IPv4
Lecture 17

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

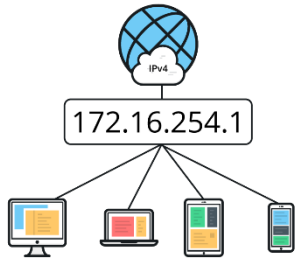
Slides from Muhammad **Rizwan** Asghar

August 25, 2021

Source of some slides: **Princeton University**
Also thanks to **J.F Kurose and K.W. Ross**

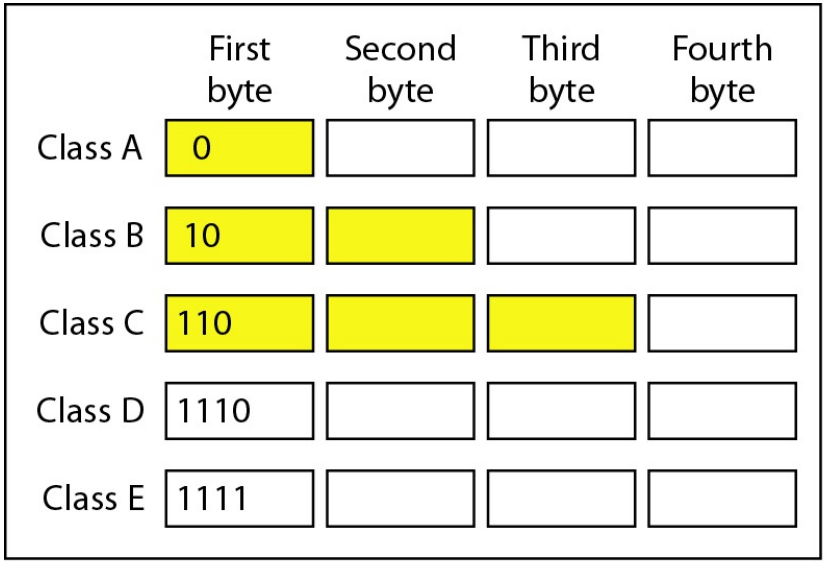
THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

IPv4

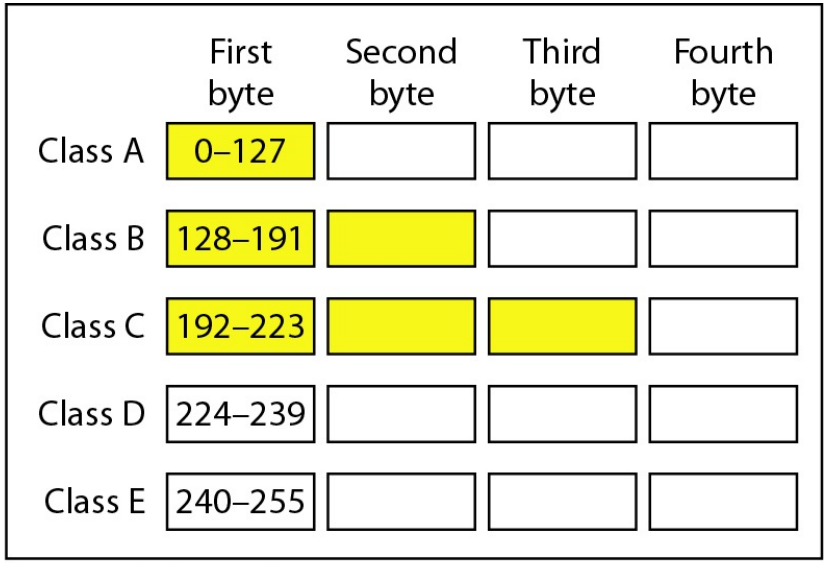


- Internet Protocol (IP) is the principal communication protocol in TCP/IP
- IP was proposed in the early 1970s
- IPv4 is IP version 4
- A 32-bit address that uniquely and universally identifies a host on the Internet
  - E.g., 203.118.141.95 (ping www.google.com)

IPV4 ADDRESSING: 5 CLASSES



a. Binary notation



b. Dotted-decimal notation

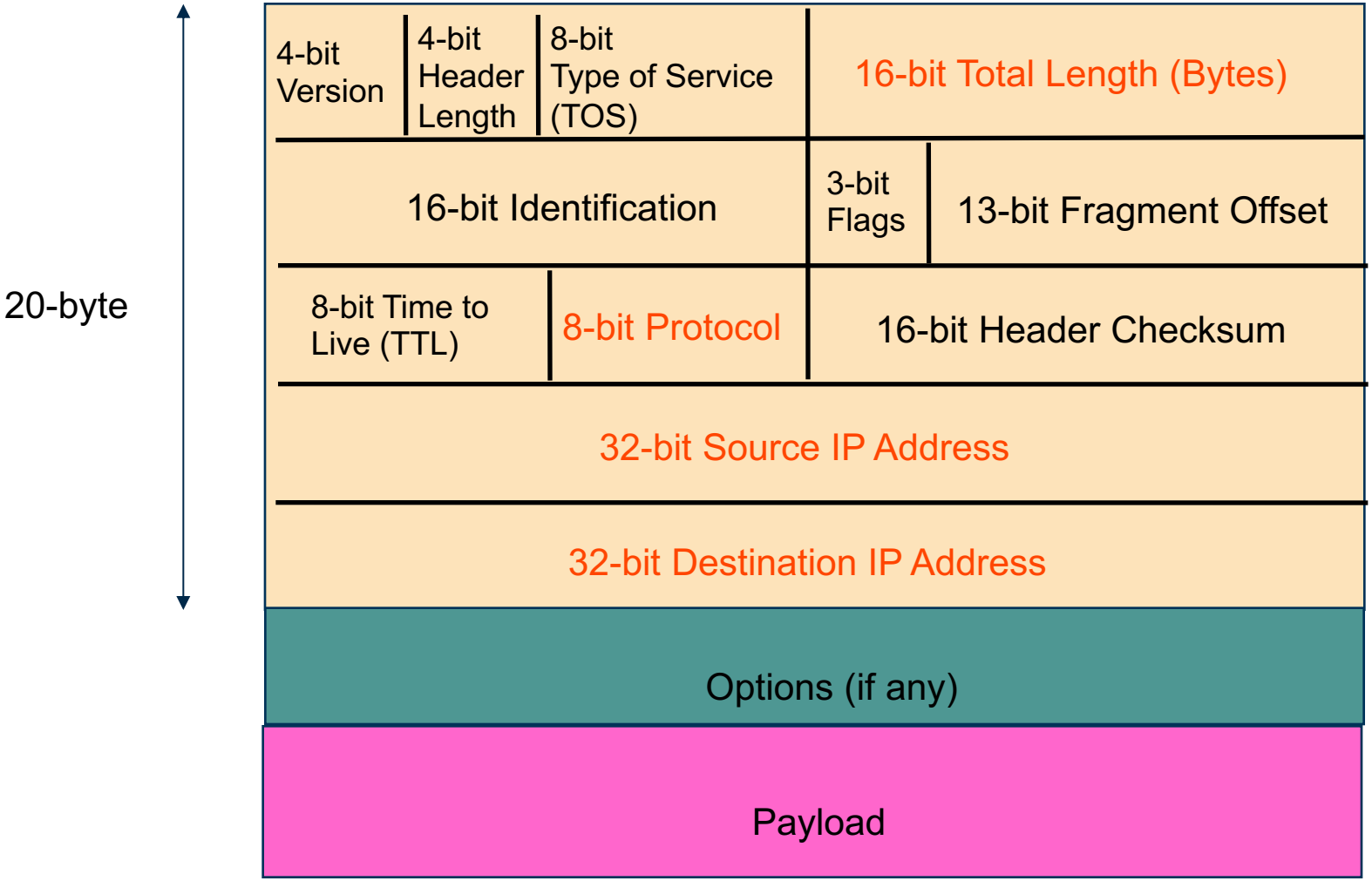
Source: **Data Communications and Networking by Behrouz A. Forouzan**

IPV4 ADDRESSING: BLOCKS AND BLOCK SIZE

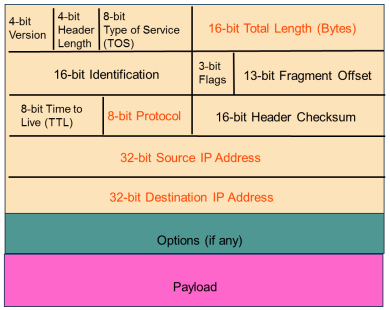
Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Source: **Data Communications and Networking by Behrouz A. Forouzan**

IPV4 PACKET FORMAT

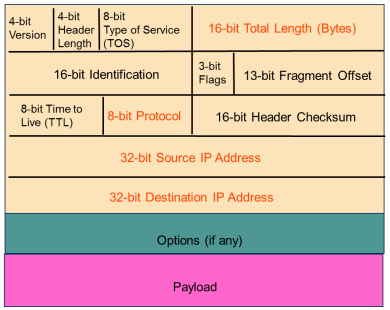


IP HEADER FIELDS



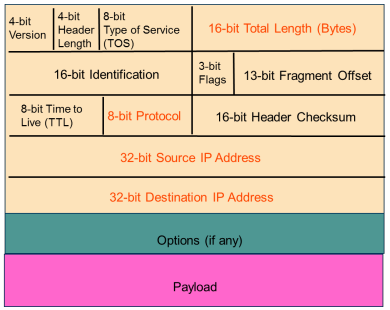
- Version number (4-bit)
  - Indicates the version of the IP protocol
  - Typically 4 (for IPv4) and sometimes 6 (for IPv6)
- Header length (4-bit)
  - Number of 32-bit words in the header
  - Typically 5 (for a 20-byte IPv4 header)
- Type of service (8-bit)
  - Used to manage quality of service
  - E.g., low delay for audio and high bandwidth for bulk transfer

IP HEADER FIELDS CONT



- Total length (16-bit)
  - Number of bytes in the packet (header+payload)
  - Maximum size can be 64KB
    - Underlying links may impose harder limits
- Fragmentation information (32-bit)
  - Packet identification, flags and fragmentation offset (see later)
  - Supports dividing a large IP packet into fragments when a link cannot handle that packet
- Time-to-live (8-bit)
  - Lifetime of a packet
  - Used to prevent loops – reduces as the packet traverses

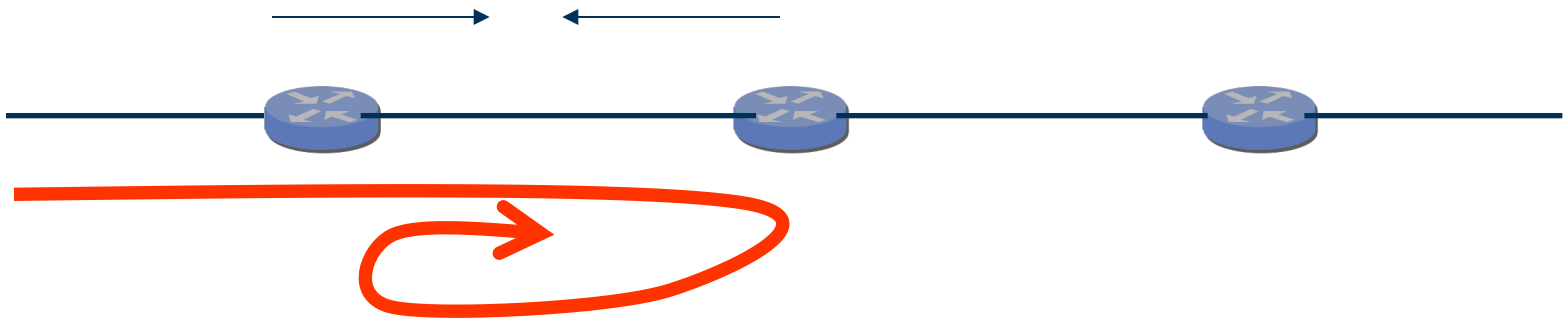
IP HEADER FIELDS CONT



- Protocol (8-bit)
  - A value that specifies the type of payload
  - E.g., TCP or UDP
- Header checksum (32-bit)
  - It includes all other fields in an IP header
  - Recalculated by each router since TTL changes
- Source or destination address (32-bit)
  - IP address

TTL

- Potential robustness problem
  - Forwarding loops can cause packets to cycle forever
  - Confusing if the packet arrives later



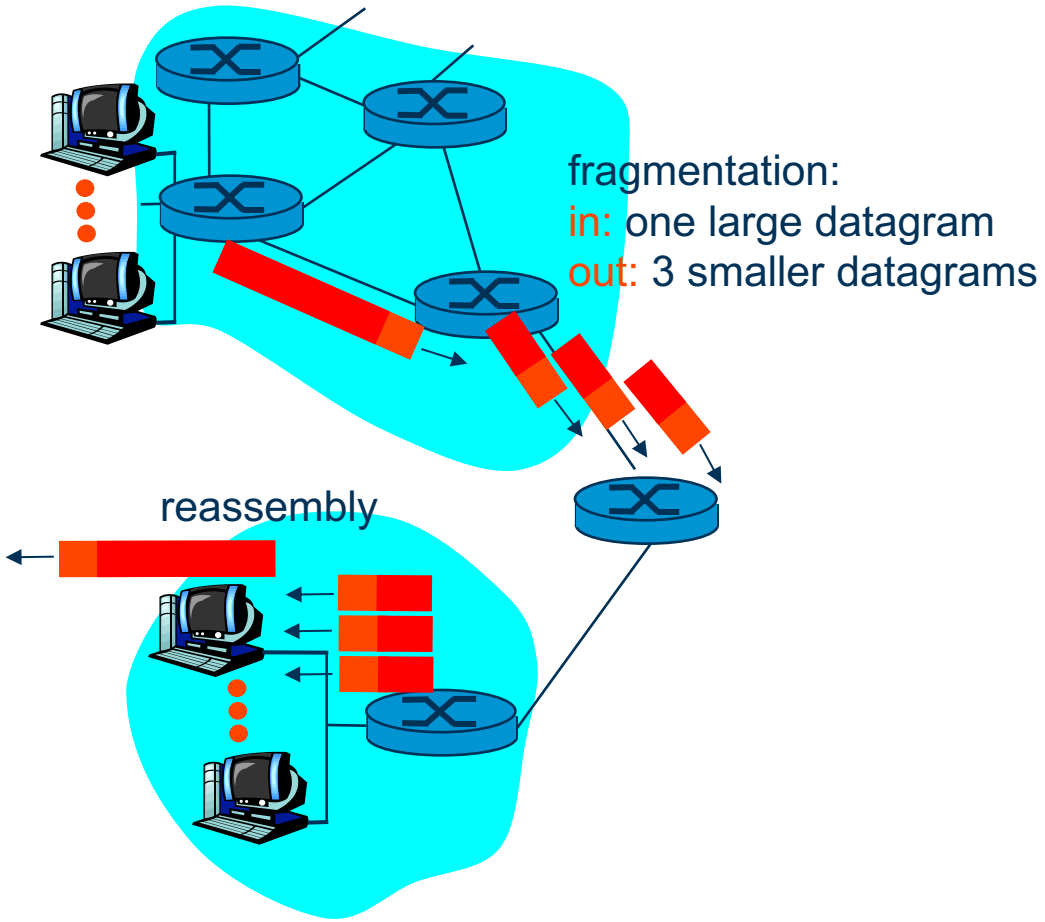
- TTL in packet header (8-bit)
  - TTL decremented by each router on the path
  - A packet is discarded when TTL reaches 0
  - A ‘time exceeded’ message is sent to the source

IP SPOOFING

- Source IP address should be the sending host
  - But, who is checking that?
  - You could send packets with any source you want
- Why would someone want to do this?
  - Launch a DoS attack
  - Evade detection
  - An attack against the spoofed host
    - Spoofed host is wrongly blamed
    - Spoofed host may receive return traffic from the receiver

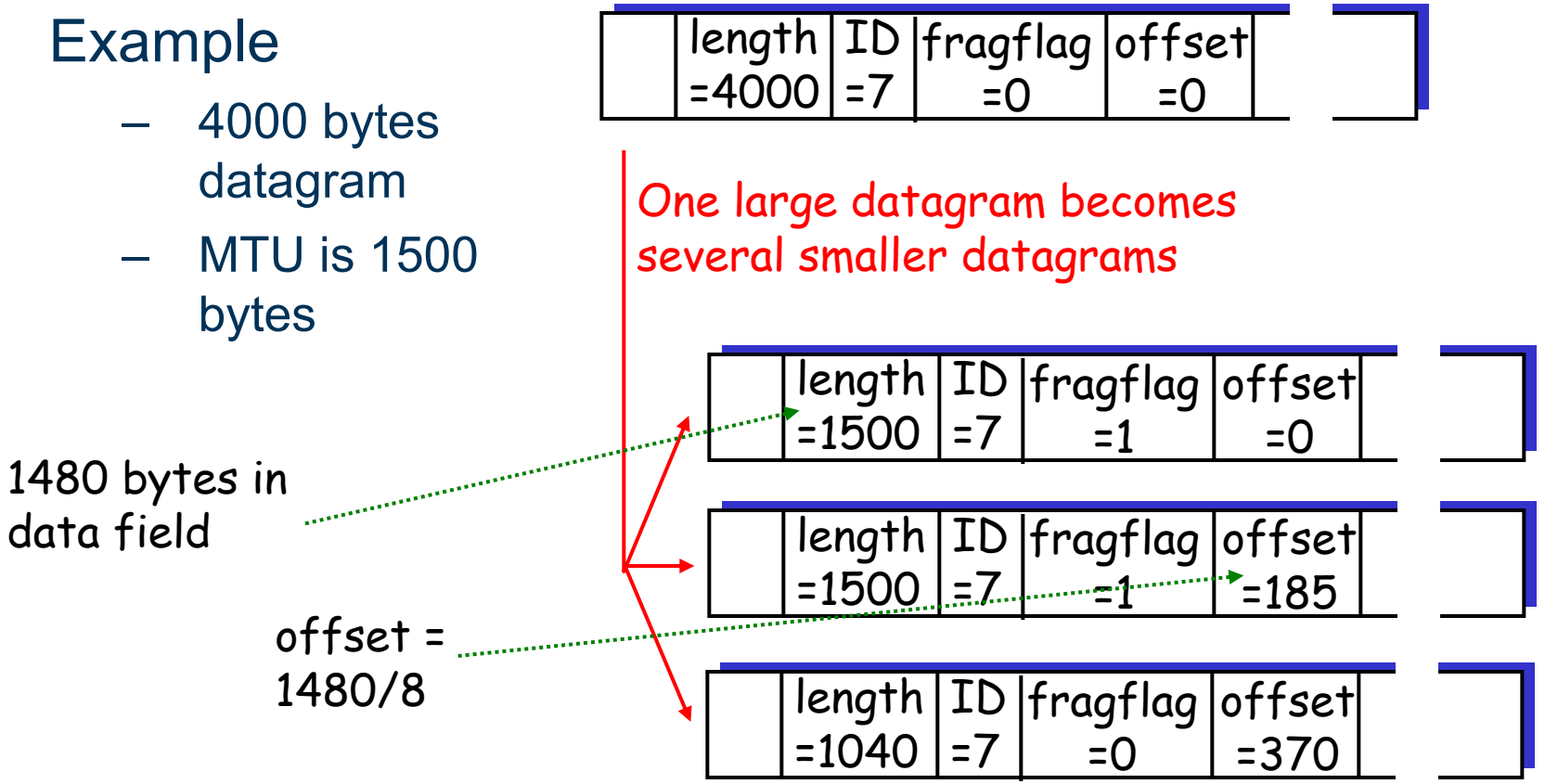
IP FRAGMENTATION AND REASSEMBLY

- Max IP datagram: 64KB
- Network links have Maximum Transfer Unit (MTU)
- Large IP datagrams can be fragmented
- Reassembled at destination



IP FRAGMENTATION AND REASSEMBLY CONT

- Example
  - 4000 bytes datagram
  - MTU is 1500 bytes



length=header+payload

ID identifies IP datagram

fragflag=1 means more fragments available

offset points fragment offset (in octet)

ISSUES WITH FRAGMENTATION

- Uses resources poorly
  - A bit shorter MTU will require a full fragment and a smaller fragment
- Poor end-to-end performance
- Reassembly is hard
  - Buffering constraints
- Reassembly is slow
- Interferes with TCP control flow

Questions?

Thanks for your attention!