October 28, 1996

Ascend

COMPETITIVE BULLETIN

Virtual Private Networks

Virtual Private Networks (VPNs) connect both branch offices and telecommuters into an enterprise-wide corporate network, and can eliminate all long-distance charges, along with the management and security responsibilities of maintaining private networks. A local telephone call is made to the nearest Internet Service Provider Point-of-Presence (POP). From there the user session is routed to a private network for authentication and final connection. Private information, encapsulated in each packet transmitted via the Internet, may then be securely transferred to and from remote users. This is made possible through "tunneling."

What is Tunneling?

Tunneling is a technique by which one networking protocol is carried within another. Usually, a tunnel is created to allow functionality supported by a protocol natively. For example, IPX packets may be inserted into IP packets to allow the Internet to effectively interconnect IPX networks. These protocols are very general and allow multiple protocols along with robust authentication to operate over IP-only Internets.

Recent interest in tunneling to support VPNs has prompted new "tunneling protocols." For instance, L2TP (Layer-2 Tunneling Protocol) is an extension to the standard Point-to-Point Protocol (PPP), which is used to create multi-protocol VPNs via the public Internet.

Internet Tunneling and Ascend's Position Explained

Internet tunneling or Virtual Private Networking (VPN) is an emerging capability which affects Ascend and nearly all of its customer base: ISP's, carriers, and Fortune 1000 customers. At a minimum, Ascend employees should be able to speak knowledgeably about Internet tunneling or VPNs at a general level, and to clearly communicate Ascend's strategy with regard to tunneling.

For enterprise networks

Tunneling allows enterprise networks to outsource some or all of their network access to ISPs. Tunneling facilitates a new level of cooperation between carriers and enterprise networks. Issues such as authentication, network addressing and non-IP protocols are addressed by tunnel schemes.

Some large enterprise networks are organizationally constructed of internal service providers (MIS, telecom) and end-users (departments or work groups). For these networks, tunneling allows organizations to centralize their access capabilities and realize economies of scale.

Many organizations have made extensive use of unregistered IP addresses for their Intranets, which makes it difficult for them to connect to the Internet at large. Although the next version of IP (IPv6) will accommodate these unregistered addressees, it will not be broadly deployed for several years. In the meantime, tunneling is the answer to many of the addressing problems.

ASCEND

Non-IP protocols

Many enterprise networks make heavy use of non-IP protocols, specifically IPX. Tunneling allows an ISP to offer access to enterprise IPX networks using the ISP's IP-only network.

Internet Service Providers

Tunneling allows ISPs to offer new suites of services including secure Virtual Private Networks (VPNs). Tunneling over an ISP network may eventually replace X.25-based VPNs.

Carriers

Tunneling allows carriers to offer raw transparent dial-access for ISPs. An ISP can "rent" private or shared dial-in ports within a wide service area. The carrier tunnels the dial-in traffic over frame relay or ATM VCs to the Internet Service Provider. This is not only a new source of revenue for the carrier but also helps use their dial network more efficiently and may reduce circuit-switched facility requirements.

Tunneling's two end-points

On the client (user) side

The tunnel is established and maintained on the user's host computer. For example, users attempting to tunnel to their enterprise network LAN use tunneling software on their laptops. The laptops connect normally with PPP to an ISP, and then the software establishes the tunnel. The ISP has no knowledge of the tunnel.

The network access server (NAS) initiates and maintains the tunnel on the user's behalf. This arrangement is usually considered "involuntary tunneling" because the user and the client machine are not aware that the tunnel is established. The ISP network directs the user to the appropriate tunnel termination point.

On the enterprise side

The tunnel is terminated at the boundary between the ISP and the enterprise network. The ISP may separate the tunneled traffic by routing it over a dedicated physical (leased line) or logical (PVC) connection.

Ascend's ATMP "gateway" mode operates the same way. An ATMP tunnel is terminated at a NAS on the enterprise network. ATMP "router" mode also operates this way. The tunnel is terminated on a dedicated server such as a Windows NT or Solaris.

The IETF

The Internet Engineering Task Force (IETF) is actively working on specifying tunnel protocols. There are two classes of protocols, Layer-2 and Layer-3. The distinction between these protocols is often clear in terms of how they operate but not clear in terms of the customer benefits. Generally, ISPs seem more interested in Layer-3 while enterprise networks and carriers are more interested in Layer-2.

STRATEGY: *It is far too early now to make any conclusions about who will use what or to hard-sell either technique. You should consult with your customer to understand their requirements, preferences if any, and if appropriate also provide them with informational briefings on the full range of tunneling issues. Demonstrating Ascend's full working knowledge of this technology area will increase customer confidence in Ascend, and limit competitors' ability to spread misinformation. Competitors hard-selling any particular tunneling approach at this stage may well damage their position in those accounts.*

Layer 2 Protocols (L2TP, PPTP, L2F)

These protocols are all based on tunneling PPP sessions. A user dials into a NAS which connects the PPP session to somewhere else by using an IP or frame relay network. In some ways, this arrangement is analogous to "call forwarding" where the call is being forwarded through an IP or frame relay network.

Layer 3 Protocols (ATMP, VTP, Mobile-IP)

Layer 3 protocols do not carry PPP messages but instead tunnel IP, IPX and Appletalk packets directly through the tunnel. They all have their own authentication schemes, which often rely on RADIUS.

ATMP (Ascend Tunnel Management Protocol)

Ascend's version of a Layer-3 protocol is based loosely on mobile-IP and the requirements from an MCI specification. ATMP has been documented and submitted to the IETF as an informational draft, which allows anyone to look at the specification. ATMP is not a standard and is not on a track to becoming one. Ascend has complete control of ATMP and can modify it quickly to meet specific customer requirements. ATMP will continue to be an Ascend proprietary tunnel protocol. There is work underway to build a server based on Solaris, which can terminate an ATMP tunnel. This is an option for customers that already have Sun Solaris running and prefer not to terminate the tunnel on a NAS Ascend. We are not aware of other companies that have or are developing ATMP products.

STRATEGY: *You should continue to actively promote ATMP as an immediately available Layer-3 tunneling solution from Ascend.*

L2TP (Layer-2 Tunneling Protocol)

L2TP is a Layer-2 protocol that is being actively developed by the IETF PPP-extensions working group chaired by Karl Fox of Ascend. It is a combination of L2F and PPTP but will probably be altered significantly as it moves through the IETF process. There have been two special interim IETF meetings so far where L2TP has been specifically discussed. It is expected that L2TP will become a solid specification 1Q97 and move through the standards track 3Q97 or 4Q97.

STRATEGY: *Currently it is Ascend's stated direction that L2TP is the long-range Layer-2 tunnel protocol. It will be implemented on Ascend products once the protocol is stable, estimated at mid-year 1997.*

PPTP (Point to Point Tunneling Protocol)

PPTP was developed primarily by Microsoft, Ascend, USR and 3COM. It has been implemented on Ascend products as well as Microsoft Windows NT. PPTP has been submitted as a draft to the IETF as a basis for L2TP but the original draft is not expected to be considered as a standard. Ascend will support PPTP as a mechanism to tunnel to Windows NT server. Microsoft may migrate to L2TP next year and make PPTP unnecessary. This comment, however, is completely speculative and the past behavior of the players in the past.

STRATEGY: *For Layer-2 tunneling, PPTP is Ascend's committed direction today. It is supported in the Ascend OS now, and it has been extensively tested with Windows NT 4.0. Ascend will migrate to L2TP at the same time Microsoft does.*

L2F (Layer 2 Forwarding)

Cisco's proprietary Layer-2 tunneling protocol, L2F, is designed to operate over both IP and frame relay networks. L2F does not have explicit call control protocols incorporated but does a reasonable job of authentication. L2F has been implemented in Cisco routers. Presumably, Cisco will implement L2TP since they have heavy involvement in its development. There is no assurance, of course, that they will stop advocating the use of L2F and may decide to enhance L2F to be more feature-rich than a future L2TP offering. This is also speculation but their history with routing protocols (IGRP, E-IGRP) are examples of this type of action.

STRATEGY: *This is Cisco's current approach to Layer-2 tunneling. Ascend does not support L2F and has no plans to do so.*

VTP (Virtual Tunnel Protocol a.k.a. CCA, SDTP, Layer 3)

This is USR's Layer-3 proprietary protocol. Like ATMP, VTP has been made public to the IETF but currently is not under consideration to be considered as a standard. VTP has been implemented by USR, Bay Networks and possibly other undisclosed companies. USR is attempting to assemble a Birds of the Feather (BOF) to discuss Layer 3 tunneling protocols. This area is highly politically charged and several major Ascend customers have been led to think that VTP is on a standards track within the IETF. **VTP is NOT currently on a standards track within the IETF**, and there are no expectations that it will be in the near future as USR does not have the support of a working group to host the discussions.

STRATEGY: *Ascend may become involved in the standardization of a Layer-3 standard if Ascend's customers continue to express interest in a standard Layer-3 tunneling protocol. Ascend will not push ATMP to the IETF but rather consider IETF-accepted protocols such as Mobile-IP as a basis for industry-wide consensus. Ascend does not support the USR VTP protocol and has no plans to do so.*

Mobile-IP

This has been developed by the Mobile-IP working group inside the IETF. It is designed to handle mobile clients but also contains much of the functionality to support VPN's

For questions or comments, please contact David Mayes.

ASCEND
Remote Networking
Solutions That Work.™

Ascend Communications, Inc.
One Ascend Plaza
1701 Harbor Bay Parkway
Alameda, CA 94502, USA
TEL: 510.769.6001
FAX: 510.747.2300

Toll Free: 800.621.9578
FAX Server: 415.688.4343
E-mail: info@ascend.com
Internet Web Site:
http://www.ascend.com