University of Pittsburgh

ECE 1150: Computer Networks

The Network Layer- IP Addressing & subnetting

Mai Abdelhakim, PhD

ECE Department

Swanson School of Engineering

University of Pittsburgh

Different Parts of IP address

- 2 parts of IP address
  - Net ID
  - Host ID
- In practice –IP address can be 3 parts
  - Net ID
  - Subnet ID
  - Host ID

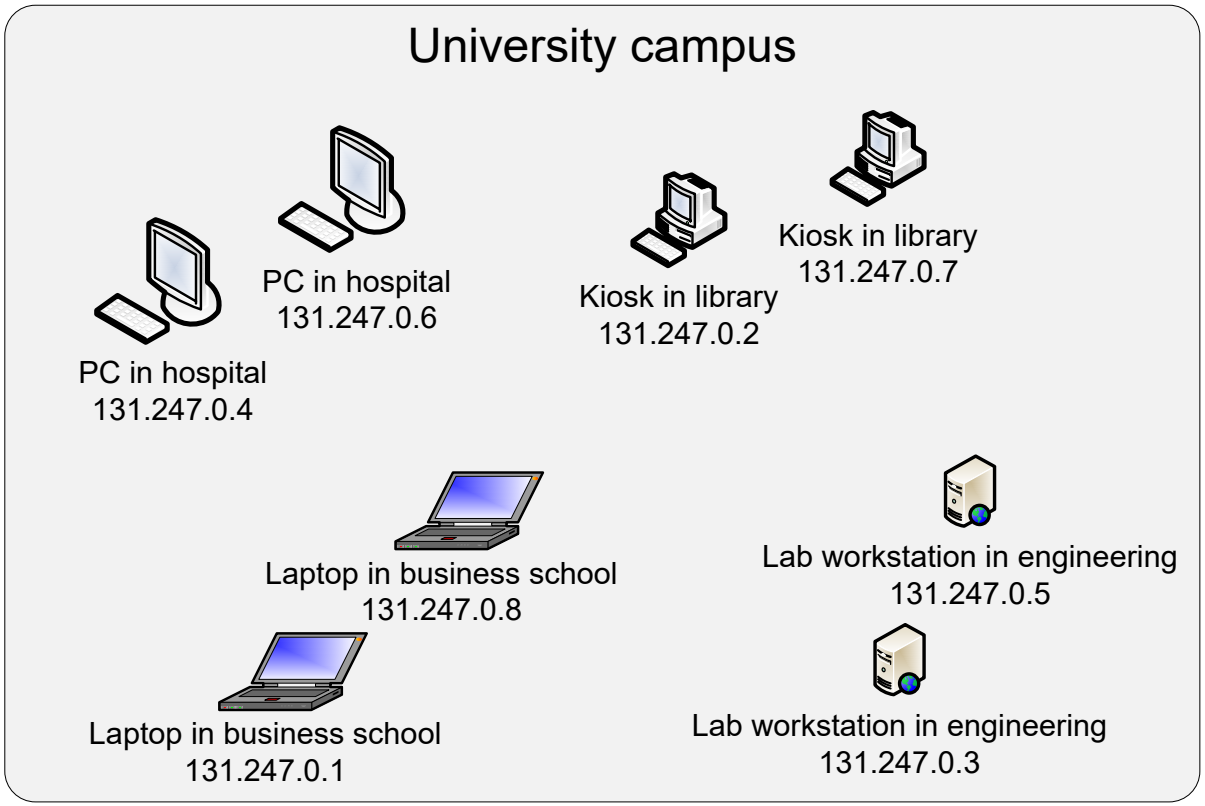
Subnetting

- Help **organize IP addresses within networks** and organizations

- Subnetting allows organizations to **distribute total pool of IP addresses in subnets**
  - Depending upon organization structure

IP Address Allocation Without Subnetting

Without subnetting: Network administrators may not know where is the IP address located on campus. (If someone called IP for help, troubleshooting will be difficult)



IP Address Allocation With Subnetting – simplifies routing & troubleshooting

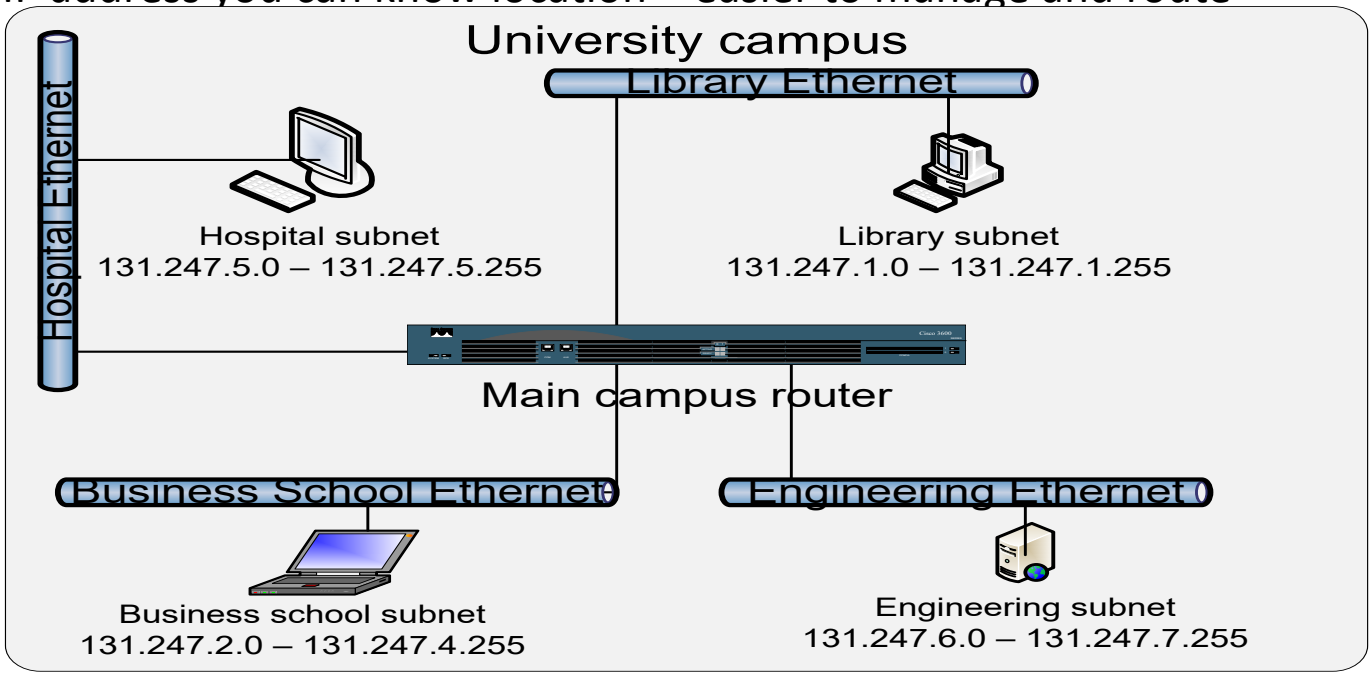
Subnetting enables the partition of a large address pool into multiple smaller blocks

Each subnetwork (e.g. schools in a university) can be **allocated contiguous set of IP addresses**:

Example:

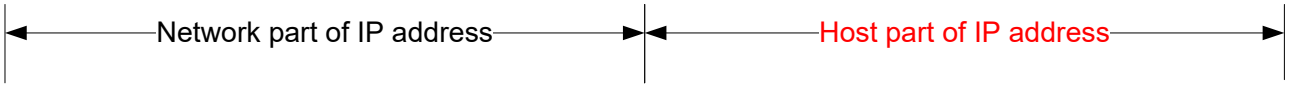
- Allocate to library: 131.247.1.0 – 131.247.1.255
- Business school: 131.247.2.0 – 131.247.4.255

➔ From IP address you can know location – easier to manage and route



2-Part Interpretation of IP Addresses

Address example in University of South Florida (USF)



10000011 11110111 00010000 11101011

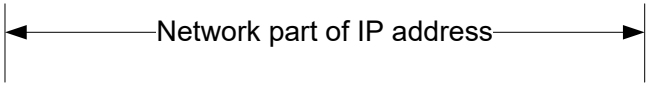
131 . 247 . 16 . 235

Network ID
(USF)

Host ID
(worskstation 24 in lab)

3-part interpretation of IP addresses

In subnetting the IP address is split into 3 parts



10000011 11110111 **00010000** 11101011

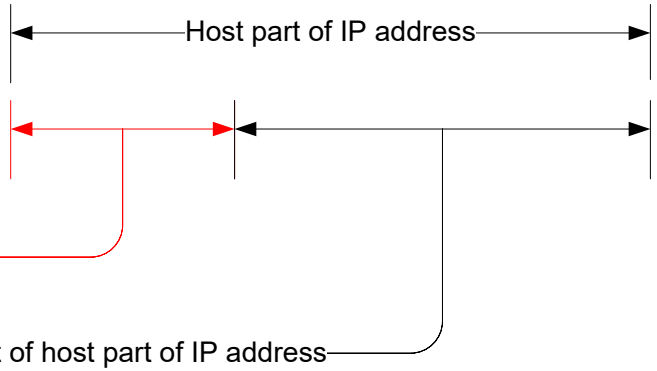
131 . 247 . 16 . 235

Network ID (USF)

Subnet ID (College of Business)

Host ID (worskstation 24 in lab)

Address example in University of South Florida



Subnetting example

- Say the organization needs to have **32 subnets**. How many bits in subnet ID needed?
    - Note: $2^5 = 32$ subnets

Example: Network ID + Subnet ID for 10 Colleges

Campus unit	Subnet ID	First 2 parts of IP addresses by college
College 1	00001	10000011.11110111.00001_ _ _ . _ _ _ _ _ _ _ _
College 2	00010	10000011.11110111.00010 _ _ _ . _ _ _ _ _ _ _ _
College 3	00011	10000011.11110111.00011 _ _ _ . _ _ _ _ _ _ _ _
College 4	00100	10000011.11110111.00100 _ _ _ . _ _ _ _ _ _ _ _
College 5	00101	10000011.11110111.00101 _ _ _ . _ _ _ _ _ _ _ _
College 6	00110	10000011.11110111.00110 _ _ _ . _ _ _ _ _ _ _ _
College 7	00111	10000011.11110111.00111 _ _ _ . _ _ _ _ _ _ _ _
College 8	01000	10000011.11110111.01000 _ _ _ . _ _ _ _ _ _ _ _
College 9	01001	10000011.11110111.01001 _ _ _ . _ _ _ _ _ _ _ _
College 10	01010	10000011.11110111.01010 _ _ _ . _ _ _ _ _ _ _ _

Question

Consider an organization with a /16 network address block (131.247.0.0/ 16) and 32 subnets, how many bits in host ID part of the address?

- Most medium-large organizations are /16

- Answer: Number of bits for host ID part is
  b = 32 – # bits in net ID – # bits in subnet ID
  - 32 is the length of IPv4 address
  - In previous example, # bits in Host ID: 32 -16 -5 =11 bits

Subnet Masks

- **Sequence of 1's followed by sequence of 0's**
- Number of 1's == network ID + subnet ID bits
- Number of 0's == # host ID bits
- Example: If we have /16 network, with 5 bits subnet ID has subnet mask:
  11111111.11111111.11111000.00000000

Number of 1's is 16+5=21

  - Written as 255.255.248.0
    - The first 21 bits of any IP address in the organization identifies network + subnet

Subnet Address

- Subnet address:
  - Obtained by setting host ID to all zeros

- Example:

Campus unit	Subnet address (binary)	Subnet address (decimal)
College 1	10000011.11110111.00001000.00000000	131.247.8.0
College 2	10000011.11110111.00010000.00000000	131.247.16.0
College 3	10000011.11110111.00011000.00000000	131.247.24.0
College 4	10000011.11110111.00100000.00000000	131.247.32.0
College 5	10000011.11110111.00101000.00000000	131.247.40.0

Subnet Mask & Subnet Address

- Facilitates routing:
  - **Router** needs to know the subnet address of a given IP address to forward the packet to the correct subnet
    - This is done by **masking** the IP address with the subnet mask to get subnet address

Subnet Mask Operation

- What does a subnet mask do?
  - The 0's in the subnet mask block (mask) the corresponding bits in any destination address
    - Bits are seen as 0
  - The 1's in the subnet mask allow the corresponding bits to be seen
  - Result is the subnet address

Example: Subnet mask operation
Two hosts in different collages in same organization

	Host 1 (131.247.8.45)	Host 2 (131.247.27.231)
Destination IP address	10000011.11110111.00001000.00101101	10000011.11110111.00011011.11100111
Subnet mask	11111111.11111111.11111000.00000000 (255.255.248.0)	11111111.11111111.11111000.00000000 (255.255.248.0)
Masked IP address = subnet address	10000011.11110111.00001000.00000000	10000011.11110111.00011000.00000000
Matching college	131.247.8.0 = College 1	131.247.24.0 = College 3

Determining subnet ID - example

131.247.00010111.10000111	Packet 5
131.247.00111011.10011000	Packet 4
131.247.00100111.01100110	Packet 3
131.247.00011011.10110100	Packet 2
131.247.00001010.10000101	Packet 1

Main campus router

Main campus router routing table	
Destination	**Address**
College 1	131.247.08.0/21
College 3	131.247.24.0/21
College 4	131.247.32.0/21
College 7	131.247.56.0/21

College 2; To Campus West router	131.247.00010111.10000111 255.255.11111000.00000000 **131.247.00010000.00000000**	Masked packet 5
College 7; To Campus East router	131.247.00111011.10011000 255.255.11111000.00000000 **131.247.00111000.00000000**	Masked packet 4
College 4; To Campus South router	131.247.00100111.01100110 255.255.11111000.00000000 **131.247.00100000.00000000**	Masked packet 3
College 3; To Campus West router	131.247.00011011.10110100 255.255.11111000.00000000 **131.247.00011000.00000000**	Masked packet 2
College 1; To Campus West router	131.247.00001010.10000101 255.255.11111000.00000000 **131.247.00001000.00000000**	Masked packet 1

Tophat question

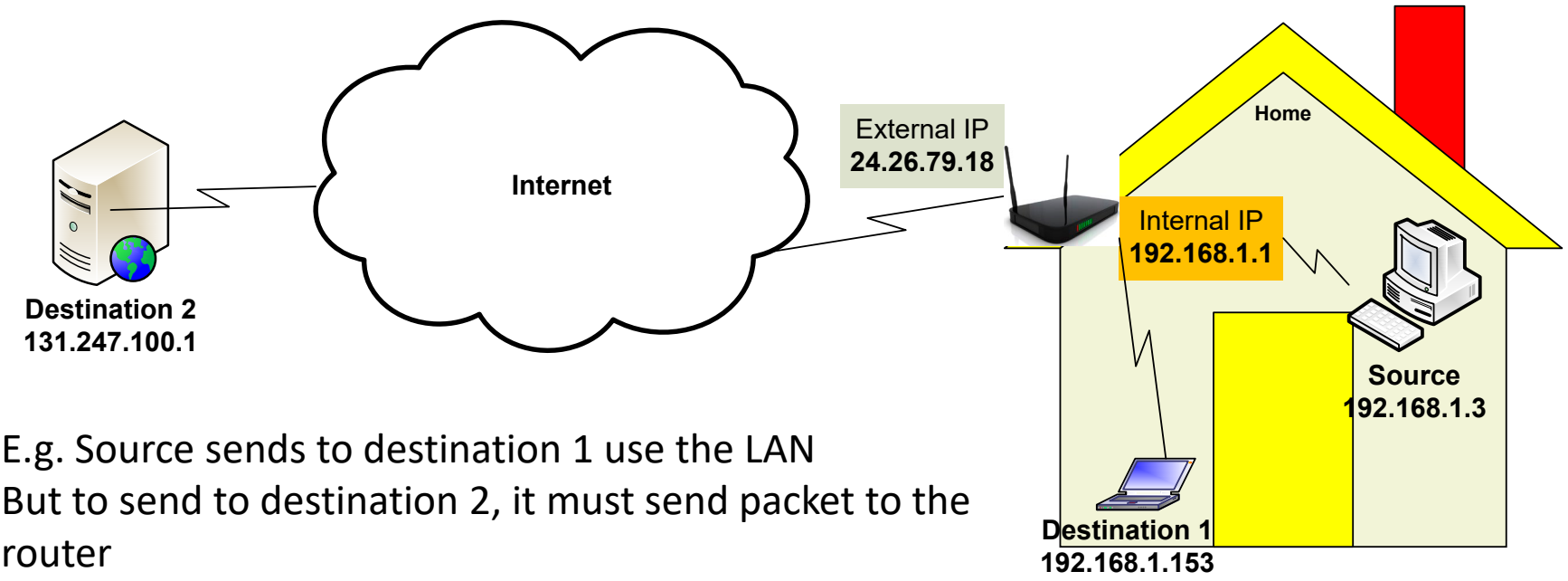
Q2_Subnetting

All subnets within an organization have the same subnet address?

A	True
B	False

Communicating with host inside and outside the subnet

- **If destination is in same subnet/LAN, then you can use LAN to communicate**
  - First need to get MAC address of the destination
- Note: **MAC address** is **portable** (analogy: social security number), **IP address** is **not portable** (analogy: your location)



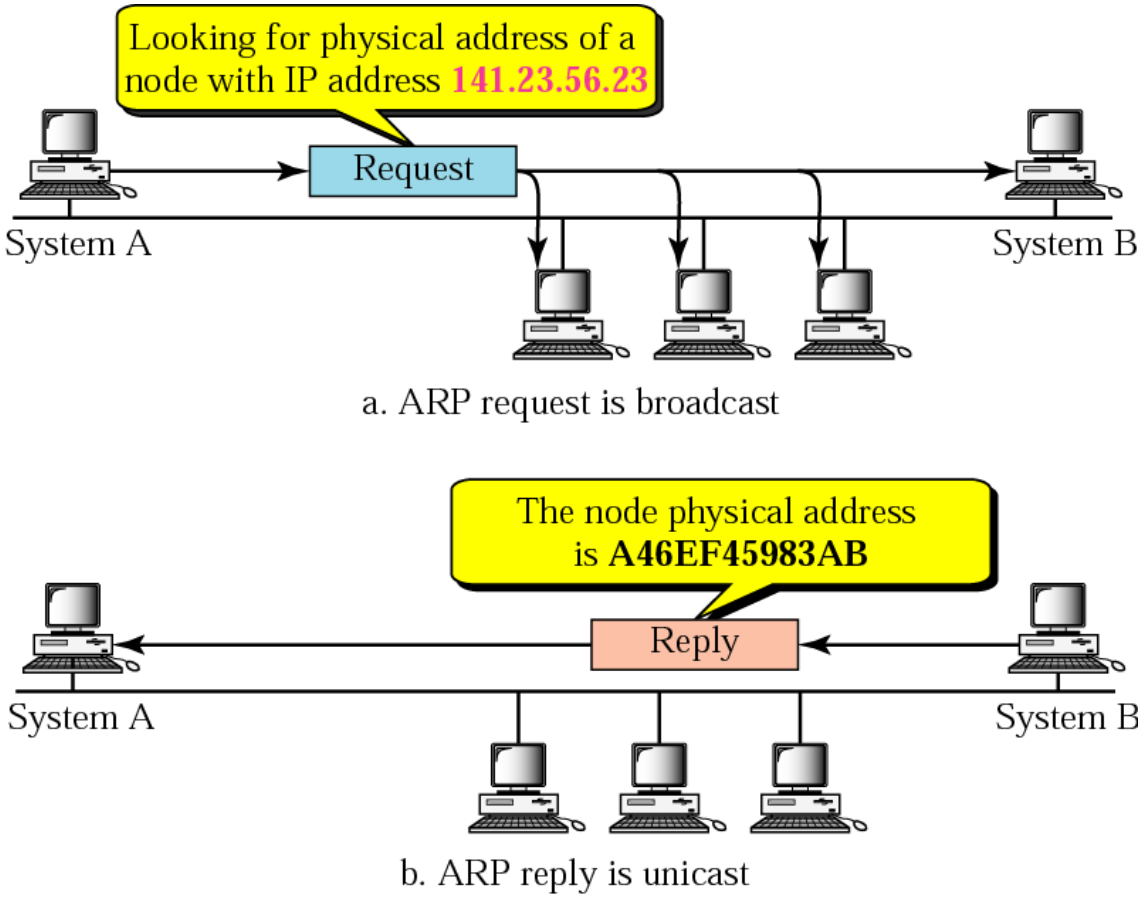
E.g. Source sends to destination 1 use the LAN
But to send to destination 2, it must send packet to the router

Address Resolution Protocol (ARP)

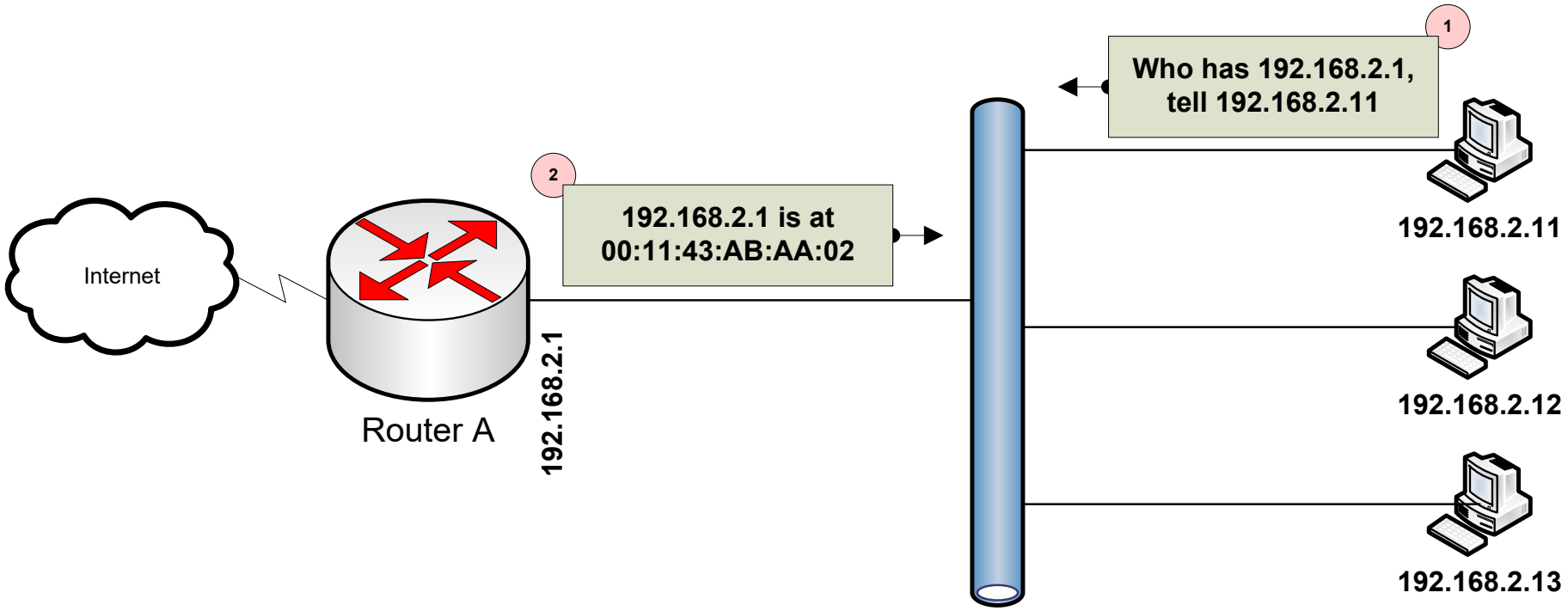
- **How to get MAC address from IP Address?**
  - **Through ARP: Address Resolution Protocol**
    - ARP is used to find MAC address for destination in the same LAN with known IP address
      - MAC address will then be included in the data link layer header
    - Defined in RFC 826 (1982)
    - ARP is implemented in operating system (OS)

ARP Operation

- Before the first packet is transmitted, the sender creates a special packet called an **ARP request** and **broadcasts** it on the LAN
  - Destination MAC address in frame is FF:FF:FF:FF:FF:FF
- The computer/ router with the IP address replies with its MAC address

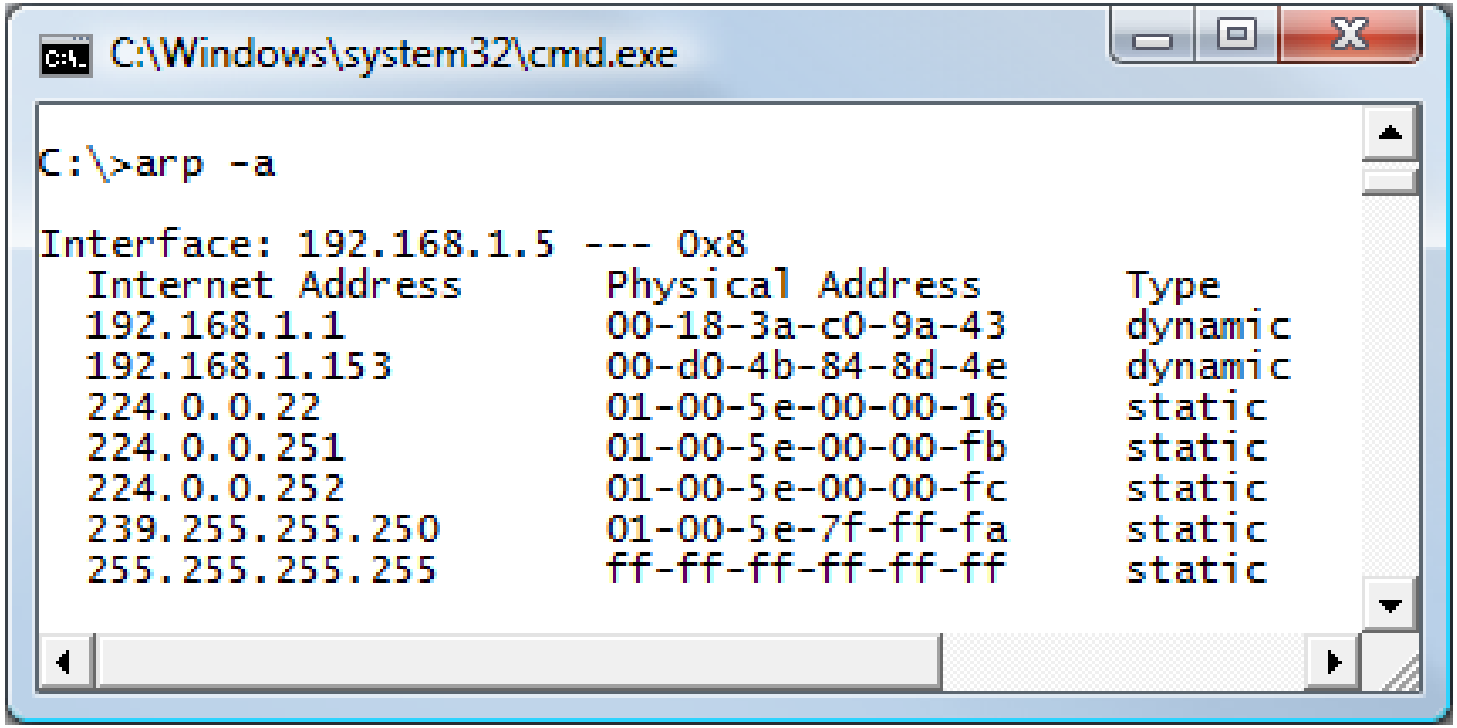


ARP Operation



ARP Cache

- Resolved MAC addresses are saved in cache for some time
  - You can check MAC address and their corresponding IP address using arp -a command



Key takeaways so far

- IP addressing - CIDR
- Subnetting helps delegate IP addresses within large organizations
  - IP address is divided into three parts
    - Network ID -- Subnet ID – Host ID
- Routers use the subnet mask to get the subnet address
  - The 1's in subnet masks indicate network ID and subnet ID
    - 0's indicate the host part
- ARP use to get MAC address of a given IP address

Hands-On

Download Wireshark

A) Open a terminal. Use “arp – a” to view contents of ARP cache. **Describe what is displayed.**

B) Check ARP messages:

Steps:

1. Open Wireshark, and start capturing packets (click on the interface you will capture form)
2. In the terminal, delete ARP cache: use “sudo arp –a –d”.
3. Start browser and go to www.pitt.edu
4. Stop capturing packets
5. From the Wireshark captured packets, find ARP packets (you can arrange packet captured by protocol by clicking on the protocol column)

Note the destination address in the ARP request (destination column). Is it broadcast or unicast?

From the ARP response message: is it broadcast or unicast?

What is the purpose of these ARP messages?