شبكات

Network Address Translation NAT

A technology that allows a private network to use a set of private addresses for internal communication and a set of global Internet addresses for external communication.

It provides a mapping between internal IP addresses and officially assigned external addresses.

The Internet authorities have reserved three sets of addresses as private addresses, shown below:

| 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}

NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally. The traffic inside can use the large set; the traffic outside, the small set.

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.
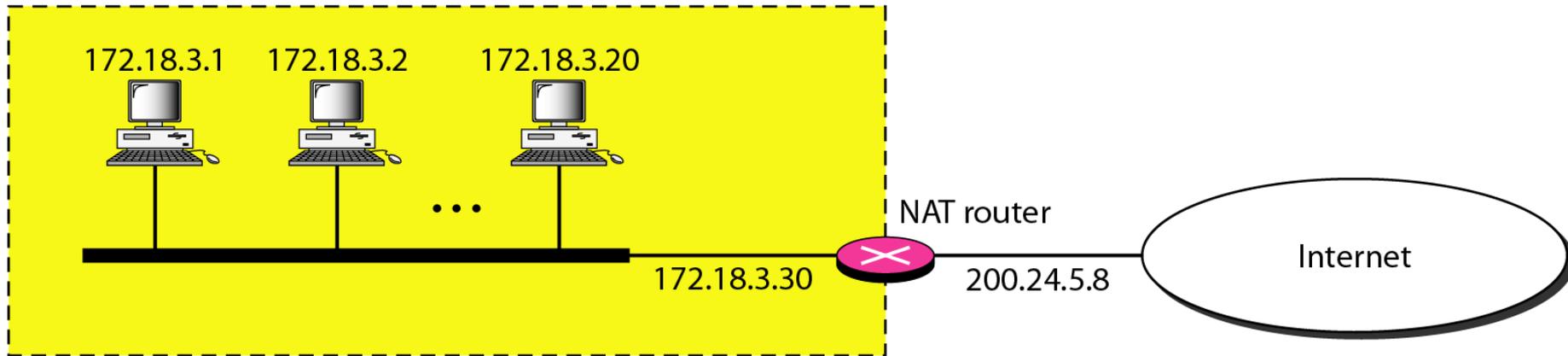
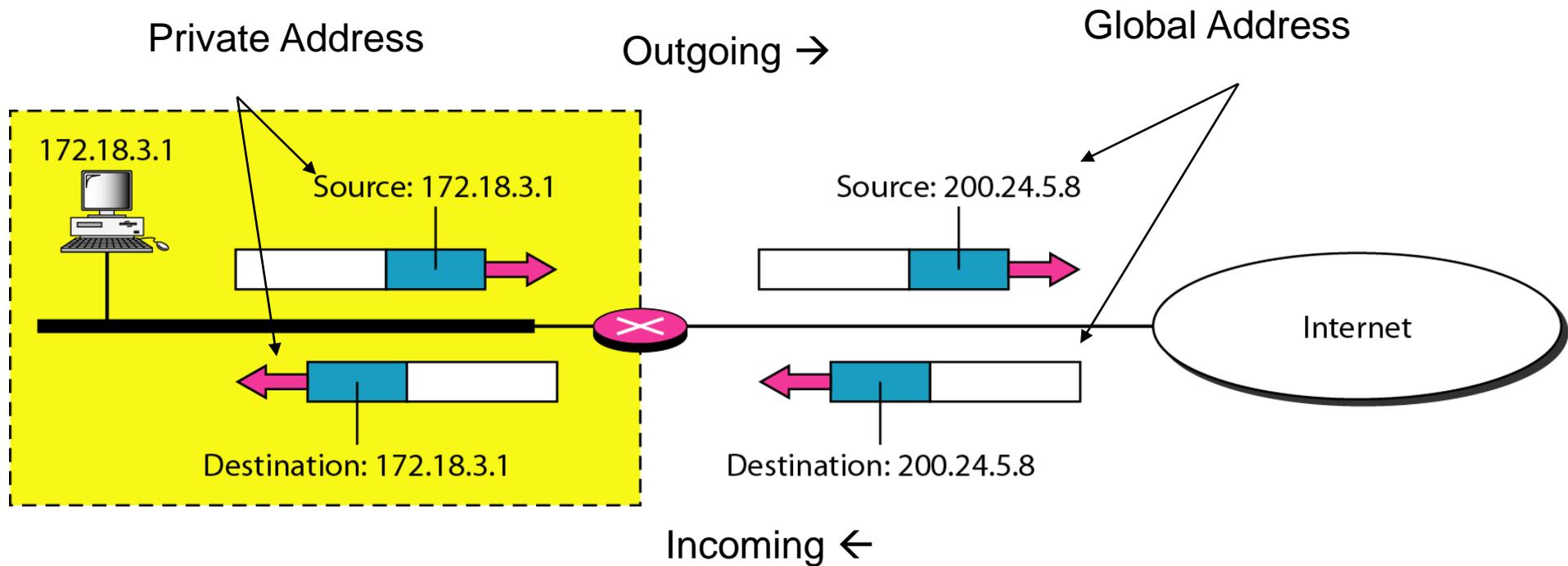*A NAT implementation*

The router that connects the network to the global address uses one private address and one global address.

All 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 with the appropriate private address.

Private Address

Outgoing →

Global Address

172.18.3.1

Source: 172.18.3.1

Source: 200.24.5.8

Internet

Destination: 172.18.3.1

Destination: 200.24.5.8

Incoming ←

Translation Table

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

The translation table configuration in NAT router has three types:

1. Using One IP Address:

A translation table has only two columns: the private address and the external address.
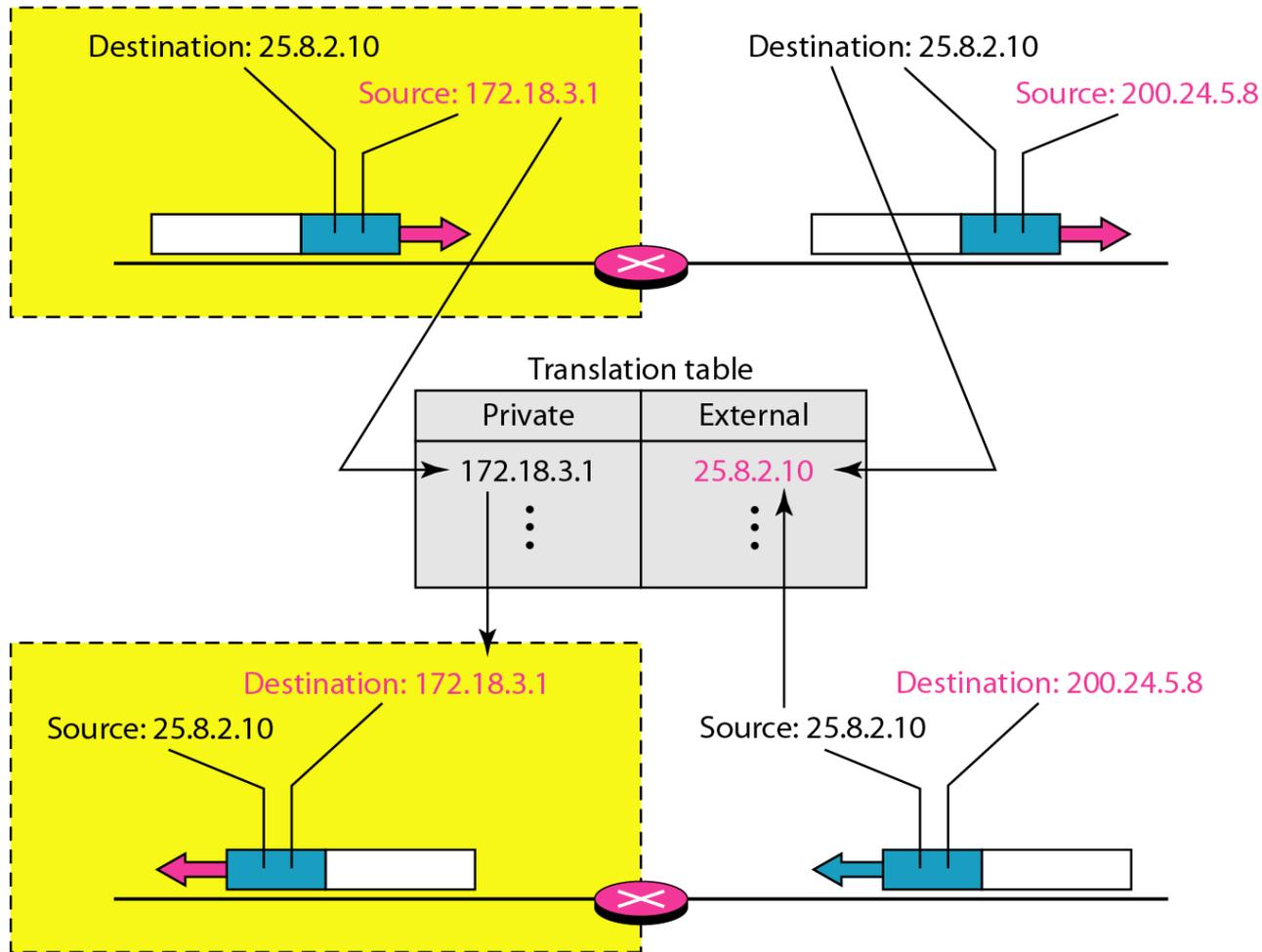
In this strategy, communication must always be initiated by the private network. The NAT mechanism described requires that the private network start the communication.

2. *Using a Pool of IP Addresses*

Since the NAT router has only one global address, only one private network host can access the same external host.

To remove this restriction, the NAT router uses 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.

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 with addresses 172.18.3.1 and 172.18.3.2 inside a private network 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 numbers of the transport layer protocol, the ambiguity is eliminated.

Table 2.4 *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
. . .	. . .	. . .	. . .	. . .

The transport layer is responsible for the delivery of a message from one process to another.

Service-point addressing (Port Address): source-to-destination delivery means from a specific process (running program) on one computer to a specific process (running program) on the other. Such as http:// is Port 80, FTP:// is the port 21 and Telnet is the port 23

Figure 2.21 *Port addresses*
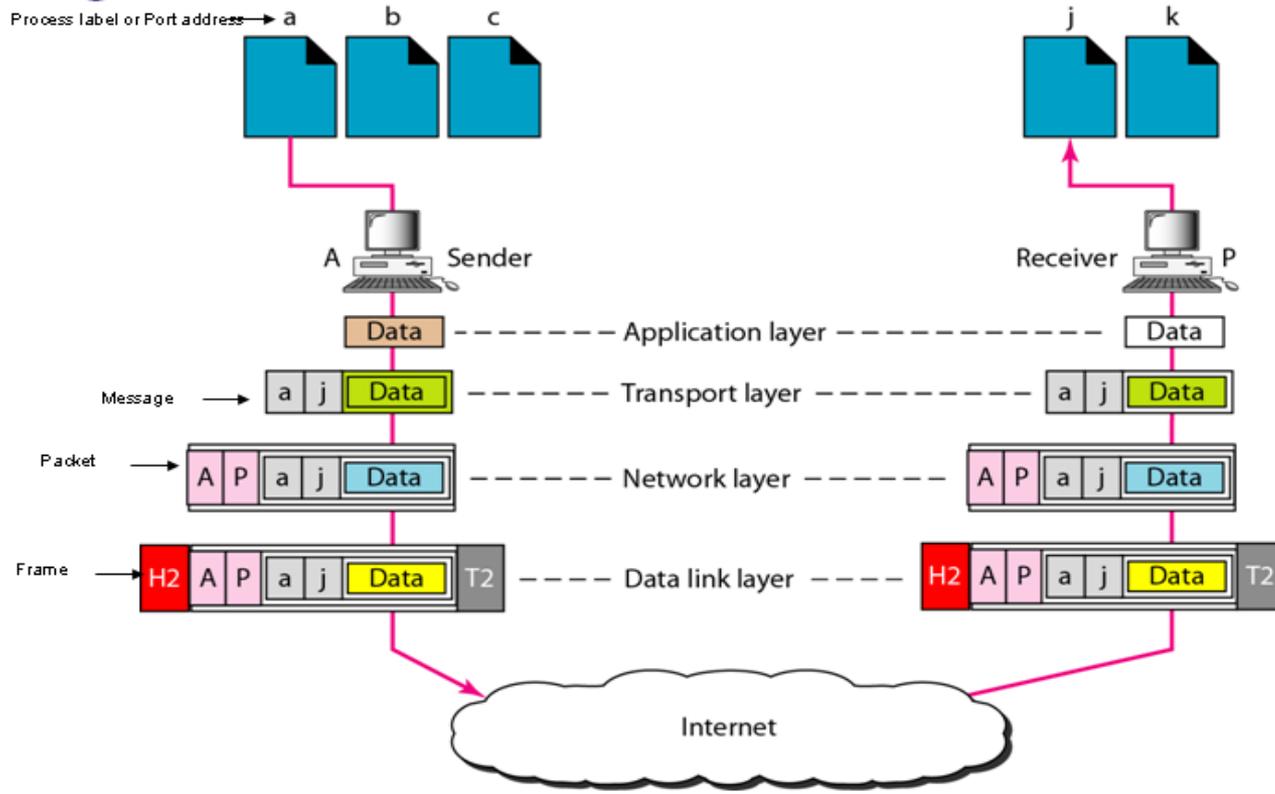
NAT and ISP

An ISP that serves dial-up customers can use NAT technology to conserve addresses.

For example, suppose 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 2.13 shows this concept.

172.18.3.1

172.24.1.1

172.30.100

ISP
site

1000
addresses

Internet
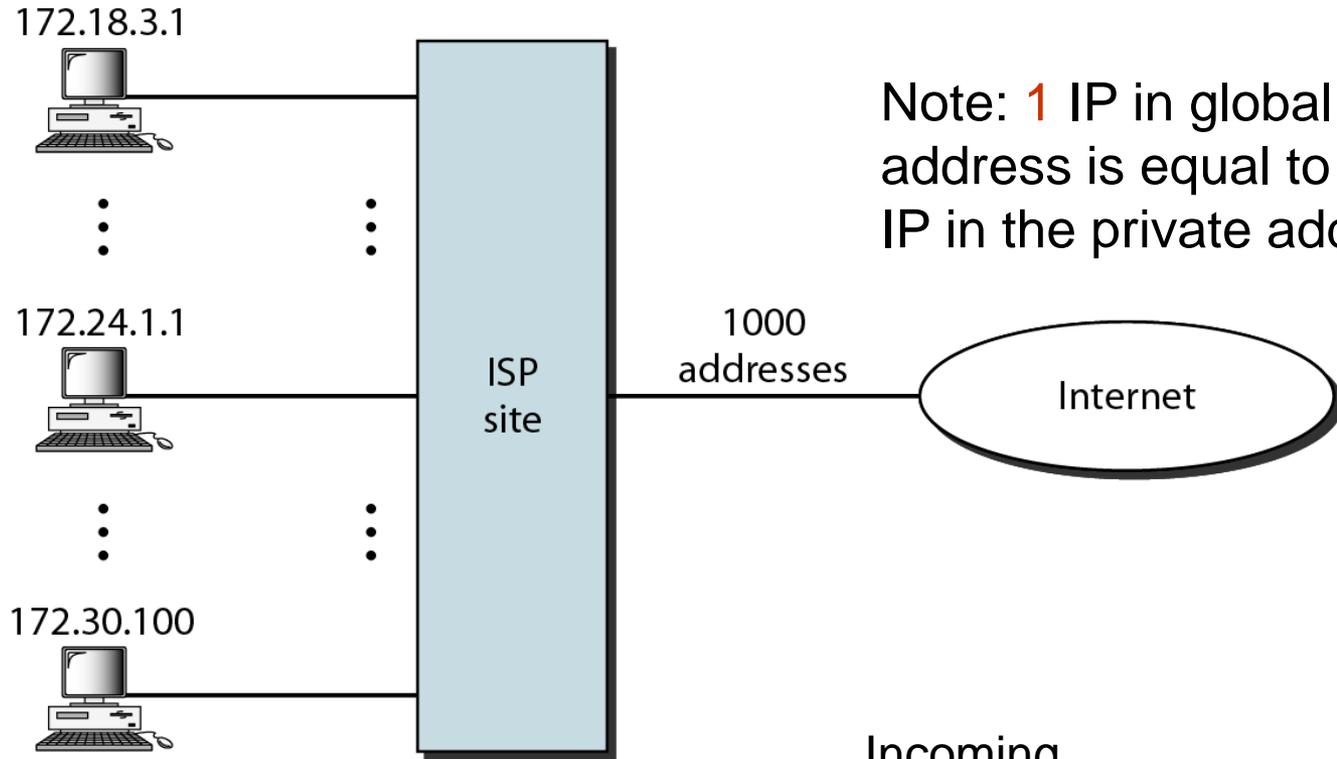
Note: 1 IP in global
address is equal to 100
IP in the private address.

Incoming

Outgoing:

100,000 IP

ISP Translate
————————————→ 1000 IP
By using NAT
Technology

$$100{,}000 \text{ IP} \xleftarrow[\substack{\text{By using NAT} \\ \text{Technology}}]{\text{ISP Translate}} 1000 \text{ IP}$$