Technical Paper

3Com®

Tunnel Switching

3Com Technology Boosts VPN Security and Flexibility

Tunnel Switching

3Com Technology Boosts VPN Security and Flexibility

Contents

Acronyms and Abbreviations

ASIC	*application-specific integrated circuit*
BITW	*bump in the wire*
DMZ	*demilitarized zone*
FTP	*File Transfer Protocol*
ICSA	*International Computer Security Association*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
IPX	*Internetwork Packet Exchange*
L2F	*Layer 2 Forwarding*
L2TP	*Layer 2 Tunneling Protocol*
LAN	*local area network*
LDAP	*Lightweight Directory Access Protocol*
MPPE	*Microsoft Point-to-Point Encryption*

Tunnel Switching

3Com Technology Boosts VPN Security and Flexibility

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.

What Is Tunnel Switching?

Tunnel switching is a 3Com technology that increases the security, manageability, performance, and scalability of virtual private networks (VPNs). It provides these benefits by allowing organizations to bring multiple VPNs into the network through a single edge device, efficiently aggregate them for internal delivery, and flexibly locate their end points anywhere in the enterprise.

A VPN is a secure connection that offers the privacy and management controls of a dedicated point-to-point link but actually occurs over a shared, routed network. VPNs are enabling enterprises to use the Internet and other public networks as their own private wide area network (WAN), connecting remote users, and in some cases branch offices, with enterprise resources at a fraction of the cost of 800 number dial-in, leased lines, or Frame Relay.

VPNs are created using encryption, authentication, and tunneling—a method by which data packets in one protocol are encapsulated in another protocol. Tunneling enables traffic from multiple enterprises to travel across the same network unaware of each other, as if enclosed in their own private pipes (something like pulling serial cables across a WAN cloud). It can also enable packets to travel across incompatible networks (for example, IPX or SNA packets across an IP network). At the destination point (tunnel termination), packets are unwrapped, returning them to their underlying protocol format.

While tunnels are generally terminated at the enterprise network edge, tunnel switching allows them to be extended safely across firewalls to specific tunnel termination points within local area network (LAN) administrative domains. In this way, all tunneled traffic can be addressed to the tunnel switch, with its single publicly known address, while actually being terminated at any number of internal destinations, whose addresses and security measures are hidden from the Internet.

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 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

Acronyms and Abbreviations

NAT
Network Address Translation

PPP
Point-to-Point Protocol

PPTP
Point-to-Point Tunneling Protocol

QoS
Quality of Service

RADIUS
Remote Authentication Dial-In User Service

SNA
Systems Network Architecture

TI
tunnel initiator

TS
tunnel switch

TT
tunnel terminator

VLAN
virtual local area network

VPN
virtual private network

WAN
wide area network

xDSL
digital subscriber line

How Does Tunnel Switching Work?

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

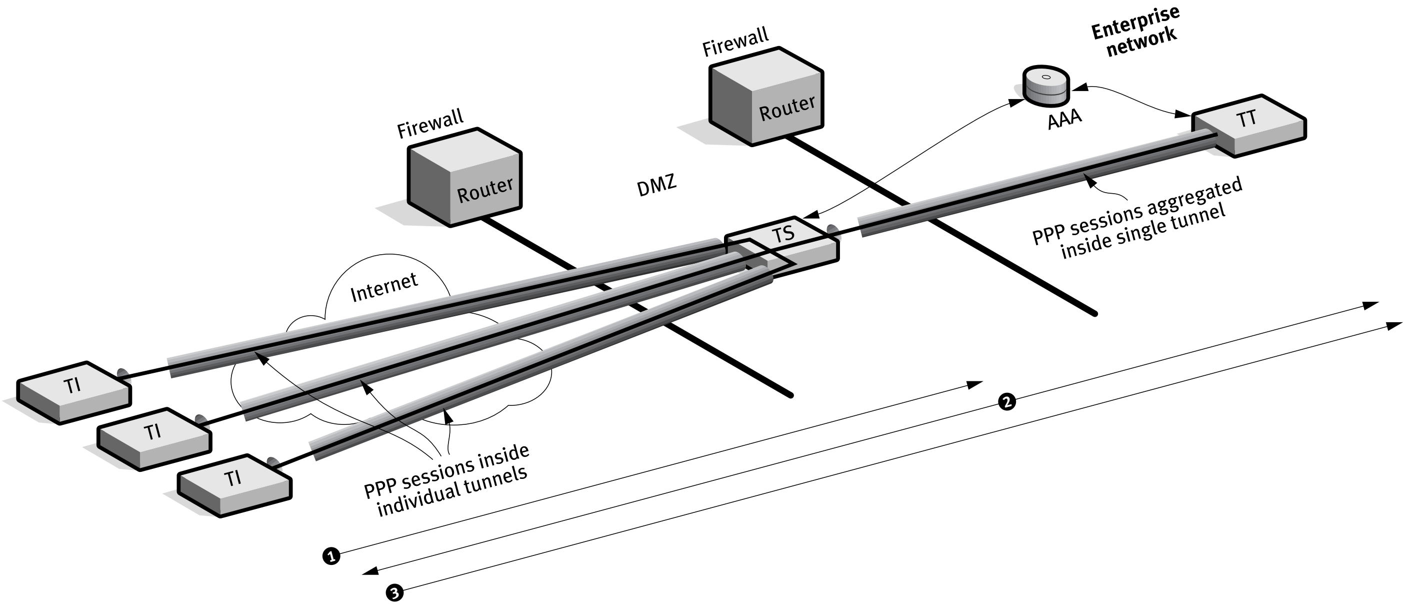

Firewall
Router
Firewall
Router
Enterprise network
AAA
TT
DMZ
TS
PPP sessions aggregated inside single tunnel
Internet
TI
TI
TI
PPP sessions inside individual tunnels
1
2
3

Figure 1. *True Tunnel Switching Extends the Original Tunnel to a New Destination*

attributes, which it ignores except for the tunnel type and tunnel terminator's address.

Stage 2. The tunnel switch combines the two tunnels and forwards messages between the two end points:

a The tunnel switch builds an outgoing tunnel to that terminator or, if a tunnel to that destination already exists, it multiplexes the new traffic onto it.

b The tunnel switch sends a PPP reset message back to the tunnel initiator.

Stage 3. The tunnel terminator reauthenticates the user and completes setup of the PPP session:

a The tunnel initiator resubmits the user name and password.

b The tunnel switch, which no longer looks at the contents of the packets, forwards them to the tunnel terminator.

c The tunnel terminator authenticates the user again. It may query the same RADIUS server consulted previously by the tunnel switch, a different RADIUS server, its own local database, or a Lightweight Directory Access Protocol (LDAP) directory. The terminator receives back a validation of the user's name and password along with the list of user attributes, which it processes. Attributes may include domain name, IP address, and policy-based authorization information that controls which network resources the user may access.

d The tunnel terminator completes the end-to-end PPP connection with the client and provides appropriate network access.

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

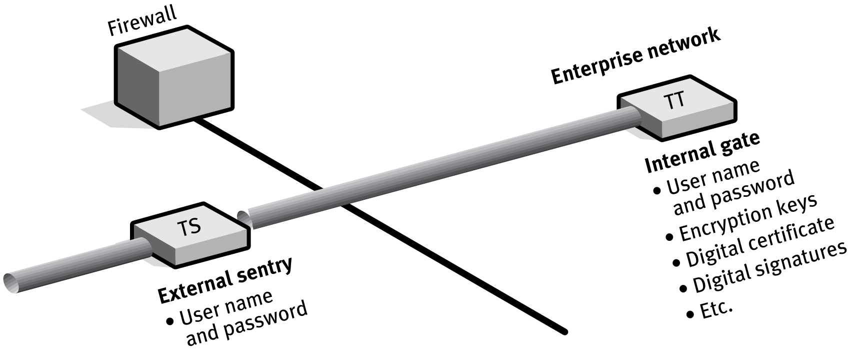


Figure 2. *Creating a Double Line of Security*

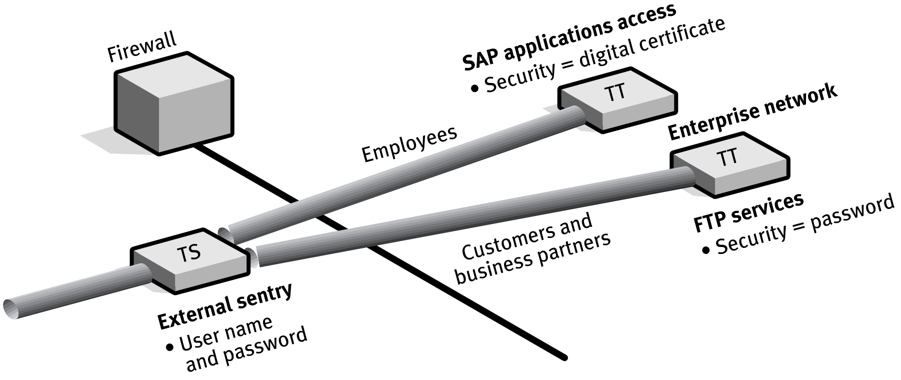


Figure 3. *Applying Different Levels of Security to Tunneled Traffic*

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

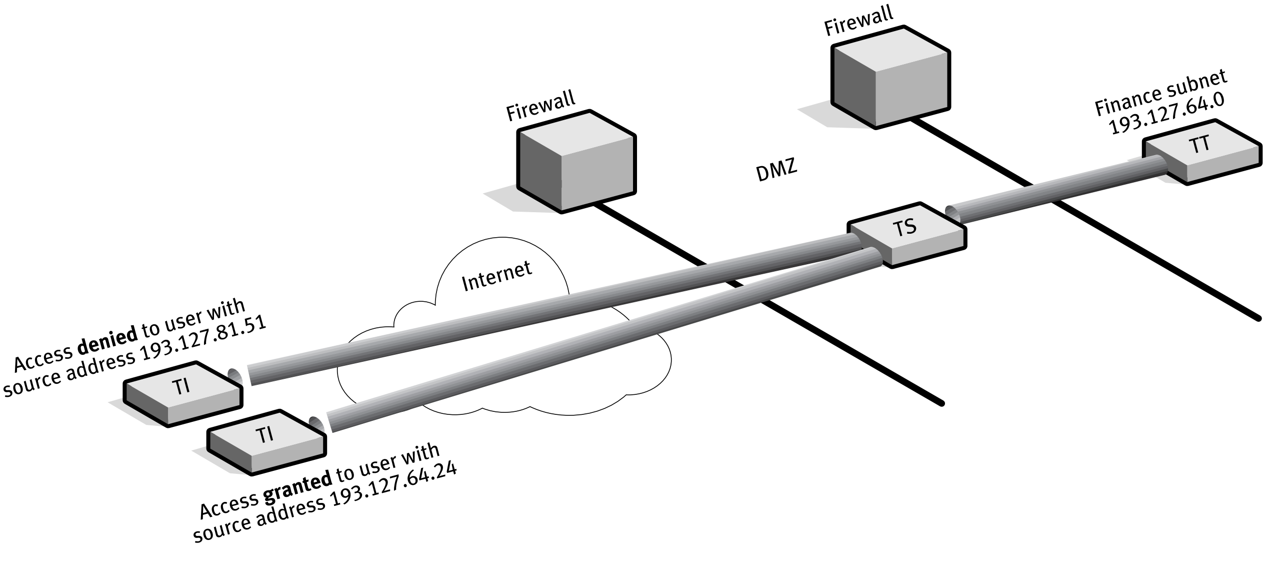

Firewall
Firewall
Finance subnet 193.127.64.0
TT
DMZ
TS
Internet
Access **denied** to user with source address 193.127.81.51
TI
TI
Access **granted** to user with source address 193.127.64.24

Figure 4. *Restricting Access to LAN Administrative Domains*

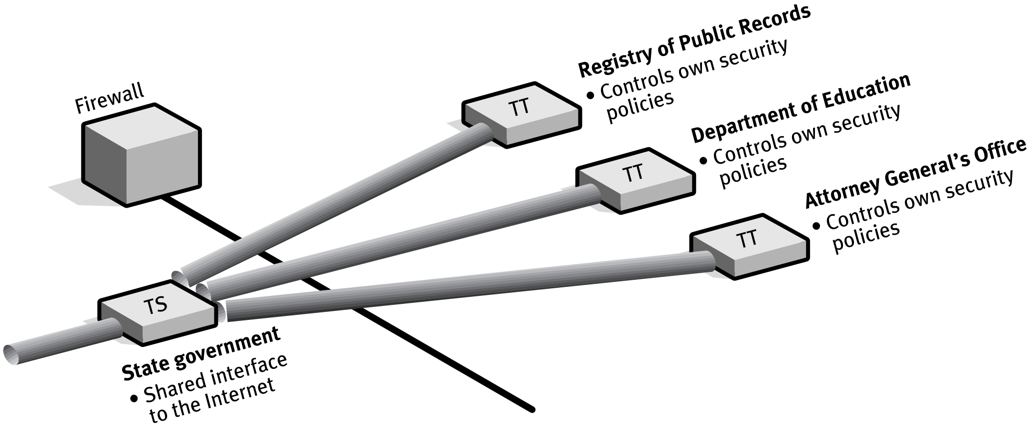

Firewall
TT
TT
TT
TS
Registry of Public Records
• Controls own security policies
Department of Education
• Controls own security policies
Attorney General's Office
• Controls own security policies
State government
• Shared interface to the Internet

Figure 5. *Combining Local Control with Economies of Scale*

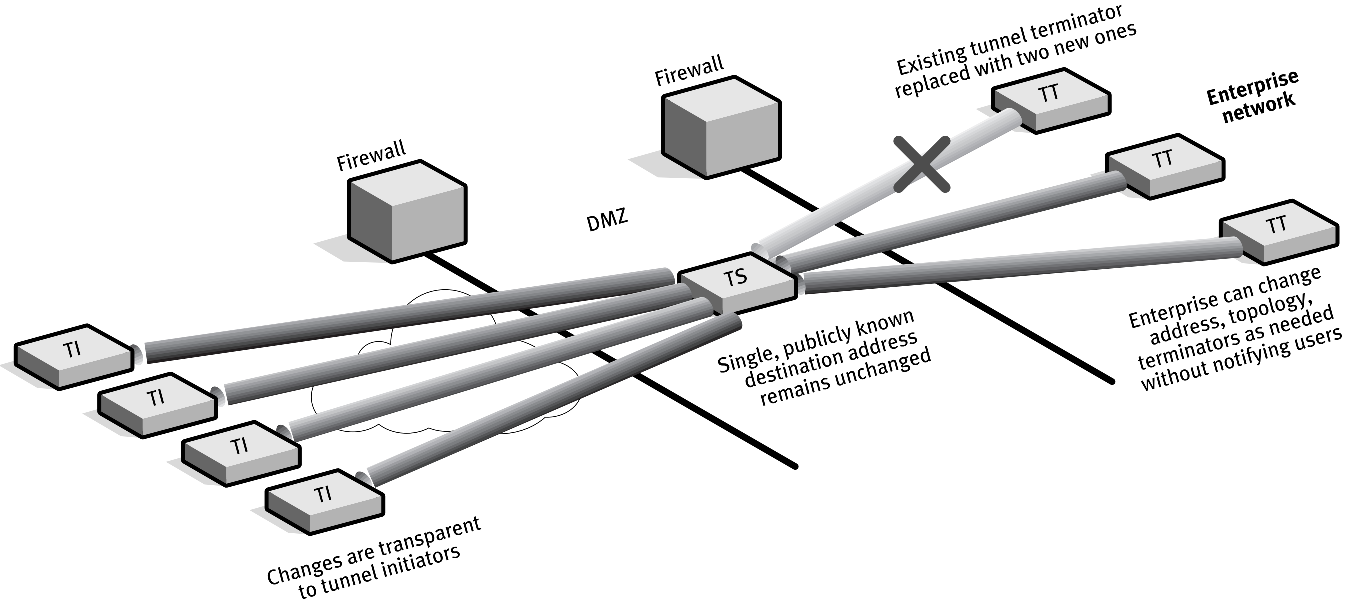

Existing tunnel terminator replaced with two new ones
Firewall
Firewall
DMZ
TT
TT
TT
Enterprise network
TS
TI
TI
TI
TI
Single, publicly known destination address remains unchanged
Enterprise can change address, topology, terminators as needed without notifying users
Changes are transparent to tunnel initiators

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

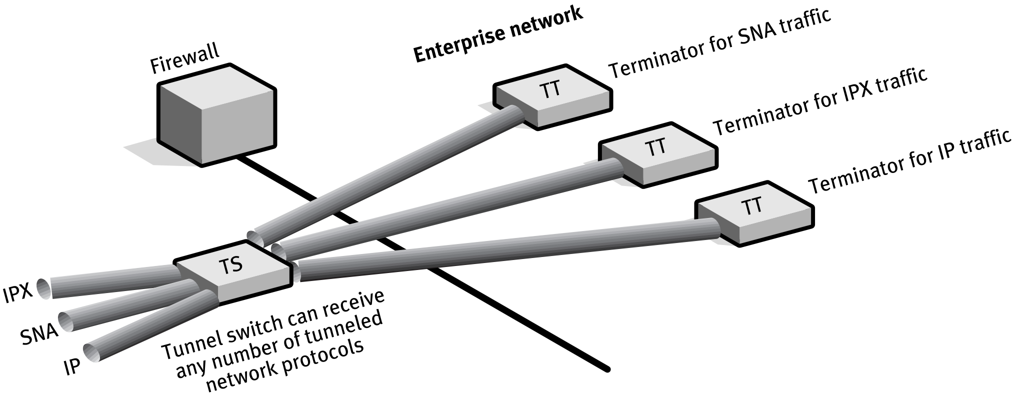

Firewall
Enterprise network
Terminator for SNA traffic
Terminator for IPX traffic
Terminator for IP traffic
TT
TT
TT
TS
IPX
SNA
IP
Tunnel switch can receive any number of tunneled network protocols

Figure 7. *Providing VPN Users with Access to Legacy Protocols*

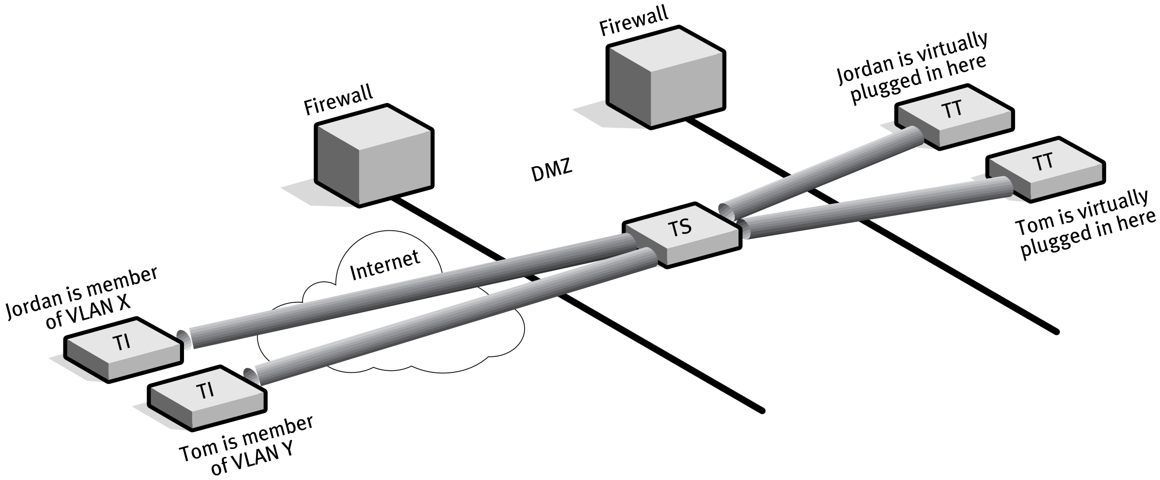

Firewall
Firewall
Jordan is virtually plugged in here
TT
TT
DMZ
TS
Tom is virtually plugged in here
Internet
Jordan is member of VLAN X
TI
TI
Tom is member of VLAN Y

Figure 8. *Plugging VPN Users into VLANs*

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.

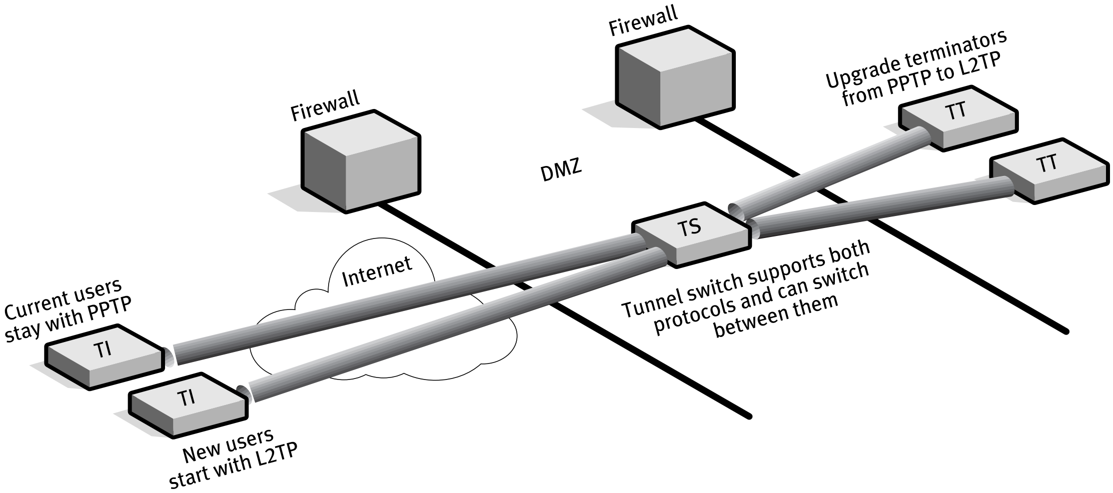

Firewall
Firewall
Upgrade terminators from PPTP to L2TP
TT
TT
DMZ
TS
Internet
Tunnel switch supports both protocols and can switch between them
Current users stay with PPTP
TI
TI
New users start with L2TP

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,

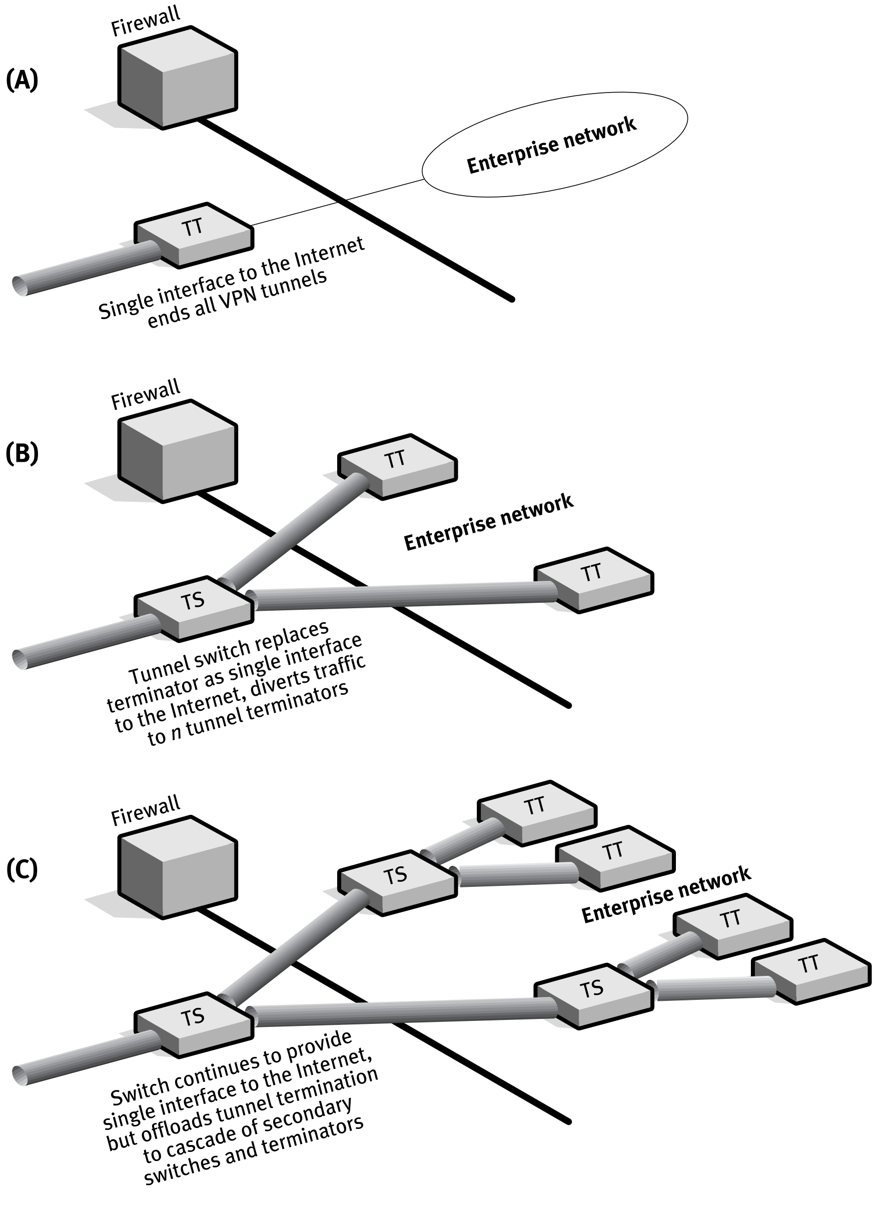

Firewall
(A)
Enterprise network
TT
Single interface to the Internet ends all VPN tunnels
Firewall
(B)
TT
Enterprise network
TT
TS
Tunnel switch replaces terminator as single interface to the Internet, diverts traffic to *n* tunnel terminators
Firewall
(C)
TT
TT
TS
Enterprise network
TT
TT
TS
TS
Switch continues to provide single interface to the Internet, but offloads tunnel termination to cascade of secondary switches and terminators

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. ◘

3Com®

More connected.™

About 3Com Corporation

With more than 300 million customers worldwide, 3Com Corporation connects more people in more ways to information than any other networking company. 3Com delivers innovative information access products and network system solutions to large, medium, and small enterprises; carriers and network service providers; PC OEMs; and consumers. **3Com. More connected.**™

3Com Corporation
5400 Bayfront Plaza
P.O. Box 58145
Santa Clara, CA
95052-8145
Phone: 1 800 NET 3Com
or 1 408 326 5000
Fax: 1 408 326 5001
World Wide Web:
www.3com.com

3Com Americas International
U.S. Headquarters (serving Canada and Latin America)
Phone: 1 408 326 6328/1 408 326 6075
Fax: 1 408 326 5730/
1 408 326 8914
Miami
Phone: 1 305 461 8400
Fax: 1 305 461 8401/02

3Com Canada
Burlington
Phone: 905 336 8168
Fax: 905 336 7380
Calgary
Phone: 403 265 3266
Fax: 403 265 3268
Edmonton
Phone: 780 423 3266
Fax: 780 423 2368
Montreal
Phone: 514 683 3266
Fax: 514 683 5122
Ottawa
Phone: 613 566 7055
Fax: 613 233 9527
Toronto
Phone: 416 498 3266
Fax: 416 498 1262
Vancouver
Phone: 604 434 3266
Fax: 604 434 3264

3Com Latin America
Argentina (serving Argentina, Paraguay, and Uruguay)
Phone: 54 11 4510 3200
Fax: 54 11 4314 3329
Brazil
Phone: 55 11 5641 5001
Fax: 55 11 5641 3444
Chile (serving Bolivia, Chile, and Peru)
Phone: 562 240 6200
Fax: 562 240 6231
Colombia
Phone: 57 1 629 4110
Fax: 57 1 629 4503
Costa Rica
Phone: 506 280 8480
Fax: 506 280 5859
Mexico
Phone: 525 201 0000
Fax: 525 201 0001
Peru
Phone: 51 1 221 5399
Fax: 51 1 221 5499
Venezuela
Phone: 582 267 5550
Fax: 582 267 3373

Asia Pacific Rim
Melbourne, Australia
Phone: 61 3 9934 8888
Fax: 61 3 9934 8880
Sydney, Australia
Phone: 61 2 9937 5000
Fax: 61 2 9956 6247
Beijing, China
Phone: 8610 6588 0568
Fax: 8610 6588 0602
Shanghai, China
Phone: 86 21 6350 1581
Fax: 86 21 6350 1531
Hong Kong
Phone: 852 2501 1111
Fax: 852 2537 1149
India
Phone: 91 11 629 3177
Fax: 91 11 623 6509
Indonesia
Phone: 62 21 572 2088
Fax: 62 21 572 2089
Osaka, Japan
Phone: 81 6 6379 1767
Fax: 81 6 6379 0871
Tokyo, Japan
Phone: 0120 31 3266
(toll free from Japan)
Phone: 81 3 5977 3266
Fax: 81 3 5977 3370
Korea
Phone: 82 2 3455 6300
Fax: 82 2 319 4710
Malaysia
Phone: 60 3 715 1333
Fax: 60 3 715 2333
New Zealand
Phone: 64 9 366 9138
Fax: 64 9 366 9139
Philippines
Phone: 632 849 3979
Fax: 632 849 3970
Singapore
Phone: 65 538 9368
Fax: 65 538 9369
Taiwan
Phone: 886 2 2 377 5850
Fax: 886 2 2 377 5860
Thailand
Phone: 662 231 8151 5
Fax: 662 231 8158

3Com Austria
Phone: 43 1 580 17 0
Fax: 43 1 580 17 20

3Com Benelux B.V.
Belgium
Phone: 32 2 711 94 00
Fax: 32 2 711 94 11
Netherlands
Phone: 31 346 58 62 11
Fax: 31 346 58 62 22

3Com Eastern Europe/CIS
Bulgaria
Phone: 359 2 962 5222
Fax: 359 2 962 4322
Czech Republic
Phone: 420 2 21845 800
Fax: 420 2 21845 811
Hungary
Phone: 36 1 250 83 41
Fax: 36 1 250 83 47
Poland
Phone: 48 22 6451351
Fax: 48 22 6451352
Russia
Phone: 7 095 258 09 40
Fax: 7 095 258 09 41
Slovak Republic
Phone: 421 7 317 850
Fax: 421 7 317 849

3Com France
Phone: 33 1 69 86 68 00
Fax: 33 1 69 07 11 54

3Com GmbH
Unterfoehring, Germany
Phone: 49 89 992200
Fax: 49 89 9577 220

3Com Iberia
Portugal
Phone: 351 1 3404505
Fax: 351 1 3404575
Spain
Phone: 34 91 509 69 00
Fax: 34 91 307 66 63

3Com Italia S.p.A.
Milan, Italy
Phone: 39 02 253011
Fax: 39 02 27304244
Rome, Italy
Phone: 39 06 5279941
Fax: 39 06 52799423

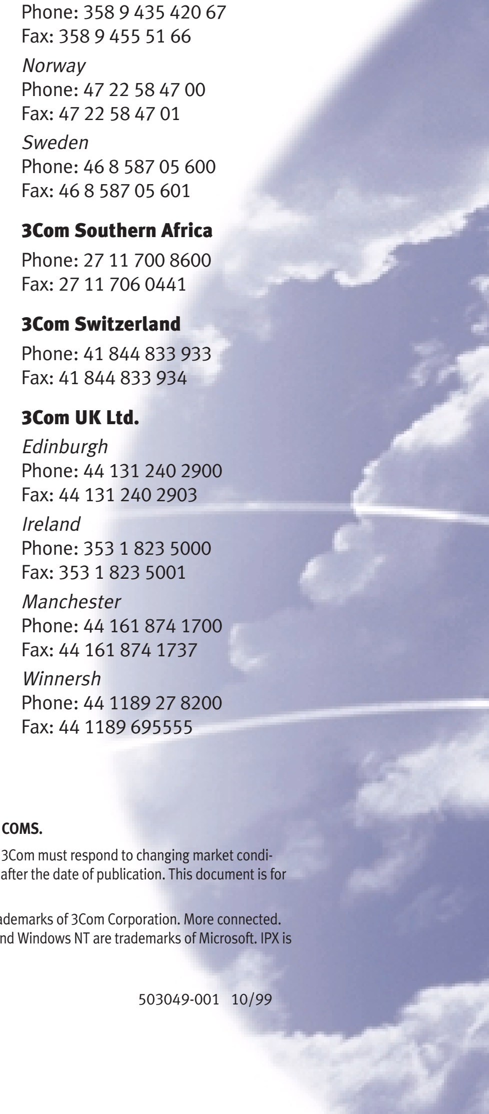
3Com Middle East
Phone: 971 4 319533
Fax: 971 4 316766

3Com Nordic AB
Denmark
Phone: 45 48 10 50 00
Fax: 45 48 10 50 50
Finland
Phone: 358 9 435 420 67
Fax: 358 9 455 51 66
Norway
Phone: 47 22 58 47 00
Fax: 47 22 58 47 01
Sweden
Phone: 46 8 587 05 600
Fax: 46 8 587 05 601

3Com Southern Africa
Phone: 27 11 700 8600
Fax: 27 11 706 0441

3Com Switzerland
Phone: 41 844 833 933
Fax: 41 844 833 934

3Com UK Ltd.
Edinburgh
Phone: 44 131 240 2900
Fax: 44 131 240 2903
Ireland
Phone: 353 1 823 5000
Fax: 353 1 823 5001
Manchester
Phone: 44 161 874 1700
Fax: 44 161 874 1737
Winnersh
Phone: 44 1189 27 8200
Fax: 44 1189 695555



To learn more about 3Com products and services, visit our Web site at www.3com.com. 3Com Corporation is publicly traded on Nasdaq under the symbol COMS.

The information contained in this document represents the current view of 3Com Corporation on the issues discussed as of the date of publication. Because 3Com must respond to changing market conditions, this paper should not be interpreted to be a commitment on the part of 3Com, and 3Com cannot guarantee the accuracy of any information presented after the date of publication. This document is for informational purposes only; 3Com makes no warranties, express or implied, in this document.

♻ Printed in U.S.A. on recycled paper

503049-001 10/99