National University of Computer & Emerging Sciences

CS 3001 - COMPUTER NETWORKS

Lecture 17

Chapter 4

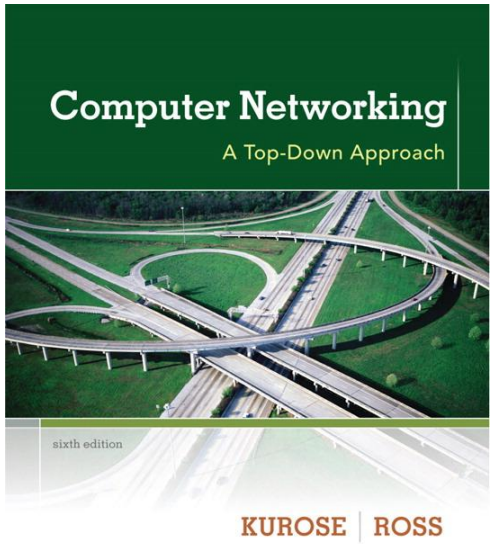
20th October, 2022

Nauman Moazzam Hayat

nauman.moazzam@lhr.nu.edu.pk

Office Hours: 02:30 pm till 06:00 pm (Every Tuesday & Thursday)

Chapter 4
Network Layer



A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

Chapter 4: outline

4.1 introduction

4.2 virtual circuit and datagram networks

4.3 what's inside a router

4.4 IP: Internet Protocol

- datagram format
- IPv4 addressing
- ICMP
- IPv6

4.5 routing algorithms

- link state
- distance vector
- hierarchical routing

4.6 routing in the Internet

- RIP
- OSPF
- BGP

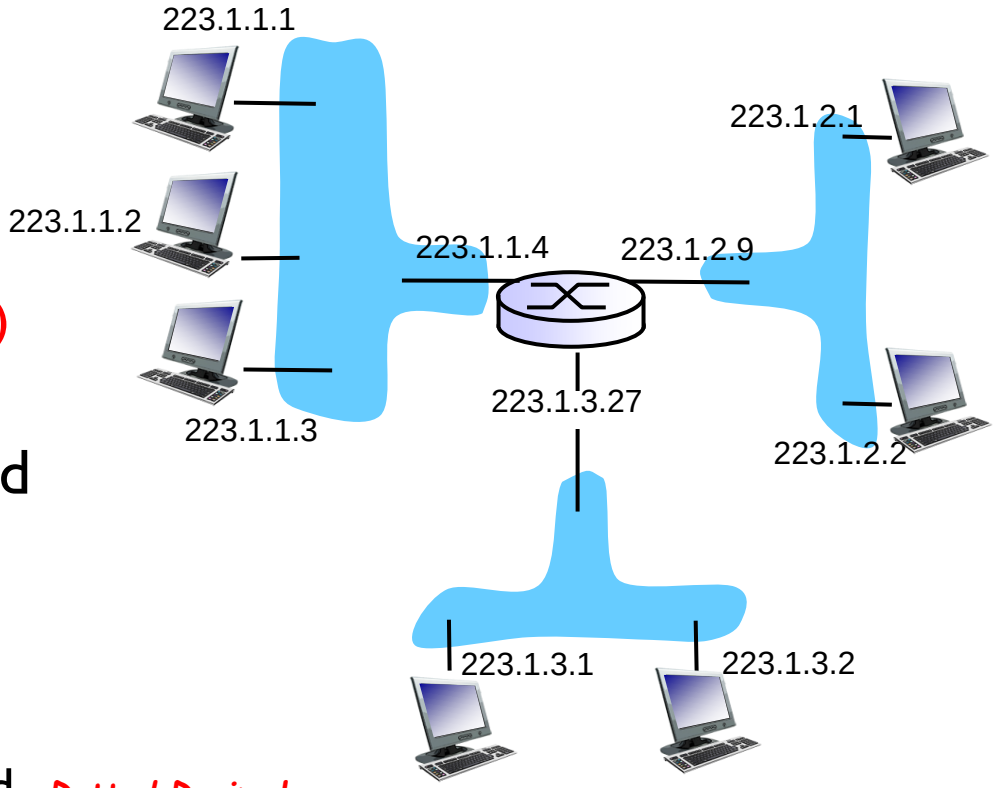
4.7 broadcast and multicast routing

IPv4 Addressing

- The Internet is made of combination of LANs and WANs connected via routers
- A host needs to be able to communicate with another host without worrying about which physical network must be passed through
- Hosts must therefore be identified uniquely and globally at the network layer
- For efficient and optimum routing, routers must also be identified uniquely and globally at the network layer

IPv4 addressing: introduction

- *IP address:* 32-bit identifier for each host, router *interface* (thus 2^{32} i.e. approx. 4 billion globally unique IP addresses possible)
- *interface:* connection between host/router and physical link
  - router's typically have multiple interfaces
  - host typically has one or two interfaces (e.g., wired Ethernet, wireless 802.11)
- *IP addresses associated with each interface (& not with host or router)*



Dotted Decimal Notation

223.1.1.1 = 11011111 00000001 00000001 00000001

223 1 1 1

IPv4 Addressing

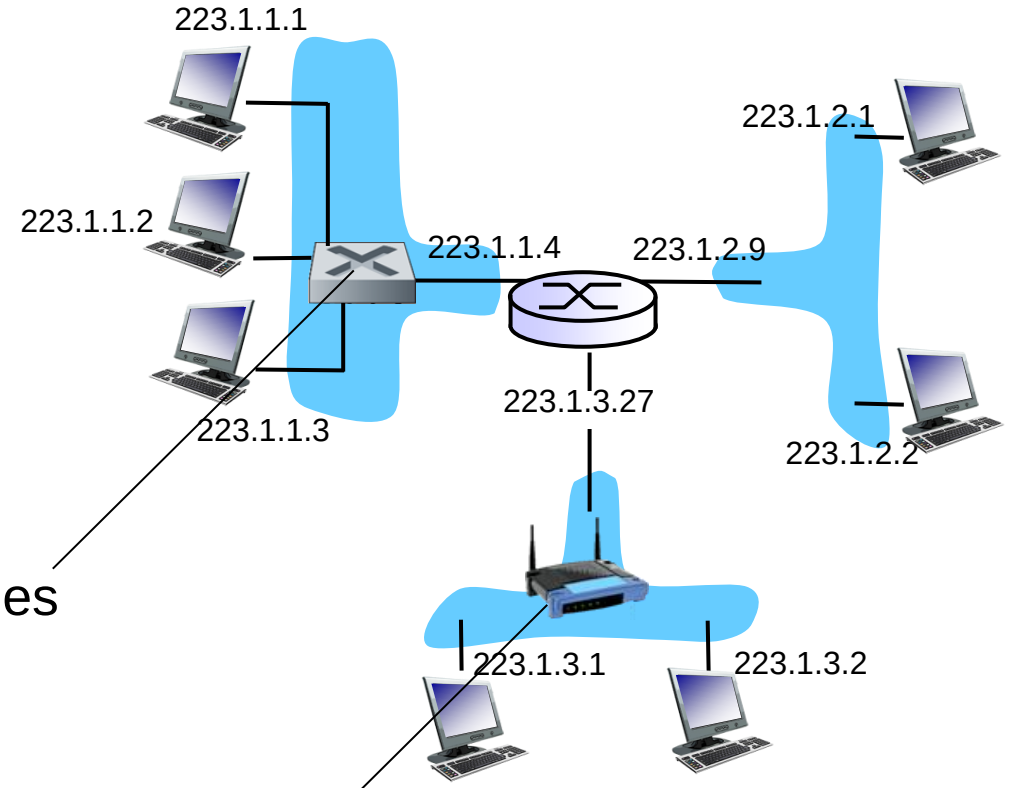
- IPv4 address is a 32-bit address, implemented in software, is used to uniquely and globally identify a host or a router on the Internet
- A device can have more than one IP address if it is connected to more than one network (multi-homed)
- An IP address have two parts, the netid and the hostid. They have variable lengths depending on the class of the address
- All devices on the same network have the same netid

- Two types of IPv4 addressing schemes, i.e.
  - Classful IP Addressing
  - Classless IP Addressing

IPv4 addressing: introduction

Q: how are interfaces actually connected?

A: we'll learn about that in chapter 5, 6.

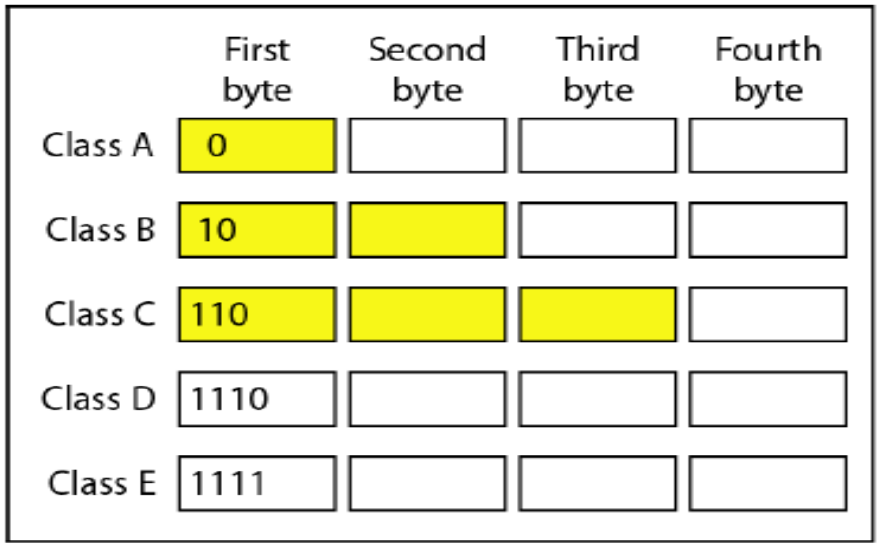


A: wired Ethernet interfaces connected by Ethernet switches

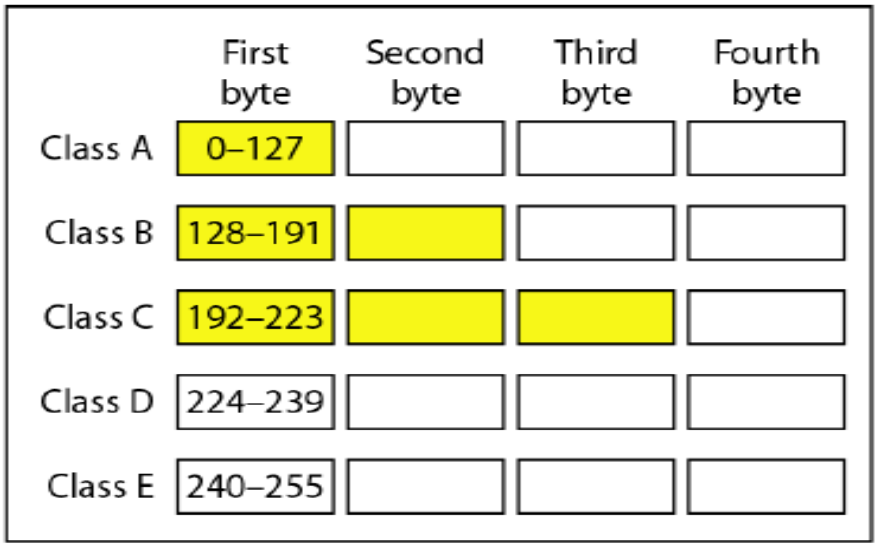
For now: don't need to worry about how one interface is connected to another (with no intervening router)

A: wireless WiFi interfaces connected by WiFi base station

Classful IPv4 Addressing



a. Binary notation



b. Dotted-decimal notation

⇒ Where ▭ = net ID & ▭ = host ID - ***Big Big Waste, thus being replaced by Classless IP Addressing***

Class	Max. Number of Networks (Blocks)	Max. # of nodes in the network (Block Size)	Application
A	$2^7 = 128$	$2^{24} = 16,777,216$	Unicast
B	$2^{14} = 16,384$	$2^{16} = 65,536$	Unicast
C	$2^{21} = 2,097,152$	$2^8 = 256$	Unicast
D	1	$2^{28} = 268,435,456$	Multicast
E	1	$2^{28} = 268,435,456$	Reserved

Special IP addresses (Reserved)

Special Address	Netid	Hostid	Source/Destination
▪ Network Address	Specific	All 0's	None Example: For IP Address 75.3.1.28, it will be 75.0.0.0
▪ Direct Broadcast Address	Specific	All 1's	Destination When source host in one network sends data to all hosts in another network (e.g. 75.255.255.255 for the above network.)
▪ Limited Broadcast Address	All 1's	All 1's	Destination Data reaches from source to all the hosts in the same network (i.e. 255.255.255.255)
▪ This host on this network	All 0's	All 0's	Source Reserved for this host when it boots up (temporary) (i.e. 0.0.0.0)
▪ Specific host on this network	All 0's	Specific	Destination Example: For IP Address 75.3.1.28, it will be 0.3.1.28
▪ Loopback address	127	Any	Destination Packets do not leave the node (NIC).

Private IP Addressing

- One of the problems in IP network address allocation is that many hosts do not require access to hosts in other networks ⇒ Assigning Globally unique public IP addresses for such hosts may be wasteful
- IETF proposed the use of Private IP addresses that are not advertised outside the private network.

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

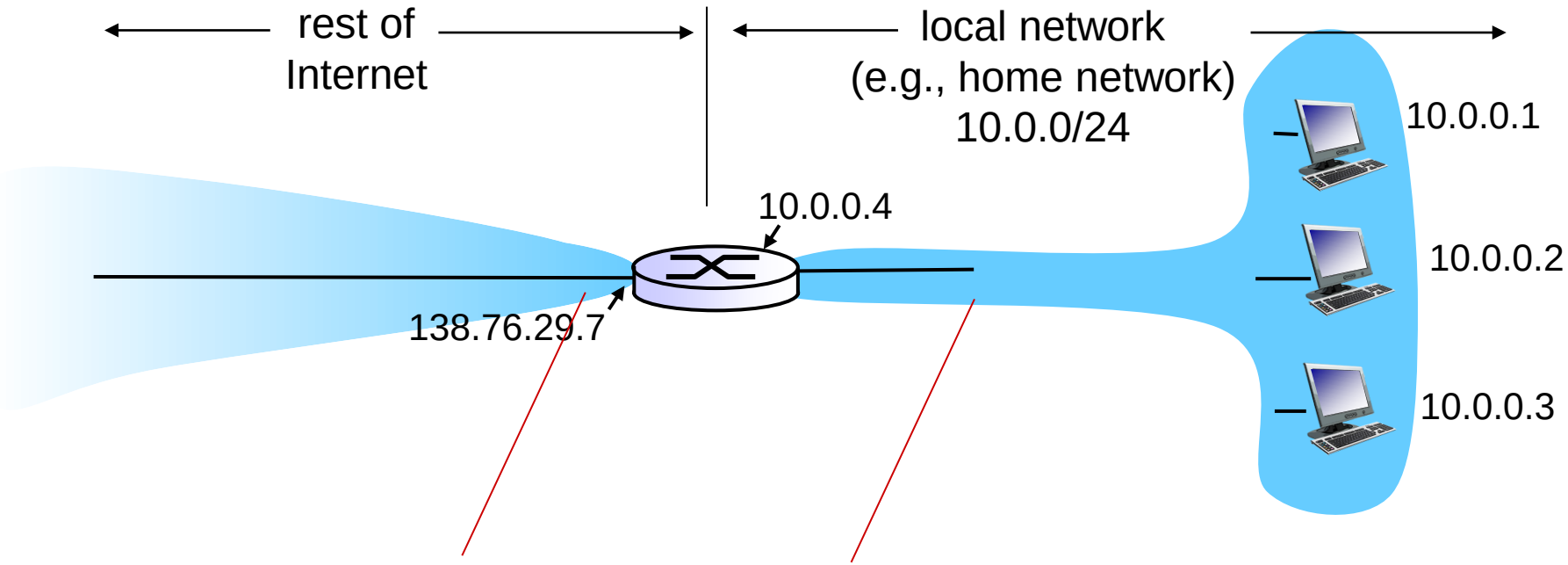
Private IP Addresses are non-routable

NAT: network address translation

motivation: local network uses just one public / global IP address as far as outside world is concerned:

- range of addresses not needed from ISP: just one IP address for all devices
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- devices inside local net not explicitly addressable, visible by outside world (a security plus)
- Implemented in the border (access) router separating the private & the public network
- Was introduced with Windows 2000

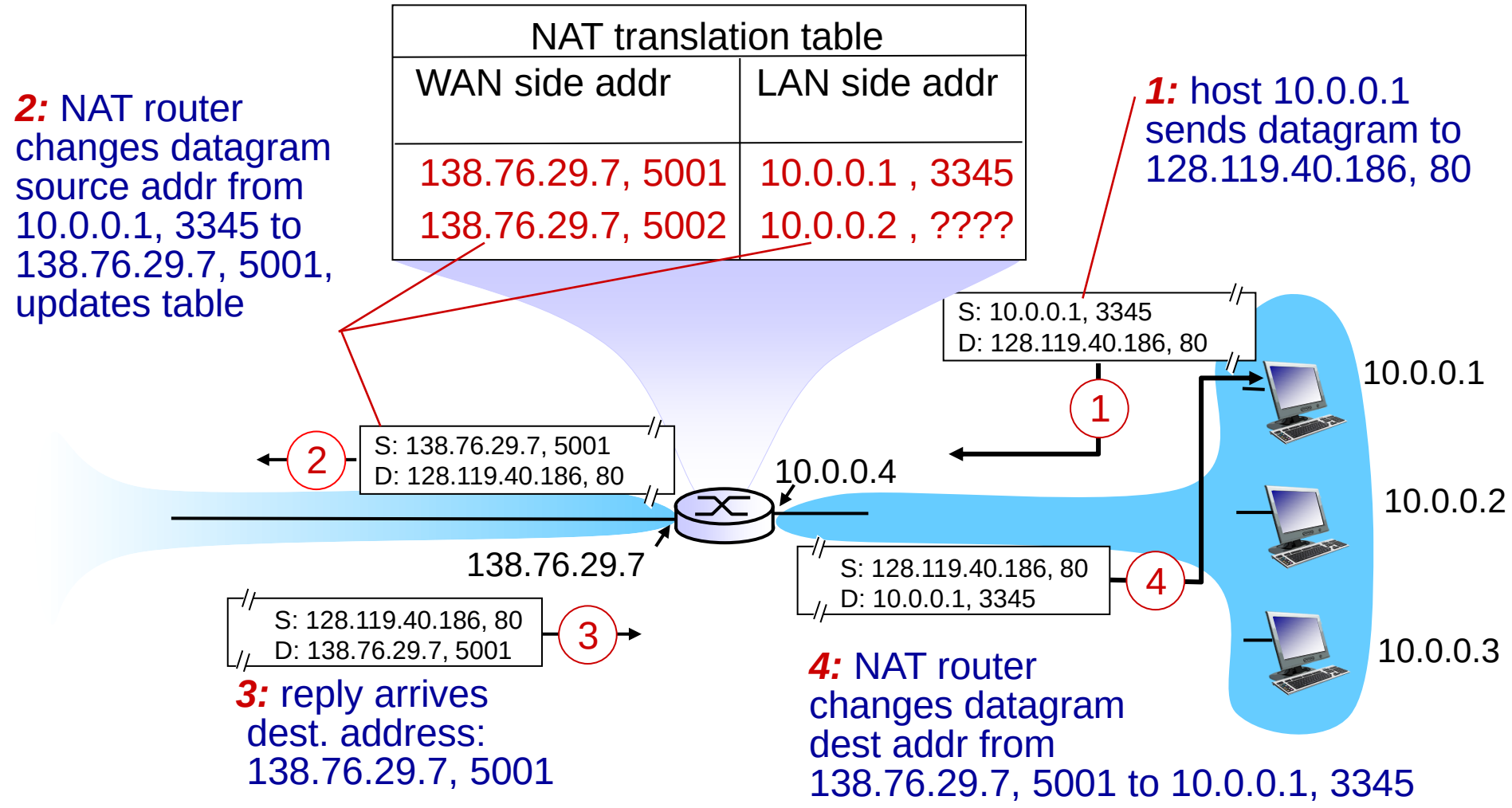
NAT: network address translation



all datagrams *leaving* local network have *same* single source NAT IP address: 138.76.29.7,different source port numbers

datagrams with source or destination in this network have 10.0.0/24 address for source, destination (as usual)

NAT / PAT: network address translation



NAT: network address translation

implementation: NAT router must:

- *outgoing datagrams: replace* (source IP address, port #) of every outgoing datagram to (NAT IP address, new port #)
  - . . . remote clients/servers will respond using (NAT IP address, new port #) as destination addr
- *remember (in NAT translation table)* every (source IP address, port #) to (NAT IP address, new port #) translation pair
- *incoming datagrams: replace* (NAT IP address, new port #) in dest fields of every incoming datagram with corresponding (source IP address, port #) stored in NAT table

NAT: network address translation

- 16-bit port-number field:
  - 60,000 plus ($=2^{16}$) simultaneous connections with a single IP address!
- NAT is controversial:
  - routers should only process up to layer 3
  - violates end-to-end argument
    - NAT possibility must be taken into account by app designers, e.g., P2P applications
  - address shortage should instead be solved by IPv6
  - ***Study*** NAT Traversal Problem & Solutions (including static configuration, UPnP / IGD & relaying from the textbook, page 351,352…)

Quiz # 3 (Chapter – 3)

- ~~***On: Thursday, 20th October, 2022 (During the lecture)***~~

- ***Rescheduled To: Tuesday, 25th October, 2022 (During the lecture)***

- ***Quiz to be taken during own section class only***