Tapestry: Software Infrastructure Enabling Virtual Private Networks

K. Balakrishnan, N. Chokshi, R. Huang, A. Konrad
S. Kumar, O. Sakdamnuson, B. Zhao

Project Paper, Opportunity Recognition SP'01, Prof. Drew Isaacs

1. INTRODUCTION

In this paper, we describe Tapestry, a technology that enables scalable, efficient and fault-tolerant wide-area network applications, and analyze its potential markets and strategies. By analyzing several application markets, we select the market of Virtual Private Networks. We then analyze current pains felt by customers and providers, and describe solutions made possible by the Tapestry technology. Finally, we outline market entry strategies and analyze our options.

2. TECHNOLOGY

Today's network is increasing in both reach and bandwidth. Together with exponential growth in computing resources, it is setting the stage for the proliferation of large-scale, wide-area network applications. Barring the path to deployment of these applications are familiar issues of scalability, fault-tolerance and adaptability, issues that have been solved in the client-server and cluster-based computing models.

Instead of asking application developers to solve these hard problems on a per-application basis, current research in computer networking seeks to provide a unified solution in the form of a wide-area application infrastructure. Our goal is a network layer that bestows these key properties upon any application built on top of it.

2.1 Tapestry

The Tapestry project [7] at UCB's computer science division is working to solve this application infrastructure problem. It strives to be scalable to millions of users and requests in the wide-area, tolerant of multiple hardware and software faults, and reduce management costs by providing mechanisms for self-monitoring and repair.

Tapestry is built in the context of the OceanStore project [4], an effort to provide a world-wide network of storage servers which guarantee files to be secure and durable over thousands of years despite natural disasters and catastrophes. Tapestry provides the mechanism by which OceanStore components locate each other and communicate in a reliable fashion.

The key functionality that Tapestry provides is as follows:

- Locating the nearest copy of a named object
- Forwarding a message to a given named location

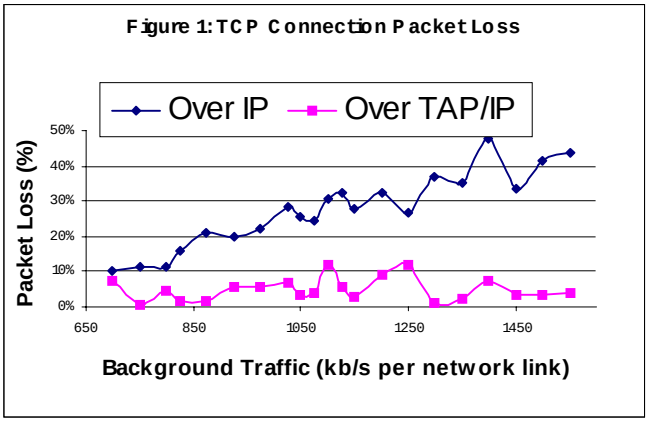
The main objective of Tapestry is to provide a set of key system properties that applications can benefit from, and hiding the complexity involved into the infrastructure. The key properties for applications seeking to leverage the growing wide-area network are:

- **Scalability**: These applications need the ability to handle volume in clients, network communication traffic, and server requests.
- **Fault-tolerance**: Network traffic between components of the application, and between clients and the application should successfully reach its destination with very high probability, despite the presence of expected machine and network failures. Similarly, requests to locate an object/file/component should guarantee successful results if and only if the object exists.
- **Self-management**: The system needs to adapt to changing conditions in a dynamic environment, detecting and working around failures when they occur, detecting and integrating new resources as they become available.
- **Isolation**: A local network event such as a request, failure, a flood of requests or an attack should have its effects localized to affect as few external nodes as appropriate. A server should not be involved in operations originating from a distant network node unless absolutely necessary.
- **Resilience to Attacks**: The system should be sufficiently decentralized in order to minimize reliance on any single component, and therefore minimize its susceptibility to an attack on a single component. It should also contain enough redundancy at every level of operation, such that application will continue servicing requests despite all but the largest scale attacks.

To provide these properties, Tapestry takes the approach of an application-level protocol; that is, Tapestry software components sit as regular programs on top of the operating system, and provide service to other applications.

We refer to machines running the Tapestry software as "nodes." Tapestry nodes can take on one of three roles: "servers," which store objects and make them available to other machines; "clients" are machines which make requests to read and use those objects; and "routers," which participate in the network by forwarding messages between other servers along its own network links. The function calls that an application can call from Tapestry are:

- PublishObject(ObjectID)
- RouteMessageToObject(ObjectID)
- RouteMessageToNode(ObjectID)
- MoveObject(ObjectID, NewLocationID)



2.2 Message Routing

The key novelty that Tapestry provides consists of a set of "routing tables" and distributed algorithms that provide message routing in a decentralized scalable fashion. Current Internet routing algorithms are limited in scalability, and can only work inside the network of a single backbone provider such as BBN or Sprint. Other algorithms must be used to control message forwarding between backbones in order to make possible point-to-point communication across the Internet. Furthermore, existing IP routing algorithms are more or less static. Routers in the backbone must handle a large volume of traffic efficiently, forcing them to statically remember a single path for any destination. This means any failure along the chosen path can make communication inoperative for a matter of minutes, before the algorithm detects and corrects for the failure.

In contrast, Tapestry messages are routed to their destinations using a variety of paths. This occurs, since messages in Tapestry are routed towards their destination by incrementally approaching the destination ID digit by digit. For instance, a message from node 3459 destined for node 9621 might take the path:

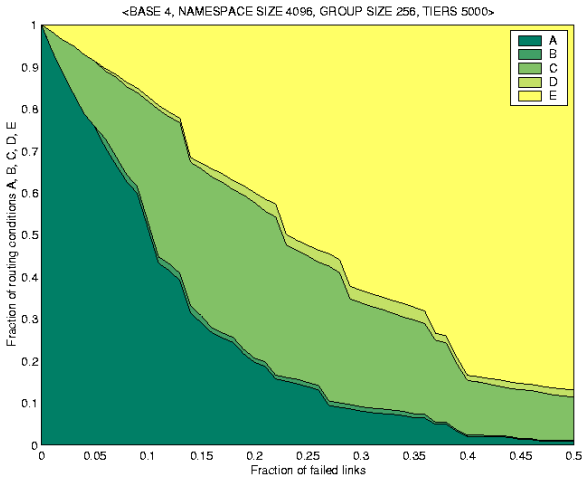
3459→3251→1521→0621→9621

This is one of many paths that can be taken, since 3251 can be replaced by any node ending in "1," 1521 can be replaced by any node ending in "21," and so on. This means communication between A and B can take any of a variety of paths. Furthermore, since traffic is spread across many paths, each node is less restricted in complexity. Each Tapestry node actively monitors (via periodic maintenance messages) a small set of other nodes they use for routing for failures and efficiency. In the case where a link to a forwarding node or the forwarding node itself has failed, the original node quickly switches to a backup node, and routing continues despite a small negligible delay (on the order of milliseconds).

2.3 Current Results and Applications

Tapestry has been implemented and studied in several large-scale network simulators. It will be deployed on a real wide-area network composed of the combined networks of a set of educational collaborators, including U. Washington, Berkeley, Stanford, UCLA, and USC. Simulations have shown that Tapestry solves most of the objectives set forth in Section 2.1 [5][7].

Figure 2: Routing w/ Failures



We now present some simulation results to demonstrate some of Tapestry's impact in providing reliability and fault-tolerance. First, we show the effectiveness of Tapestry's redundant routing paths in quickly routing around failures when network links and servers fail. We compare a version of the commonly used TCP/IP network protocol enhancing with Tapestry routing against a standard TCP/IP implementation. As the ambient network traffic increases, the number of packets (messages) lost by the standard TCP/IP network increases proportionally, while the Tapestry TCP/IP stays relatively constant with respect to percent of messages lost. This is very significant, given that serious packet loss is prevalent in common uses of a large variety of today's network applications.

Next, we show the effectiveness of Tapestry mechanisms in finding paths for messages to reach destinations when one or more failures occur. In Figure 2, we show the probability graph of successfully delivering a message to a destination as failures increase in the network. Region **A** represents the probability of both IP (the current network protocol) and Tapestry succeeding in reaching the destination. Region **B** is when IP succeeds, and Tapestry fails. Region **C** is the most important feature, since it represents the significant probability where IP fails to find a path to the destination, and Tapestry does. Region **D** is where neither IP nor Tapestry succeeds, even though a path does exist, and region **E** represents the probability that failures have made the destination unreachable. The key result is that where paths exist to the destination (A+B+C+D), Tapestry finds one such path with very high probability (A+C), and improves greatly over IP (A+B).

2.4 Tapestry Applications

The routing properties of Tapestry provide a unique foundation for interesting network applications. In addition to OceanStore [4], several applications have been built to leverage Tapestry's properties. We first built Bayeux [8], an efficient multicast application that provides efficient delivery of content to a large audience. Bayeux is different from existing multicast systems, in that it leverages Tapestry to provide fault-tolerant delivery of data and to scale up to many thousands of users per multicast session.

Another interesting application is Silverback [6], a global-scale archival component of OceanStore that acts like a long-term file backup service, and uses Tapestry to efficiently and reliably locate and reconstruct old file fragments.

Having demonstrated the usefulness of Tapestry as an application infrastructure, we now examine the possible application markets we can enter with Tapestry.

3. THREE POTENTIAL APPLICATIONS

Given the strengths of the Tapestry technology that offers a new level of reliability and scalability, we present three potential applications that will leverage these strengths: multimedia streaming, electronic content distribution, and Virtual Private Networks (VPNs). Table 1 in Appendix A shows the comparison of three applications discussed below. After examining the potential markets, we conclude that the VPN market is the most promising.

3.1 Streaming Multimedia

There are two approaches to delivering audio/video over the Internet or within an intranet: distribution of video or audio files, or multimedia streaming. In the multimedia streaming approach, the user software decodes and plays the incoming audio or video on real time, without having to wait for files to be downloaded. The server delivers recorded or live web content "on demand."

The reason we consider the streaming multimedia market as a potential application of Tapestry is because the challenges to multimedia streaming delivery over the Internet are scalability and reliability. In 1999 there were two events that show these limitations. One was when the Star Wars Episode I trailer was released on the Web, and the second was the Victoria's Secret Super Bowl. Both events lead to the overload of network capacity.

Scalability challenges to video streams on entertainment sites are more severe than those experienced by most companies. For example, MediaX, a company which hosts dozen of artist web sites, experienced more than 11 Gbytes worth of video in 24 hours when they posted on-line the video for the new N'Sync single [1].

There are several players in the multimedia streaming market with Real Networks, as the market leader in Internet media delivery. RealNetworks develops and markets software products designed to enable owners of audio, video, and other multimedia content to send their content to users of personal computers over the Internet. RealNetworks charges customers according to the capacity on their networks and the number of server boxes they deploy. The net revenues for the first quarter of 2001 were $50.4 million. Net revenues increased 98% to $131.2 million in 1999 and they reported net earnings of $6.9 million, or $.04 per diluted share. Figure 1 in Appendix A illustrates the streaming media market share in 1999.

Akamai Technologies developed FreeFlow Streaming, which relies on content distribution to deliver multimedia to the end users. FreeFlow Streaming will be priced at $2,000 per Mbps of transport. As of December 31, 2000, Akamai has accumulated a deficit of $944.4 million.

The streaming multimedia market is clearly dominated by established players such as RealNetworks, Inktomi, Akamai and Microsoft – each provides a product to enable or directly run multimedia applications. The opportunity for Tapestry in the multimedia market is not compelling. Existing players have not been able to grow the market.

3.2 Electronic Content Distribution

Electronic content distribution delivers user-defined information such as breaking news, stock quotes and software updates to the users automatically. Marimba and PointCast introduced the first "push" Internet technology to automatically deliver information directly to users' computers rather than forcing them to go out and fetch it.

The reason why we consider electronic content delivery as a potential application of Tapestry is because we can "out-deliver" the current competition. When compared to the traditional push technology, the Tapestry technology can deliver contents with less bandwidth. For example, if two geographically close users in a cluster both want the same piece of data, "push" technology will deliver two pieces of data, while with Tapestry technology the server will only deliver the data once.

Although electronic content delivery is a good fit with the Tapestry technology, there are several reasons why we do not think this is a good market opportunity: (1) It is a small market: PointCast with $18M of revenue in the year 1998, and BackWeb $30M of revenue in the year 2001, (2) There are many competitors. For example, the push technologies are built-in feature in both netscape and Microsoft Internet explorer browsers. Yahoo also provides free download software that implements push technology, (3) The market is polluted - since many companies have implemented electronic content distribution and none of them have succeeded, it would be hard for any new company to get funded in this particular market.

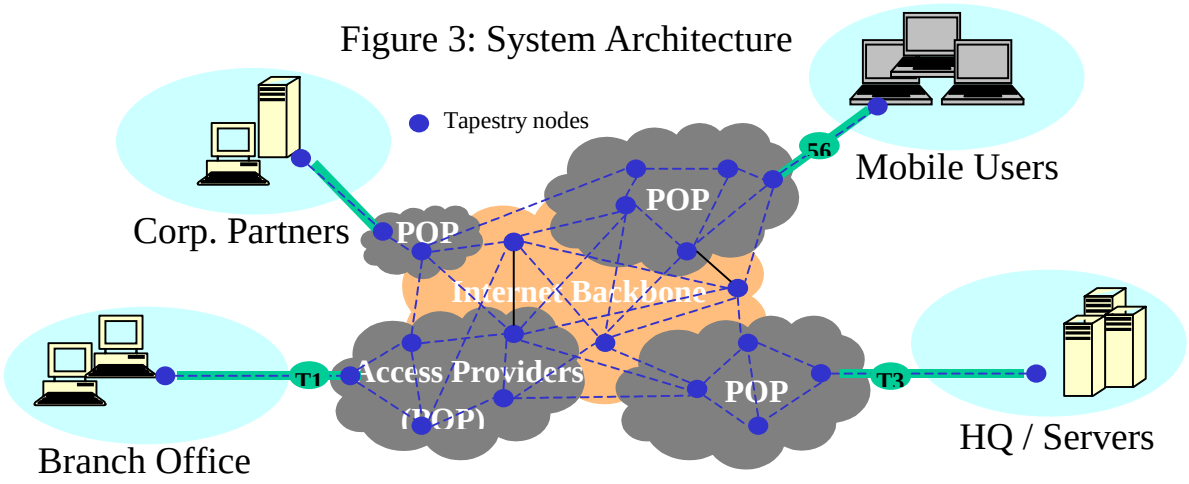
3.3 Virtual Private Networks

Virtual Private Networks (VPN) extends the corporate network to distance offices and homes, by using the worldwide IP network (i.e., the Internet cloud and the service providers). It provides reliable, secure and mobile data communications. The three basic types of VPN are Access VPN, Intranet VPN and Extranet VPN (see Figure 2 in Appendix A). While VPNs offer direct cost savings over other communications methods (such as leased lines and long-distance calls), they can also offer other advantages, including indirect cost savings as a result of reduced training requirements and equipment, and increased flexibility.

A traditional corporate network built using leased T1 (1.5 Mbps) links and T3 (45 Mbps) links must deal with tariffs that are structured to include an installation fee, a monthly fixed cost, and a mileage charge, adding up to monthly fees that are greater than typical fees for leased Internet connections of the same speed. Leased Internet lines offer another cost advantage because many providers offer prices that are tiered according to usage.

In a VPN, not only can T1 or T3 lines be used between the main office and the ISP, but many other media can be used to connect smaller offices and mobile workers to the ISP and, therefore, to the VPN without installing any added equipment at headquarters. A company's information technology (IT) department can reduce wide-area network (WAN) connection setup and maintenance by replacing modem banks and multiple frame-relay circuits with a single wide-area link that carries remote user, local-area network

Figure 3: System Architecture



to local-area network (LAN–to–LAN), and Internet traffic at the same time.

Thus the key benefits of VPN are the following: (1) Network managers: increases the reach of the corporate network cost efficiently, (2) Remote users: secure access to corporate network, and (3) Corporations: secure communications via extranets to business partners.

We consider the VPN market as a potentially compelling application for Tapestry because Tapestry technology can provide greater scalability, lower management costs, Quality of Service without dedicated networks, and resilience against malicious attacks.

VPN savings are typically 20% to 40% for site-to-site domestic networks (more for international networks), and 60% to 80% for traveling and telecommuting employee access.

We consider VPN as the most promising market because of its large market size and growth potential. Studies from different research groups have shown significant opportunity for both US VPN market and worldwide VPN markets (see Figure 3 in Appendix A). Projections by IDC show $3.3B market by 2001, $7.7B by 2003, and $10B by 2005 [3].

4. VPN MARKET AND PAINS

Before we continue with our analysis of how to leverage Tapestry for the VPN market, we look closer at the current market segmentation and current market pains faced by customers and providers in the VPN market, and how they can be addressed with the Tapestry technology.

The key players in the VPN market can be segmented into three classes:

1. Facilities-based ISPs and other data service providers (e.g. Nortel, Qwest, Sprint, AT&T, Alcatel)
2. Regional Bell Operating Companies (RBOCs) (e.g. Verizon)
3. Secure network and access specialists (e.g. Lucent, Cisco – VPN routers, Checkpoint Software – VPN client software)

Secure network and access specialists manufacture hardware and software elements that are necessary components to any VPN (whether it's a managed service or not). These players include the likes of Cisco and Lucent (both of whom manufacture VPN router devices), Checkpoint software (which creates VPN software that resides on an end-user's client device), and iPass Solutions (which provides international points of presence for VPN service providers – notably, iPass has partnered with AT&T to enable international access to AT&T's VPN service).

Facilities-based ISPs and data service providers usually offer VPN services as a managed solution (i.e. an enterprise hires out an ISP and contracts them to host a VPN along with other network services). These players often utilize components manufactured by secure network and access specialists to provide a complete VPN service. Regional Bell Operating Companies have just begun to offer managed VPN services and are also partnering with the secure network and access players. Building out the infrastructure for a VPN service tends to be costly (especially for service providers with legacy networks). This high cost has played a large role in slowing down the RBOCs' entrance into the VPN service provider market.

4.1 Current Pains

In the current VPN market, there are three key deficiencies that customers face in choosing VPN solutions. The three keys are inflexibility of access, high cost of management, high cost of Quality of Service, and vulnerability to attacks.

- **Access point constraints:** In current VPN solutions, a VPN provider can only provide VPN service through one of its own access points. Corporations choose one single VPN provider for simplicity and cost. For most corporate users, this means using a dedicated phone line to access the VPN provider's Internet service. This is less than ideal for locations where local access to the provider's network is unavailable, or where faster network access is available via another provider, such as broadband DSL.
- **High management costs**: Current VPN provides employ a number of personnel, who monitor the state of the network continuously, both to detect and repair faults, and to optimize

system parameters for optimum performance. The personnel cost is passed on to the client.

- **Expensive Quality of Service**: Currently, quality of service can only be provided on dedicated physical private networks (PPNs). Such networks are expensive to deploy and manage. Cheaper alternatives, however, route through the uncontrolled environment of the Internet. As a result, they do not offer any level of QoS.
- **Vulnerability to Attacks**: Another consequence of being constrained to using one VPN provider is that it gives a clear point of attack for malicious entities in the network. Knowing which VPN provider a company uses means an attacker can either physically disable their dedicated network lines, or simply flood their network access points with bogus data in order to prevent the targeted company from doing useful work.

4.2 Tapestry Solutions

We now discuss briefly how Tapestry solves each of these pains.

- **Access point flexibility**: Because a Tapestry-enabled VPN would be software-based, it is not tied down to any single network access provider. A user should be able connect to whatever network provider is locally available with the Tapestry software, and immediately access the VPN. This allows users to reduce cost as well as make use of the fastest access available.
- **Self-managing software**: Once tied into the infrastructure, Tapestry software components communicate with and monitor each other, detecting and repairing failures, and tuning system parameters where appropriate for better performance. This self-management translates into savings in manpower, and can be directly passed on to the client.
- **Software-based QoS**: Given Tapestry's multi-path approach to message routing, components can offer different levels of QoS guarantees given the level of resources a client wishes to utilize. This QoS is offered while routing through the current Internet, eliminating the high cost of dedicated PPNs.
- **Resilience to Attacks**: The decentralized, integrated nature of a Tapestry-based VPN means that data for a company can come from any network access point and go to any network point. Potential attackers have no way of identifying traffic as belonging to a targeted company, nor can they identify an access point that would cripple such traffic. Furthermore, given a large enough deployment of Tapestry infrastructure nodes, any attack that disables a set of nodes will have negligible impact on the overall performance of any corporation, since their traffic will simply route around the affected regions.

Preliminary test results done at UCB's Computer Science Division show that the Tapestry technology can solve current VPN pains in novel ways. These approaches are unique to Tapestry's decentralized, fault-tolerant approach to communications, and would be very difficult to copy or reverse engineer by competitors.

5. SYSTEM ARCHITECTURE

Before we begin our discussion of the market opportunities in VPN, we present a summary of the proposed software-based VPN system architecture.

In Figure 3, we show a diagram of a large scale Tapestry VPN network. The VPN consists of four key groups: the headquarters of the company that stores its file servers, a branch office, a group of mobile users, and corporate partners on an extranet. These four groups are connecting to the distributed VPN via different Internet access providers, and applications are linked by an overlay network of Tapestry nodes. Note that each group has different type of access capability to the large-scale network: the servers are connected via T3 lines, the branch office via T1 lines, mobile users via 56K modems, and partners via their own POP. The key is that Tapestry links all the parties together with heterogeneous access points in a well-connected network mesh. Note that because Tapestry's benefits depend on the ability to route along multiple paths from every Tapestry node, there is a "critical mass" of initial server deployment necessary in order to see the benefits of our architecture (one possible scenario is to partner with ISPs and infrastructure companies such as Akamai to deploy Tapestry on their servers). Another consequence is that if a user's connection to the network is a single faulty link, use of Tapestry will not improve overall performance.

More specifically, each Tapestry node location depicted in Figure 3 represents the Tapestry software component as depicted below:

Application – User Interface
Tapestry Infrastructure
Network Software (IP)
Hardware – Network Interface

6. MARKET ENTRY

This product architecture enables us to capitalize on a market opportunity in two ways. First, we can license the Tapestry technology to VPN service providers. Alternatively, we can develop our own VPN service offering. The following paragraphs will evaluate both options and examine the customer targets, competition, and entry considerations for each option.

6.1 Licensing Option

We see from the above points that the Tapestry technology can solve current VPN pains in novel ways. These approaches are unique to Tapestry's decentralized, fault-tolerant approach to communications, and would be very difficult to copy or reverse engineer by competitors.

As Tapestry solves a very visible pain for current VPN service providers, we believe that we can license the technology, which would enable them to address the quality of service issues. VPNs solve the QoS issue today by issuing service-level agreements (SLAs) for each customer. An SLA is essentially a contract that guarantees the maximum number of packets that are lost on its network. If the VPN service provider loses more than this maximum number, most SLAs entitle the customer to a rebate if a certain level of service is not met (depending on the number of

packets lost). As a licensee of the Tapestry technology, VPN service providers can lower the cost of maintenance and offer a stronger QoS guarantee to their customers.

Potential licensees would include AT&T, Worldcom (UUNet), Genuity (formerly GTE Internetworking), Infonet and the like. Currently AT&T Labs, MIT labs and Microsoft Research are all exploring similar technologies focusing on decentralized peer-to-peer location services. In comparison with those projects, Tapestry is more complex in nature, but offers stronger analytical bounds on performance. Furthermore, the other efforts focus primarily on locating objects in the network, whereas Tapestry also provides reliable communication and resilience to faults and attacks.

The licensing option obviously carries less perceived risk. At the same time, there are limited revenue opportunities, as well. We feel that while we should pursue the licensing option, it should not be our primary strategy.

6.2 VPN Service Offering

In addition to licensing Tapestry, we can also build a competing VPN service with the Tapestry technology embedded within. Our non-SLA mechanism for enabling a quality of service would be a strong competitive advantage of this offering.

The value proposition for our offering is as follows:

Our product is for enterprises and homes that need mobile, secure, and reliable data communication. The Tapestry-enabled VPN is a software-based solution that delivers scalability and reliability. Unlike existing VPN solutions, our product provides portability, lower cost QoS, self-management capabilities and resilience to network attacks.

6.2.1 Customer Targets

It is not surprising to find that enterprises are the biggest customers of the reliable, flexible, and secure communication services that VPNs provide. Substitutes such as leased line and frame relay services are ill suited to the needs of organizations that, in increasing numbers, need to exchange critical data with business partners as they implement outsourcing strategies. These substitutes tend to be very inflexible and costly to set-up and maintain (See Figure 4 in Appendix A). In addition, as markets are turning increasingly global, many companies are faced with high costs whenever data cross international boundaries. At the same time, as more workers telecommute and travel, traditional remote access services have become too expensive and cumbersome to serve the needs of the increasingly dispersed and mobile workforce.

Although the cost of service is a big factor, enterprise customers require their data communication services to be:

- Secure – the data communication has to be safe from prying eyes, tampering, and spoofing. Outsiders must not be able to read the data, alter the data, or masquerade as insiders.
- Convenient and flexible – Data communication should be as transparent as possible for users and corporate network management staff. Users in particular should be able to connect as easily as they do over leased lines or by long distance dial-up.
- Easy to manage – enterprises must be able to 1) install and provision equipment in a secure fashion, 2) scale the data communication service, when the requirements grow beyond its current capabilities, 3) track problems that may occur beyond their own borders, 4) establish extranet relationships with a range of business partners, some highly trusted and some not.
- Reliable – Enterprises want the service provider to guarantee certain level of reliability and quality of service. For example, the communication service between XYZ corporate head quarter in San Francisco and the branch office in Tokyo, Japan has to provide bandwidth of 10Mbit 90% of the time, 5Mbit 95% of the time, and 1Mbit 99% of the time.

As an aside, we have observed a growing need for individual users to have reliable, secure access to the Internet with a relatively high quality of service. For instance, a user may have access to the Internet for personal use using AOL, and may want a certain level of reliability and fault-tolerance that AOL cannot provide today. We have the opportunity here to partner with ISPs like AOL to provide high quality, highly reliable Internet access for the average consumer. This is a concept we need to explore further.

6.2.2 Competitors

Most service providers offer a managed solution, which is provisioned with a router or VPN device from vendors such as Lucent, Time Step, or Nortel. Currently, most IP VPNs are implemented and packaged as a managed solution that includes the transport link. These packaged solutions include circuit provisioning, implementation, management, and in many cases, security monitoring. Most managed solutions are dedicated site-to-site VPNs (i.e. VPNs that connect one facility to another).

Most competitors in this market try to provide a diverse array of options with the managed VPN service (they take the “menu” approach – customers pick and choose only those services they want thereby enabling the VPN service providers to provide fairly customized products). Some of these “menu items” include level of reliability (e.g. 99% uptime/year versus 97% uptime/year), consolidated billing (e.g. one bill for all network services provided to an enterprise), and geographic accessibility for end users (e.g. domestic US only access versus international access).

Competitive differentiation seems to be around the following factors:

- Ease of use
- Flexibility of options offered as part of the managed service (e.g. billing, international support)
- Performance and QoS
- Remote access versus site-to-site connectivity (i.e. players differentiate based on whether they offer VPN services for employee remote access versus connectivity between enterprise sites)
- Security services

6.2.3 SUCCESS FACTORS

Success in the VPN service provider market depends on how we address several key challenges. These are the challenges that are facing existing players in the VPN service provider market and have great bearing on a particular player's success in the market.

- In order for our offering to be successful, we need to achieve "critical mass." This means that we would need to have Tapestry software embedded within most of the ISPs as well as the Internet backbone in order to facilitate a secure and reliable connection between the client and the service it is requesting (see Figure 3). The challenge here will be structuring the appropriate partnerships with ISPs and backbone providers.
- We are observing a trend where companies are increasingly outsourcing their network services (including VPNs). Since this is a software solution that resides at the client location, our model might be perceived as a shift towards the "do-it-yourself VPN model" where the customer must play a larger role in setting up and managing the VPN service. We can manage this issue by providing consultant services, in which case we run into scalability issues.
- We must be able to provide a migration strategy from existing solutions (substitutes such as private/leased-line networks).
- The challenge we face with companies expanding towards global-scale networks is that most of them already utilize VPN solutions from global Internet service providers. Convincing these customers to switch to our VPN service would be a challenge because it would increase the number of points of contact for the customer. Network service providers also bundle VPN services as part of a larger package, thereby giving them a pricing advantage that we might not be able to overcome (for instance, a network service provider might provide discounted VPN services if the customer has already committed to using other network services such as VoIP).
- There is the challenge associated with managing deployment of our solution. Specifically, Tapestry software needs to be incorporated at every client node. We need to determine a cost efficient and scalable mechanism for managing the deployment to these nodes.

7. REFERENCES

[1] Boyd, J. MediaX cuts streaming pain. http://www.internetweek.com/infrastructure/infra111300.htm

[2] Czerwinski, S., Zhao, B. Y., Hodes, T., Joseph, A. D. and Katz, R. An architecture for a secure service discovery service. Proceedings of ACM MobiCom (August 1999).

[3] Harris, S. and Munroe, C. IP VPN Services: U.S. Market Forecast and Analysis, 2000-2005. Available at: http://www.idc.com

[4] Kubiatowicz J. D. et al. OceanStore: An architecture for global-scale persistent storage. Proceedings of ACM ASPLOS (November, 2000).

[5] Rhea, S., Wells, C., Eaton, P., Geels, D., Zhao, B. Y., Weatherspoon, H. and Kubiatowicz, J. D. Maintenance-free global storage in OceanStore. Submitted for publication, (March, 2001).

[6] Weatherspoon, H., Wells, C., Eaton, P., Zhao, B. Y., and Kubiatowicz, J. D. Silverback: A global-scale archival system. U.C.B. Technical Report #UCB/CSD-01-1139 (March 2001), also submitted for publication. Available at *http://oceanstore.cs.berkeley.edu/publications.*

[7] Zhao, B. Y., Kubiatowicz, J. D., and Joseph, A. D. Tapestry: An infrastructure for fault-tolerant wide-area location and routing. U.C.B. Technical Report #UCB/CSD-01-1141 (April 2001). Available at *http://oceanstore.cs.berkeley.edu/publications*

[8] Zhuang, S., Zhao, B. Y., Joseph, A. D., Katz, R. and Kubiatowicz, J. D. Bayeux: An architecture for scalable and fault-tolerant wide-area data dissemination. Proceedings of ACM NOSSDAV (June 2001).

Appendix A

Figure 1: Streamming Media Marketshare.

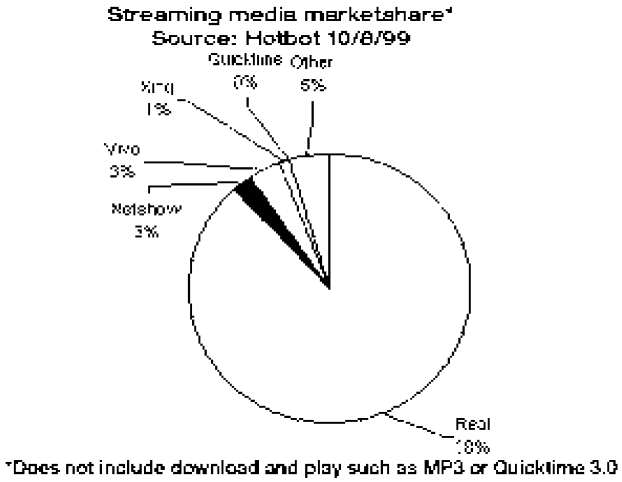


Figure 2: VPN Application of Intranet, Extranet, Remote Access, and Hosting.

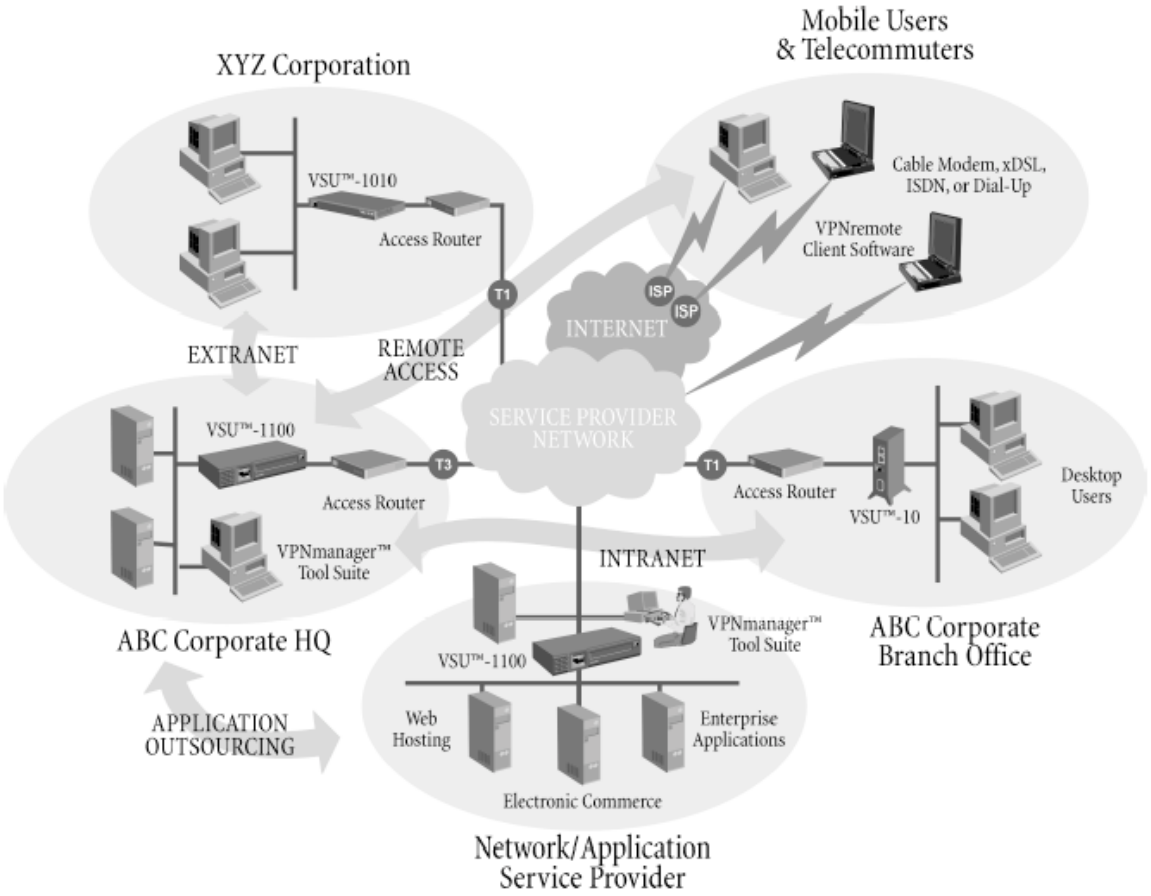
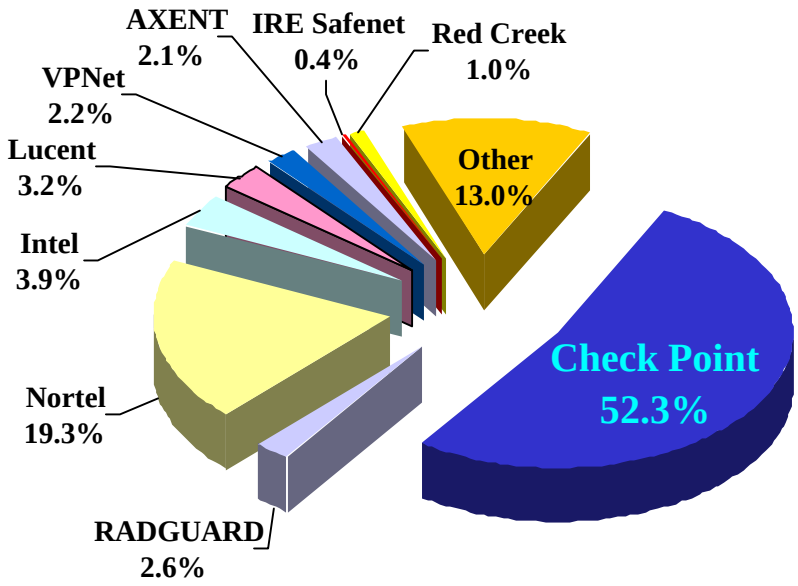


Figure 2 above shows three different basic kinds of VPN: Access VPN, Intranet VPN and Extranet VPN. Intra-company VPN (intranet) is used for communication among different corporate offices of a company and an inter-company VPN (extranet) is used for secure communication across different company. Access VPN appeals to a highly mobile work force, handling remote-access connectivity for mobile users, telecommuters, and small offices through a broad range of technologies. VPN reduces long distance communication costs. One just needs to make local Internet call to connect to the network and share data securely.

Figure 3: 1999 Worldwide VPN Revenue Market Share.



Source: "IPSec VPNs Go Mainstream", Gartner Group Inc., July 10, 2000

Table 1: Summary of the analysis of three potential applications.

Application	Attractiveness of Underlying Market	*1.1.1.1 Rationale*
Multimedia Streaming	Low	400 M (2000) Uncertain future demand
EACD	Low	500 M (2000) Flat growth, Unproven market
VPNs	High	2B annual (2000), 3.5B (2001)* High projected growth

Figure 4: Private Line Versus IP VPN.

Private Line Versus IP VPN – Monthly Operating Costs

5 Site Private Line Solution

Capital Costs

	Unit Cost ($)	Total Costs ($)
Integrated CSU/DSU	1,000	5,000
Router	2,000	10,000
T-1 Installation	300	1,500
Total Capital Costs	*3,300*	*16,500*

Monthly Operation Costs

	NRC ($)	Unit Cost ($)	Monthly Costs ($)
T-1 Local Connection	1,000	600	3,000
T-1 WAN Connection	3,500	1,200	6,000
T-1 Line Mileage (500 miles)		1,000	5,000
Hub & Spoke Network			
Total Operations	*4,500*	*2,800*	*14,000*

5 Site IP VPN Solution

Capital Costs

	Unit Cost ($)	Total Costs ($)
VPN Box	0	0
T-1 Installation	300	1,500
Total Capital Costs	*300*	*1,500*

Monthly Operation Costs

	NRC ($)	Unit Cost ($)	Monthly Costs ($)
Local Connection	1,000	600	3,000
T-1 Port Costs	15,000	1,695	8,475
Total Operations	*16,000*	*2,295*	*11,475*

IP VPN Capital Cost Savings = 91%
Monthly Operations Cost Savings = 12%

Source: IDC Estimates, WorldCom VPN Prices,