Each provides both Internet and VPN access, and can be implemented as a small "pilot" or trial application to gain experience and confidence. Others, such as SNA and combined voice/data networks may need the sophistication of Frame Relay and/or ATM.

© 1997 Ascend Communications, Inc.

4. IP Options for Non-IP Networks

Having decided to migrate to a purely IP enterprise backbone, the next step is to determine how. The challenge here is finding a solution. Rather, the challenge is selecting the best option from among the myriad available. Often the choice is clear; sometimes a more in-depth evaluation is required.

Whatever protocol(s) your organization now uses, there are numerous alternatives available for providing enterprise compatibility with the Internet Protocol. In general, the choices include:

- **TCP/IP protocol stacks** to complement or displace the existing one(s) in servers and host systems or their front-ends
- **IP gateways** that convert other protocols to IP dynamically (see sidebar titled **IP Gateways**)
- **Tunneling and encapsulation techniques** that "wrap" another protocol's packets in IP packets (see sidebar titled **IP Tunneling**)

It is important to note that IP compatibility is only required in the enterprise backbone.

This chapter outlines specific ways of providing enterprise IP compatibility for the three most popular networking environments — IBM's SNA, Novell's NetWare and Microsoft's Windows NT — and presents options for other non-IP applications, as well as for converting private IP address schemes to standard Internet addresses. Midrange systems from Hewlett-Packard, Digital Equipment and other vendors, whether running UNIX or the vendor's proprietary operating system, are not addressed here because nearly all now support TCP/IP directly and fully.

IBM's SNA

IBM's Systems Network Architecture (SNA) utilizes LU 6.2 as its primary protocol, but also encompasses APPN/APPC (Advanced Peer-to-Peer Networking/Communications), NetBIOS and other protocols. The full spectrum of IP compatibility options is available from IBM and, owing to IBM's dominance in enterprise networking, from numerous third-party suppliers as well.

The option with the best long-term gain is simply to use TCP/IP for all IBM host/host and client/server communications. Such a seemingly radical change is now not only possible, it is quite viable. IBM's TCP/IP stacks are robust and compatible with the free suite of host systems software: CICS, VTAM, APPC, IMS, DB2 and so on. IBM's host-based IP applications are equally robust. IBM's comprehensive offering allows companies to be part of the IP revolution and to provide solid solutions to penetrate this UNIX-dominated market. IBM's midrange and mainframe systems make excellent servers with their high capacity, reliability, security and integrity.

IP Gateways

IP gateways work by translating another protocol to IP and vice versa. Normally, an IP gateway supports the clients assigned to a particular server, but one gateway can support several servers' clients. The server has a Network Operating System (NOS) with a "native" protocol. The gateway software converts traffic to/from the native protocol from/to IP. For example, Novell NetWare clients running browser-like applications on Novell's IPX protocol can access Web servers on the Internet via one of the many gateways available. IP gateways used for Internet access can be used without modification for Internet-based VPNs.

© 1997 Ascend Communications, Inc.

Here is just a partial listing of IBM's current TCP/IP offerings:

- TCP/IP protocol stacks for AS/400 and S/390 systems. The stack is included with OS/400, and available as an add-on for MVS and VM. Newer mainframes have a built-in Open Systems Adapter that also supports TCP/IP.
- Full TCP/IP support for IBM's 37XX communications controllers.
- IBM's AnyNet offering, based on the MultiProtocol Transport Networking (MPTN) architecture, makes applications independent of the underlying protocol stack. MPTN is the foundation for IBM's Networking Blueprint. For example, AnyNet allows APPC to run over IP and is available for MVS, OS/400, AIX, OS/2 and Windows.
- TN3270 and TN5250 for telnet-based workstation/PC terminal emulation.
- IBM's establishment controllers can route IP traffic for LAN-attached devices.
- Web server and Web gateway software for AS/400 and S/390 systems. A number of choices exist for mainframes: OS/390 Internet BonusPak for MVS, Internet Connect Server, Webshare for VM and a variety of CICS gateways.

Tunneling

Tunneling, also called encapsulation, works by wrapping one protocol's packet entirely within another. For example, a Novell NetWare user may want to access a server across the enterprise IP backbone. The router at the user's end places the NetWare IPX packet in an IP packet with its own address as the source and the address of the router at the other end as the destination. The remote router receives the IP packet — perhaps after it traverses several other routers and switches — strips off the IP header, and delivers the original IPX packet to the attached LAN. Tunneling can be used for all popular non-IP protocols, as well as to make private IP address schemes operate over the Internet.

For organizations that prefer to postpone wholesale conversion to TCP/IP, gateways offer the next best option. Properly deployed, gateways can confine SNA traffic to the data center. Gateway products available from IBM include the 3172 Interconnect Controller, along with the AnyNet SNA over TCP/IP Gateway for both OS/2 and MVS. Gateways are a cost-effective solution for users that interact occasionally with host systems. If PC users run a variety of TCP/IP applications regularly, the direct telnet options may make more sense. Gateways have the additional advantage of using only a single IP address for all local clients.

Another option involves use of encapsulation and tunneling techniques. There are three choices available: Data Link Switching (DLSw), GRE tunneling for LU 6.2 and APPC and the Point-to-Point Tunneling Protocol (PPTP) for NetBIOS. DLSw, invented by IBM and now an Internet standard (RFC 1795), encapsulates Logical Link Control Type 2 (LLC2) frames carrying LU 6.2, APPN and NetBIOS traffic in IP packets. DLSw is supported in IBM's 22XX series Nways routers, 37XX communications controllers and a variety of third-party offerings. GRE, an Internet standard (RFCs 1701/1702), is supported on many IP edge devices. PPTP, invented jointly by Microsoft and Ascend, supports NetBIOS and certain non-IBM protocols. PPTP's successor, the Layer-2 Tunneling Protocol (L2TP), is scheduled to become an RFC standard, as well.

© 1997 Ascend Communications, Inc.

Novell's NetWare

All three options — TCP/IP stacks, gateways and tunneling — are available for NetWare environments. Native TCP/IP protocol stacks are supported for IntranetWare clients now and are planned for regular NetWare clients. For organizations that prefer IPX in the local environment, Novell offers server-based IP gateway software. Finally, PPTP (and soon L2TP) tunneling can be used to carry IPX packets across the IP-based enterprise backbone.

Windows NT

With Microsoft's support of TCP/IP in both the NT server and all Windows clients, native IP is the logical choice. For organizations that still want to use NetBIOS/NetBEUI, server-based IP gateways and/or PPTP/L2TP tunneling software can be used for enterprise IP backbone compatibility.

Other Non-IP Network Environments

There are many other LAN protocols still in use such as XNS, OSI and DECnet/LAT. However, the best long-term solution is to convert the applications to native TCP/IP if possible. Another choice is to use protocol-independent bridging at the edge of the enterprise backbone. Bridging, however, has major drawbacks and should only be used as a last resort.

Private IP Networks

Many organizations that use IP have "private" IP addresses. The reason is simple: obtaining a block of official Internet addresses large enough to facilitate subnetting is nearly impossible. Subnets simplify address administration and router/switch management, but "waste" precious addresses.

This practice is so common that a standard was published (RFC 1597) to set aside or sanction certain IP addresses for private use. Three such address blocks, or subnets, are available to suit an organization of any size:

- *10.0.0.0 - 10.255.255.255 (24 bits for nearly 17 million addresses)*
- *172.16.0.0 - 172.31.255.255 (20 bits for approximately 1 million addresses)*
- *192.168.0.0 - 192.168.255.255 (16 bits for slightly over 65,000 addresses)*

Routers in the Internet block these sanctioned private IP addresses to avoid any ambiguity among private networks. Note that private IP address schemes that do not *use the sanctioned private subnets must be administered carefully with similar blocking or filtering techniques. If two nodes have the identical address (one official, one not), serious problems can result for both users.*

The next generation IP (IPng, which is also called version 6 or IPv6) will eliminate the need for private address schemes. IPv6 quadruples the current 32-bit address space. Even with waste from rampant subnetting, 128 bits is generous enough to yield about 50,000 registered IP addresses for every square meter of land on Earth!

Private IP

Many organizations have already selected TCP/IP as their strategic protocol and implemented it throughout the enterprise. The problem is, owing to the shortage of official or registered IP addresses, some of these private networks are incompatible with the Internet's addressing scheme (see sidebar titled **Private IP Networks**). Organizations with such "private IP" networks have two choices; each option requires obtaining a sufficiently large block of Internet addresses:

© 1997 Ascend Communications, Inc.

- Assign addresses *dynamically* using the Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT) or tunneling (PPTP/L2TP, GRE or Mobile IP). The idea here is to share a small block of registered addresses among only those sessions that require access to the Internet or Internet-based VPN. With dynamic addressing, a client host is assigned a registered IP address to replace, translate or tunnel its regular private IP address temporarily. With translation, a registered IP address is substituted for the private IP address. With tunneling, the original private IP packet is encapsulated in another IP packet that uses a registered Internet address. Both translation and encrypted tunneling also serve to shield internal addresses from public view in the Internet.
- Convert all hosts, both clients and servers, *permanently* to registered Internet addresses. This undertaking is less daunting of a task than it might at first appear to be. Nevertheless, many organizations may be better served by waiting for IPV6. IPV6 has a generous 128-bit address space, which will make it easy to obtain address blocks large enough for subnetting purposes.

Scenarios for Today's Enterprise Networks

The following four scenarios demonstrate the flexibility provided by the various IP compatibility options. Each also shows a different level of commitment to the Internet Protocol. One of these scenarios may be appropriate for your organization.

Scenario #1: A Large Manufacturer

This large manufacturer has mainframes at the headquarters and each of several plants, along with Windows NT servers at all sites. Because the network still contains thousands of older terminals for both engineering and business applications, migrating to a purely IP backbone presented too long a payback for senior management approval. The vice-president of MIS decided to link all sites with a Frame Relay network that integrates all SNA and IP traffic (RFC 1490). All client PCs are equipped with TCP/IP; an SNA gateway that runs on select IP-based NT servers provides access to all mainframes. For international offices where Frame Relay services are not yet available, the company uses low-speed leased lines connected to the enterprise backbone.

The resulting VPN is much less expensive to operate than the previous private network configured with leased lines. As a packet-oriented public data network, Frame Relay allows any facility to communicate with any other — using either SNA or TCP/IP — over

Scenario #2: A Regional Consortium of Hospitals

The organization has a single mainframe, an AS/400 at each medical facility and department-level NetWare servers. The board of directors made a strategic commitment to IP for three reasons: the wealth of resources available on the Internet, the user-friendly browser interface and emerging multimedia and multicast capabilities. For AS/400-to-S/390 communications, the IT Director chose IBM's AnyNet over TCP/IP, which allowed all existing host-to-host applications to run unaltered. Each host is also equipped with a TCP/IP stack and applications to support PCs with TN5250 or TN3270 terminal emulation. IPX is used for all local NetWare traffic. PPTP tunnels all NetWare traffic that traverses the backbone. Because this requires dual stacks in many PCs, the organization plans to use TCP/IP instead of IPX for all NetWare applications in the near future. Over time, the IT Director even plans to migrate every application to a Web browser interface. Because all of the member hospitals are with a 200-mile radius, leased lines in a hub and spoke topology proved to be quite cost-effective. A network access switch at each hospital provides the backbone link, as well as dial-in capabilities for the local medical staff. The switch supports dial-up access to the enterprise over a single ISDN PRI line by both ordinary modems and ISDN BRI small office/home office (SOHO) routers.

The primary benefit to the consortium is the interoperability afforded by TCP/IP, which now serves as a standard platform for all existing and any future member hospitals. Gone are the days of trying to integrate each facility's own network and applications. The consortium can now take advantage of this enterprise-wide uniformity to add new applications, such as medical imaging, easily and affordably.

Scenario #2

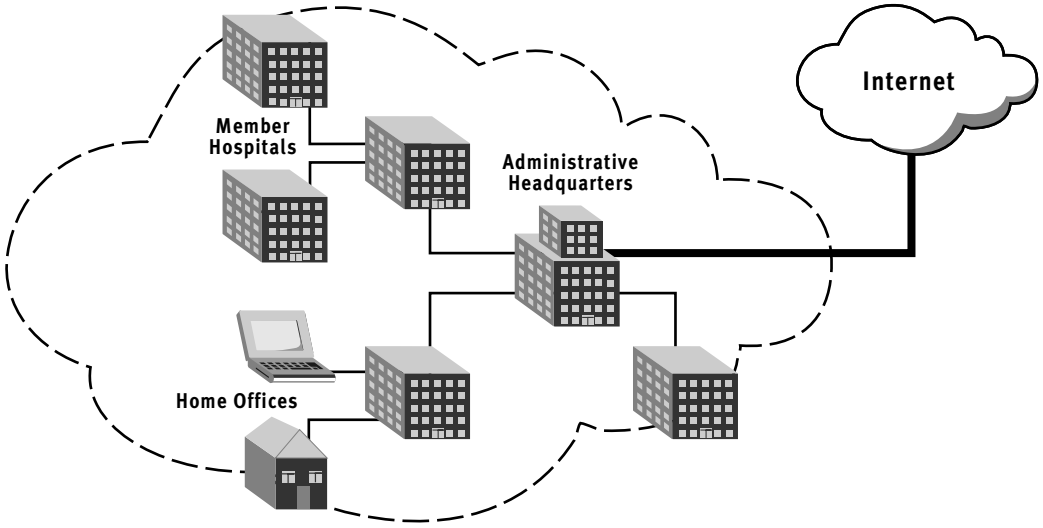


Figure 7 — Many traditional private networks are migrating to IP exclusively for seamless integration between the intranet and the Internet,

© 1997 Ascend Communications, Inc.

Scenario #3: An Insurance Company

Both the headquarters and the claims processing center have mainframes and several midrange systems from DEC and HP. All of the field offices throughout the U.S. have Windows NT servers. The CIO decided to implement TCP/IP end-to-end on a combination PSTN/Frame Relay IP backbone to facilitate future migration to an Internet-based VPN. As an interim solution — while the mainframe applications are being rewritten to support native TCP/IP — DLSw was installed on the two communications controllers to establish the mainframe-to-mainframe link. Native TCP/IP is used to network among midrange systems, as well as for downloading policy information and rate schedules from the central mainframe. A pilot Internet-based VPN for several of the smaller offices is working so well, that all new offices are being added to the enterprise network as members of the VPN. IPSec's ESP is used for confidentiality and integrity during transit via the Internet. Because the company still has some private IP addresses, PPTP is used to tunnel this traffic (IP within IP) across the backbone.

The network is now substantially easier to manage. By consolidating on IP exclusively, the company has eliminated parallel networks and their associated infrastructures and costs. Now, a single infrastructure exists with a single management solution —SNMP — and the entire enterprise backbone can be managed from a single console.

Scenario #3

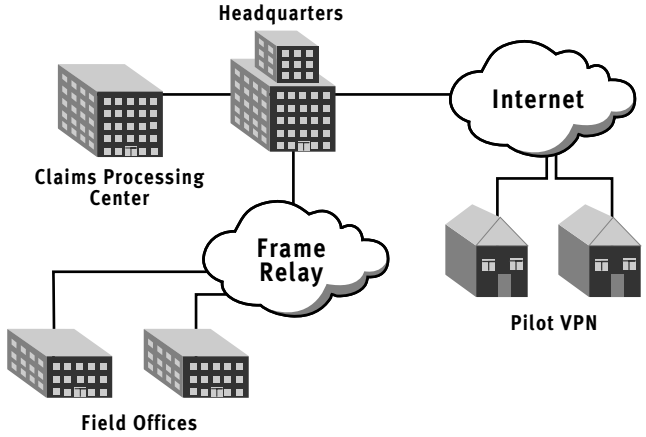


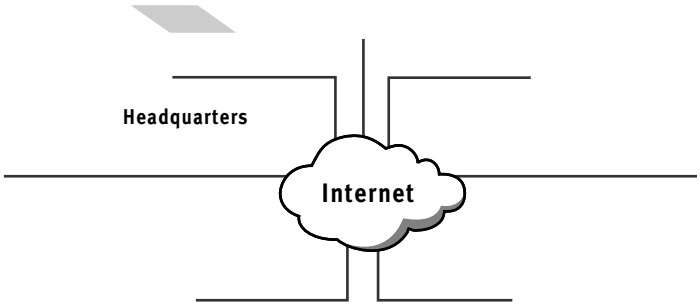
Figure 8 — Choosing IP as the strategic protocol allows VPNs to be introduced into the enterprise network infrastructure in manageable and affordable steps.

© 1997 Ascend Communications, Inc.

Scenario #4: A Small International Distributor

With sales offices around the globe and a small support staff, the MIS director of a small international distributor knew that an Internet-based VPN provided the only viable solution for the growing company's worldwide enterprise network. Each sales office handles its own arrangement with a local ISP. Small offices use SOHO routers for dial-up access; larger offices with LANs and IntranetWare servers use remote access routers. The inventory, price lists and order processing system are on a midrange system running Web server software. To isolate all internal information from any unauthorized use, the director uses password security on hosts and servers, IPSec Authentication Headers and firewalls — integral to the network access equipment at each site. The company plans to establish an extranet soon for better communications with its key suppliers.

The benefit to the organization is virtually unlimited flexibility. Existing connections can be changed and new sites added instantaneously owing to the Internet's vast presence and capacity. Even third party suppliers can be integrated almost effortlessly. The small staff can take on as much responsibility as they can handle or they can outsource any needs to a local ISP. The future of enterprise networking can indeed be a reality today.



© 1997 Ascend Communications, Inc.

Putting It All Together

All of the pieces and effort come together to create the PDN-based enterprise network of the future. The diagram shows a VPN that connects an organization's headquarters with remote offices and individual workers. The example uses the Internet, but could also employ Frame Relay or ATM directly in the backbone. Certain customers and suppliers are also members of a VPN-based extranet. And herin lies the power of an Internet-based virtual private network: wherever you, your customers or your suppliers locate or travel, your very own VPN is just a local phone call away.

The Enterprise Network of the Future

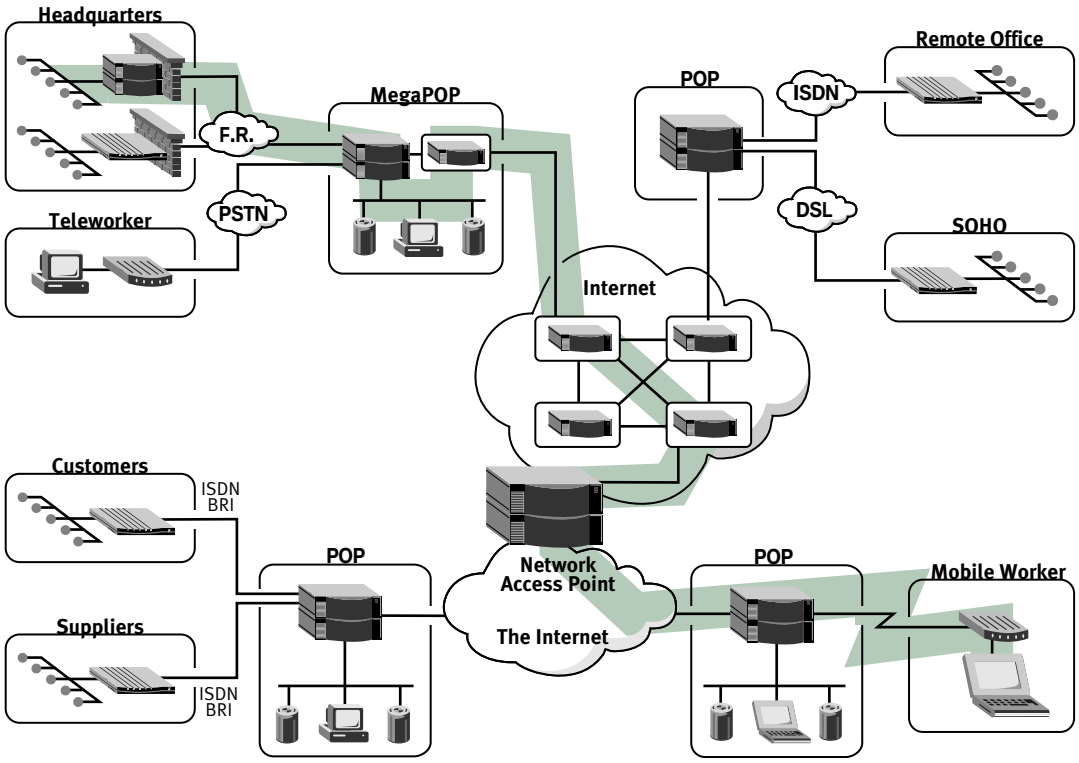


Figure 10 — The enterprise network of the future offers unparalleled flexibility by exploiting the power of "IP dialtone" in the global Internet for all communications, including access to the World Wide Web, intranets and extranets.

5. "How-To" Checklists

Network Management Tools Checklist

Managing through and across public networks or the Internet requires managing all equipment and links with an end-to-end approach. This higher level perspective allows the enterprise to be viewed logically in its entirety, as well as physically in its detail.

The capabilities needed to manage enterprise networks effectively include:

- ❑ Auto-discovery and dynamic mapping of the end-to-end network topology
- ❑ Real-time network monitoring with fault alert/alarm generation based on user-defined thresholds
- ❑ Capacity planning and performance trending through collection and analysis of traffic statistics that show both the level and patterns of usage by individuals and multi-user sites
- ❑ Integrated accounting to track network usage by user/department for bill-back or other purposes
- ❑ Remote configuration management for bringing new locations on-line and 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
- ❑ RADIUS database support for security and accounting administration

© 1997 Ascend Communications, Inc.

Network Access Switch Checklist

The network access switch, or WAN access switch, is normally installed in larger sites, where it provides a complete, integrated solution in a single unit. One or more high-speed lines to the WAN exchange traffic with the Internet, as well as with all remote offices and individual users. A single link can even combine PDN and PSTN traffic, which may be needed for direct analog modem and ISDN dial-in from local sites/users. A capable network access switch also supports high-speed backbone and/or Internet connections, making them suitable for Internet-based VPNs. Essential features include:

- ❑ Multi-port WAN capabilities supporting a wide range of PDN and PSTN services, including T1/E1, ISDN PRI/BRI, xDSL, DS-3/E3, analog modems, cellular, Frame Relay and ATM
- ❑ High-speed channelized trunk lines to consolidate traffic from numerous remote locations, which are likely to use different WAN services
- ❑ Digital modem technology for peak performance and compatibility with a broad assortment of analog modems, including new asymmetric 56 Kbps modems
- ❑ A suitable LAN interface such as Ethernet (10 Mbps) or Fast Ethernet (100 Mbps)
- ❑ Strong security provisions, especially authentication and authorization
- ❑ Optional dynamic firewall protection that is integrated with the switch's other security provisions
- ❑ Support for VPNs through standard tunneling and IPSec encryption
- ❑ Built-in compression to maximize throughput
- ❑ Dynamic bandwidth management for enhanced performance
- ❑ Ability to accommodate IP multicast applications
- ❑ Robust local and remote management to maximize uptime at minimal cost
- ❑ Call detail reporting to track usage by all users
- ❑ RADIUS database support for administering security and accounting
- ❑ Resiliency with redundant power supplies and hot-swappable interface cards
- ❑ Sufficient capacity (WAN ports and overall throughput) to support the anticipated number of sites/users and traffic volume
- ❑ Compatible family of scalable products to keep pace with network growth
- ❑ Certification for operation with carrier services worldwide

© 1997 Ascend Communications, Inc.

Remote Office Router Checklist

The remote access router, sometimes called a WAN router, provides a cost-effective solution for multi-user offices and divisions. Depending on the number of users and expected traffic patterns, most remote access routers will use Frame Relay, ISDN, xDSL or leased lines for uncompressed throughput ranging from 56/64 Kbps to 1.544/2.048 Mbps. ISDN's bandwidth on demand makes it the preferred choice for most sites needing enterprise network, Internet and/or VPN access. Essential features include:

- ❑ Either a leased line (DDS56, T1/Fractional T1 or E1, Frame Relay or xDSL) or dial-up (SW56 or ISDN BRI) WAN interface with the desired throughput
- ❑ A dual-WAN unit provides both a primary leased line and a secondary high-speed dial-up link for backup and overflow needs
- ❑ Integral CSU/DSU and/or NT-1 line adapters (required by the carrier) to simplify installation and management
- ❑ Ethernet LAN connectivity to assure application interoperability
- ❑ Sufficient capacity or scalability to support all users
- ❑ Standards-based security that supports authentication, integral dynamic firewall protection and IPSec encryption for VPNs
- ❑ Built-in compression to maximize throughput and lower the cost of ownership
- ❑ Dynamic bandwidth management for enhanced performance
- ❑ Call detail reporting to track each employee's network usage
- ❑ Ease of installation and simplicity of operation
- ❑ Remote manageability and downloading of software upgrades via the WAN to eliminate the need for an on-site technician
- ❑ A compatible family of products to handle the wide diversity of remote office needs
- ❑ Certification for operation with local carrier services

© 1997 Ascend Communications, Inc.

SOHO Router Checklist

The SOHO router offers a solution for integrated data, voice and fax communications — making it ideal for offices with one or a few users, including telecommuters. Advanced bandwidth management techniques let users access the enterprise network, Internet and/or VPN on both ISDN BRI channels (at up to 512 Kbps with compression) and still receive incoming voice and fax calls — all on a single line. xDSL can normally be used instead of ISDN. Essential features include:

- ❑ A single WAN connection that handles all data, voice and fax communications
- ❑ An integral NT-1 interface (for ISDN BRI) to eliminate the need for an external adapter
- ❑ Ethernet LAN connectivity for highest performance and greatest flexibility
- ❑ One or two analog POTS — Plain Old Telephone Service — ports for connecting the telephone (plus optional answering machine) and a fax machine
- ❑ Standards-based security that supports authentication, integral dynamic firewall protection and IPSec encryption for VPNs
- ❑ Built-in compression to maximize throughput and lower the cost of ownership
- ❑ Support for advanced dynamic bandwidth management to optimize user productivity by handling data, voice and fax concurrently and interchangeably
- ❑ Tamper-proof configuration and security provisions that are almost effortless to use
- ❑ Ease of installation and simplicity of operation
- ❑ Remote manageability to facilitate centralized support
- ❑ Certification for operation with local carriers

© 1997 Ascend Communications, Inc.

Bandwidth Manager Checklist

A WAN bandwidth manager allows a single WAN line to combine multiple forms of data, voice and video traffic, and, optionally, add backup and overflow bandwidth over dial-up links. All traffic can traverse the private enterprise network or be directed via the PSTN for switched access to other locations. One WAN bandwidth manager is required at each site where such integration is desired. Essential features include:

- ❑ Dynamic bandwidth management for optimum utilization of the private line
- ❑ Built-in interfaces for routers, the PBX and videoconferencing equipment
- ❑ Support for both T1/E1 and ISDN PRI WAN lines
- ❑ Ability to handle 56 and 64 Kbps channels for calls to virtually anywhere in the world
- ❑ Drop-and-insert capability for making the private line channels available to the PBX
- ❑ PRI/T1 conversion adds support for older PBX systems
- ❑ Compliance with inverse multiplexing standards, such as BONDING
- ❑ Optional ISDN dial-up ports for supplemental backup and overflow bandwidth on demand
- ❑ Integral CSU/DSU and/or NT-1 WAN line interfaces to eliminate the need for external units
- ❑ Full remote management, including loopback diagnostics, to minimize on-site support needs
- ❑ Call detail reporting to track usage for billback and other accounting purposes
- ❑ Certification for operation with popular switches and carrier services

© 1997 Ascend Communications, Inc.

Appendix

Ascend Product Line Overview

CBX 500	· High performance, high density · Quality of service for thousands of VCs · T3/E3 through OC12/STM-4	Carrier-class ATM switching
GRF™ Family	· Up to 10 million pps throughput · Route table of up to 150,000 routes · Scalable, media independent	IP switching
B-STDX and STDX Family	· High-capacity multiservice support · Scalable broadband packet switching · High system and network reliability	Frame Relay-to-ATM interworking Carrier-class Frame Relay switching
MAX TNT™	· Highest port density in its class · Carrier class reliability and redundancy · Scales to HSSI, FDDI, DS3	New generation WAN access
SA Family	· High-performance ATM concentrate · T1/E1 through OC3/STM-1 · Circuit emulation support	Broadband access
MAX™ Family	· Multiprotocol, multiservice WAN access · Scalable multiservice platform supports analog, ISDN, T1/E1, and frame relay · Most widely used in ISP networks	High-performance WAN access
MultiDSL™ Family	· Leverages existing copper infrastructure for on-demand, high-speed access · Data rates from 128 Kbps to 6.4 Mbps · Turnkey solution for practical DSL migration	End-to-end xDSL
Pipeline™ Family	· Multiprotocol routing/bridging · Dynamic Bandwidth Allocation · Wide range of applications	Access delivery
Multiband™ Family	· Integrated audio, video and data · Dynamic bandwidth allocation and management · Affordable, flexible, easy to use	Cost-effective multimedia delivery
SecureConnect™ Family	· Integrated, standards-based encryption ·	Network security and VPNs

© 1997 Ascend Communications, Inc.

Additional Resources

The following materials are available from Ascend Communications:

- The *Corporate Remote Access Guide* discusses various aspects of remote networking, including an overview of the main building blocks.
- *The Virtual Private Network* is a resource guide that provides a wealth of information on Internet-based VPNs.
- Ascend's Web site **http://www.ascend.com** has an extensive glossary along with a technical library that includes numerous white papers and technical briefs on pertinent topics.

The following is a list of Requests for Comments (RFCs) applicable to enterprise networking. RFCs are the way the Internet Engineering Task Force (www.ietf.org) establishes standards for IP and the Internet. Copies of the RFCs are available on the Information Sciences Institute Web site at **info.internet.isi.edu/1/in-notes/rfc**

- RFC 1001: Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Concepts and Methods
- RFC 1002: Protocol Standard for a NetBIOS Service on a TCP/UDP Transport: Detailed Specifications
- RFC 1041: Telnet 3270 Regime Option
- RFC 1205: 5250 Telnet Interface
- RFC 1234: Tunneling IPX Traffic Through IP Networks
- RFC 1490: Multiprotocol Interconnect over Frame Relay
- RFC 1533: DHCP Options and BootP Vendor Extensions
- RFC 1534: Interoperation Between DHCP and BootP
- RFC 1538: Advanced SNA/IP: A Simple SNA Transport Protocol
- RFC 1576: TN3270 Current Practices
- RFC 1597: Address Allocation for Private Internets
- RFC 1631: The IP Network Address Translator
- RFC 1646: TN3270 Extensions for LU Name and Printer Selection
- RFC 1647: TN3270 Enhancements
- RFC 1701: Generic Routing Encapsulation (GRE)
- RFC 1702: GRE Over IPV4 Networks
- RFC 1795: DLSw Switch-to-Switch Protocol (replaces RFC 1434)
- RFC 1853: IP in IP Tunneling
- RFC 2024: Definitions of Managed Objects for DLSw
- RFC 2106: DLSw Remote Access Protocol
- RFC 2114: DLSw Client Access Protocol
- RFC 2131: Dynamic Host Configuration Protocol (Obsoletes 1531 and 1541)
- RFC 2132: DHCP Options and BootP Vendor Extensions

© 1997 Ascend Communications, Inc.

Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502
Tel: 510.769.6001
Fax: 510.747.2300
Toll Free: 800.621.9578
E-mail: info@ascend.com
Fax Server: 415.688.4343
Web Site: http://www.ascend.com

© Copyright 1997, Ascend Communications, Inc.
06-12
09/97

