Tunnel Switching

3Com Technology Boosts VPN
Security and Flexibility
Tunnel Switching
3Com Technology Boosts VPN Security and Flexibility

Contents
What Is Tunnel Switching? 2
   An Important Part of Enterprise VPN Strategies 2
   A Flexible Means of Supporting Current and Future VPNs 3
Benefits of Tunnel Switching 3
   Improved VPN Security 3
   How Does Tunnel Switching Work? (box) 4
   Flexible VPN Management and Easier Administration 6
   Increased VPN Performance, Capacity, and Scalability 9
Adding a Tunnel Switch to Your Network 10
Evolving Your VPNs with New Standards 10
   From Point-to-Point Tunneling Protocol to Layer 2 Tunneling Protocol 10
   The Impact of IPSec 10
3Com Tunnel Switching Solutions 11
Conclusion 11
Virtual private networks (VPNs) are becoming an increasingly popular means for organizations to provide wide area connectivity to remote users and, in some cases, to branch offices and business partners. These private connections over shared public networks, such as the Internet, offer substantial cost savings compared with dedicated point-to-point connections like 800 numbers or leased lines.

Tunnel switching is an innovative technology that increases VPN security and flexibility by making it possible to extend tunnels inside firewalls and terminate them at any location. Tunnel switching also improves manageability by shielding remote tunnel users from changes in the internal network, boosts VPN performance by reducing tunnel set up and tear down overhead, and increases scalability by allowing multiple tunneling components to be cascaded as VPN demand grows.

This paper explains tunnel switching and its role in enterprise VPN strategies. It describes how tunnel switches work and the benefits of various tunnel switch deployment options. It also discusses how tunnel switches can simultaneously support multiple protocols (PPTP, L2TP, IPSec) and enable smooth transitions between them.

Tunnel Switching
3Com Technology Boosts VPN Security and Flexibility

An Important Part of Enterprise VPN Strategies
Tunnel switching increases security by moving primary security controls inside the network and adding a second layer of security at the edge. Instead of terminating the tunnel outside the firewall or in a “demilitarized zone” (DMZ) between two firewalls, then transmitting packets over an unsecured link to an internal server, enterprises can maintain packets in their secure tunnels through the firewall to the other side. This approach allows multiple protocols and applications to be supported while opening only a “pinhole” in the firewall for the tunneling protocol.

In addition, while the tunnel switch performs preliminary authentication on incoming tunnels, it need not be aware of encryption keys, digital signatures, and other security measures employed by tunnel terminators. As a result, the amount of security information

**Acronyms and Abbreviations**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIC</td>
<td>application-specific integrated circuit</td>
</tr>
<tr>
<td>BITW</td>
<td>bump in the wire</td>
</tr>
<tr>
<td>DMZ</td>
<td>demilitarized zone</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>ICSA</td>
<td>International Computer Security Association</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>IPX</td>
<td>Internetwork Packet Exchange</td>
</tr>
<tr>
<td>L2F</td>
<td>Layer 2 Forwarding</td>
</tr>
<tr>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MPPE</td>
<td>Microsoft Point-to-Point Encryption</td>
</tr>
</tbody>
</table>
stored at the network edge, requiring protection against potential threats from the Internet, is minimized. Nor does the tunnel switch participate in the Point-to-Point Protocol (PPP) sessions between the source and ultimate destination host; in the event that the tunnel switch is compromised, the PPP session is not.

Organizations can determine the level of security that will be applied to various types of tunneled traffic. Tunnel switches can direct employee traffic, for example, to one tunnel terminator, while traffic from consultants and suppliers is directed to another terminator that enforces stricter security. Government organizations and universities often use tunnel switching to allow internal agencies or departments to implement their own security policies, while still providing a single address for tunnels coming in from the outside world.

Other advantages of tunnel switching include improved VPN manageability. Enterprises can change the location of tunnel terminators, addressing schemes, or indeed the entire network topology behind the firewall without having to notify all tunnel initiators (which could comprise tens of thousands of remote users). Tunnel switching also facilitates VPN access to legacy applications and allows VPN users to be members of virtual local area networks (VLANs), simplifying user moves and changes.

Tunnel switching improves VPN performance, since aggregating PPP sessions within a single tunnel dramatically reduces overhead for tunnel set up, tear down, and state maintenance. As demand for VPN services grows and users opt for high-bandwidth connections (such as cable modems and xDSL), tunnel switching enables enterprises to smoothly scale their VPN infrastructure by adding multiple tunnel terminators or even cascading multiple tunnel switches and terminators. These changes to the network are transparent to users, who continue to address tunnels to the single publicly known IP address, that of the tunnel switch.

A Flexible Means of Supporting Current and Future VPNs
A tunnel switch can be “dropped into” most existing VPN architectures without changing network topology. Tunnel switches can handle tunneled legacy network protocols (IPX, SNA, DECnet, VINES, NetBEUI, etc.) and interoperate with existing network infrastructure (address provisioning, authentication, authorization, accounting).

Tunnel switches support both the Point-to-Point Tunneling Protocol (PPTP), a de facto standard, and the Layer 2 Tunneling Protocol (L2TP), a new industry standard. Enterprises thus gain the flexibility to offer VPN services to users who have a variety of client machines, or to gradually transition all users to a single protocol.

Moreover, tunnel switches, which serve a dual purpose as routers, also support Internet Protocol Security (IPSec) scenarios, including both transport mode and tunnel mode. IPSec transport mode is clearly going to become the dominant method of securing VPNs, including those that use PPTP and L2TP for tunneling. IPSec tunnel mode (sometimes called “Layer 3 tunneling”) will provide an alternative to L2TP, which will be attractive to IP-only networks but will coexist with L2TP for as long as most networks remain heterogeneous. Tunnel switches can be used in any of these situations. In fact, the same device could potentially switch both PPTP and L2TP tunnels while routing IPSec tunnels to IPSec security gateways inside the enterprise. For more information about tunneling standards and smooth transitions between them, see “Evolving Your VPNs with New Standards” on page 10.

Benefits of Tunnel Switching
VPNs with tunnel switches are more secure, easier to manage, and better equipped to handle rising traffic levels than nonswitched VPNs. The ability to terminate tunnels at multiple points behind the firewall offers both technical and business advantages.

Improved VPN Security
Tunnel switching improves security by providing a double line of security and reducing the exposure of IP addresses, passwords, encryption keys, digital certificates, and other security information at the network edge. In
Tunnel switches are true multiprotocol switches. Just as Ethernet switches can accept multiple LAN input streams and aggregate them into a single outgoing LAN connection, tunnel switches can accept multiple tunnels and aggregate them into a single outgoing tunnel. And while tunnel switches facilitate connections and forward traffic, they do not participate in the point-to-point conversation between source and destination hosts.

Figure 1 shows what happens in a tunnel-switched VPN. Two points are worthy of special note:

- Throughout this process, only pinholes are opened up through the firewall: one for the tunneling protocol and another for the initial Remote Authentication Dial-In User Service (RADIUS) inquiry.
- The tunnel switch extends the original tunnel to the tunnel terminator (TT) by switching the destination address. To do this, the tunnel switch only partially unwraps the PPP packet it received from the tunnel initiator (TI) before forwarding it on to the terminator. In contrast, some vendors that claim tunnel switching are actually performing routing. Routers must first terminate the tunnel, fully processing its contents, then initiate a new tunnel to the terminator. This adds latency and exposes security information at the network edge. Also, if the router cannot aggregate outgoing tunnels, there is additional overhead for setting up multiple individual tunnels.

It's helpful to think about the tunnel switching process as occurring in three stages:

**Stage 1.** The tunnel switch receives the tunnel and performs the initial setup of a PPP connection with the TI:

a. The initiator builds a tunnel to the tunnel switch (TS). In most cases, the initiator will be the PPP client. (In some cases, the tunnel will be initiated by an access concentrator on a service provider’s network after receiving PPP packets from the client.)

b. The tunnel switch performs the initial authentication phase of PPP session setup. Normally it will query an external authentication mechanism such as a RADIUS server, but the tunnel switch can also consult its own local database. The tunnel switch receives back a validation of the user’s name and password. It also receives a list of user...
Figure 2, the tunnel switch acts as a “main gate sentry post” that performs initial screening of visitors. Those it allows to reach the tunnel terminator, the “internal gate,” are subject to more stringent security measures that control exactly which network resources they can access.

Tunnel switches also increase security by allowing enterprises to differentiate and direct VPN traffic to specific end points. In Figure 3 on page 6, tunnels from employees and external users are directed to separate tunnel terminators, which apply appropriate security measures to provide access to appropriate resources.

Tunnel switching enables enterprises to allow only clients with acceptable IP addresses to access particular LAN administrative domains. For example, in Figure 4 on page 6, the Finance Department restricts access to only users with IP address in the Finance subnet. Tunnel switches facilitate this process because tunnel terminators provide the required IP address directly to the PPP client. If a router were used instead of a true tunnel switch, the router would either have to build a tunnel to request the address, then proxy it back to the client, or perform address translation (in addition to encoding/decoding, encryption/decryption) for every packet.

Organizations that comprise departments or agencies operating with considerable autonomy can use tunnel switches to allow these...
entities to control their own security policies while still enjoying the economies of scale that come from a single VPN connection to the Internet. In Figure 5, all VPNs into a state government come in over the same tunnel switch, which forwards them to agency-managed tunnel terminators. In this way, the attorney general’s office could enforce much stronger security measures than, for example, a registry of public records.

**Flexible VPN Management and Easier Administration**

Tunnel switching allows enterprises to employ their choice of addressing schemes. Because the tunnel switch provides a single publicly known address for all incoming traffic, tunnel terminators, as shown in Figure 6, do not have to be assigned globally unique addresses. And the enterprise is free to change addresses or even the entire topology of the network without regard to their effect on VPNs. Because the tunnel switch intervenes between remote clients and the rest of the network, enterprises can add, move, or remove tunnel terminators at will, without having to notify users.

Enterprises that employ tunnel switching can more easily provide remote access to legacy application protocols not usually available in the DMZ. In Figure 7, mobile employees are able to work with SNA applications over VPNs without the enterprise having to put an SNA interface on the publicly exposed portion of the network. Based on the
Figure 5. Combining Local Control with Economies of Scale

Figure 6. Making Internal Network Changes Without Impact on Remote Users

Figure 7. Providing VPN Users with Access to Legacy Protocols
user name, tunnel switches can direct VPN users to a tunnel terminator that supports the protocols they need to access.

Tunnel switching enables enterprises to assign VPN users to any VLAN, increasing network efficiency by directing traffic only to where it needs to go and simplifying user moves and changes. Assignment to VLANs is usually based on the hub port a user is plugged into. As Figure 8 shows, by forwarding VPN tunnels to specific tunnel terminators, users can be virtually “plugged into” various network segments. Without a tunnel switch, all VPN users would be plugged into the same tunnel terminator, and thus have to be members of the same VLAN.

Tunnel switches enable a single VPN infrastructure to support multiple tunneling protocols and allow orderly transitions between protocols. By adding a tunnel switch to the network, as shown in Figure 9, enterprises can avoid “forklift upgrades” to the new L2TP protocol, supporting users with PPTP and users with L2TP simultaneously while executing a phased migration.

Figure 8. Plugging VPN Users into VLANs

Figure 9. Supporting Multiple Protocols and Transitioning Between Them
Increased VPN Performance, Capacity, and Scalability

Tunnel switching improves VPN performance. By forwarding rather than processing tunneled packets, switches minimize latency. Aggregating PPP sessions into a single tunnel has two benefits: It minimizes connection overhead, and it also increases capacity, since multiple sessions use the virtual port allocated to that tunnel, leaving more ports available for other VPN users.

Tunnel switching, as shown in Figure 10, enables enterprises to smoothly scale their VPN infrastructure by transparently adding any number of tunnel termination devices at the network edge or inside internal LAN subdomains. The tunnel switch automatically forwards tunneled traffic to tunnel terminators. (In the future, tunnel switching will also support automatic VPN load balancing and failover.) To add even more capacity as well as control over tunnel termination points,

Figure 10. Scaling to Meet Growing VPN Demand
enterprises can cascade tunnel switches and terminators.

Adding a Tunnel Switch to Your Network
Tunnel switches can easily be added to existing VPN infrastructures, interoperating with tunnel initiators and terminators from any leading vendor.

Generally, tunnel switches are deployed outside a single firewall or between two firewalls in a DMZ. No topology changes are required. Tunnel initiators need only be told to address tunnels to the tunnel switch instead of to the tunnel terminator. (From the terminator's point of view, the tunnel switch looks like any other tunnel initiator—although a very busy one.)

Where no firewall is currently in place, a tunnel switch can be introduced as a "bump in the wire" (BITW) between the edge router and tunnel terminator. Companies can introduce tunnel switching now and increase their security infrastructure later—transitioning, for example, from a single firewall to a double firewall architecture—without having to notify or reconfigure tunnel initiators.

Evolving Your VPNs with New Standards
Tunneling standards are evolving rapidly. As VPNs become widely used not only for remote access, but for a growing range of Internet-based applications, standards will continue to change. Enterprises need to select VPN architectures and components that support multiple standards simultaneously and facilitate smooth migrations.

From Point-to-Point Tunneling Protocol to Layer 2 Tunneling Protocol
PPTP is widely used in existing VPNs. This de facto standard, which was developed by 3Com, Microsoft, and Ascend Communications, is an extension of PPP. Support for PPTP is currently bundled into Microsoft Windows 95/98 and Windows NT.

PPTP is gradually being displaced by L2TP. An industry standard sanctioned by the Internet Engineering Task Force (IETF), it is a combination of the best features of PPTP and the Layer 2 Forwarding (L2F) protocol developed by Cisco Systems. Support for L2TP will be bundled into Windows 2000 and perhaps into upcoming releases of Windows NT. Because tunnel switches support both PPTP and L2TP, organizations can make the transition gradually.

Both of these protocols are for "Layer 2 tunneling," a technology that encapsulates PPP (a Layer 2 protocol) inside the PPTP or L2TP tunneling header, which is then encapsulated by an IP header for transport across the network. Anything that can be encapsulated within PPP—higher-level protocols such as IPX, VINES, DECnet, SNA, NetBEUI, even an inner IP packet—can be transported inside a Layer 2 tunnel. As a result, Layer 2 tunneling enables multiprotocol VPNs.

The Impact of IPSec
IPSec transport mode will become the dominant means of securing VPN tunnels. IPSec, a set of IETF protocols, provides standard ways of authenticating VPN users, encrypting and decrypting tunnel contents, and exchanging and managing encryption keys. 3Com tunneling devices, including tunnel switches and terminators, fully support IPSec.

In IPSec transport mode, IPSec is used to secure IP frames transmitted between two hosts, one of which can be a Layer 3 tunnel switch or tunnel terminator. When used this way, IPSec authentication and encryption is usually performed on the outer IP packet, eliminating the need for PPP-level security such as Microsoft Point-to-Point Encryption (MPPE). Enterprises moving to IP but still supporting multiple network protocols can take this approach to gain experience with the new standard, gradually replacing PPP-level security protocols with IPSec on some VPN links.

IPSec tunnel mode will emerge as an alternate means of creating VPN tunnels for IP-only networks, coexisting with L2TP for multiprotocol networks. While enterprises with IP-only networks will likely readily adopt IPSec tunnel mode, the majority of organizations will continue to need to support multiple network protocols. For the foreseeable
future, the two methods will probably coexist, with L2TP being the most widely used.

IPSec tunnel mode is often called “Layer 3 tunneling” because the payload in this type of tunnel is an IP packet (a Layer 3 protocol) rather than PPP. The IP payload is encapsulated within another IP packet serving as the tunneling protocol. Because IP-based tunnels can be routed, there is no need for tunnel switching. Enterprises can achieve the same benefits by having a router forward tunnels to multiple “secure gateways,” which is the IPSec term for a tunnel terminator. All secure gateways must be equipped to receive and process IPSec.

Because tunnel switches serve a dual function as routers, they can forward IPSec tunnels to secure gateways. At the tunnel end points, existing 3Com tunnel terminators can easily be software-reconfigured to function as IPSec secure gateways. 3Com VPN devices simultaneously support PPTP, L2TP, and both IPSec modes.

3Com Tunnel Switching Solutions
3Com is the inventor of tunnel switching and has applied for a patent on this uniquely valuable technology. 3Com provides tunnel switching capabilities throughout all its product lines that use Enterprise OS software: the entire NETBuilder® family, including SuperStack® NETBuilder models, and OfficeConnect® NETBuilder routers, the PathBuilder™ S500 series, and the new PathBuilder S400 series. For network service providers, the 3Com Total Control® multi-service access platform also supports tunnel switching.

All of these products can perform multiple functions, including routing, tunnel switching, and tunnel termination. Industry-leading features such as ASIC-based wire-speed encryption processing, Network Address Translation (NAT), and ICSA-certified firewalls are built in and ready to come into play as necessary, depending on where and how the device is deployed. Transcend® Secure VPN Manager provides a simple graphical user interface for monitoring tunnels, including session statistics, Quality of Service (QoS) breaches, and potential faults.

Conclusion
VPNs support increasingly mobile workforces and farflung businesses by providing wide area access to enterprise resources using public networks at a fraction of the cost of private connections. Tunnel switching substantially improves VPN scalability, security, and manageability. Corporations need the benefits of these technologies now—even though VPN protocols are still evolving.

3Com provides multipurpose tunnel switches and other VPN devices that smoothly evolve with tunneling standards. Our solutions allow enterprises to maximize the benefits of VPNs now, with today’s requirements for supporting legacy network and application protocols, while pacing the introduction of the standards that will eventually dominate as networks become purely IP. No matter which type of VPN an enterprise deploys—PPTP, L2TP, IPSec, or a mix of all three—3Com tunnel switches can support them simultaneously, maximizing return on investment.

Enterprises that implement 3Com tunnel switches today gain immediate benefits as well as long-term strategic advantages in leveraging the increasingly rich array of public networks and services available for private use.