ET0730

Chapter 8
Network Address Translation

Singapore Polytechnic

School of Electrical & Electronic Engineering

Objectives

- Understand IPv4 Addressing Space and its limitation.
- Explain the differences between Public and Private IP Addresses.
- Explain the need of Network Address Translation (NAT).
- Describe different types of NAT.
- *Appendix - Explain how PAT works.*

Outline

- IPv4 Addressing Space and its limitation
- Public and Private IP Addresses
- What is Network Address Translation (NAT)?
- Types of NAT
  - Static NAT
  - Dynamic NAT
  - Overloading (PAT)
- Broadband Router's NAT Configuration
- How does PAT work?

Introduction to Network Address Translation (NAT)

https://www.youtube.com/watch?v=QBqPzHEDzvo

IPv4 Addressing Space

- IPv4 uses 32 bits for addressing.
- 32 bits gives 2^{32} = 4.3 billions different IP addresses.
- Some IP addresses have been reserved for special use. Examples are:
  - Local loopback IP addresses
    - 127.x.x.x
  - Class D IP addresses (start with "1110", for multicast)
    - 224.0.0.0 to 239.255.255.255
  - Class E IP addresses (start with "1111", for research, testing and experimentation)
    - 240.x.x.x – 254.xxxx
- Available IPv4 addresses (Classes A, B and C) ≈ 3.7 billions.

Limitation of IPv4 Addressing

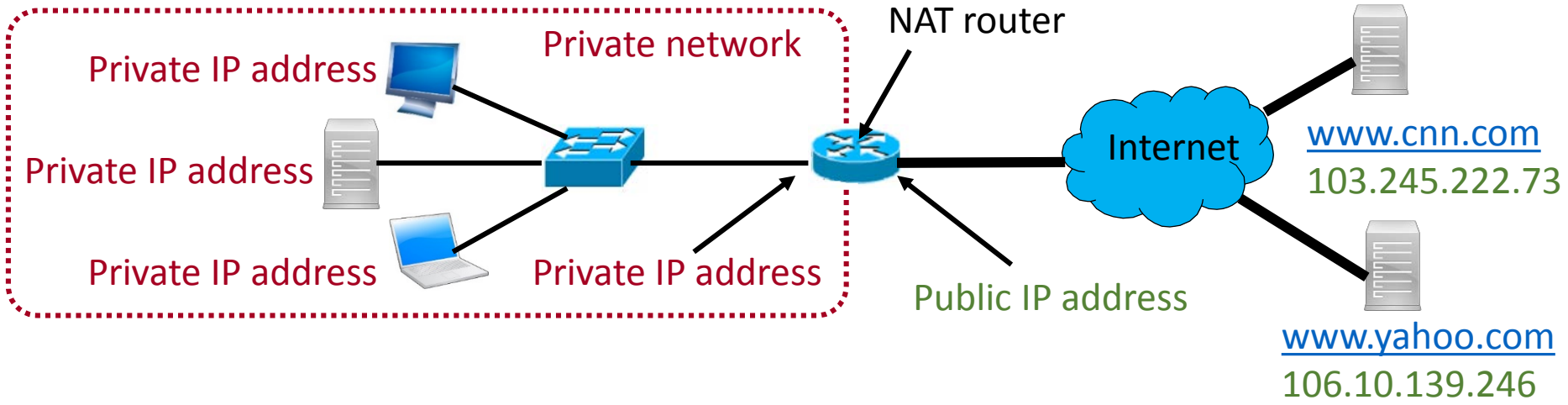
- 3.7 billions of usable IP addresses are insufficient.
  - World population is 7 billions.
  - Each person may have multiple communication devices.
- Temporary solution: Sharing of IP Addresses.
  - Long term solution is IPv6, to be discussed in next chapter.

How to share IP Addresses?

- There are only 3.7 billions IP addresses available.
- If IP addresses can be shared, we can support more users in the internet.
  - But IP address of each device on the internet must be unique!
- How to share IP addresses?
  - DHCP – only assign IP address to a device when it is connected. But, what if too many devices want to be connected?
- Solution: Network Address Translation (NAT)
  - A concept using “public IP addresses” and “private IP addresses”.

Public and Private IP Addresses

- Public IP addresses are IP addresses that routers in the internet will route.
- Private IP addresses can only be used in private networks only.
  - Routers in the internet will not forward packets destined for private IP addresses.



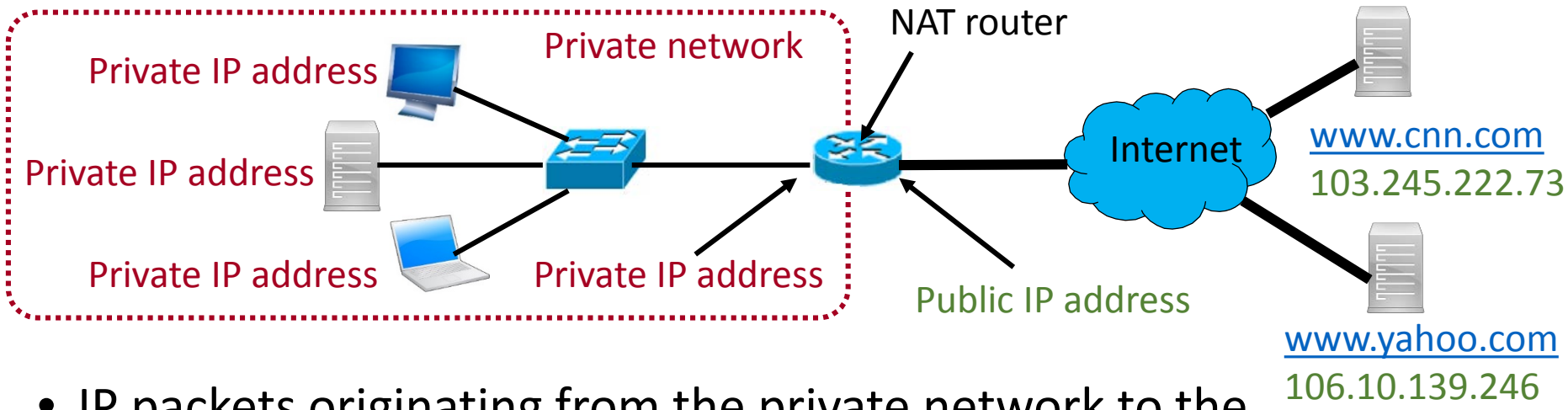
Private IP Addresses

- Three ranges of IPv4 addresses have been defined as “Private IP addresses”
  - 10.x.x.x
  - 172.16.0.0 to 172.31.255.255
  - 192.168.x.x
- Private IP addresses are to be used in private networks only.
- Try this at home:
  - When you are at home (the LAN in your home is considered a private network), if your laptop is connected to the internet through your broadband router, check the IP address of your laptop. You should find that the IP address is something like 192.168.xxx.xxx (e.g. 192.168.1.101).

Public IP Addresses

- Public IP addresses are IP addresses that can be assigned to internet users by the ISPs.
- Routers in the internet will route IP packets destined for public IP addresses.
- Public IP addresses are IPv4 addresses that are not reserved for:
  - local loopback
  - private IP addresses
  - multicast address
  - Class E (experiment) address, and
  - a few more small groups of IP addresses reserved for other purposes.

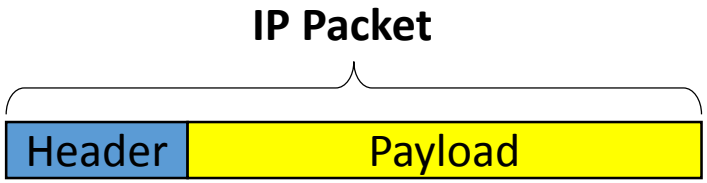
What is Network Address Translation (NAT)?



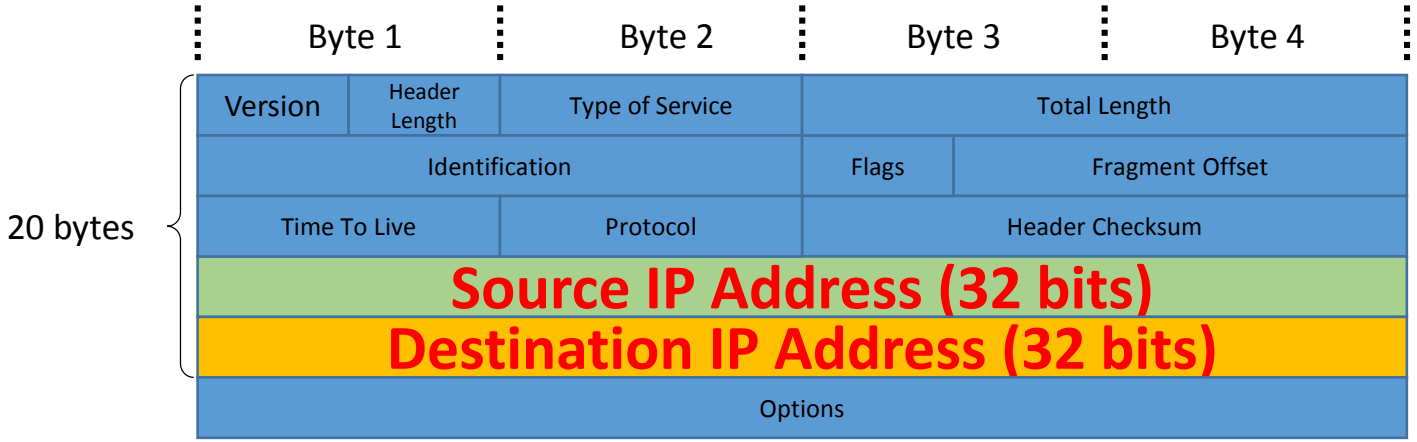
- IP packets originating from the private network to the internet is "translated" from "private IP address" to "public IP address" by the router before the IP packet is forwarded to the internet.
- For IP packets received from the internet, the router translates the "public IP address" to "private IP address" before forwarding the packet to devices in the private network.
- Translation is done by modifying the IP packet header.

What does NAT do to the IP Packet Header? (1)

- An IP packet comprises of the IP Packet Header and the Payload.



- The IP packet header comprises of 12 compulsory fields.
- Two fields are used by NAT:
  - **Source IP address** – the source that originates the IP packet.
  - **Destination IP address** – recipient of the IP packet.

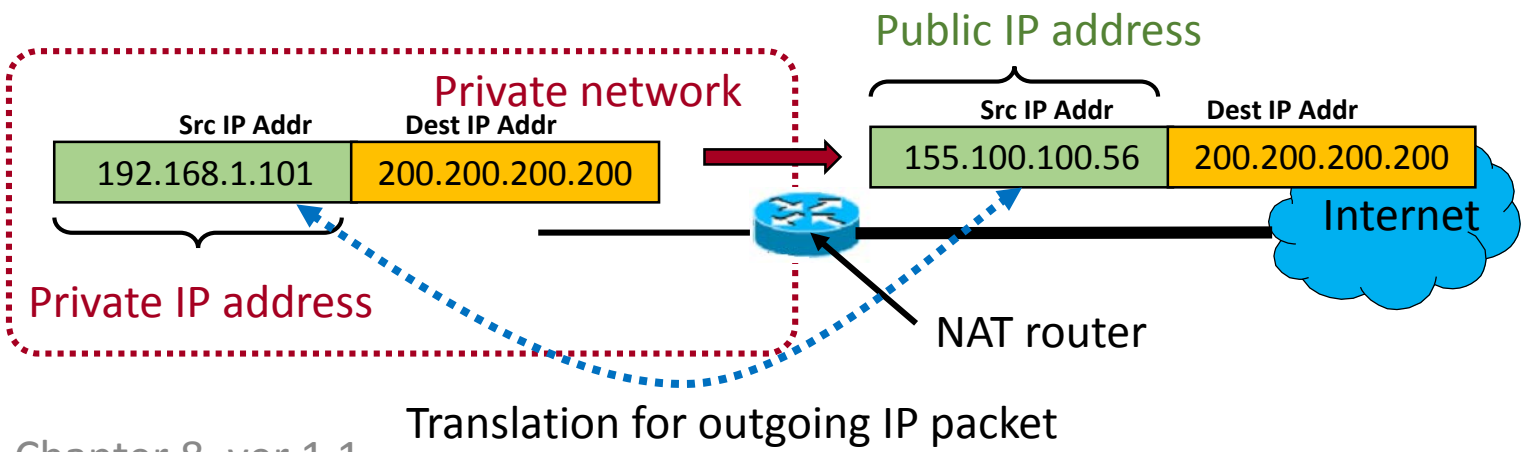


What does NAT do to the IP Packet Header? (2)

- For outgoing (private network to internet) IP packets, the router modifies the Source IP Address field.
- For incoming (internet to private network) IP packets, the router modifies the Destination IP Address field.
- Replacement of Src/Dest IP Address is based on records in the Address Translation Table.

Address Translation Table

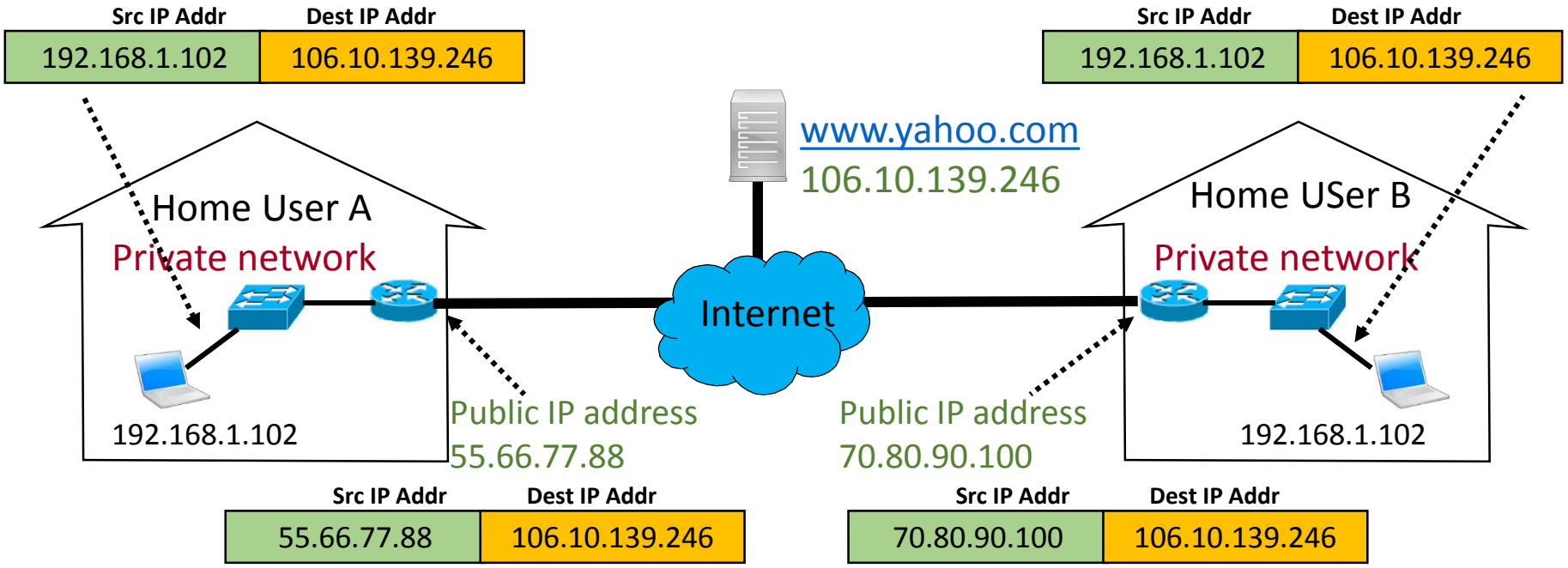
Private IP Address	Public IP Address
192.168.1.101	155.100.100.56
10.10.10.20	50.60.70.80



Translation for outgoing IP packet

Why is NAT necessary when using private IP Addresses?

- Reason: Devices in different private networks may be using identical private IP addresses.
  - Example: 192.168.1.102 for both laptops for the two home users in the figure.
- If the private IP address is not "translated" into a public IP address, the two devices' identical IP addresses will cause IP address conflict.

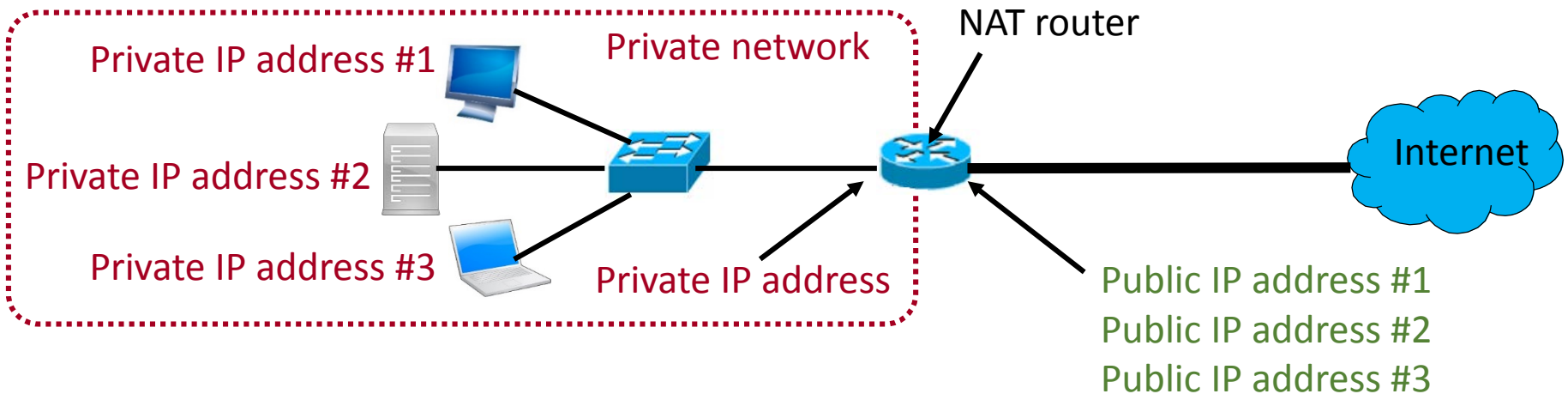


Types of NAT

- Four types of NAT:
  - Static NAT
  - Dynamic NAT
  - Overloading (or “Port Address Translation”, PAT)
  - Overlapping (not covered in this module)

Static NAT (1)

- The mapping of private-public IP addresses is fixed, on a one-to-one basis.
- A private IP address is always translated to the same public IP address.
  - Private IP Address #1 ↔ Public IP Address #1
  - Private IP Address #2 ↔ Public IP Address #2
  - Private IP Address #3 ↔ Public IP Address #3
- Useful when a device in the private network needs to be accessible from the public network.



Static NAT (2)

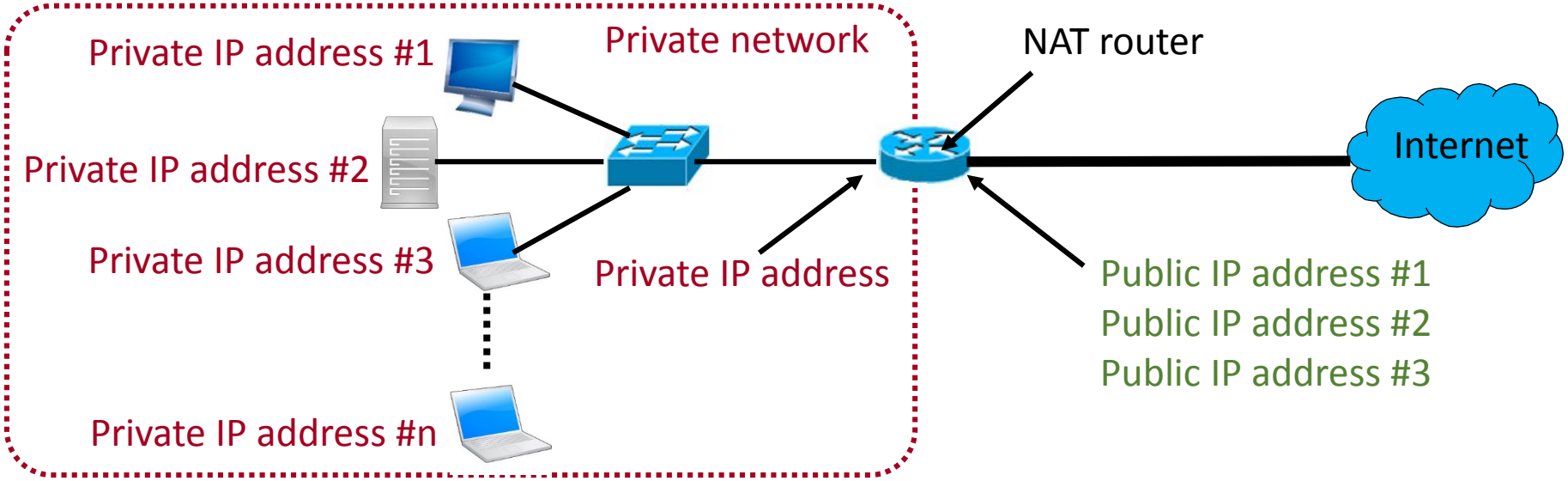
- Example: If a router has an Address Translation Table as shown below:

Private IP Address		Public IP Address
192.168.1.101	⟷	55.66.77.85
192.168.1.102	⟷	55.66.77.86
192.168.1.103	⟷	55.66.77.89

  - Private to Public Translation:
    - 192.168.1.101 is always translated to 55.66.77.85.
    - 192.168.1.102 is always translated to 55.66.77.86.
    - 192.168.1.103 is always translated to 55.66.77.89.
  - Public to Private Translation:
    - 55.66.77.85 is always translated to 192.168.1.101.
    - 55.66.77.86 is always translated to 192.168.1.102.
    - 55.66.77.89 is always translated to 192.168.1.103.

Dynamic NAT (1)

- The mapping of private-public IP addresses is dynamic, depending on the available public IP address at the time of translation.
- A private IP address is translated to the first available public IP address.
- Can support more devices in the private network, since not all devices use the translation at the same time.



Dynamic NAT (2)

- Example: If a router has a pool of three public IP addresses as shown below, and the first public IP address has been assigned:

Private IP Address		Public IP Address
192.168.1.123	⟷	55.66.77.85
None (available)	⟷	55.66.77.86
None (available)	⟷	55.66.77.89

  - The next private IP address translation request will be translated using the public IP address 55.66.77.86.

Overloading (1)

- This is a special type of NAT, where there is only one public IP address available for translation.
- All private IP addresses from the private network will be translated to the same public IP address.
- Also known as "Port Address Translation", or PAT.
  - Reason for that name will be explained later.
- Other commonly known names are:
  - Single-address NAT
  - Port-level Multiplexed NAT

Overloading (2)

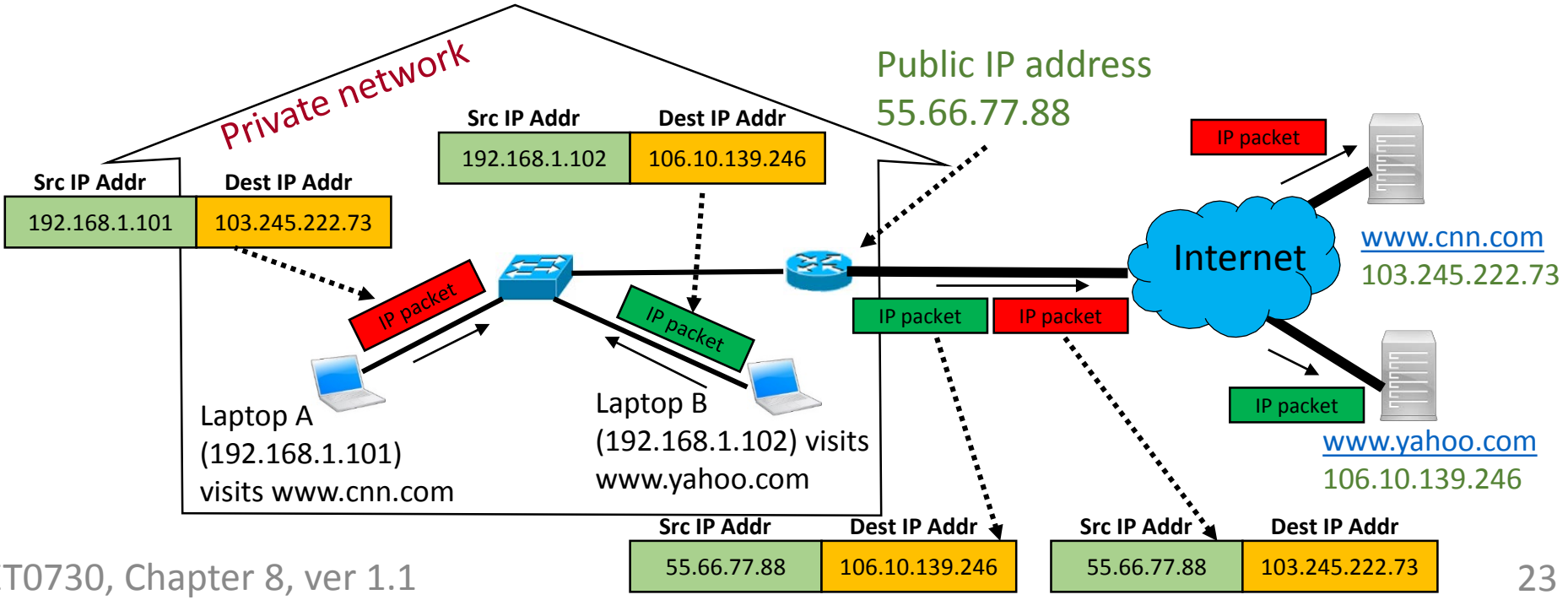
- "Overloading" (or PAT) is used in your broadband router at home.
- When your modem (ADSL, cable, ONT) is connected to the internet, the ISP issues a single, temporary, public IP address to your modem.
  - This address is also known as "WAN IP Address".
- All the laptops, computers and mobile devices in your home network use private IP addresses issued by the broadband router (via DHCP).
- The broadband router translates all IP packets between the home network and the internet.

Problem of having only one Public IP Address (1)

- Problem of having only one public IP address:
  - All IP packets from different devices in your home network leave your home with identical source IP address – your public IP address.
  - When the IP packets are returned (replies) from the internet, your public IP address becomes the destination IP address in the IP packets.
  - All returning IP packets have the same destination IP address (your public IP address).
  - How can your broadband router tell which IP packet is for which device in your home network?

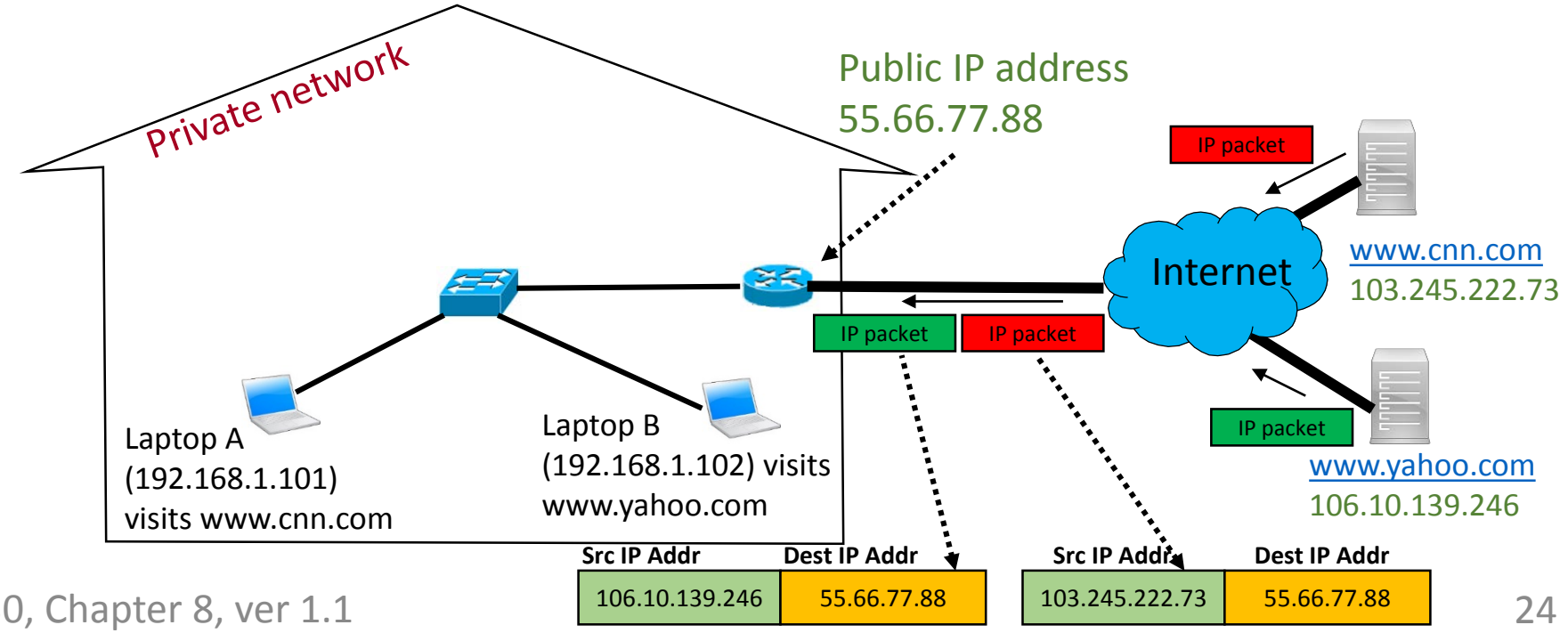
Problem of having only one Public IP Address (2)

- Problem of having only one public IP address:
  - All IP packets from different devices in your home network leave your home with identical source IP address – your public IP address.
  - When the IP packets are returned (replies) from the internet, your public IP address becomes the destination IP address in the IP packets.
    - All returning IP packets have the same destination IP address (your public IP address).
  - How can your broadband router tell which IP packet is for which device in your home network?



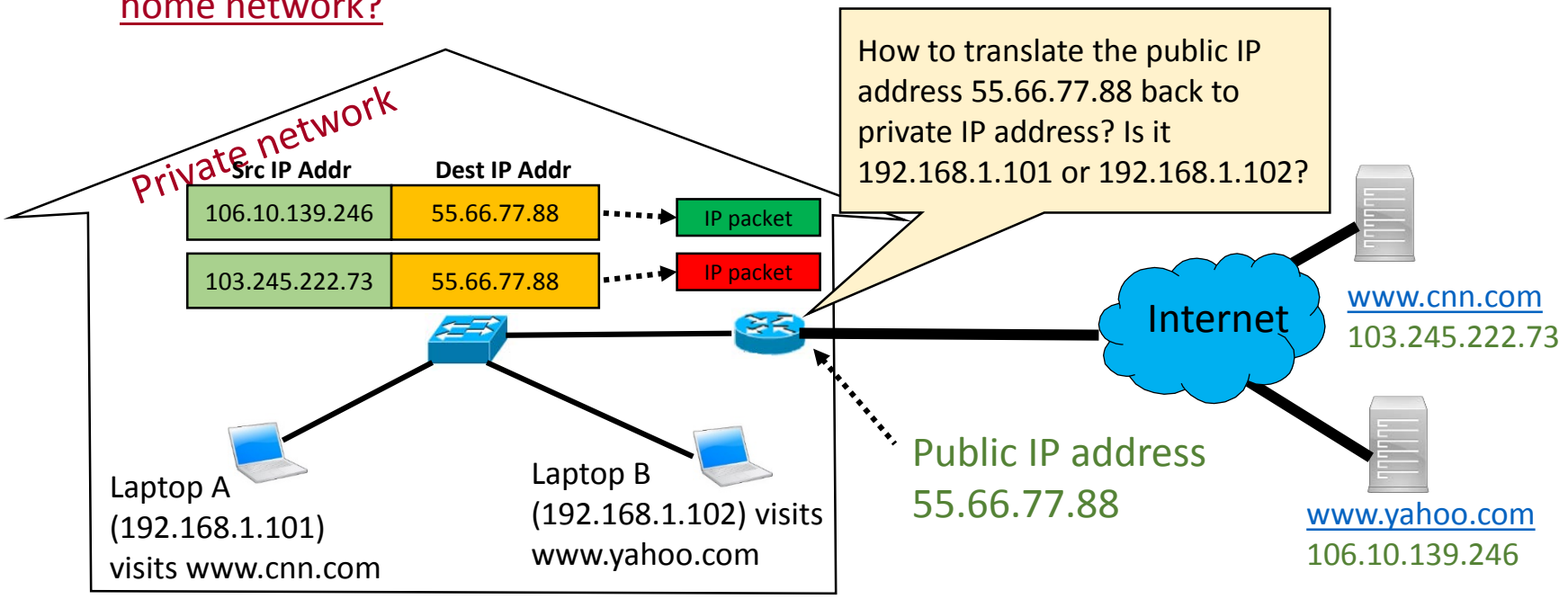
Problem of having only one Public IP Address (3)

- Problem of having only one public IP address:
  - All IP packets from different devices in your home network leave your home with identical source IP address – your public IP address.
  - When the IP packets are returned (replies) from the internet, your public IP address becomes the destination IP address in the IP packets.
    - All returning IP packets have the same destination IP address (your public IP address).
  - How can your broadband router tell which IP packet is for which device in your home network?



Problem of having only one Public IP Address (4)

- Problem of having only one public IP address:
  - All IP packets from different devices in your home network leave your home with identical source IP address – your public IP address.
  - When the IP packets are returned (replies) from the internet, your public IP address becomes the destination IP address in the IP packets.
    - All returning IP packets have the same destination IP address (your public IP address).
  - How can your broadband router tell which IP packet is for which device in your home network?



Solution: Port Address Translation (PAT, or Overloading)

- Solution: Use IP Address + Port Number (Transport Layer) to differentiate the IP packets.
- The Address Translation Table maintains the mapping between [**Private IP Addr + Private Port**] and [**Public IP Addr + Public Port**].
- For simplicity, we can write IP address + port number as {IP_Addr}:{Port}.
- Example: 192.168.1.123:5000
  - IP address = 192.168.1.123
  - Port number = 5000

An Example of Broadband Router's NAT Configuration (1)

- A home network has three IP cameras (HomeCam1, HomeCam2 and HomeCam3) and one web server.
- The broadband router (model: Linksys WRT160NL) is to be configured to allow the IP cameras and web server to be accessible from the internet.
- Private IP addresses and port numbers of the 4 devices are chosen as shown below:

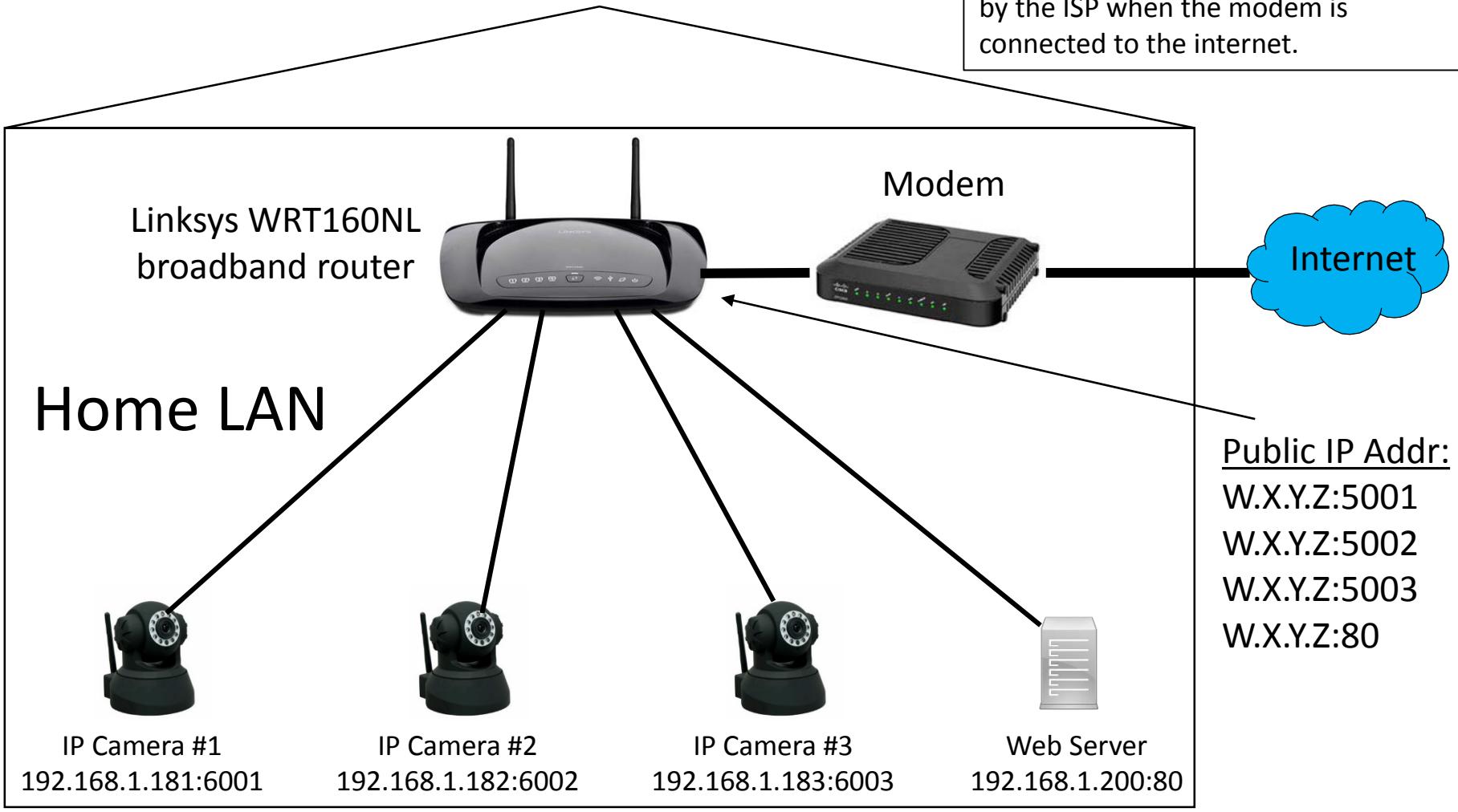
Device name	Private IP Address	Private Port Number	Public IP Address	Public Port Number
HomeCam1	192.168.1.181	6001	From ISP	5001
HomeCam2	192.168.1.182	6002	From ISP	5002
HomeCam3	192.168.1.183	6003	From ISP	5003
Web Hosting	192.168.1.200	80	From ISP	80

An Example of Broadband Router's NAT Configuration (2)

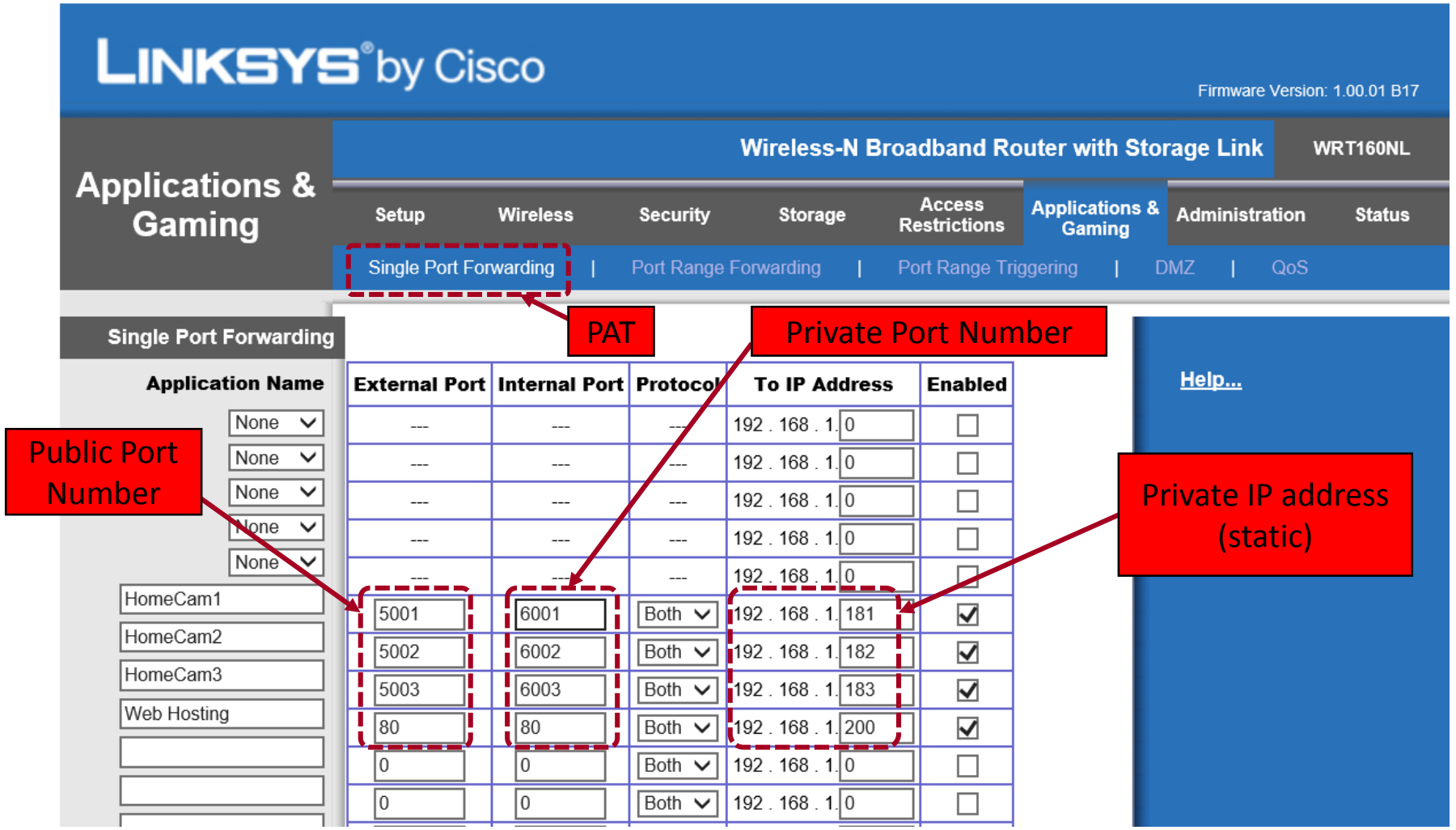
- Choice of Private IP Addresses
  - The private IP addresses of the IP cameras and web server are configured manually (i.e. static IP address).
  - DHCP is not chosen because the IP addresses of the IP cameras and web server have to be fixed.
  - Although it is possible to use the "DHCP Reservation" feature of the broadband router to assign the desired IP addresses to the four devices automatically, there is no obvious advantage in doing so.
- Choice of Private Port Numbers
  - The port numbers of the IP cameras have been chosen arbitrarily.
  - The port number of the web server is 80 since this is the well-known port number for HTTP service.

An Example of Broadband Router's NAT Configuration (3)

Public IP address is W.X.Y.Z (unknown) because it is dynamic, to be assigned by the ISP when the modem is connected to the internet.



An Example of Broadband Router's NAT Configuration (4)



Questions & Answers

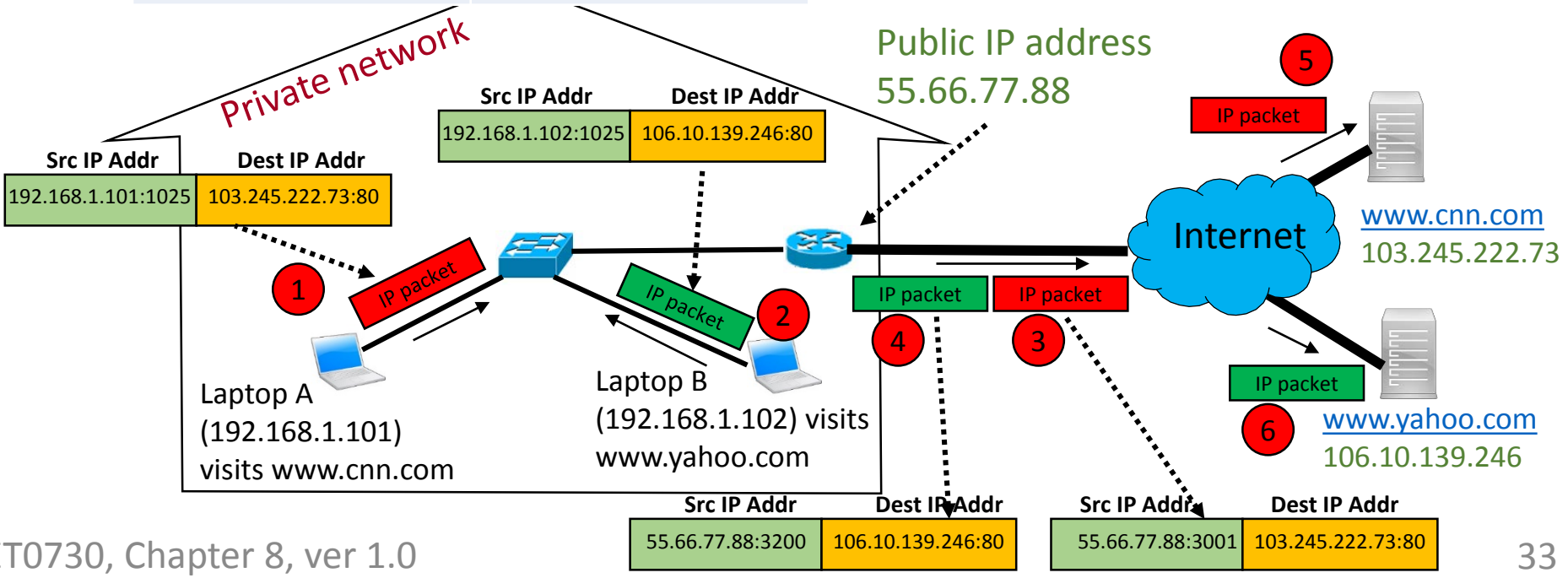
APPENDIX

How does Port Address Translation (PAT) works?

How does PAT works? (1)

- An private network has two laptops visiting two different web sites simultaneously.
- Next two slides describe how the PAT works.

Private IP Address	Public IP Address
192.168.1.101:1025 ⟷	55.66.77.88:3001
192.168.1.102:1025 ⟷	55.66.77.88:3200



How does PAT works? (2)

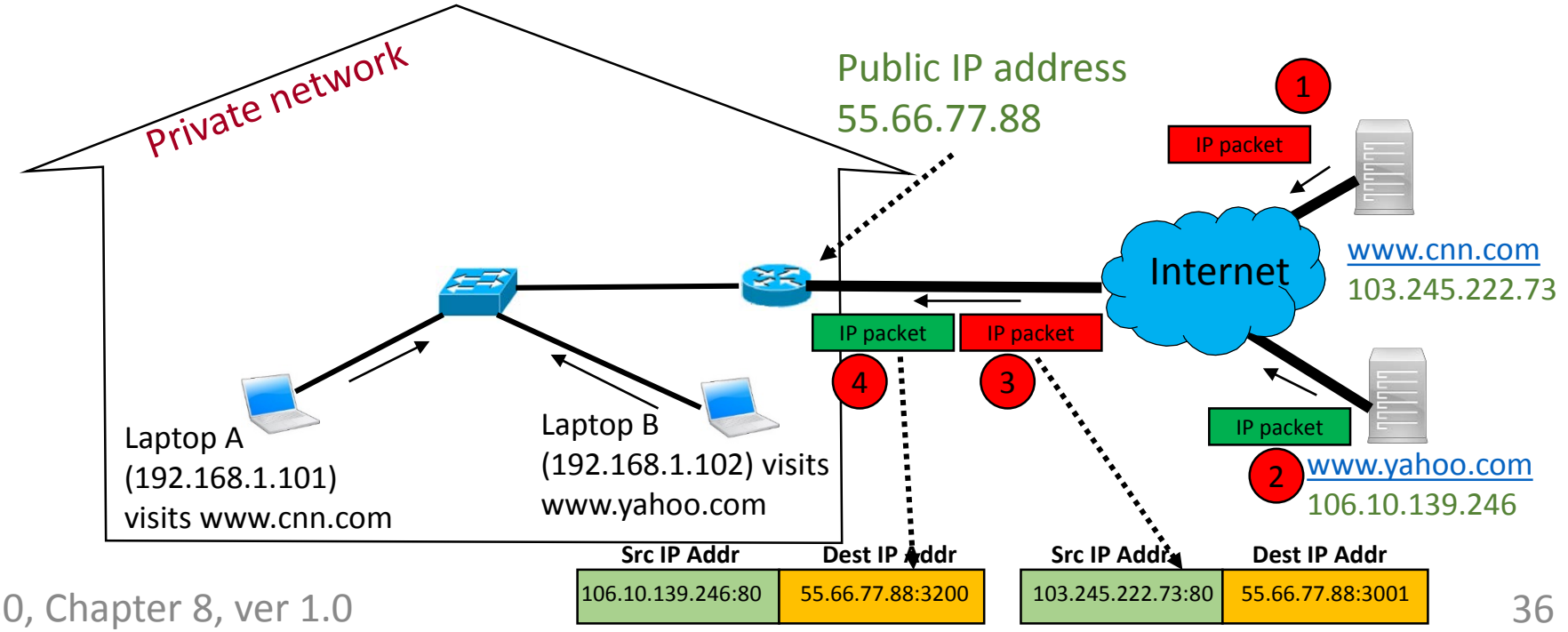
1. Laptop A visits **www.cnn.com**. The outgoing IP packet carries the HTTP Request. The Source IP address is Laptop A's IP address, 192.168.1.101. Port number is arbitrarily chosen to be 1025 (hence, 192.168.1.101:1025). The Destination IP address is CNN web server's IP address, 103.245.222.73, and the port number is 80, the well-known port number for HTTP (hence, 103.245.222.73:80).
2. Laptop B visits **www.yahoo.com**. The outgoing IP packet's Source IP address is Laptop B's IP address, 192.168.1.102. Port number is arbitrarily chosen to be 1025 (hence, 192.168.1.102:1025). The Destination IP address is Yahoo web server's IP address, 106.10.139.246, and the port number is 80 (hence, 106.10.139.246:80).

How does PAT works? (3)

3. After PAT, the outgoing IP packet from Laptop A now has its Source IP address translated to the public IP address of the router, 55.66.77.88. The Source port number is also arbitrarily translated to 3001 (hence, 55.66.77.88:3001). Notice that the Destination IP address and Destination Port Number are not affected.
4. After PAT, the outgoing IP packet from Laptop B now has its Source IP address translated to the public IP address of the router, 55.66.77.88. The Source port number is also arbitrarily translated to 3200 (hence, 55.66.77.88:3200). Notice that the Destination IP address and Destination Port Number remain unchanged.
5. In the internet, the IP packet originated from Laptop A is routed to CNN's web server.
6. In the internet, the IP packet originated from Laptop B is routed to Yahoo's web server.

How does PAT works? (4)

- When the two web servers receive the HTTP Request, they reply with web page content in the IP packet.
- The returning IP packets have their Source and Destination IP addresses & Port numbers swapped.

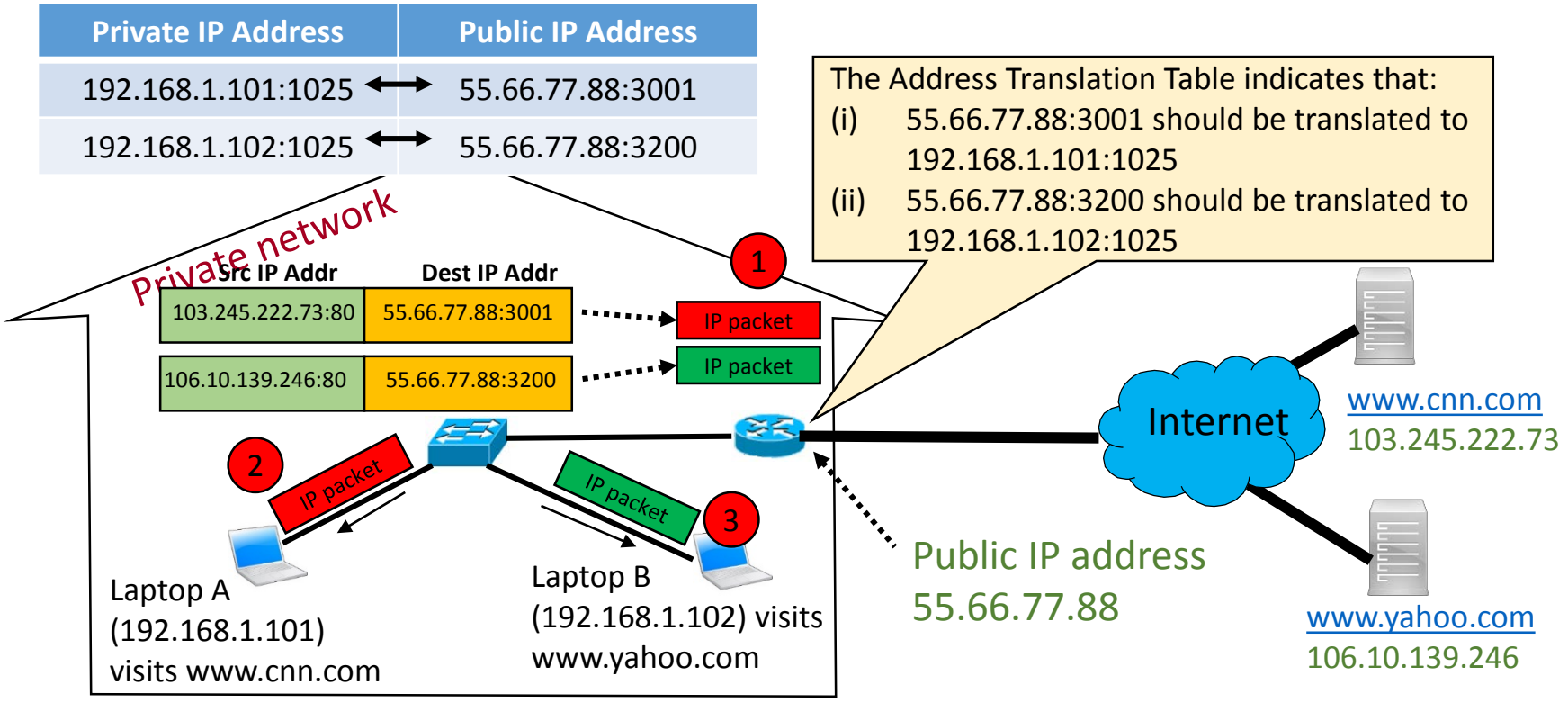


How does PAT works? (5)

1. CNN's web server replies to the HTTP Request from Laptop A with an IP packet. The IP packet's Source IP address is CNN web server's IP address, 103.245.222.73. The Source Port number is 80 (hence, 103.245.222.73:80). The Destination IP address is the router's IP address, 55.66.77.88. The Destination Port Number is 3001 (hence, 55.66.77.88:3001).
2. Yahoo's web server replies to the HTTP Request from Laptop B with an IP packet. The IP packet's Source IP address is Yahoo web server's IP address, 106.10.139.246. The Source Port number is 80 (hence, 106.10.139.246:80). The Destination IP address is the router's IP address, 55.66.77.88. The Destination Port Number is 3200 (hence, 55.66.77.88:3200).
3. The internet routes the IP packet from CNN's web server to the router 55.66.77.88.
4. The internet routes the IP packet from Yahoo's web server to the router 55.66.77.88.

How does PAT works? (6)

- Both IP packets arrive at the router.
- The router translates the public IP address back to the private IP address.



How does PAT work? (7)

Private IP Address	Public IP Address
192.168.1.101:1025 ⟷	55.66.77.88:3001
192.168.1.102:1025 ⟷	55.66.77.88:3200

1. When the router receives the two IP packets, it checks the **Destination IP Address** and **Destination Port Number** of the IP packets against the Address Translation Table.
2. For the IP packet from CNN's web server, the router finds a match at the first entry of the Address Translation Table. The router translates the Destination IP Address from 55.66.77.88 to 192.168.1.101, and the Destination Port Number from 3001 to 1025. It then routes the IP packet to Laptop A.
3. For the IP packet from Yahoo's web server, the router finds a match at the second entry of the Address Translation Table. The router translates the Destination IP Address from 55.66.77.88 to 192.168.1.102, and the Destination Port Number from 3200 to 1025. It then routes the IP packet to Laptop B.