CHAPTER 26

Private Networks, Virtual Private Networks, and Network Address Translation

In this chapter, we discuss three related topics that are becoming increasingly important as the Internet grows. We first discuss the idea of private networks—networks that are isolated from the Internet but use the TCP/IP protocol suite. We then discuss virtual private networks—networks that use the Internet and at the same time require privacy like a private network. Finally, we discuss network address translation—a technology that allows a private network to use two sets of addresses: one private and one global.

26.1 PRIVATE NETWORKS

A **private network** is designed to be used only inside an organization. It allows access to shared resources and, at the same time, provides privacy. Before we discuss some aspects of these networks, let us define two commonly used related terms: intranet and extranet.

Intranet

An **intranet** is a private network (LAN) that uses the TCP/IP protocol suite. However, access to the network is limited to only the users inside the organization. The network uses application programs defined for the global Internet, such as HTTP, and may have Web servers, print servers, file servers, and so on.

Extranet

An **extranet** is the same as an intranet with one major difference. Some resources may be accessed by specific groups of users outside the organization under the control of the network administrator. For example, an organization may allow authorized customers access to product specifications, availability, and on-line ordering. A university or a college can allow distance learning students access to the computer lab after passwords have been checked.

Addressing

A private network that uses the TCP/IP protocol suite must use IP addresses. Three choices are available:

1. The network can apply for a set of addresses from the Internet authorities and use them without being connected to the Internet. This strategy has an advantage. If in the future the organization desires Internet connection, it can do so with relative ease. However, there is also a disadvantage: The address space is wasted.
2. The network can use any set of addresses without registering with the Internet authorities. Because the network is isolated, the addresses do not have to be unique. However, this strategy has a serious drawback: Users might mistakenly confuse the addresses as part of the global Internet.
3. To overcome the problems associated with the first and second strategies, the Internet authorities have reserved three sets of addresses, shown in Table 26.1.

Table 26.1 *Addresses for private networks*

Range	*Total*
10.0.0.0 to 10.255.255.255	2^{24}
172.16.0.0 to 172.31.255.255	2^{20}
192.168.0.0 to 192.168.255.255	2^{16}

Any organization can use an address out of this set without permission from the Internet authorities. Everybody knows that these **reserved addresses** are for private networks. They are unique inside the organization, but they are not unique globally. No router will forward a packet that has one of these addresses as the destination address.

26.2 VIRTUAL PRIVATE NETWORKS (VPN)

Virtual private network (VPN) is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and interorganization communication, but require privacy in their intraorganization communication.

Achieving Privacy

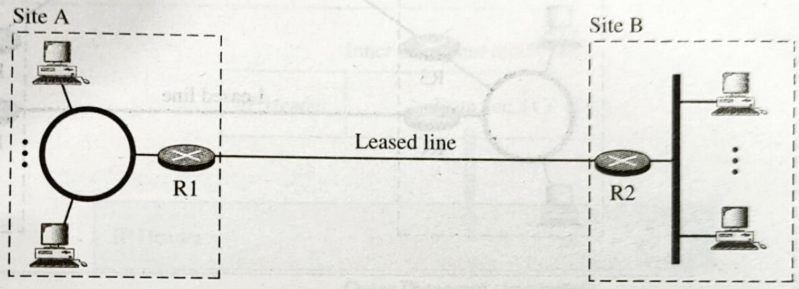
To achieve privacy, organizations can use one of three strategies: private networks, hybrid networks, and virtual private networks.

Private Networks

An organization that needs privacy when routing information inside the organization can use a private network as discussed previously. A small organization with one single site can use an isolated LAN. People inside the organization can send data to one another that totally remain inside the organization, secure from outsiders. A larger organization with several sites can create a private internet. The LANs at different sites can

be connected to each other using routers and leased lines. In other words, an internet can be made out of private LANs and private WANs. Figure 26.1 shows such a situation for an organization with two sites. The LANs are connected to each other using routers and one leased line.

Figure 26.1 *Private network*



In this situation, the organization has created a private internet that is totally isolated from the global Internet. For end-to-end communication between stations at different sites, the organization can use the TCP/IP protocol suite. However, there is no need for the organization to apply for IP addresses with the Internet authorities. It can use private IP addresses. The organization can use any IP class and assign network and host addresses internally. Because the internet is private, duplication of addresses by another organization in the global Internet is not a problem.

Hybrid Networks

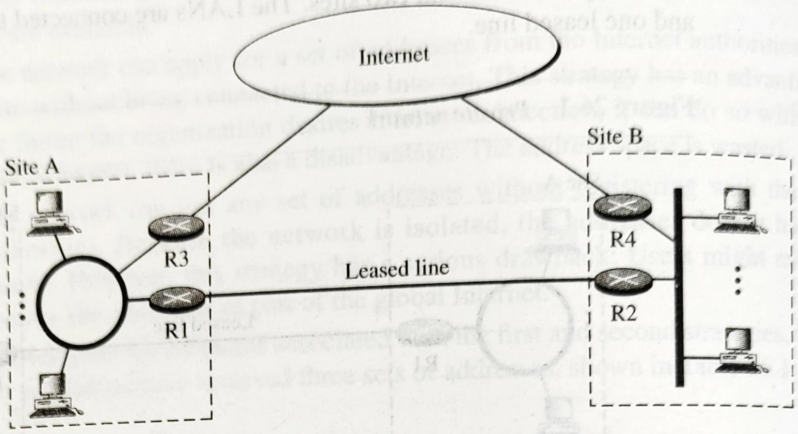
Today, most organizations need to have privacy in intraorganization data exchange, but, at the same time, they need to be connected to the global Internet for data exchange with other organizations. One solution is the use of a **hybrid network.** A hybrid network allows an organization to have its own private internet and, at the same time, access to the global Internet. Intraorganization data is routed through the private internet; interorganization data is routed through the global Internet. Figure 26.2 shows an example of this situation.

An organization with two sites uses routers R1 and R2 to connect the two sites privately through a leased line; it uses routers R3 and R4 to connect the two sites to the rest of the world. The organization uses global IP addresses for both types of communication. However, packets destined for internal recipients are routed only through routers R1 and R2. Routers R3 and R4 route the packets destined for outsiders.

Virtual Private Networks

Both private and hybrid networks have a major drawback: cost. Private wide area networks are expensive. To connect several sites, an organization needs several leased lines, which can lead to a high monthly cost. One solution is to use the global Internet for both private and public communication. A technology called virtual private network (VPN) allows organizations to use the global Internet for both purposes.

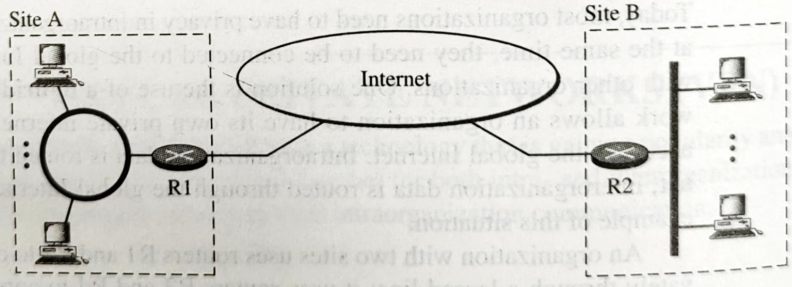
Figure 26.2 *Hybrid network*



VPN is a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.

Figure 26.3 shows the idea of a virtual private network. Routers R1 and R2 use VPN technology to guarantee privacy for the organization.

Figure 26.3 *Virtual private network*



VPN Technology

VPN technology uses two simultaneous techniques to guarantee privacy for an organization: IPSec and tunneling.

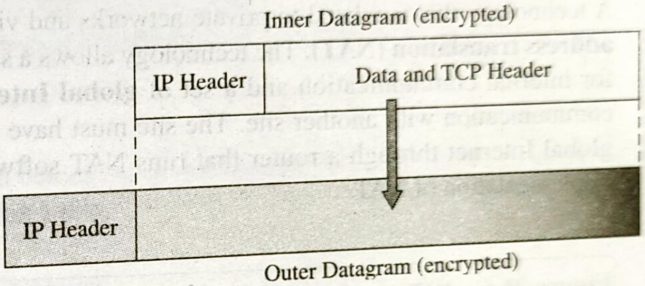
IPSec

We will discuss IPSec in Chapter 28.

Tunneling

To guarantee privacy for an organization, VPN specifies that each IP datagram destined for private use in the organization must be encapsulated in another datagram as shown in Figure 26.4.

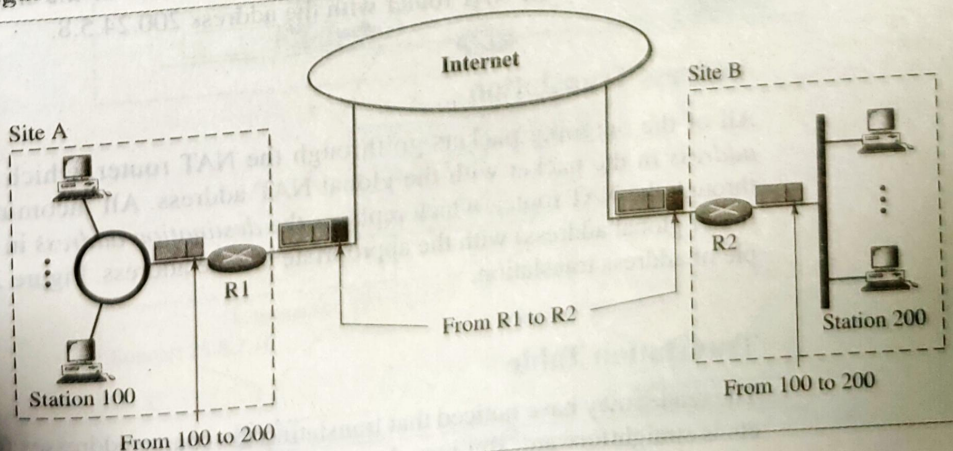
Figure 26.4 *Tunneling*



This is called **tunneling** because the original datagram is hidden inside the outer datagram after exiting R1 in Figure 26.5 and is invisible until it reaches R2. It appears that the original datagram has gone through a tunnel spanning R1 and R2.

As the figure shows, the entire IP datagram (including the header) is first encrypted and then encapsulated in another datagram with a new header. The inner datagram here carries the actual source and destination address of the packet (two stations inside the organization). The outer datagram header carries the source and destination of the two routers at the boundary of the private and public networks as shown in Figure 26.5.

Figure 26.5 *Addressing in a VPN*

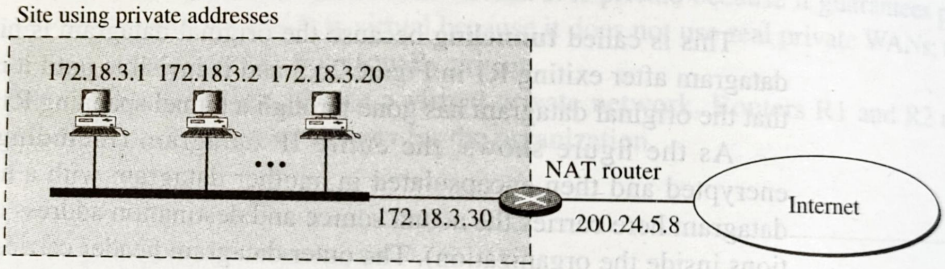


The public network (Internet) is responsible for carrying the packet from R1 to R2. Outsiders cannot decipher the contents of the packet or the source and destination addresses. Deciphering takes place at R2, which finds the destination address of the packet and delivers it.

26.3 NETWORK ADDRESS TRANSLATION (NAT)

A technology that is related to private networks and virtual private networks is **network address translation (NAT).** The technology allows a site to use a set of private addresses for internal communication and a set of **global Internet** addresses (at least one) for communication with another site. The site must have only one single connection to the global Internet through a router that runs NAT software. Figure 26.6 shows a simple implementation of NAT.

Figure 26.6 *NAT*



As the figure shows, the private network uses private addresses. The router that connects the network to the global address uses one private address and one global address. The private network is transparent to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8.

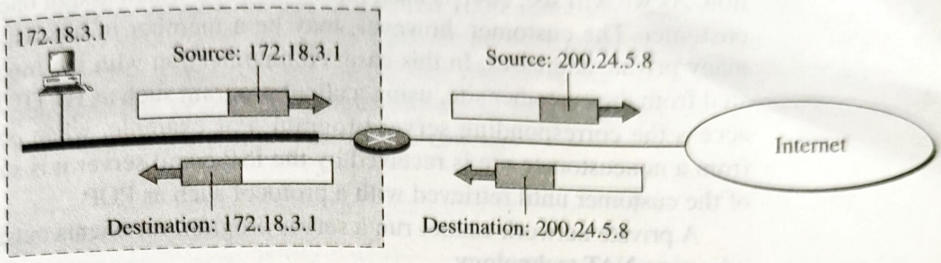
Address Translation

All of the outgoing packets go through the NAT router, which replaces the *source address* in the packet with the global NAT address. All incoming packets also pass through the NAT router, which replaces the *destination address* in the packet (the NAT router global address) with the appropriate private address. Figure 26.7 shows an example of address translation.

Translation Table

The reader may have noticed that translating the source addresses for an outgoing packets is straightforward. But how does the NAT router know the destination address for a packet coming from the Internet? There may be tens or hundreds of private IP

Figure 26.7 *Address translation*

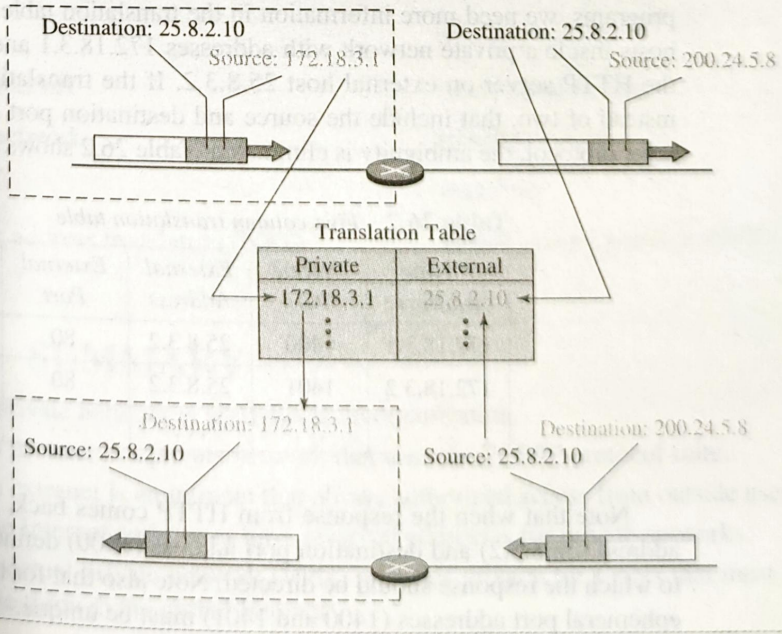


addresses, each belonging to one specific host. The problem is solved if the NAT router has a **translation table.**

Using One IP Address

In its simplest form, a translation table has only two columns: the private address and the external address (destination address of the packet). When the router translates the source address of the outgoing packet, it also makes note of the destination address—where the packet is going. When the response comes back from the destination, the router uses the source address of the packet (as the external address) to find the private address of the packet. Figure 26.8 shows the idea. Note that the addresses that are changed (translated) are shown in color.

Figure 26.8 *Translation*



In this strategy, communication must always be initiated by the private network. The NAT mechanism described requires that the private network start the communication. As we will see, NAT is used mostly by ISPs which assign one single address to a customer. The customer, however, may be a member of a private network that has many private addresses. In this case, communication with the Internet is always initiated from the customer site, using a client program such as HTTP, TELNET, or FTP to access the corresponding server program. For example, when email that originates from a noncustomer site is received by the ISP email server it is stored in the mailbox of the customer until retrieved with a protocol such as POP.

A private network cannot run a server program for clients outside of its network if it is using NAT technology.

Using a Pool of IP Addresses

Using only one global address by the NAT router allows only one private-network host to access the same external host. To remove this restriction, the NAT router can use a pool of global addresses. For example, instead of using only one global address (200.24.5.8), the NAT router can use four addresses (200.24.5.8, 200.24.5.9, 200.24.5.10, and 200.24.5.11). In this case, four private-network hosts can communicate with the same external host at the same time because each pair of addresses defines a connection. However, there are still some drawbacks. No more than four connections can be made to the same destination. No private-network host can access two external server programs (e.g., HTTP and TELNET) at the same time. And, likewise, two private-network hosts cannot access the same external server program (e.g., HTTP or TELNET) at the same time.

Using Both IP Addresses and Port Addresses

To allow a many-to-many relationship between private-network hosts and external server programs, we need more information in the translation table. For example, suppose two hosts inside a private network with addresses 172.18.3.1 and 172.18.3.2 need to access the HTTP server on external host 25.8.3.2. If the translation table has five columns, instead of two, that include the source and destination port addresses and the transport layer protocol, the ambiguity is eliminated. Table 26.2 shows an example of such a table.

Table 26.2 *Five-column translation table*

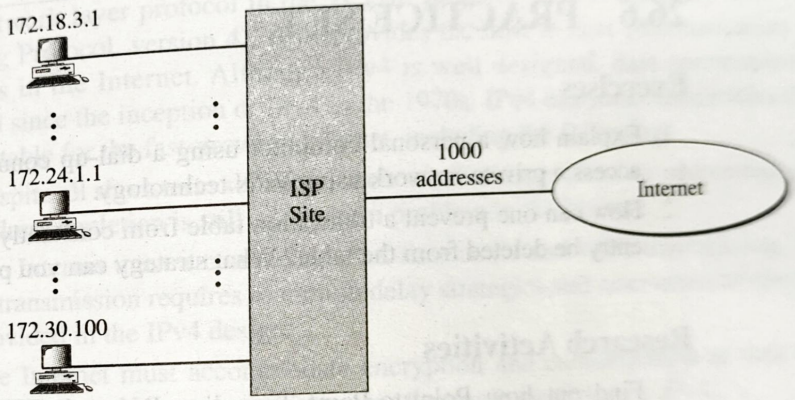
Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

Note that when the response from HTTP comes back, the combination of source address (25.8.3.2) and destination port address (1400) defines the private network host to which the response should be directed. Note also that for this translation to work, the ephemeral port addresses (1400 and 1401) must be unique.

NAT and ISP

An ISP that serves dial-up customers can use NAT technology to conserve addresses. For example, imagine an ISP is granted 1000 addresses, but has 100,000 customers. Each of the customers is assigned a private network address. The ISP translates each of the 100,000 source addresses in outgoing packets to one of the 1000 global addresses; it translates the global destination address in incoming packets to the corresponding private address. Figure 26.9 shows this concept.

Figure 26.9 *An ISP and NAT*



26.4 KEY TERMS

extranet
global Internet
hybrid network
intranet
network address translation (NAT)
private network
reserved addresses
translation table
tunneling
virtual private network (VPN)

26.5 SUMMARY

- A private network is used inside an organization.
- An intranet is a private network that uses the TCP/IP protocol suite.
- An extranet is an intranet that allows authorized access from outside users.
- The Internet authorities have reserved addresses for private networks.
- A virtual private network (VPN) provides privacy for LANs that must communicate through the global Internet.