Internet Architecture
Second Stage
Asst. Lect. Noor Razaq

COLLEGE OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SECURITY

Lecture 5

Network Address Translation (NAT)

Lecture Outline

1 Introduction

2 Address Translation

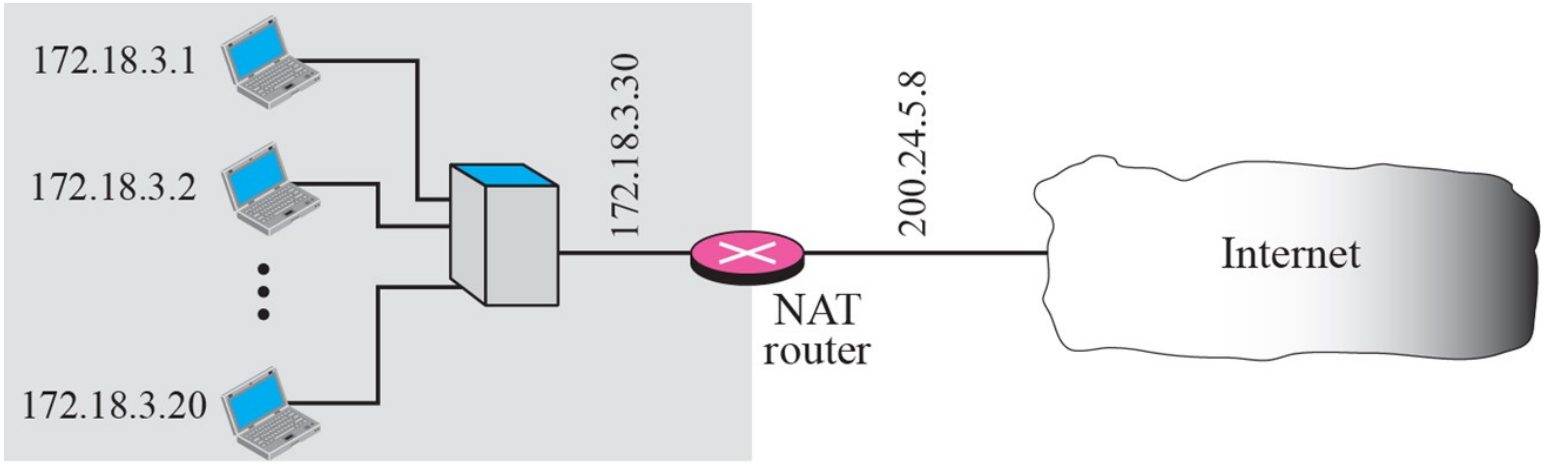
3 Translation Table

1. Introduction

- The distribution of addresses through ISPs has created **a new problem.** If the business grows or the household needs a larger range, the ISP may not be able to grant the demand because the addresses before and after the range may have already been allocated to other networks.
- **In most situations,** however, only a portion of computers in a small network need access to the Internet simultaneously.
- A technology that can help in this cases is Network Address Translation (NAT).

1. Introduction

- The NAT 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 the rest of the world.
- The site must have only one single connection to the global Internet through a NAT-capable router that runs NAT software.



Site using private addresses

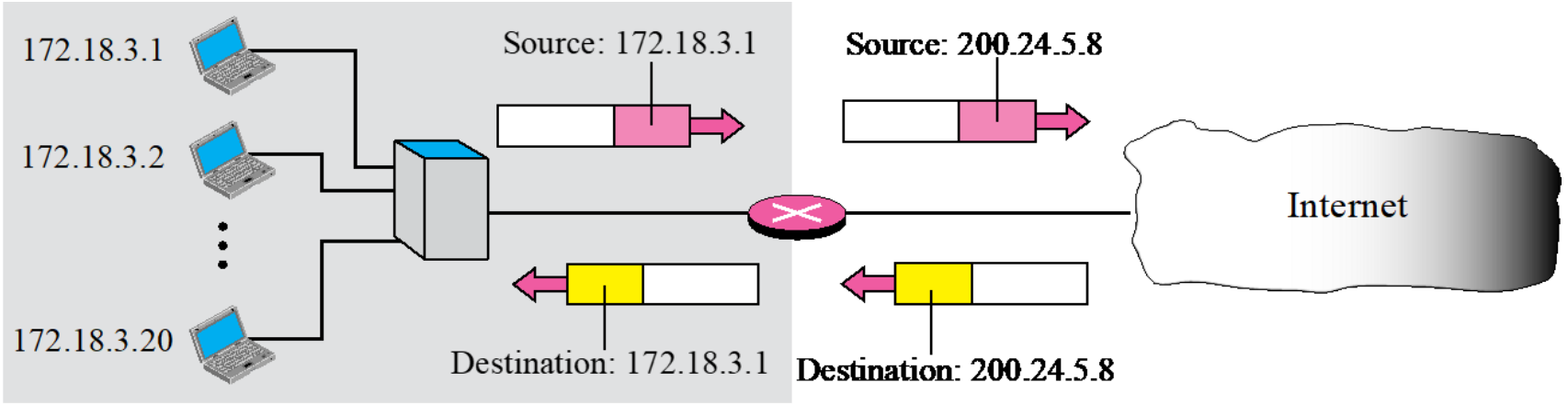
Private Addresses

- A number of blocks are assigned **for private use**. They are not recognized globally.
- These addresses are used either in isolation or in connection with network address translation techniques **(Network Address Translation (NAT)) .**

Block	*Number of addresses*	*Block*	*Number of addresses*
10.0.0.0/8	16,777,216	192.168.0.0/16	65,536
172.16.0.0/12	1,047,584	169.254.0.0/16	65,536

2. 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.**



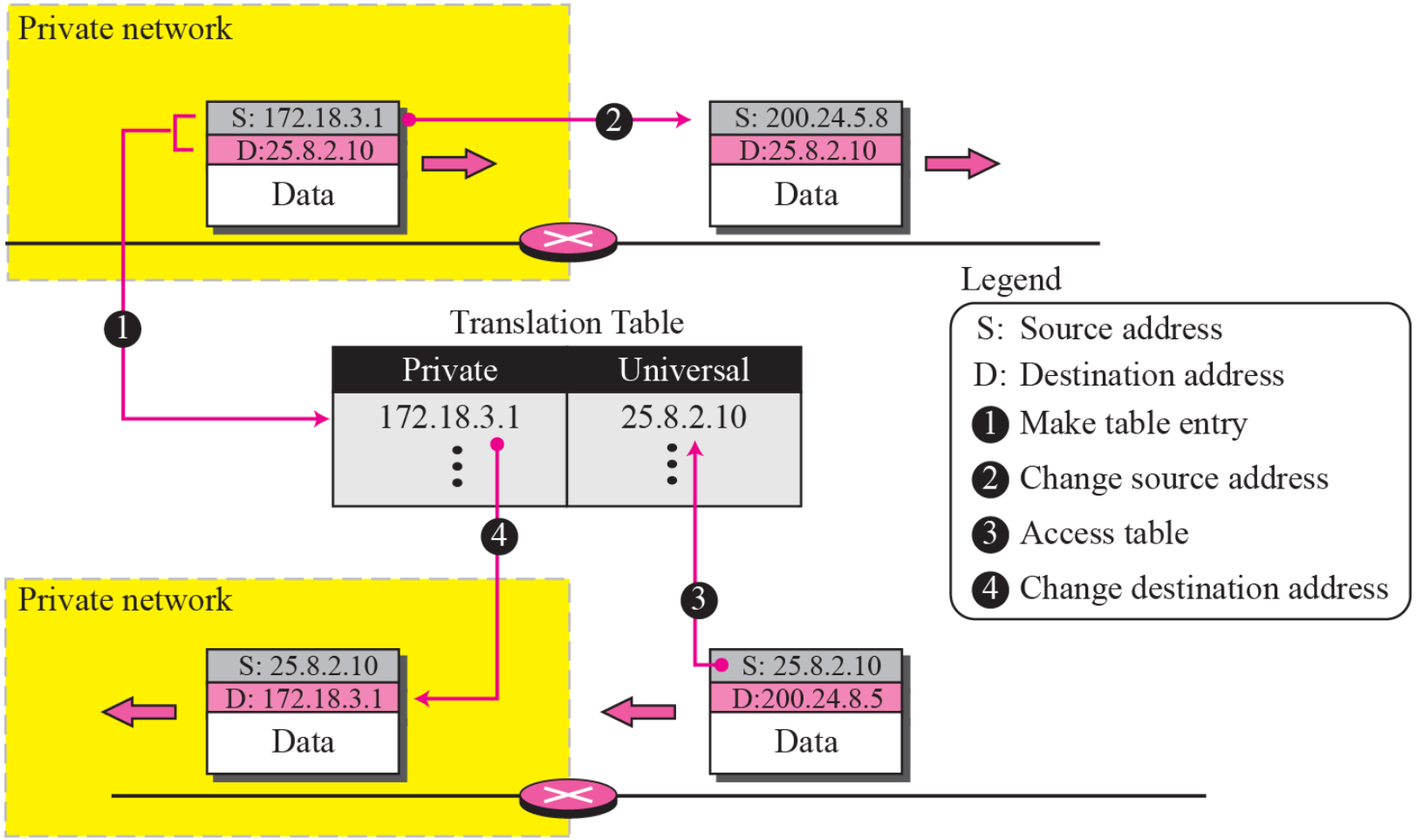
3. Translation Table

- We may have noticed that translating the source addresses for an outgoing packet 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**.

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.
- In this strategy, 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.
- NAT is used mostly by ISPs that assign one single address to a customer.

Using One IP Address



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 (e.g., 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.

Using Both IP Addresses and Port Addresses

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
…	…	…	…	…

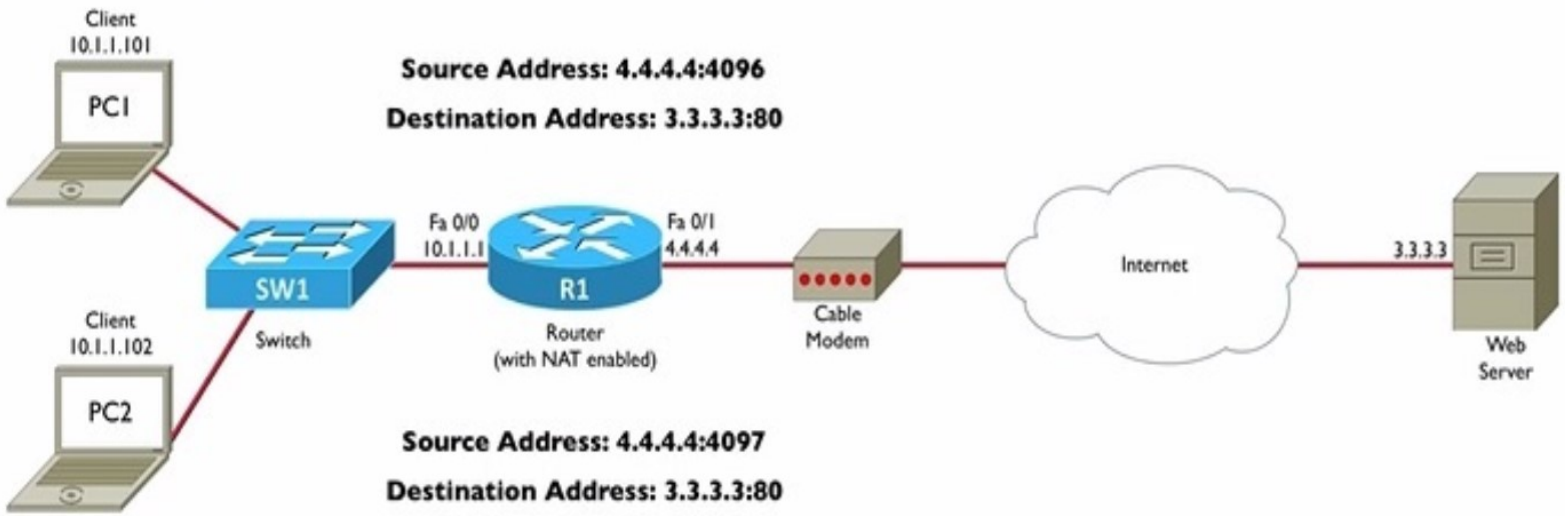
- **Note that** when the response from HTTP comes back, the combination of source address (25.8.3.2) and destination port address (1400) defines the private network host to which the response should be directed.
- **Note also that** for this translation to work, **the ephemeral port addresses (1400 and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

Example for Using Both IP Addresses and Port Addresses

Port Address Translation (PAT)

Source Address: 10.1.1.101:44252

Destination Address: 3.3.3.3:80



Source Address: 10.1.1.102:17116

Destination Address: 3.3.3.3:80

Inside Local Address	Inside Global Address	Outside Global Address
10.1.1.101:44252	4.4.4.4:4096	3.3.3.3:80
10.1.1.102:17116	4.4.4.4:4097	3.3.3.3:80

Addressing: Port Numbers

- To define the processes, we need second identifiers called port numbers. In the TCP/IP protocol suite, the port numbers are integers between 0 and 65,535.

- TCP/IP has decided to use universal port numbers for **servers**; these are called **well-known port numbers**. **The client program** defines itself with a port number, called **the ephemeral port number.**

Addressing: Port Numbers

- Internet Corporation for Assigned Names and Numbers (ICANN) has divided the port numbers into three ranges: **well-known, registered, and dynamic (or private).**
- **Well-known ports:** The ports ranging from 0 to 1,023 are assigned and controlled by ICANN.
- **Registered ports:** The ports ranging from 1,024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.
- **Dynamic ports:** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers.