Understanding and Implementing Dial Virtual Private Networking (VPN) Services

Bay Networks

Table of Contents

Executive Summary

Corporate interest in outsourcing remote access is increasing as some companies focus more strongly on their core businesses by off-loading support and purchase of dial-access solutions. As confidence in using the Internet as a viable network infrastructure builds, customer demand for value-added services that use the Internet is increasing. The number of mobile workers and telecommuting workers is also growing, making Dial Virtual Private Networks (VPNs) one of the most popular of these value-added services.

Dial VPNs benefit both the enterprise and the service provider:

- Corporations that outsource remote access forego costs incurred in purchasing and supporting an enterprise remote access infrastructure.
- Corporations can leverage the ubiquity of the Internet to provide seamless and secure connectivity to both employees and business partners over a single network infrastructure.
- From the enterprise perspective, Dial VPN-based extranets can enhance relationships with customers, business partners, and suppliers.
- Phone companies can alleviate end-point congestion in the PSTN by implementing Dial VPN services.
- ISPs can increase revenues by offering secure, outsourced remote access services to corporations.
- ISPs may choose to differentiate their Dial VPN offerings by layering in extranet and content-related services, as well.

Secure communications, industry-standard network management, and rich network administration services are important features for network managers implementing Dial VPN services. Secure communications are provided through a combination of tunneling, encryption, and user authentication.

Tunneling links two network devices such that the devices appear to exist on a common, private backbone. Encryption and user authentication provide necessary security services for private traffic traversing the public network.

In deploying Dial VPN services, network managers require device and element-level management capabilities, value-added applications, and the ability to customize. Value-added applications include network design, network simulation and validation features, and network operations tools. Accounting and billing features are critical utilities for service providers, particularly those looking to increase net income via these services. The network management service must provide both user and subscriber accounting. These features not only support efficient, profitable operations but also help to measure the reliability of the service.

In choosing a remote access solution, corporations and service providers should look toward a vendor with broad-based expertise in the networking industry paired with a set of industry-leading, standards-based products and technologies. Vendors providing high-value, carrier-class, interoperable solutions will dominate in the Dial VPN marketplace.

Introduction

One of the fastest growing areas of the networking industry is remote access to virtual private networks (VPNs). Driven by the boom in inexpensive Internet access and by increasing use of remote access to corporate networks, dial-up access to corporate networks over the public IP infrastructure makes access to network resources less expensive, more efficient, and more secure for corporations. As switching solutions are introduced to alleviate Internet backbone congestion, Internet users and corporations look to the Internet as a viable remote access highway. For ISPs, telephone companies, and cable operators, Dial VPN services are both a growing revenue base and a differentiator in the competitive telecommunications industry.

Traditionally, VPNs were provided in the form of broadband packet switched services such as Frame Relay or X.25. Now, with the advent of the Internet as a viable service infrastructure, it is possible to run VPN services over an alternative protocol — IP. And, while traditional VPNs are very useful for LAN-to-LAN connectivity, they do not easily accommodate individual users whose only access to the outside world is in the form of their PC, a modem,and the public switched telephone network (PSTN). VPNs that run over IP are easily accessed by these users.

When network trade publications and analysts address VPNs, focus is typically on alternate tunneling protocols. Tunneling, however, is only one of the key issues important in deploying VPNs. Network security and network management are both vitally important in implementing VPNs successfully.

What exactly is a VPN? A VPN is a service that appears to users as if they were connected directly to their private network, yet the service actually uses a public infrastructure to facilitate the connection.

This paper describes the market for Dial VPNs and the applications for which they are best suited. It also provides perspective on the technologies that make Dial VPNs possible. The paper cites key issues that service providers should consider when deploying VPN services. A checklist is included to help customers choose a Dial VPN vendor. Last is a discussion of VPN market trends.

The Need For Dial VPNs

The tremendous growth in demand for service provider-based, dial access to VPNs is being driven by the many factors described below.

The Internet as a Viable VPN

There is ever-increasing demand for dial access to corporate networks, the Internet, and other online services. Confidence in the Internet as a viable infrastructure for conducting business is increasing. Meanwhile, advanced technologies make the Internet a viable VPN infrastructure, like the public Frame Relay and X.25 packet-switched networks.

Growth in Mobile Computing

There is an emerging paradigm in personal computer use featuring mobile and work-at-home telecommuters, and an increase in small office/home office (SOHO) access to corporate data centers and intranets. Much of this is being fueled by the increased availability of inexpensive Integrated Services Digital Network (ISDN), which offers better performance and reliability than analog dial services, particularly for Internet access and telecommuting. ISDN is pervasive throughout Europe.

Corporate Focus on Outsourcing Remote Access Service

Corporate IS departments are seeking to offload the significant costs of purchasing and supporting remote access infrastructures. Small service providers, offering specialized information services, are also becoming interested in outsourcing their dial access infrastructure to larger service providers. They look to outsourcing as a way to contain their own costs and to increase their efficiency in receiving data from the carrier network.

Differentiation for Service Providers

Service providers increase revenues and attract new customers by allowing local users to access their dial infrastructure and tunnel through to their corporate networks. This provides secure point-to-point communications for corporate users. With tunneling, data is encapsulated inside IP packets and routed from the tunnel origination point, such as a sales representative's laptop, through the service provider network to the tunnel endpoint, such as the sales representative's enterprise network. Additionally, VPNs are ideal for supporting extranets, which use the public Internet and Internet tools such as web browsers to provide value-added services to end users. An extranet can be used by a company to give its preferred customers access to internal resources such as online ordering or inventory tracking systems that may reside on the company's intranet. More and more companies are implementing extranets as one way to improve customer satisfaction. Other example applications include distance learning and online gaming in which authorized users have access to specific resources.

Congestion in the PSTN

Traditional voice carriers, including many of the Regional Bell Operating Companies (RBOCs), report that the circuit switches that comprise the PSTN are becoming overloaded. This congestion is due to the long hold times of computer users accessing corporate networks, the Internet, and other online services. Dial VPNs can be used by phone companies to alleviate congestion at the end point.

Carriers are playing a key role in providing dial access to the Internet, whether or not they provide IP routing or Internet services. There is tremendous interest among the telcos in offering both remote access and whole network outsourcing services to corporate customers, as well as direct Internet access using a common remote access infrastructure.

Applications for the Market

Service providers have evolved a variety of models for offering VPN solutions that provide secure, point-to-point data communications to their users. In fact, different providers define VPNs in different ways and the diversity of their offerings reflect this. For the purposes of this paper, however, two primary types of VPN services are most relevant.

The first type of VPN service is one in which a company outsources its remote access resources, including modem banks and analog or digital circuits. The company might also outsource the personnel resources required to support a remote access user community. The second is a service in which an ISP "wholesales" its remote access out to a larger provider. The motivating factors are primarily cost and efficiency. With many ISPs now offering low cost or even free Internet access, profit margins for "plain old" access have eroded significantly. Instead, many ISPs focus on content-related services such as gaming, Internet fax, multicasting, and others. Additionally, the same T1 facilities that previously delivered 24 analog modem-connected subscribers can support many more subscribers since the data is now delivered via a statistically multiplexed network such as Frame Relay.

Service providers offer VPN or intranet services for companies choosing to outsource remote access service. An intranet uses Web-based technology to connect an organization's distributed LANs, branch offices, mobile users, and telecommuters to applications such as:

- Internal e-mail
- Company-provided (and controlled) Web access
- Internal database access
- Intranet Web serving and publishing

For organizations looking to spread remote access over their extended enterprise, providers can offer "external" VPN, or extranet services. This adds controlled, secure connections between the organizations' users and its suppliers, business partners, contractors, and vendors for applications such as:

- Joint product development
- Online ordering and electronic commerce
- Inventory management
- Sharing of proprietary or confidential data
- Customer support and service
- Data backup and warehousing

ISP-based Remote Access

Because ISPs already sell access to the Internet and often own their own Remote Access Server (RAS) equipment, it's logical for them to host connections for their remote clients. This allows the service provider to develop a comprehensive set of new services, including customized news and information services, workgroup/workflow applications, Web site development, and others that can be targeted at the appropriate customer.

Telco-based Remote Access

With Dial VPN technologies, telcos can offer a service wherein the remote access infrastructure, including analog phone circuits, ISDN circuits, access concentrators, communications servers, multi-service switches, software, and the associated customer service functions are found not at the customer premise or service provider's point of presence (POP), but in the telco's Central Office (CO). Typical subscribers to this service are corporate customers or regional service providers looking to outsource their remote access infrastructure in order to cut costs and improve efficiency.

Telco-based service can take two forms. In one form, the service is offered as a path to the customer premise or service providers' POP. User administration and authentication are handled by the subscriber, although there is a subscriber database, which includes billing information that is maintained by the telco. In the second form, the telco offers direct access as well as advanced IP services. Advanced services might include hosting World Wide Web sites, providing e-mail, and FTP services.

Dial VPNs

Much of the public discussion surrounding VPNs thus far has centered around tunneling. Tunneling, however is merely one component of a complete and robust Dial VPN service architecture. In addition to the tunneling techniques supported within the service, any description of a Dial VPN service must contain a description of how the service handles security, as well as network management and administration.

Figure 1 | **Typical Layout of a Tunneled Packet**

Table 1 | **Comparing Layer 3 and Layer 2 Tunneling**

Pros	Cons
Layer 3 Tunneling	
Scalability	Limited vendor participation
Security	Complex to develop
Reliability	
Layer 2 Tunneling	
Simplicity	Standards still evolving
End-to-end compression/encryption	Questions on scalability
Bi-directional tunnel initiation	Questions on reliability (PPP timers, etc.)
	Limited to PPP payload types
	Questions on security

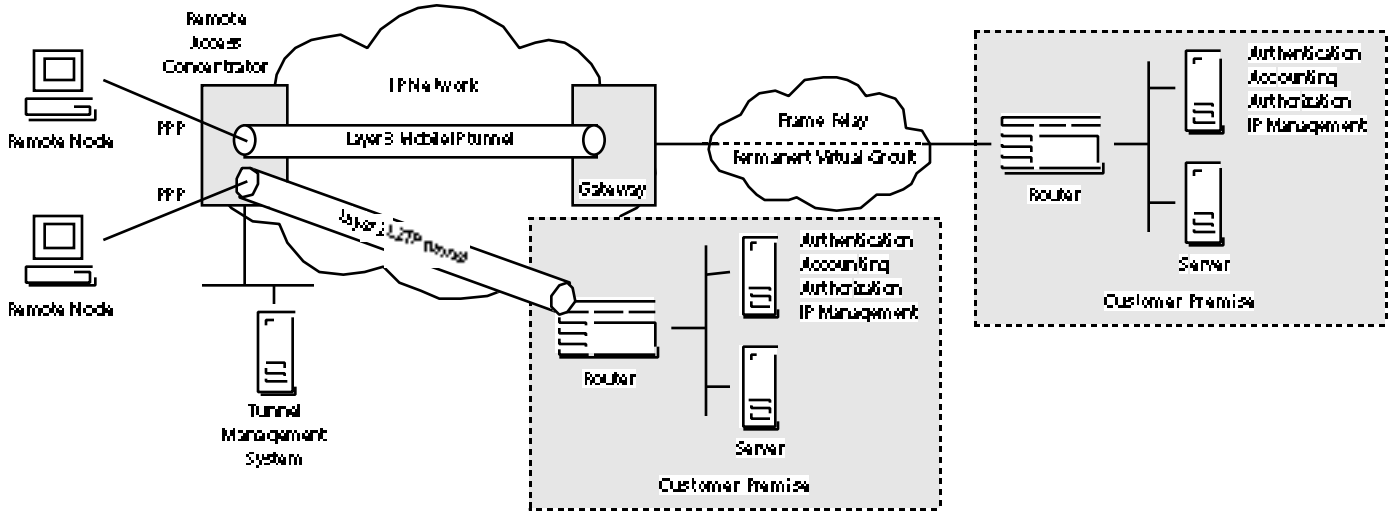
Tunneling

Dial VPNs are built upon the notion of efficiently and securely tunneling data from one point to another. With tunneling, the remote access server wraps the user data (payload) inside IP packets, which are routed through the carrier's network, or even across multiple networks in the case of the Internet, to the tunnel endpoint where the tunneled packet is unwrapped and forwarded in its original form. Tunneling is used by corporations shifting their remote access traffic from switched, long distance, and regional carriers to ISPs and the Internet. Tunneling uses point-to-point session protocols to replace switched connections, linking data addresses over a routed network. This replaces the linkage of telephone numbers over a switched telephone network. Tunneling allows authorized mobile workers, and perhaps authorized customers, to reach your enterprise network anytime and from anywhere. In tandem with authentication techniques, tunneling also prevents unauthorized access to your corporate network.

There have been a number of proposals made to the Internet Engineering Task Force (IETF) as to how this tunneling should be performed. These include Point-to-Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), Virtual Tunneling Protocol (VTP), and Mobile IP. Supported by different groups of networking vendors, these proposed standards specify how remote devices can access corporate networks and the Internet in a simple and secure manner. Figure 1 depicts a packet format used for tunneling data.

Tunneling technology is useful for a number of reasons. First, an IP tunnel can accommodate nearly any type of payload. A user with a desktop or portable computer can dial into the VPN to access their corporate IP, Internet Packet Exchange (IPX), or AppleTalk network in a transparent fashion. Second, tunnels can accommodate many users simultaneously or many different types of payload simultaneously. This is done using encapsulation types such as Generic Routing Encapsulation (GRE) as defined by IETF RFC 1701. Third, IP tunnels must be used to reach corporations, which do not advertise their IP network addresses over the Internet. Fourth, tunneling allows the recipient to filter out or report on individual, tunneled connections.

Figure 2 | **Layer 3 and Layer 2 Tunneling Implementations**



Layer 3 Tunneling and Layer 2 Tunneling

IETF proposals for tunneling traffic over Dial VPNs can be sorted into two groups: Layer 3 tunneling (like IPSEC or Mobile IP) and Layer 2 tunneling (like L2TP). The major differences between Layer 3 tunneling and Layer 2 tunneling are in the locations where the tunnels are initiated and terminated, and in the nature of the payload.

Figure 2 shows that tunnel endpoints are in different locations depending on whether Layer 3 or Layer 2 tunneling is used. Using Layer 3 tunneling, the tunnel is both created and terminated in the service provider's network with the terminating device acting as a gateway to the customer premise. Also, the remote user's Point-to-Point Protocol (PPP) session is terminated at the Remote Access Server (RAS). Using Layer 2 tunneling, the tunnel is created either in the service provider's network at the RAS, or at the remote client. In a Layer 2 implementation the tunnel is terminated at the customer premise in a router or a general purpose server.

Layer 3 tunneling terminates the Layer 2 connection at the RAS. It carries only the Layer 3 payload through the tunnel to the tunnel endpoint in either the enterprise network or a router residing somewhere in the service provider's network. Layer 2 tunneling, on the other hand, carries the entire PPP frame over the service provider's backbone to a predetermined endpoint. Table 1 compares the two tunneling types.

Layer 3 tunneling has other advantages for corporations. Network managers, employing Layer 3 tunneling, need not install special software on either their remote nodes or on their Customer Premise Equipment (CPE). Since PPP and tunnel terminations are made on the service provider's equipment, the CPE is not burdened by these functions and is used simply as a router. Layer 3 tunneling can be implemented using a CPE from any vendor.

Corporate networks using Layer 3 tunneling don't require registered Internet addresses. This tunneling implementation also has a security advantage. Corporate network and remote node addresses are hidden from the service provider's network and also from other corporate networks connected to the service provider.

Service providers, implementing Layer 3 tunneling, do not participate in corporate networks' routing. Instead, the service provider handles the enterprise traffic as data packet traffic over their network. Service providers can scale their services more easily when they choose to implement Layer 3 tunneling in lieu of Layer 2 tunneling. Using Layer 3 tunneling, a Tunnel Management System may be based on a distributed database engine so that tunnel maintenance and packet encapsulation overhead are distributed across the service provider's equipment.

Security

The second key issue in deploying or implementing Dial VPN access is network security, i.e.,allowing remote dial-up connectivity while protecting corporate information from inadvertent (or unauthorized) access or eavesdropping. For most VPN services implemented with Layer 2 tunneling, the tunnel is terminated at the customer premise. This presents potential security issues for customers. The customer's CPE is within reach of both unauthorized users and viruses via their Internet connection.

In some network designs, tunnels are terminated behind customer firewalls. Certain types of IP tunneling require customers to connect directly to the Internet which can pose a security risk to the customer. To protect their networks from unauthorized users, many corporate customers erect firewalls behind their Internet routers. This restricts access from the Internet to resources such as the corporate Web server. When using IP tunneling, the device terminating the tunnels either needs to be in front of the firewall,allowing access from the Internet to a device that has access to secure, corporate resources, or behind the firewall. If the device is behind the firewall,the firewall must be open to allow tunneled packets through to the devices that will unwrap them. There are ways around this, however they make the process of configuring the firewall complex. Also, not all firewalls can effectively handle traffic that isn't terminated in the firewall.

Certain implementations of Dial VPN service based on Layer 3 tunneling are inherently more secure than services based on Layer 2 tunneling because with Layer 3 tunneling, the tunnel need not reach into the customer network. Instead, the tunnel may be terminated at the service provider's gateway. The Internet connection is then made only to a Frame Relay device.

Network Management and Administration

Last but not least is the need for network management and administration. Two key needs in managing a Dial VPN are Network Layer Address Management (NLAM) and tunnel management. Tunnel management refers to the external software application used to setup tunnels to maintain subscriber information,and to perform subscriber-level billing and accounting. Traditional network management functionality such as performance monitoring is required to manage a Dial VPN just as it is required for any other network or network service. The focus of this section is not network management in general. Instead, it raises the key issues related to effectively managing Dial VPNs.

Network Layer Address Management

Network Layer Address Management (NLAM) refers to the capabilities found within the architecture of a Dial VPN that handle tasks such as network layer address assignment for remote nodes, other network layer protocol-related configuration (filters, routing protocols, subnet masks, etc.), and domain registration. A VPN architecture with the proper capabilities should support the following: Remote Authentication Dial-In User Services (RADIUS, with the correct set of vendor extensions), Dynamic Host Control Protocol (DHCP or a functional equivalent),and Domain Name Services (DNS). RADIUS is not only required for authentication of users, but should also be the mechanism used to perform some, or even all,of the network layer configuration information. DHCP can be used in conjunction with RADIUS to pick remote node addresses from an address pool and assign them to a dial-in user. Clearly, this method will be more scalable than manual configuration of addresses within a RADIUS database. It is important to note that the system for managing Layer 3 addresses must be "stateful," meaning that once sessions are disconnected, addresses must be returned to the address pool associated with that user's domain.

Note the term "network layer" address management, as opposed to the term "IP address management". Since many corporations are still using protocols such as IPX and AppleTalk,it is important that address management services exist for these protocols as well as for IP. Unfortunately, there are not many standards that address non-IP address pooling, so products supporting IPX or AppleTalk address management for remote nodes are scarce.

What to Look for in a Dial VPN Solution

Performance Considerations

Network Resiliency

In today's competitive market, one of the challenges service providers face as they try to obtain and then retain customers is keeping the network available 100 percent of the time. More and more frequently, customers ask providers to guarantee a given level of uptime and impose penalties for non-performance. Strict mean time between failure (MTBF) standards are passed on to network equipment suppliers.

It is critical for Dial VPNs to provide comprehensive solutions, which help the network administrator to quickly diagnose errors and implement fixes without having to disable any equipment providing service in real-time.

Scalability

The most desirable service accommodates the greatest number of users while using the least amount of equipment. Network architecture, network equipment and network management must all be scalable.

Using Layer 2 tunneling, the entire PPP frame and its contents are transported through the network as payload. This is an inefficient use of available bandwidth. (However, if end-to-end compression is used, bandwidth is better utilized.) Transporting the entire PPP frame also introduces potential reliability issues since PPP Link Control Protocol (LCP) and Network Control Protocol (NCP) are time-sensitive. Frequently, the endpoints of the tunnel are separated by long distances and/or many hops. Under these conditions, PPP connections carried over Layer 2 tunnels may be prone to timeouts or frequent resets.

As mentioned earlier, Layer 2 tunneling also presents potential scaling problems for customer premise equipment. Most CPE, including routers and file servers, cannot scale easily to handle the number of PPP sessions or "states" that must be maintained simultaneously to accommodate the large number of users attempting to access corporate networks via tunneling. Vendors offering solutions based on Layer 2 tunneling will advise customers to either upgrade the existing equipment to accommodate the additional demand, or add equipment to be dedicated to the new services.

The bottom line is this: A vendor with a complete Dial VPN solution should offer a choice of Layer 2 and Layer 3 tunneling. The scalability of solutions based on Layer 2 tunneling is still questionable.

Security

Security is critically important in deploying Dial VPNs. Dial VPNs must be secure against access by unauthorized users. Data traversing the public data network is vulnerable to breaches. The network must prevent this either directly or indirectly through accommodating external security devices.

Security features also govern access to VPN services. Both subscribers, (typically corporations and ISPs) and individual users must be authenticated to the network. Authenticated users must be authorized to use various services provided by the Dial VPN.

It is essential that an IP-based VPN provide end-to-end data encryption between the remote client and the home network. Layer 2 tunneling can easily accommodate encryption schemes based on IPSEC or PPP encryption. Since Layer 3 tunneling terminates PPP at the RAS, it must use Layer 3 encryption. As IPSEC continues to evolve, it appears it will offer the best encryption services for Layer 3 tunneling.

Network Management

No matter how many features a service has, or how well it performs, it is not really viable unless it can be provisioned and managed by the service provider. The requirements for managing Dial VPNs are similar to those used in managing standard public or private data networks. There are three key areas to examine:

- Device or Element-Level Management
- Value-Added Management Applications
- Customization

Device or Element-Level Management

It is important to understand how well a device is instrumented for network management. No matter how good the management applications may be, if the device does not support the necessary functionality, the application may not be very helpful.

Above all, the configuration of network elements, such as remote access concentrators, gateways, switches, and routers must be as simple and straightforward to use as possible. Improper configuration of networking equipment can lead to delays in service deployment, which, in turn, can lead to lost revenues for the service provider.

In addition to configuration, change control and maintenance are critical factors. Change control and maintenance refer to the ability of network operators to modify parameters, implement adds/moves/changes, and reconfigure equipment dynamically without having to reboot or worse, bring down the entire network.

Value-Added Management Applications

Most vendors provide value-added applications for managing their own networks and network components. Very few vendors however provide the full suite of functionality necessary for managing a network, i.e., network design, network simulation and validation, network visualization, and network operations tools. Most vendors focus on network operations, i.e., providing applications that help keep their devices or elements up and running. The vendors who do provide a broader range of functionality typically offer standalone, proprietary applications. Before choosing a Dial VPN vendor, examine their network management product line and strategy closely. Assess how well the vendor addresses all of your network management needs. Make sure they offer some level of integration with best-of-breed, standards-based vendors for functionality such as multi-vendor billing applications, network design and validation tools, along with typical monitoring and troubleshooting capabilities.

Service Provisioning As with element-level configuration, simplicity in provisioning is a key factor. One additional requirement, however, is the flexibility of the system, including:

- The degree to which the provisioning system is extensible to an existing customer and service infrastructure.
- Its ability to provide true "end-to-end" provisioning.
- The number of different platforms supported by the provisioning system.
- Its ability to submit and schedule batch changes to the network.
- Its support of multiple authorization levels.

Many service providers are already using sophisticated Relational Database Management Systems (RDBMs) to store and manage customer data for operational and marketing purposes. These systems often include powerful forms generation tools that can be used to build graphical configuration or service provisioning tools. These RDBMs also support built-in features like automatic and programmable database replication and synchronization crucial to supporting large distributed networks. When possible, provisioning tools should have the ability to work within the constructs of these systems.

Monitoring and Troubleshooting When one thinks about network management, monitoring and troubleshooting typically come to mind first. The ability to look at the state of a connection, the number of packets that are traversing a port (in either direction), or a table that describes the networks visible to a networking device are all critical to the operation of any network, including one that is being used for VPN services.

To help troubleshoot and diagnose problems, equipment must have extensive logging capabilities and allow the user to filter out unwanted or unneeded log messages. More than anything else, logs can tell the real story about what is happening within a network.

Equipment must also have the ability to support monitoring and diagnostics from remote locations. Graphical interfaces will not typically suffice for monitoring and troubleshooting. Network devices must provide Telnet and/or asynchronous terminal connection — in addition to GUI interfaces — for monitoring and troubleshooting.

Accounting and Billing The network management service must provide both user and subscriber accounting. The system must generate reliable billing output efficiently, and feed it into the service provider's billing system easily. User accounting generally refers to the amount of time each user is connected to the VPN. Subscriber accounting tracks data such as the subscription beginning and ending dates and the number of simultaneous connections (tunnels) allowed for that subscriber.

Many service providers, particularly regional Internet providers, are now offering flat rate access to the Internet. Most industry experts agree that this model, while effective in attracting new users, could prevent providers from diversifying their service offerings. Therefore, usage-based accounting will be important in the long term.

Industry analysts report that users of Internet or VPN services will pay a premium for high reliability, high performance, or special service levels. Users will also pay for guaranteed service quality. Quality guarantees could apply to services such as distance learning, online gaming, or multimedia which require certain throughput levels, latency, or multicast support.

A fully-featured network management system will track packet counts and may even account for packets of certain types. For example, a service provider may choose to offer Bronze, Silver, Gold, and Platinum levels of service which would assign all users within a specific domain a certain Quality of Service level. Packets marked with specific Quality of Service values may be used to generate separate byte counts so that those packets are billed at a different rate than unmarked packets.

Customization

Many vendors provide network management software and hardware if appropriate, but few address the fact that their customers have existing network management operations centers. At a minimum, the vendor's products must fit into their customers' environment without affecting the operations of the existing tools. Ideally, the vendor's network management products would integrate into and leverage the customers' existing tools. Some of this can be predetermined and addressed, but each network operations center is unique. Does your vendor of choice have any resources to address this issue?

BayStream Dial VPN Services

For service providers who want to provide Dial VPN access, Bay Networks offers BayStream™ Dial VPN Services, a complete software suite designed to run on Bay Networks 5000 Multi-Service Access Switch (MSX), standalone Remote Access Servers, and platforms running BayStream multi-service software.

BayStream Dial VPN Services make it easy to provide dial-in customers with simple, secure access to the Internet and to corporate VPNs. It is heavily standards-based, for near-plug-and-play compatibility in most existing dial-in environments.

Today, Bay Networks Dial VPN Services is based on the Mobile IP architecture defined by the IETF. In order to optimize Mobile IP for Bay Networks VPN service architecture, several extensions were added to the Mobile IP implementation. In Bay Networks implementation, the Remote Access Server (RAS) runs the Mobile IP Foreign Agent (FA) and the BayStream Gateway runs the Mobile IP Home Agent (HA). This implementation provides a very secure, efficient, and scalable Dial VPN solution.

Network Resiliency

Bay Networks has a long tradition of building highly resilient networks by building fault resiliency into its platforms. Fully redundant systems such as the Backbone Node router family are crucial to maintaining 100 percent network availability.

Also critical to the resiliency of a Dial VPN architecture is the network administrator's ability to quickly diagnose errors and implement fixes without having to disable any of the equipment that is providing service in real-time. Bay Networks 5399 Remote Access Concentrator and BayStream software provide network administrators the flexibility and ease of use required to fix problems with a minimal impact on service availability.

Bay Networks engineering is also constantly looking for ways to improve system up-time levels. By driving enhancements to existing technology within standards bodies such as the Frame Relay Forum and the IETF, network level signaling, more robust transport layer protocols, and fast network-wide convergence of routing tables can be implemented in standards and applied to heterogeneous networking environments. By improving its own platforms and systems, such as adding secondary gateway support, Bay Networks continues to lead in providing highly available platforms, systems, and services.

Scalability

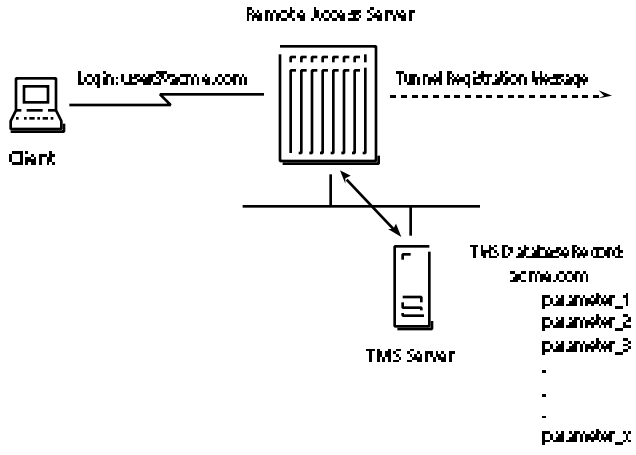
In the BayStream Dial VPN Services architecture, scalability of the gateway is critical since a large number of tunnels may terminate in a gateway simultaneously. There are two approaches to addressing scalability concerns.

In one approach the gateway is built upon Bay Networks Backbone Node router family which, because of its unique symmetric multiprocessor architecture, is highly scalable. Frame Relay ports, which act as gateway connections between the network and the customer premise, can be spread out among several slots without degrading the router's performance. Throughput is preserved because each slot is configured with its own processor which handles all calculations and forwarding activity for that slot.

In the second approach, PPP is terminated at the RAS. Therefore, the gateway is not responsible for maintaining the PPP state for each tunnel. This is different from other architectures, particularly those built on Layer 2 tunneling, where the device representing the tunnel termination point must also maintain the PPP state for each tunnel, draining processor and memory resources. In a BayStream Dial VPN Services network the gateway is responsible for only three processes: maintaining a table that maps each IP tunnel endpoint to a Frame Relay Data Link Connection Identifier (DLCI), forwarding packets through the gateway according to the entries in that table, and maintaining a proxy RADIUS client for each subscriber. These processes can be spread out over a number of slots.

The BayStream Dial VPN Services architecture is extremely scalable in that it distributes processing and forwarding decisions across the network. The RAS is responsible for handling PPP sessions and forwarding packets out its Ethernet port. These are design functions for which it is especially well-suited. The Tunnel Management Server interacts directly with each RAS that has a specifically defined and configured relationship to it. With these functions distributed over the network, the service provider's gateway can perform optimally.

Figure 3 | **BayStream Dial VPN Services Subscriber Authentication**



Security

The RAS typically provides access control while subscriber authentication is provided by the Bay Networks TMS. When a user logs into the RAS, the login includes the domain name, which may also include the Dialed Number Identification String (DNIS). The TMS's first function is to check the domain name against the TMS database. The following steps are followed for the authentication process as shown in Figure 3:

1. User logs in with domain name.
2. RAS relays the login name, including domain name, to the TMS.
3. TMS checks its database for a domain name match.
4. TMS, upon authenticating the domain name, sends accept packet to the RAS.
5. RAS initiates the tunnel registration process including all relevant parameters with the gateway. The address is identified within the accept packet.

This type of security includes RADIUS and Access Control Protocol (ACP). ACP is a Bay Networks protocol that can provide native authentication services. Alternately, this type of security could be implemented via an interface to RADIUS authentication or accounting servers.

Confidentiality

Bay Networks remote access platforms encrypt ACP authenticationmessages before sending them to the ACP server. The server decrypts the message, interprets it, and responds with another encrypted message.

Data encryption is a critical component to a VPN architecture. Phase I of BayStream Dial VPN Services also supports Layer 3 encryption,since it must route data using the information from the IP header. To provide the end-to-end encryption required by the Dial VPN service model,the remote client and the CPE must perform encryption and decryption since neither the RAS nor the gateway currently include these facilities. The RAS and gateway simply forward the encrypted data as if it were normal clear-text data.

As new techniques for encryption are integrated to the product line, and as protocols that provide "built-in" encryption services (such as IPSEC) are made available, they too will be considered an integral part of BayStream Dial VPN Services.

Audit Trail

Bay Networks TMS provides logs that give network operators a detailed picture of events that have taken place, or are taking place, within the network. As an aspect of security, audit logs can indicate such events as failed connection attempts or other attacks on network resources at the point of the attack.

TMS also provides logs indicating where and when:

1. New subscribers were entered.
2. Changes were made.
3. New circuits were created.

Network Management

Network Planning

Bay Networks provides detailed documentation for BayStream Dial VPN Services, where everything from the idiosyncrasies of configuring the CPE router to the ways in which remote clients obtain their IP addresses is described.

Element Configuration

Tools such as Bay Networks Site Manager, Quick2Config™, and Annex Manager™ are used to configure Bay Networks equipment quickly and easily. They're designed to reduce both the amount of time it takes for technicians to learn how to install the equipment and the amount of errors that technicians will make as they configure the equipment. The TMS is configured via an easy-to-use command line interface on a UNIX console.

Service Provisioning

BayStream Dial VPN Services is somewhat unique in terms of provisioning, since the service is provisioned mainly by configuration of the TMS. It supports two provisioning methods for the TMS.

First, Bay Networks has provided the Application Programming Interfaces (API) for the TMS application so that a service provider can layer a TMS application directly on top of its existing subscriber databases. Bay Networks recommends that the TMS system be built this way to take advantage of the powerful capabilities of these systems.

The second way to provision BayStream Dial VPN Services is simpler. Bay Networks provides the TMS application that is compatible with the NDBM database included with most UNIX platforms. The NDBM is flat, as opposed to relational, and utilizes a fairly simple command line interface to enter subscriber records into the TMS. It does not have the more sophisticated features of an RDBMS such as database replication and synchronization. However, it offers a more cost-effective solution and is ideal for systems where a single TMS is used, or for services that support a relatively small number of subscribers.

Monitoring and Troubleshooting

Bay Networks platforms have the most comprehensive set of built-in instrumentation in the networking industry today. In addition, all Bay Networks equipment uses embedded Simple Network Management Protocol (SNMP) agents, so any SNMP-based network monitoring tool can view statistics or other information from the network.

For each of the platforms that comprise BayStream Dial VPN Services, a comprehensive set of tools is available under the umbrella of OptivityServices that are designed to make it simple to monitor the system and diagnose problems. Tools such as PathMan™, RouterMan™, and Packet Capture and Trace and Performance (PCAP/TAP) are OptivityServices tools that can be used for network monitoring.

In addition to monitoring individual network elements such as routers and remote access concentrators, protocol-level signaling built into Bay Networks Mobile IP implementation allows the tunnel to maintain state at any given time. The state of a tunneled connection can be viewed from the perspective of either the RAS or the gateway in a BayStream Dial VPN Services network. A network administrator can also see, for example, how many tunnels are currently in use by any given subscriber by looking at statistics available from the TMS console.

Accounting and Billing

BayStream Dial VPN Services provides solutions for both user and subscriber accounting, while generating billing data that can easily be used by billing programs. User accounting is supported today via ACP and the Syslog functions of the RAS platform. Through its RADIUS interface, the RAS can also utilize RADIUS accounting services.

Change Control and Network Maintenance

Bay Networks equipment is configurable via SNMP SETs, allowing changes to be made dynamically without bringing down the node. Partial reboots are also possible as are individual port restarts. This means that new services can be configured and deployed on Bay Networks equipment easily and without service disruption.

Summary

To summarize, the Bay Networks solution offers the following benefits:

- No modifications or upgrades required to subscriber CPE.
- No modifications or upgrades required to remote client software.
- No addressing changes needed. Non-globally unique or overlapping IP addresses are allowed.
- Better security.
- Total control over the network by the service provider.
- Industry-leading network management.

The Future

When discussing the future of the VPN market, it is important to note a few of the trends, some of which are already taking place.

Whole Network Outsourcing

Customers are seriously considering outsourcing their remote access infrastructure. In the future, some enterprises will outsource their entire network to integrators and service providers with demonstrated expertise in full support of network infrastructures. In this model, the customer owns its data and its hosts. The network "plumbing," however, is managed completely by the service provider. Integrators such as Perot Systems already provide this type of service.

Alternative VPN Access Types

Most Dial VPN offerings today, including BayStream Dial VPN Services, are based on switched connectivity to the Dial VPN. While most connections to corporate intranets or the Internet are initiated via the PSTN with ISDN or analog modem calls, other means of access including cable modems and x DSL (Digital Subscriber Line) present intriguing possibilities and new challenges for service providers.

New Protocols

Today, special tunneling protocols such as Mobile IP or L2TP are required for VPN functionality. Emerging standards such as IPSEC and IP Version 6 enable secure, encrypted encapsulation and tunneling for user data. Since customers are extremely sensitive about the privacy of their data over the public network, more highly integrated VPN techniques will, no doubt, be popular.

Conclusion

Dial VPN Services represents an industry and a class of service that is still in its infancy. Carriers will meet the challenge of replacing corporations' in-house remote access solutions by delivering reliable, enhanced services. In turn, customers will foster growth of high-quality Dial VPN services through their willingness to pay a premium for service level guarantees.

Finally, many of the standards that these services will be based on are still under development. This is important, since focusing on a complete, standards-based solution will ensure that investments in outsourced networking services do, in fact, meet the availability, security, performance, and cost requirements of enterprise customers. The vendor who delivers the complete, standards-based solution will ultimately dominate.

Sources for Additional Information

A variety of VPN-related articles have been written in some of the more popular networking industry trade publications. These articles are all available from the World Wide Web via their respective publication's sites:

1. "Tunneling is Key to Secure Extranets," Network World, 3/3/97, James Kobeilus
2. "Sorting through the VPN protocols," Network World, 3/3/97, Alex Henthorn
3. "Bay Secures Remote Access," Network World, 2/24/97, Jim Duffy
4. "VPN Standards Contribute Confusion," LAN Times, 11/11/96, Joe Paone
5. "Safer Nets?," Communications Week, 3/17/97, Kelly Jackson Higgins
6. "L2TP Proposal Should Eliminate Tunnel Vision," PC Week, 3/3/97, Lauren G. Paul
7. "Tunnel Vision," PC Week, 9/17/96, Lauren G. Paul

There are also a number of VPN-related standards documents that can be found on the Internet as part of the Internet Engineering Task Force (IETF) Web site. There are separate indexes for Draft Standards and Requests for Comments (RFC). The following is a list of VPN-related standards. The list is by no means comprehensive, but is a useful start nonetheless:

1. "IP Mobility Support," IETF Network Working Group, RFC 2002, C. Perkins, 10/96
2. "Generic Routing Encapsulation," IETF Network Working Group, RFC 1701, . Hanks, T. Li, D. Farinacci, P. Traina, 10/94
3. "Layer Two Tunneling Protocol (L2TP), Internet Draft, A Valencia,K. Hamzeh, T. Kolar, M. Littlewood, G. Pall,J. Taarud, 12/23/1996, draft-ietf-pppext-l2tp-01.txt
4. "Remote Authentication Dial In User Service (RADIUS)," IETF Network Working Group, RFC 2058, C. Rigney, A. Rubens, W. Simpson,S. Willens, 1/97
5. "RADIUS Accounting," IETF Network Working Group, RFC 2059, C. Rigney, 1/97
6. "Dynamic Host Configuration Protocol (DHCP)," Internet Draft, R. Droms, 12/27/1996, draft-ietf-dhc-dhcp-09.txt
7. "Internet Security Association and Key Management Protocol (ISAKMP)", Internet Draft, D. Maughan,M.Schertler, M.Schneider,, 02/20/1997, draft-ietf-ipsec-isakmp-07.txt
8. "Simple Key-Management For Internet Protocols (SKIP)", Internet Draft, A. Aziz, T. Markson,H. Prafullchandra,, 08/14/1996, draft-ietf-ipsec-skip-07.txt
9. "Implementation of Virtual Private Network (VPNs) with IP Security", Internet Draft, N. Doraswamy, 03/14/1997, draft-ietf-ipsec-vpn-00.txt
10. "Point-to-Point Tunneling Protocol – PPTP," Internet Draft, K. Hamzeh,G. Singh Pall, W. Verthein,J. Taarud, W. Andrew Little, 6/96, draft-ietf-ppext-pptp-00.txt
11. "Layer Two Forwarding (L2F)," Internet Draft, A. Valencia,M. Littlewood, T. Kolar, 4/96, draft-ietf-ppext-l2f-02.txt

Appendix A — A Dial VPN Checklist

Review this checklist when you're determining which vendor to use for a VPN:

- Supports both Layer 2 and Layer 3 tunneling, or intends to support both.
- Provides solid and comprehensive solutions that aid the network administrator in quickly diagnosing errors and implementing fixes without having to disable any of the equipment that is providing service in real-time.
- Is scalable, specifically with equipment and network management, as well as network architecture.
- Prevents breaches, either directly or indirectly, through its accommodation of external security devices.
- Both subscribers, typically corporations and ISPs, and individual users are authenticated to the network.
- Authenticated users are authorized to use the various services of the VPN.
- Provides system level security to its subscribers.
- The configuration of network elements (e.g. remote access concentrators, gateways, switches, routers) is as simple and straightforward to use as possible.
- Provides network operators the ability to modify network parameters;add, remove, or change the location of equipment;or reconfigure the network dynamically, without having to bring down the entire network,or even portions of it.
- Provides the full suite of functionality necessary for managing a network: network design,network simulation and validation,network visualization,and network operations tools.
- Offers some level of integration with best-of-breed vendors for functionality such as multivendor billing applications, network design and validation tools, along with monitoring and troubleshooting capabilities.
- At a minimum integrates into, but hopefully leverages, the tools in the existing network environment.
- Requires no modifications or upgrades to subscriber customer premise equipment, or to remote client software.
- No addressing changes are needed. Non-globally unique or overlapping IP addresses are allowed.
- Provides complete, accurate documentation that assists network managers and network planners in the initial installation and ongoing management of the network.

Appendix B — Guide to VPN Acronyms

3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, and Accounting
ACP	Access Control Protocol
ARA	AppleTalk Remote Access
ARAP	AppleTalk Remote Access Protocol
CAP	Competitive Access Provider
CHAP	Challenge Authentication Protocol
CLI	Command Line Interface
CO	Central Office
CPE	Customer Premise Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Connection Identifier
DNIS	Dialed Number Identification String
DNS	Domain Name Service or Domain Name Server
DS0	Digital Signal 0 - 64 Kbps
DS1	Digital Signal 1 - 1.544 Mbps
DSL	Digital Subscriber Line
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
GW	Gateway
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	Internet Protocol Security
IPVPN	IP-based Virtual Private Network
IPX	Internet Packet Exchange
ISP	Internet Service Provider
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LCP	Link Control Protocol
LEC	Local Exchange Carrier
MAC	Message Authentication Code
MD5	Message Digest 5
MPEC	Microsoft's encryption control protocol
MSX	Multi-Service Access Switch
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
NCP	Network Control Protocol
NLAM	Network Layer Address Management
OSI	Open Systems Interconnect
PAP	Password Authentication Protocol
PCAP/TAP	Packet Capture and Trace & Performance
PKIX	Public Key Infrastructure using X.509 standards
POP	Point of Presence
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Authentication for Dial-In User Services
RAS	Remote Access Server
RBOC	Regional Bell Operating Company
RDBMS	Relational Database Management Systems
ROBO	Remote Office/Branch Office
RSA	Rivest-Shamir-Adelman public-key cryptosystem
SHA-1	Secure Hash Algorithm
SLIP	Serial Line Internet Protocol
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SVC	Switched Virtual Circuit
TMA	Tunnel Management
TMS	Tunnel Management Server
UNI	User Network Interface
VLAN	Virtual LAN
VPN	Virtual Private Network
VTP	Virtual Tunneling Protocol

For more sales and product information,please call **1-800-8-BAYNET**.

United States

Bay Networks, Inc.
4401 Great America Parkway
Santa Clara, CA 95054
1-800-8-BAYNET

Bay Networks, Inc.
8 Federal Street
Billerica,MA 01821-5501
1-800-8-BAYNET

Europe, Middle East,and Africa

Bay Networks EMEA,S.A.
Les Cyclades – Immeuble Naxos
25 Allée Pierre Ziller
06560 Valbonne, France
+33-4-92-96-69-96 Fax
+33-4-92-96-69-66 Phone

Pacific Rim, Canada,and Latin America

Australia +61-2-9927-8888
Brazil +55-11-247-1244
Canada 416-733-8348
China +8610-6238-5177
Hong Kong +852-2-539-1388
India +91-11-613-7401
Japan +81-3-5402-7001
Mexico +52-5-480-1241
Singapore +65-323-3522

World Wide Web: **http://www.baynetworks.com**

6/97 WP522-2746EC-A