TCP/IP – Part II

- <u>Lecture 4</u>: **TCP/IP – Part II**
  - **On completion, the student will be able to:**
    - **Explain the differences between transparent and non-transparent fragmentation in IP packets.**
    - **Identify the IP header fields used in fragmentation and reassembly.**
    - **Illustrate how a data packet gets fragmented in the IP protocol with an example.**
    - **Interpret the various IP address classes, and their capacities.**

Introduction

- Most of the fields in the header of an IP datagram have been explained.
- We now discuss the fields used for fragmentation and reassembly of packets.
  - If the packet size exceeds a certain maximum value, it is split into two or more fragment packets.
  - The fragments are reassembled at some later stage.

Fragmentation

- **Why needed?**
  - **The IP layer injects a packet into the datalink layer, and hopes for the best.**
    - **Not responsible for the reliable transport of these packets.**
  - **Each layer imposes some maximum size of packets, due to various reasons.**
    - **Called Maximum Transfer Unit (MTU).**
  - **Suppose a large packet travels through a network whose MTU is too small.**
    - **Fragmentation is required.**

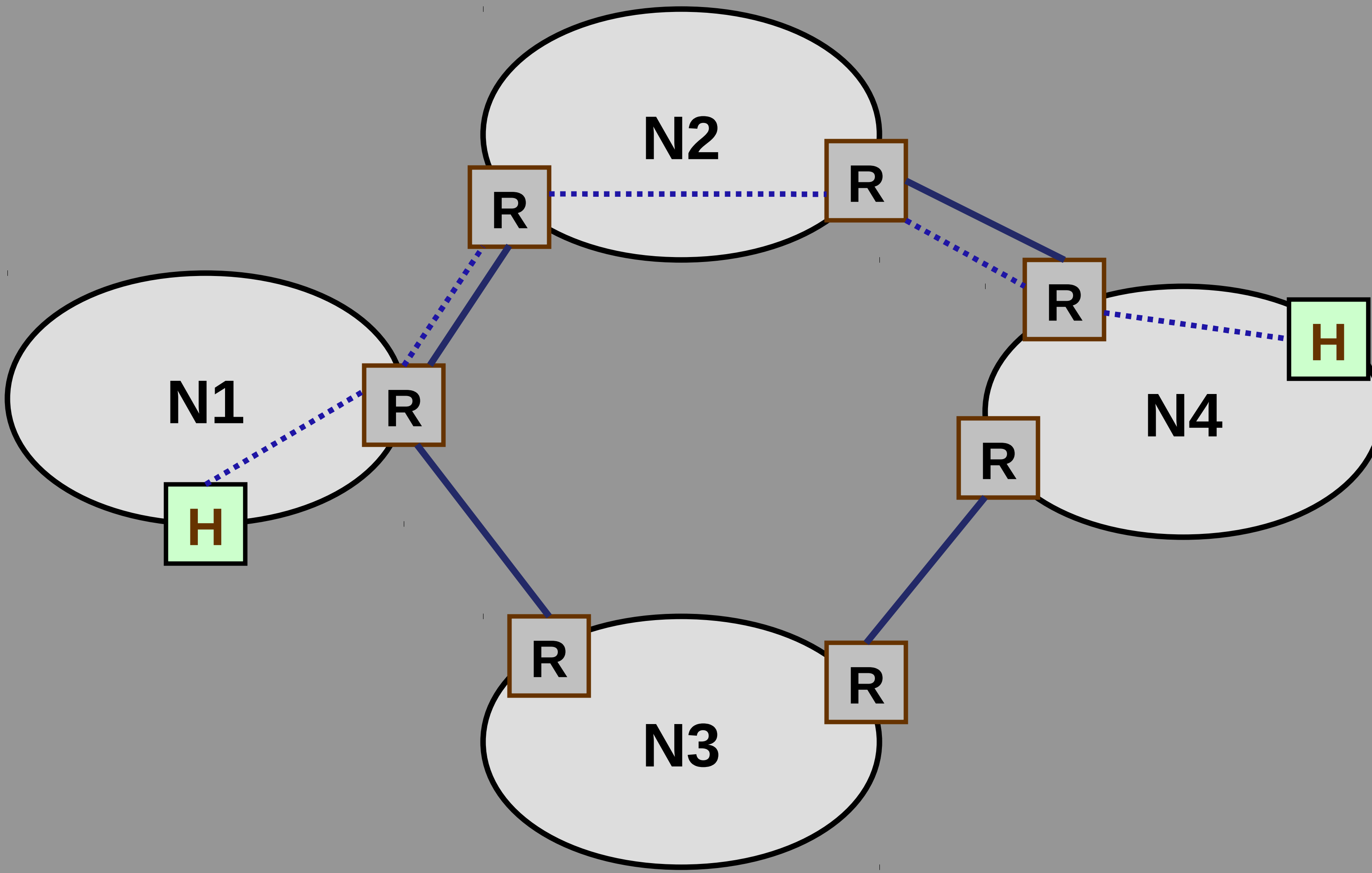
Fragmentation (contd.)

- What to do then?
  - The different networks are connected among themselves through routers.
  - Allow the routers to break the packets into fragments, if necessary.
  - Each fragment is transmitted as a separate IP packet.
  - The fragments need to be reassembled back.

Fragmentation (contd.)

- When is reassembly of fragments carried out?
  - Two alternatives:
    - Transparent fragmentation
    - Non-transparent fragmentation

Interconnection of Networks



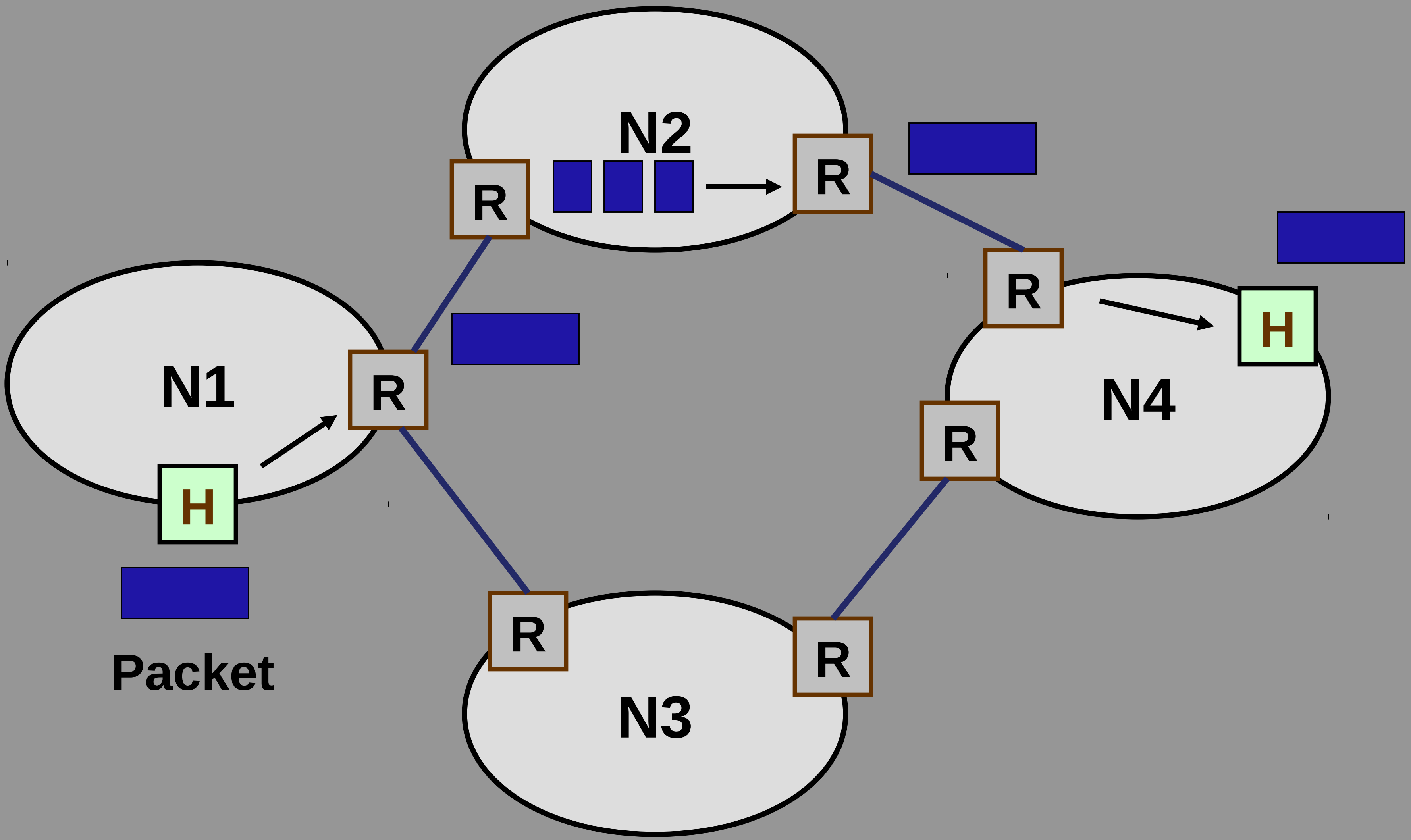
Transparent Fragmentation

- Fragmentation is made transparent to subsequent networks, through which the packet pass.
- Basic concept:
  - An oversized packet reaches a router.
  - Router breaks it up into fragments.
  - All fragments sent to the same exit router (say, R_E).
  - R_E reassembles the fragments before forwarding to the next network.

Transparent Fragmentation (contd.)

- Why called transparent?
  - Subsequent networks are not even aware that fragmentation had occurred.
- A packet may get fragmented several times on its way to the final destination.

Transparent Fragmentation (contd.)



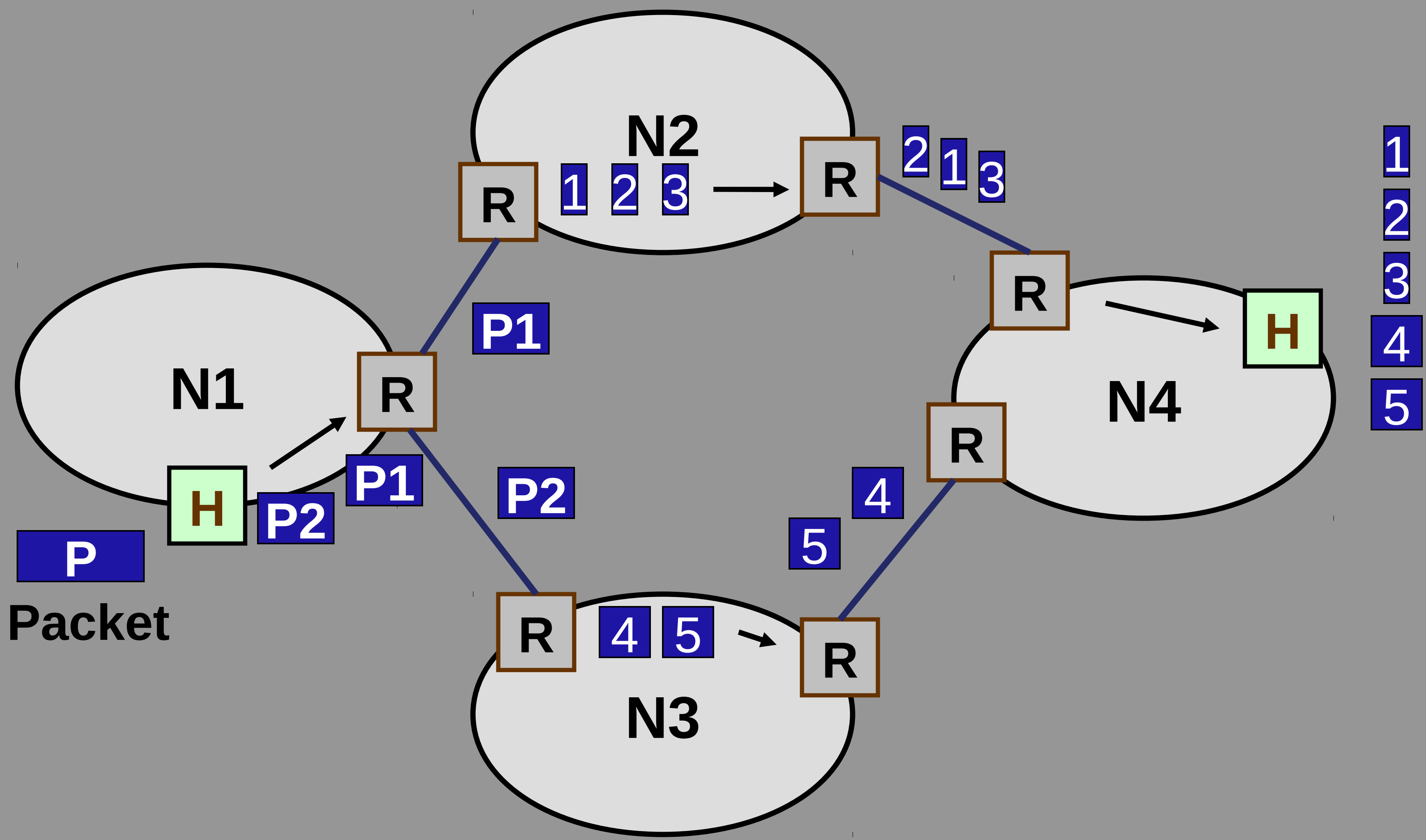
Transparent Fragmentation (contd.)

- Drawbacks:
  - All packets must be routed via the same exit router.
  - Exit router must know when all the pieces have been received.
    - Either a "**count**" field or "**end-of-packet**" field must be stored in each packet.
  - Lot of overhead.
    - A large packet may be fragmented and reassembled repeatedly.

Non-transparent Fragmentation

- Fragmentation is not transparent to subsequent networks.
- Basic concept:
  - ➢ Packet fragments are not reassembled at any intermediate router.
  - ➢ Each fragment is treated as an independent packet by the routers.
  - ➢ The fragments are reassembled at the final destination host.

Non-transparent Frag. (contd.)



Non-transparent Frag. (contd.)

- Advantage:
  - Multiple exit routers may be used.
  - Higher throughput.
- Drawback:
  - When a large packet is fragmented, overhead increases.
  - Each fragment must have a header (minimum 20 bytes).
- IP protocol uses non-transparent fragmentation.

IP Datagram

0 4 8 15 16 31

<table>
<tr><td>VER</td><td>HLEN</td><td>Service type</td><td colspan="2">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source IP Address</td></tr>
<tr><td colspan="5">Destination IP Address</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">DATA</td></tr>
</table>

-------HEADER-------

What does IP do?

- To allow fragment reassembly at the final destination, IP uses the following fields in the header:
  - **Identification (16 bits)**
    - A datagram id set by the source.
  - **Fragment offset (13 bits)**
    - Indicates where in the original datagram this fragment belongs to.
    - Specified in multiple of 8 bytes.

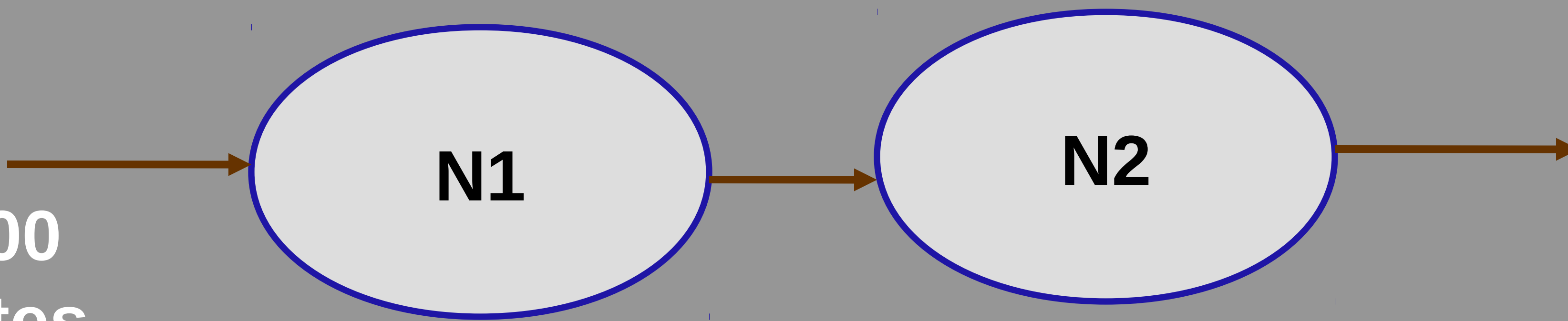
What does IP do? (contd.)

- **Flags (3 bits)**
  - **Two flags are defined:**

    D bit :: don't fragment; prevents fragmentation from taking place.

    M bit :: more fragment; specifies if this fragment is the last one in the original packet or not.

Example :: IP Fragmentation

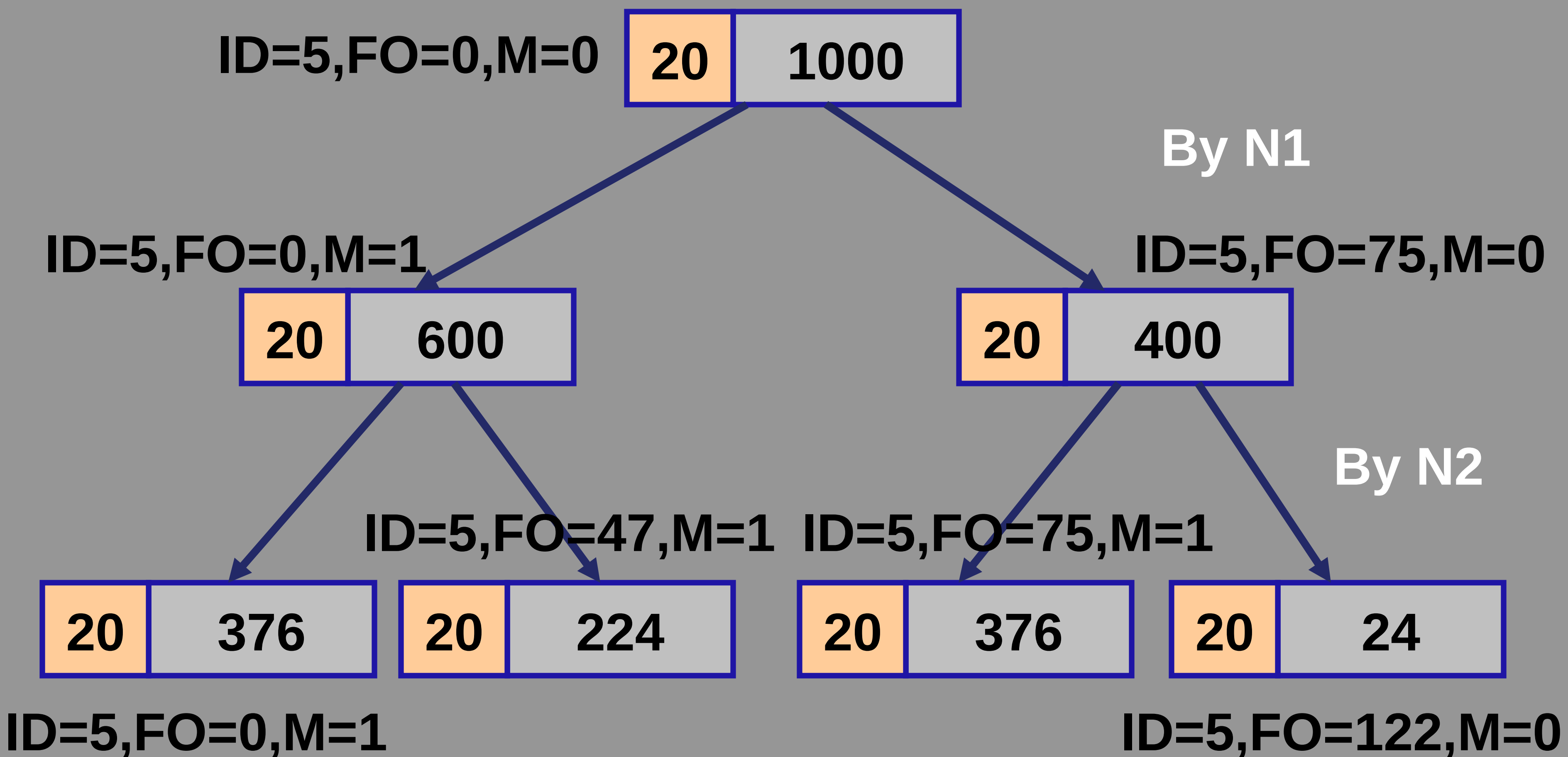


1000 bytes data

MTU = 620 bytes

MTU = 400 bytes

Example (contd.)



1020 bytes sent and 1080 bytes received

Basic IP Addressing

- Each host connected to the Internet is identified by a unique IP address.
- An IP address is a 32-bit quantity.
  - Expressed as a dotted-decimal notation W.X.Y.Z, where dots are used to separate each of the four octets of the address.
  - Consists of two logical parts:
    - A network number
    - A host number
  - This partition defines the *IP address classes*.

Dotted Decimal Notation

IP address: 01000010 10001000 00110000 01111110

01000010	10001000	00110000	01111110
(66)	(134)	(48)	(126)

Dotted Decimal Notation: 66.134.48.126

Hierarchical Addressing

- A computer on the Internet is addressed using a two-tuple:
  - The network number
    - Assigned and managed by central authority.
  - The host number
    - Assigned and managed by local network administrator.
- When routing a packet to the destination network, only the network number is looked at.

IP Address Classes

- There are five defined IP address classes.
  - Class A UNICAST
  - Class B UNICAST
  - Class C UNICAST
  - Class D MULTICAST
  - Class E RESERVED
- Identified by the first few bits in the IP address.
- There also exists some special-purpose IP addresses.

IP Address Classes (contd.)

- The class-based addressing is also known as the **classful model**.
  - Different network classes represent different network-to-hosts ratio.
  - Lend themselves to different network configurations.

Class A Address

0	Network	Host	Host	Host

- Network bits : 7
  - Number of networks = $2^7 – 1 = 127$
- Host bits: 24
  - Number of hosts = $2^{24} – 2 = 16{,}777{,}214$
- Address range:
  - 0.0.0.0 to 127.255.255.255

Class B Address

10	Network	Network	Host	Host

- Network bits : 14
  - Number of networks = $2^{14} - 1 = 16,383$
- Host bits: 16
  - Number of hosts = $2^{16} - 2 = 65,534$
- Address range:
  - 128.0.0.0 to 191.255.255.255

Class C Address

110	Network	Network	Network	Host

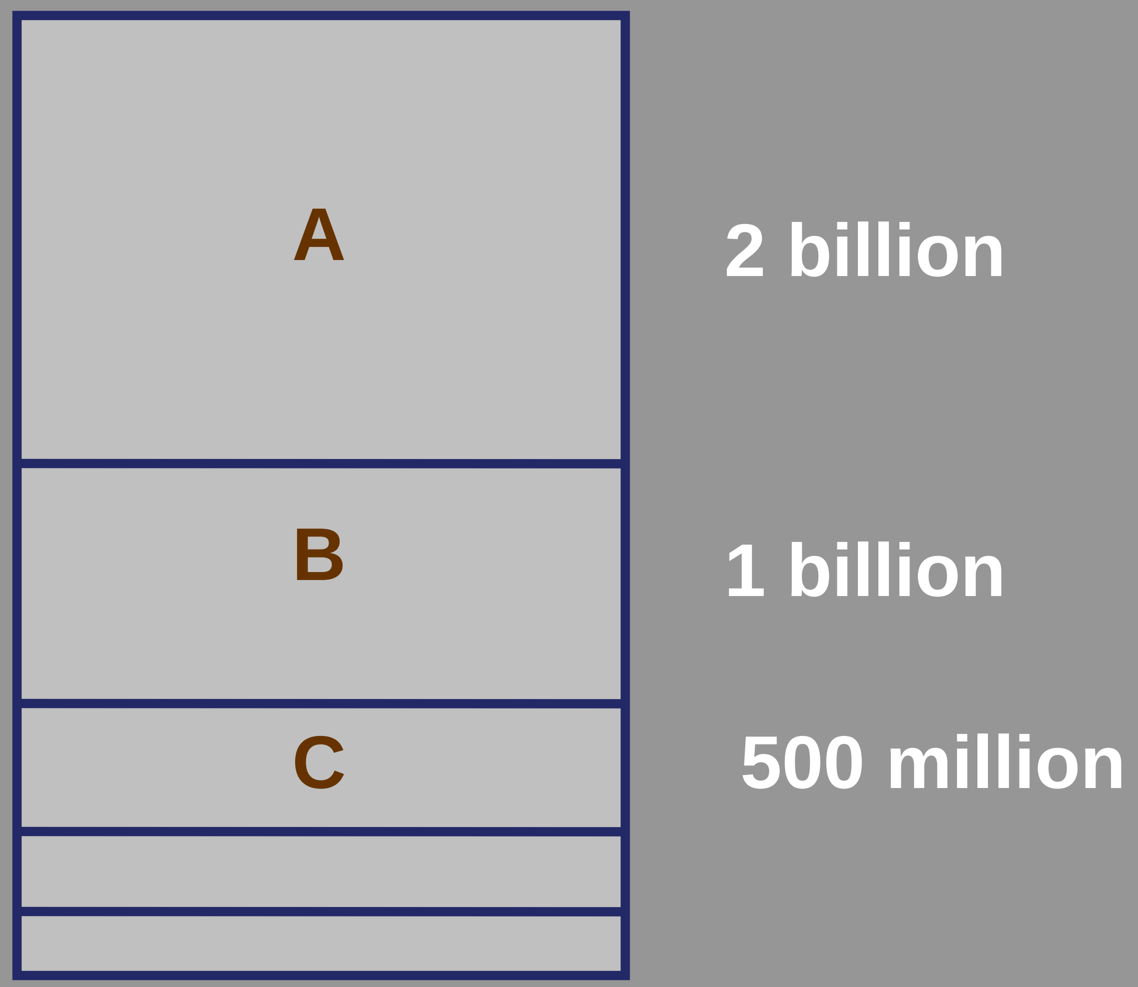
- Network bits : 21
  - Number of networks = $2^{21} - 1$ = 2,097,151
- Host bits: 8
  - Number of hosts = $2^{8} - 2$ = 254
- Address range:
  - 192.0.0.0 to 223.255.255.255

Class D Address

1110	Multicast Address

- Address range:
  - 224.0.0.0 to 239.255.255.255

Address Distribution



Special-purpose IP Addresses

- Reserved for private use
  - 10.x.x.x (Class A)
  - 172.16.x.x – 172.31.x.x (Class B)
  - 192.168.x.x (Class C)
- Loopback/local address
  - 127.0.0.0 – 127.255.255.255
- Default network
  - 0.0.0.0
- Limited broadcast
  - 255.255.255.255

Some Conventions

- Within a particular network (Class A, B or C), the first and last addresses serve special functions.
  - The first address represents the network number.
    - For example, 118.0.0.0
  - The last address represents the directed broadcast address of the network.
    - For example, 118.255.255.255

End of Lecture 4

Thank You