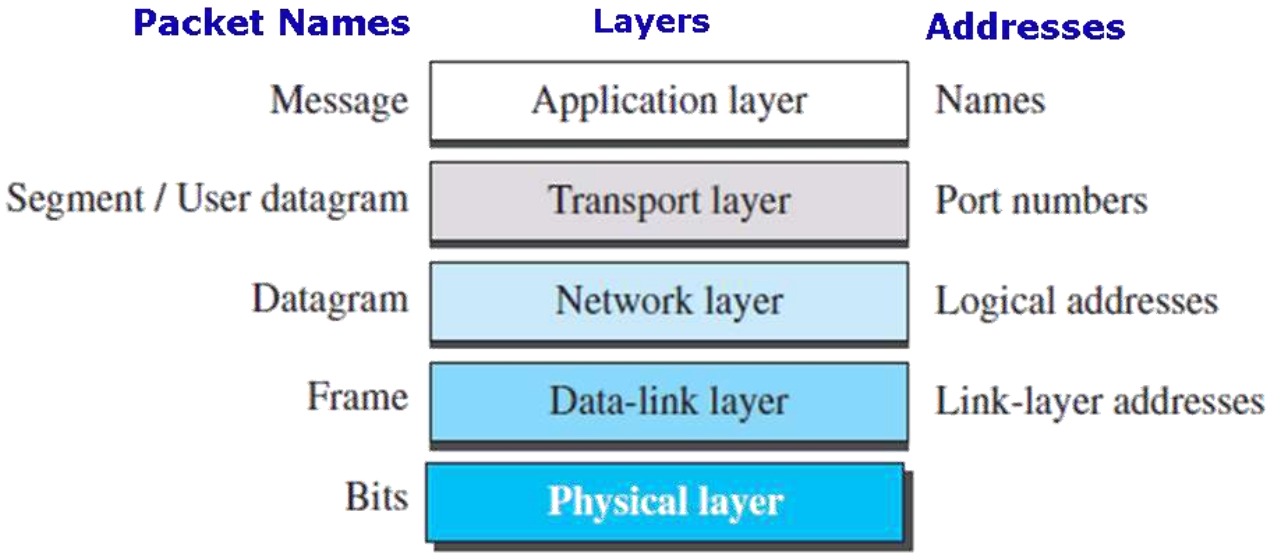
CENG210
Chapter 06
Network Layer

Objectives

- Understand the network layer responsibilities and explain:
  - Packetization
  - Routing and Forwarding
  - Packet Switching and IP4 Addressing
  - IPv4 Datagram Format, Fragmentation & Processing and ICMPv4
- Material feeds into CLO-3
  - “Explain the main functions of the network layer such as packet switching, IP addressing and fragmentation”

Introduction

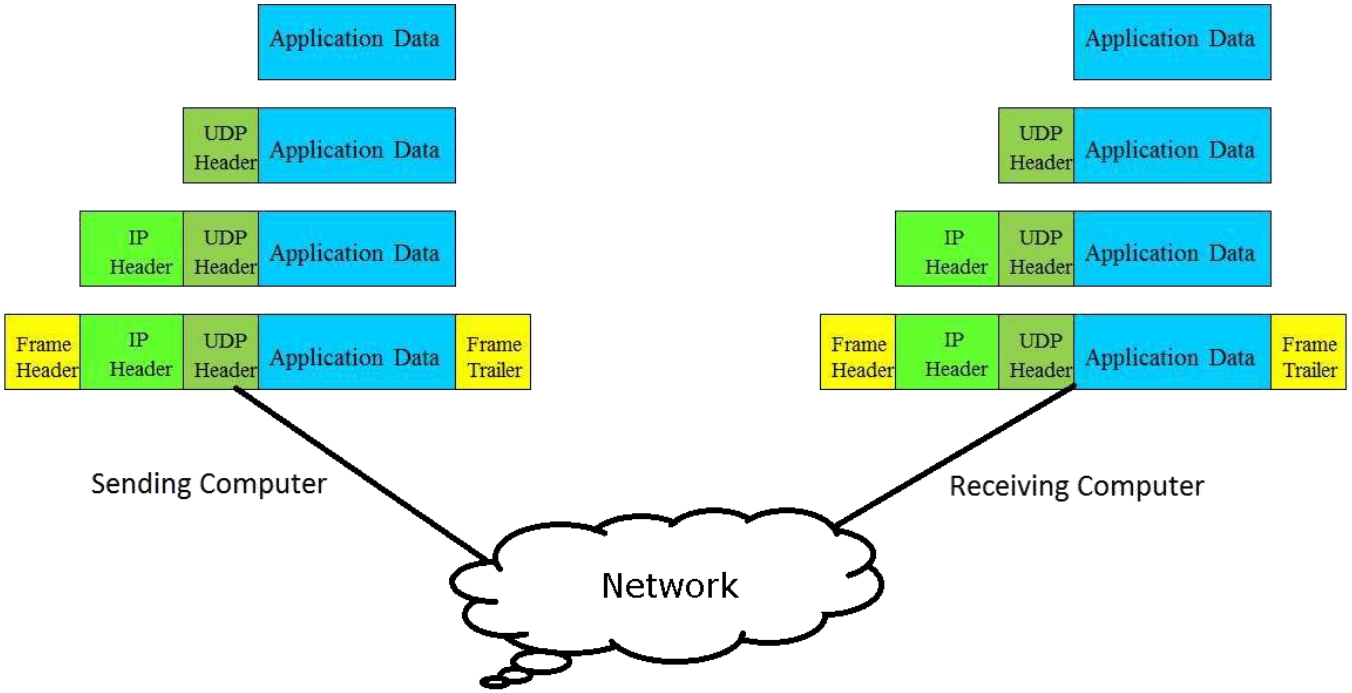
- The network layer in the TCP/IP protocol suite is responsible for the host-to-host delivery of datagrams.
- It provides services to the transport layer and receives services from the data-link layer.



Network Layer Duties

- **Packetizing**
  - encapsulating the payload (data received from upper layer) in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.
- **Fragmenting**:
  - datagram fragmentation is breaking it into smaller pieces, so that packets may be formed that can pass through a link with a smaller maximum transmission unit (MTU) than the original datagram size.
- **Routing**
  - determining optimal route for sending a packet from one host to another
- **Addressing**
  - identifying each device uniquely to allow global communication

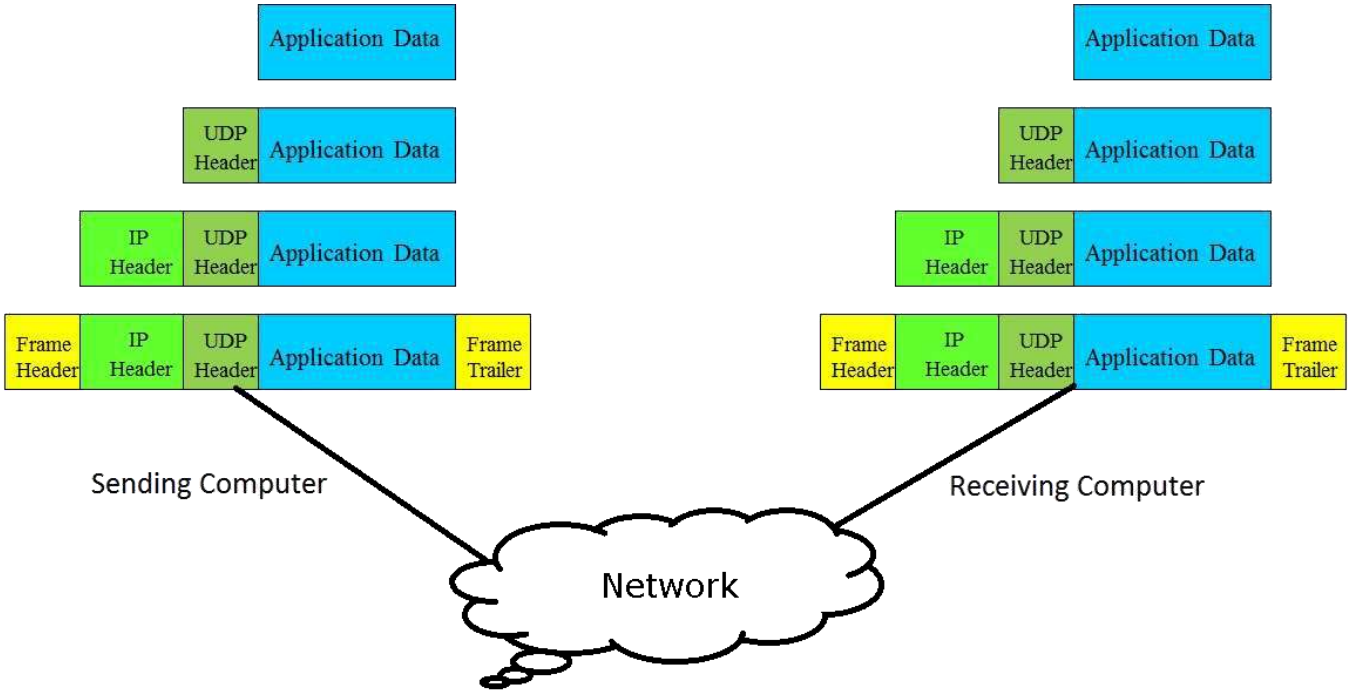
Packetizing



- Source receives payload from the upper layer
  - Network layer adds IP header, Src & Dest. Addresses
  - Other information as required & hands packet to data link layer

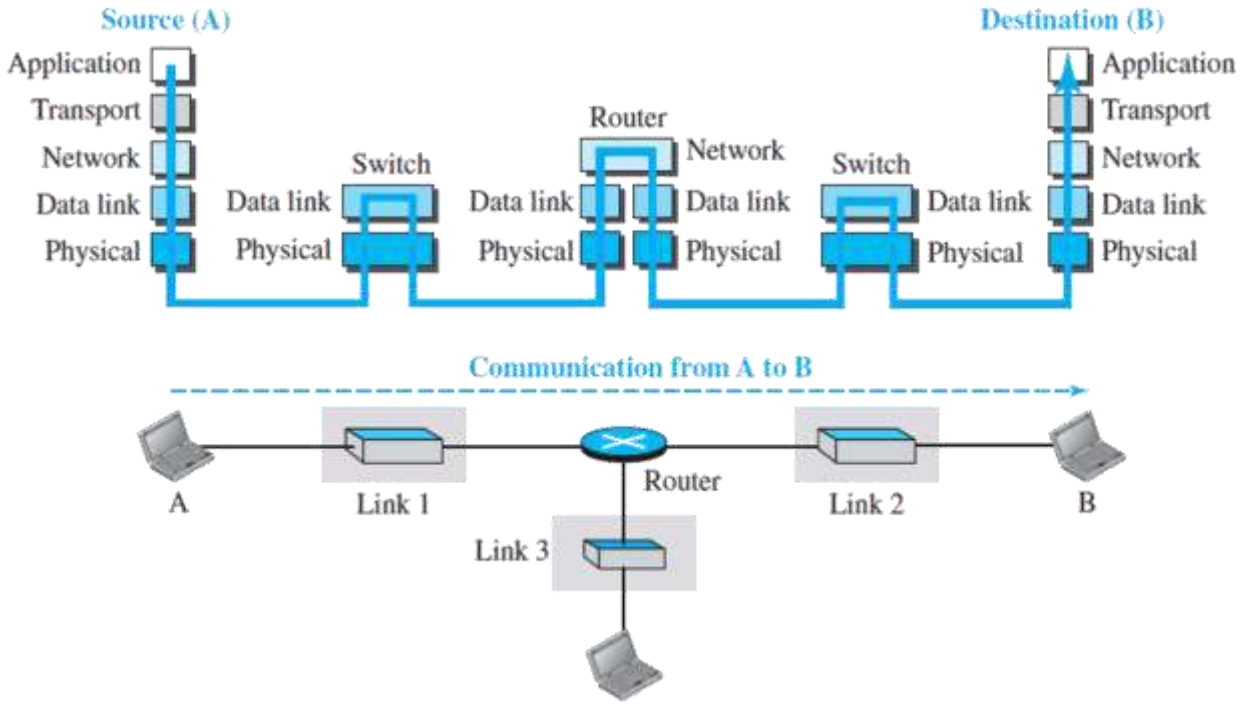
- The source is not allowed to change the content of the payload unless it is too large for delivery and needs to be fragmented

Packetizing



- The destination host receives the network-layer packet from its data-link layer, decapsulates the packet, and delivers the payload to the corresponding upper-layer protocol.

Packetizing

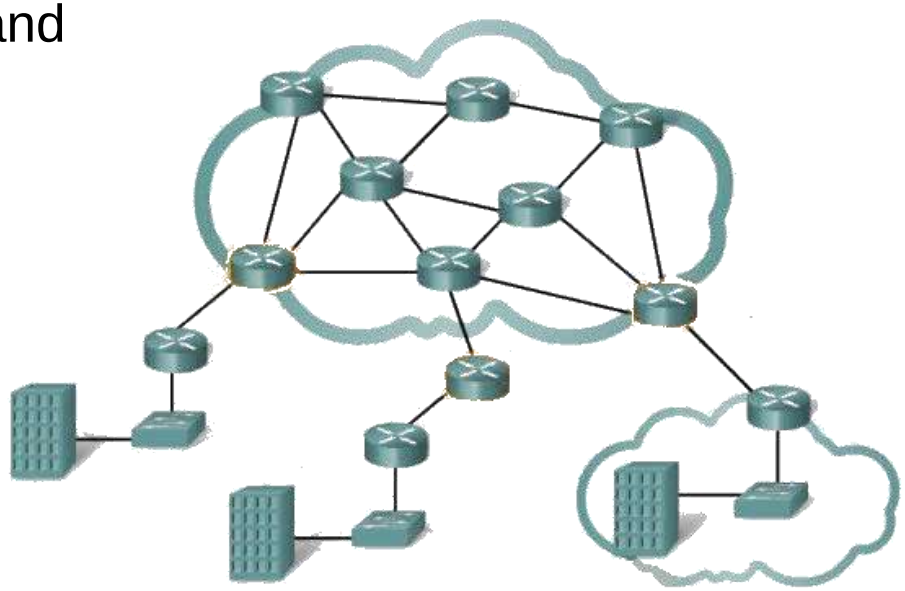


- If the packet is fragmented at the source or at routers along the path, the network layer is responsible for waiting until all fragments arrive, reassembling them, and delivering them to the upper-layer protocol

- The routers in the path are not allowed to decapsulate the packets they received unless the packets need to be fragmented. The routers are not allowed to change source and destination addresses either

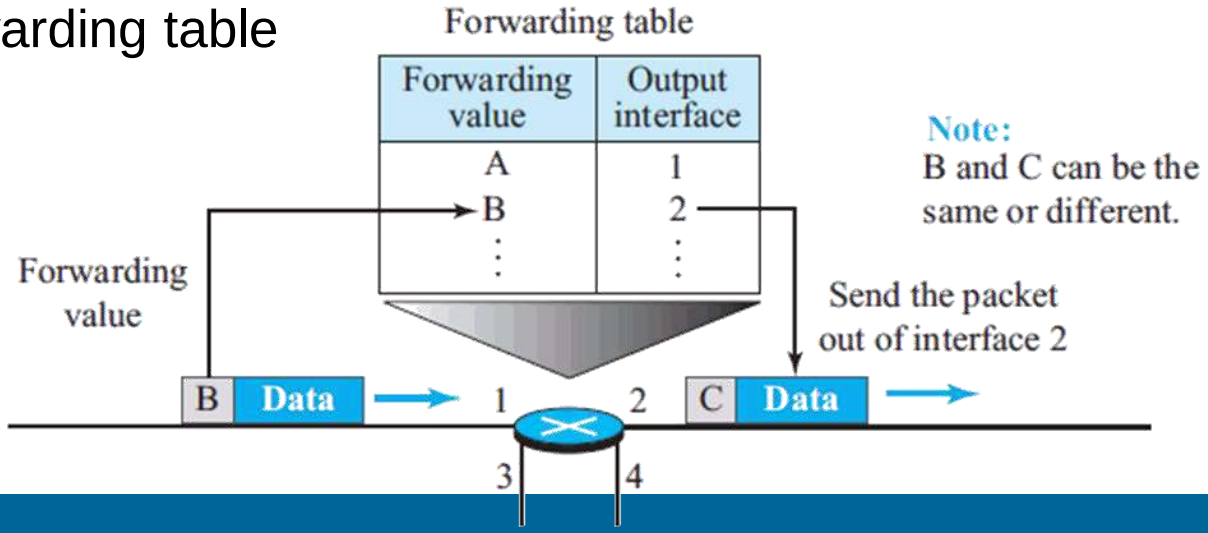
Routing and Forwarding

- **Routing**
  - Network layer responsible for routing packets from Src to Dest
  - A physical network is a combination of networks (LANs and WANs) and routers that connect them
  - Maybe more than one route from the source to the destination
    - Network layer responsible for finding the best route
    - Network layer uses routing protocols for defining the best route
  - Routing is applying strategies and running some routing protocols to create the decision-making tables for each router



Routing and Forwarding

- **Forwarding**
  - Action applied by each router when a packet arrives at one of its interfaces
  - The decision-making table a router normally uses for applying this action is sometimes called the forwarding table and sometimes the routing table
  - To make a decision, the router uses a piece of information in the packet header, which can be the destination address or a label, to find the corresponding output interface number in the forwarding table

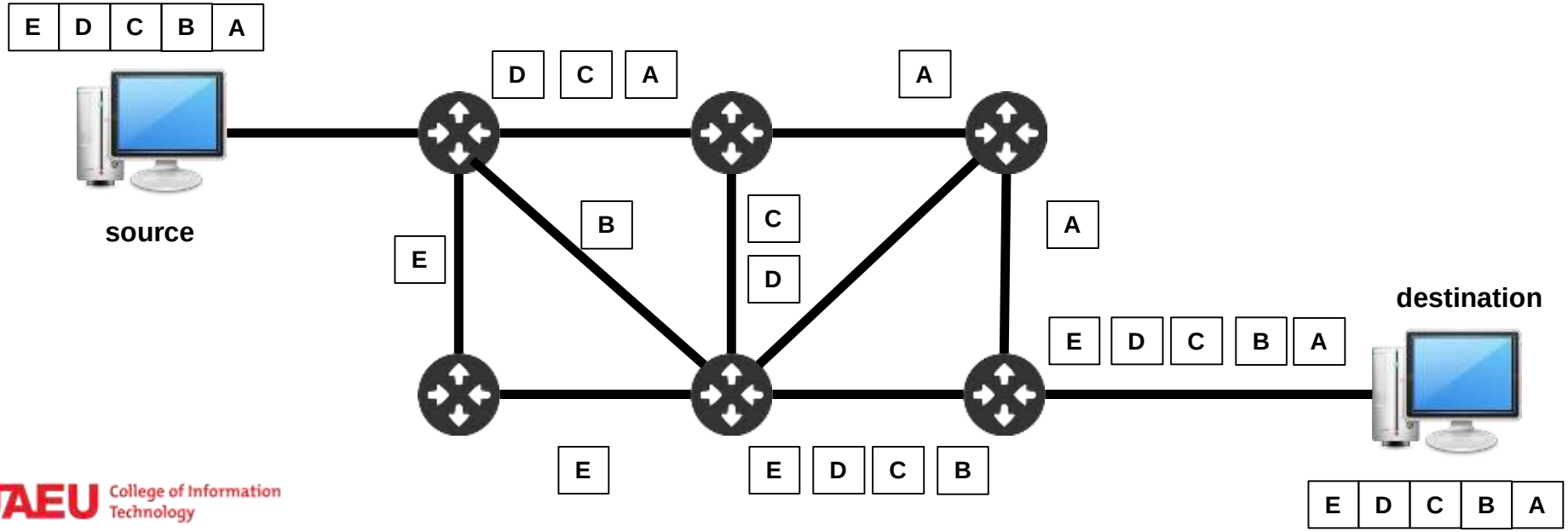


Packet Switching

- Data communication switching techniques are divided into two broad categories, **circuit switching** and **packet switching**, only packet switching is used at the network layer because the unit of data at this layer is a packet
- At the network layer, a message from the upper layer is divided into manageable packets and each packet is sent through the network
- The source of the message sends the packets one by one; the destination of the message receives the packets one by one.
- The destination waits for all packets belonging to the same message to arrive before delivering the message to the upper layer.

Packet Switching

- The connecting devices in a packet-switched network still need to decide how to route the packets to the final destination
- Packet-switched network can use two different approaches to route the packets: the datagram approach and the virtual circuit approach.



Datagram Approach: Connectionless Service

- Each packet traveling in the Internet is an independent entity; there is no relationship between packets belonging to the same message
  - The switches in this type of network are called routers.
  - A packet belonging to a message may be followed by a packet belonging to the same message or to a different message.
  - A packet may be followed by a packet coming from the same or from a different source.
  - Each packet is routed based on the information contained in its header: source and destination addresses.
  - The destination address defines where it should go; the source address defines where it comes from. The router in this case routes the packet based only on the destination address. The source address may be used to send an error message to the source if the packet is discarded.

IPV4 Addresses

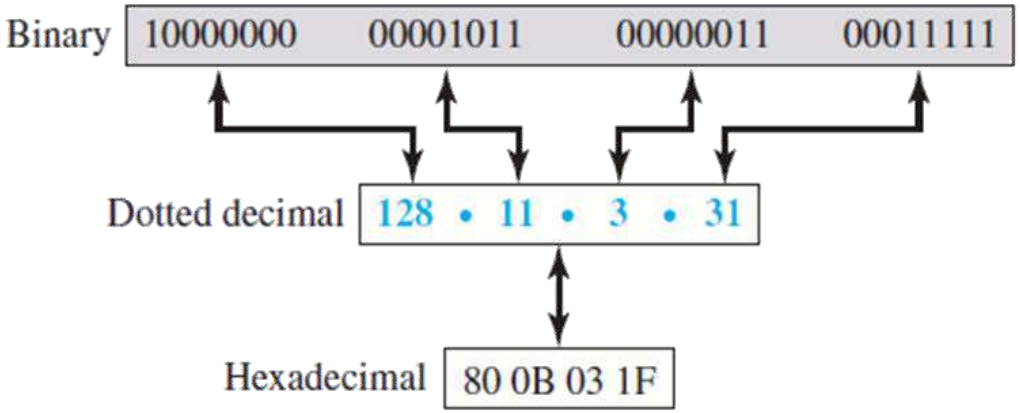
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device of (a host or a router) to the Internet.

- The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed.

- If a device has two connections to the Internet, via two networks, it has two IPv4 addresses and so on.

Address Space & Notations

- An **address space** is the total number of addresses used by the protocol. If a protocol uses b bits to define an address, the address space is 2^b because each bit can have two different values (0 or 1).
- IPv4 uses 32-bit addresses, which means that the address space is 2^32 or 4,294,967,296
- There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).



Address Notation Conversion

Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number and add dots for separation.

a) 129.11.11.239
b) 193.131.27.255

Address Notation Conversion

Change the following IPv4 addresses from dotted-decimal notation to binary notation.

a) 111.56.45.78
b) 221.34.7.82

Solution

We replace each decimal number with its binary equivalent.

a. 01101111 00111000 00101101 01001110
b. 11011101 00100010 00000111 01010010

Address Notation

Find the error, if any, in the following IPv4 addresses.

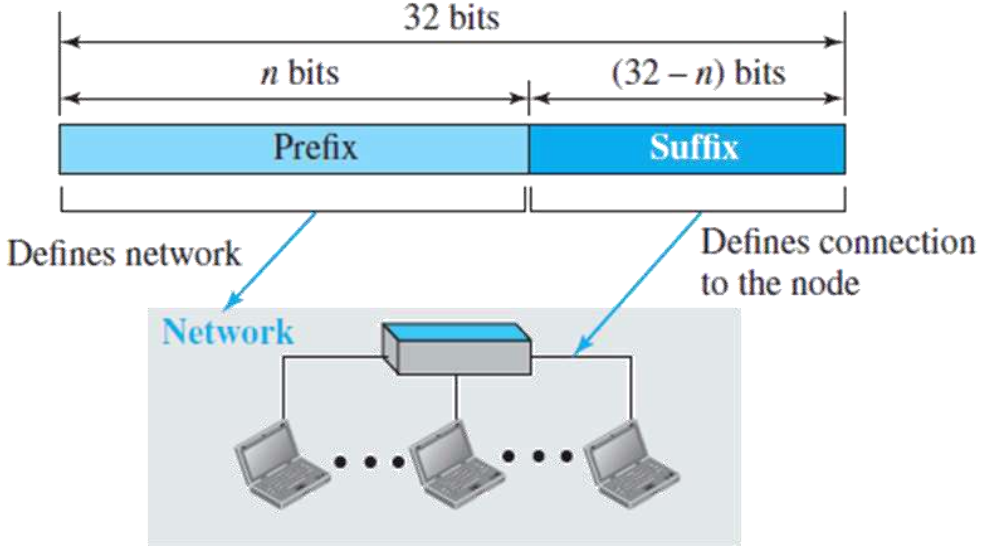
a. 111.56.045.78
b. 221.34.7.8.20
c. 75.45.301.14
d. 11100010.23.14.67

Solution

a. There must be no leading zero (045).
b. There can be no more than four numbers.
c. Each number needs to be less than or equal to 255.
d. A mixture of binary notation and dotted-decimal notation is not allowed.

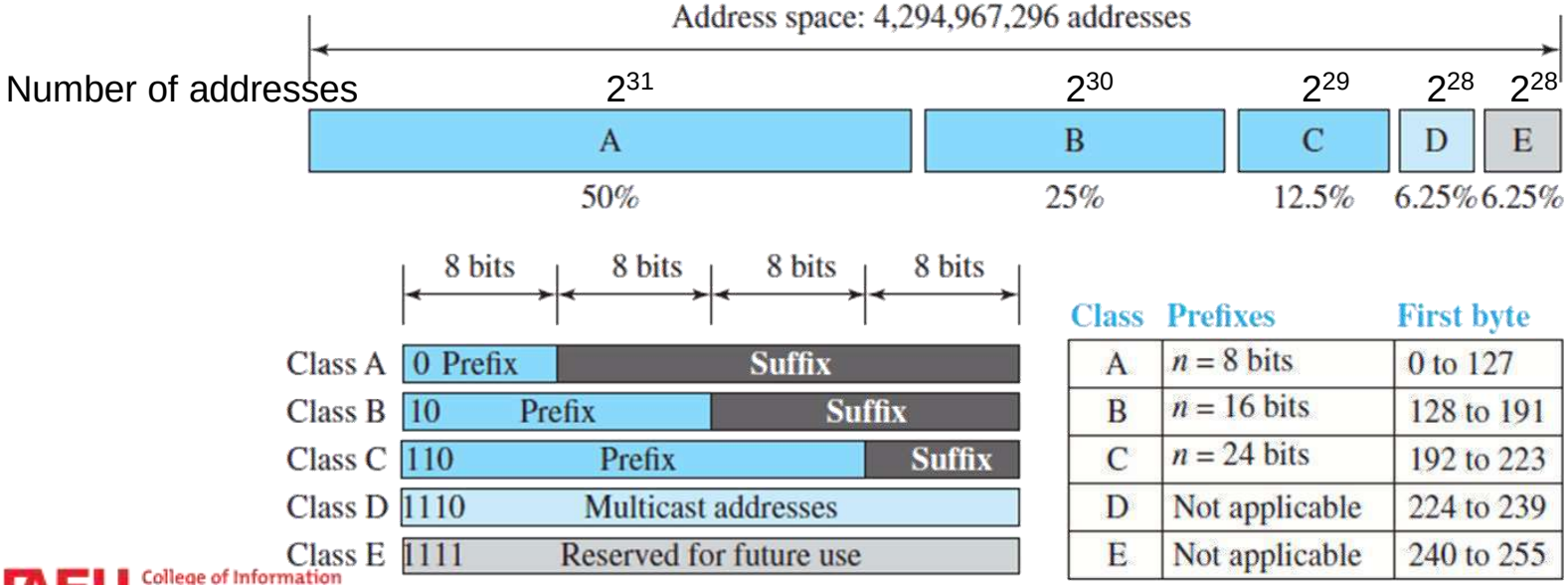
Hierarchy in Addressing

- A 32-bit IPv4 address is also hierarchical, but divided only into two parts. The first part of the address, called the prefix, defines the network; the second part of the address, called the suffix, defines the node (connection of a device to the Internet).
- A prefix can be fixed length or variable length (Classful Addressing vs Classless Addressing)



Classful Addressing

- IPv4 address was designed with a fixed-length prefix
- To accommodate both small and large networks, three fixed-length prefixes were designed instead of one
  - n = 8, n = 16, and n = 24
- The whole address space was divided into five classes (class A, B, C, D, and E).



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Classful Addressing

- Address Depletion:
  - The Internet was faced with the problem of the addresses being rapidly used up, resulting in no more addresses available for organizations and individuals that needed to be connected to the Internet.

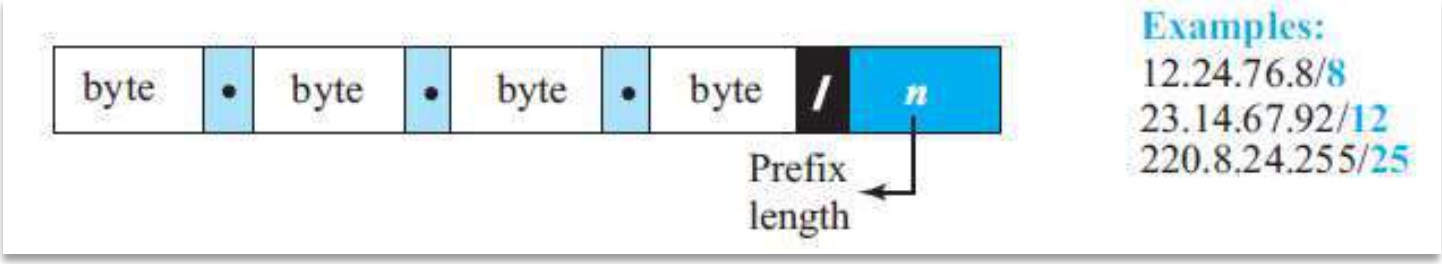
Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Classless Addressing

- In classless addressing, the whole address space is divided into variable length blocks.
- The prefix in an address defines the block (network); the suffix defines the node (device).
- Theoretically, we can have a block of 2^0, 2^1, 2^2, . . . , 2^{32} addresses.
- One of the restrictions is that the number of addresses in a block needs to be a power of 2.

Prefix Length: Slash Notation

- The prefix length, n, is added to the address, separated by a slash.
- The notation is informally referred to as slash notation
- Also, formally known as classless interdomain routing or CIDR (pronounced cider).



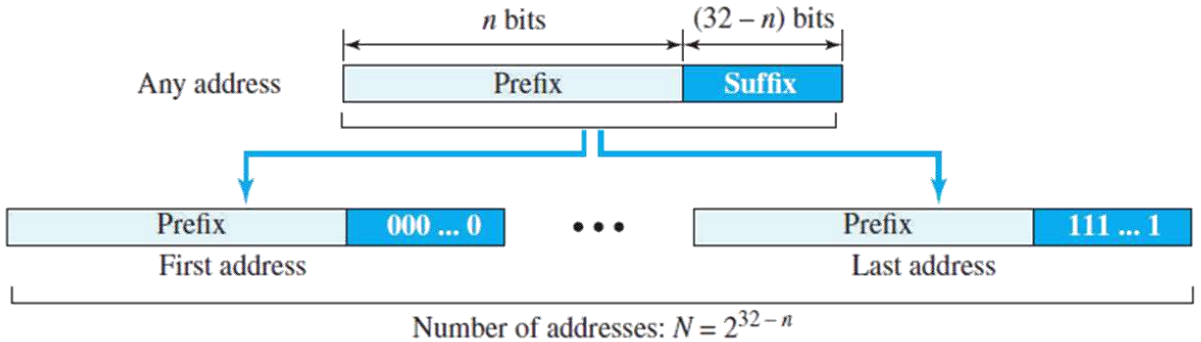
Extracting Information from a Classless Address

- Given any address in the block, we normally like to know three pieces of information about the block to which the address belongs:
  - the number of addresses,
  - the first address in the block, and
  - the last address in the block
- Given the prefix length n, we can easily find these three pieces of information:
  1. The number of addresses in the block is found as $N = 2^{32-n}$.
  2. To find the first address, we keep the n leftmost bits and set the (32 − n) rightmost bits all to 0s.
  3. To find the last address, we keep the n leftmost bits and set the (32 − n) rightmost bits all to 1s.

Example

A classless address is given as 167.199.170.82/27. We can find the number of addresses, first and last addresses as follows.

n=27 then the number of addresses in the network is $2^{32-n} = 2^5 = 32$ addresses.



Address: 167.199.170.82/**27**	**10100111 11000111 10101010 01010010**
Network Address: 167.199.170.64/**27**	**10100111 11000111 10101010 01000000**
First address:	**10100111 11000111 10101010 01000001**
Broadcast address: 167.199.170.95/**27**	**10100111 11000111 10101010 01011111**
Last address	**10100111 11000111 10101010 01011110**

Address Mask

- Another way to find the first and last addresses in the block is to use address mask

- The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits (32 − n) are set to 0s.
  - The first address can be found by ANDing the given addresses with the mask
  - The last address can be found by ORing the given addresses with the complement of the mask. The complement of a number is found by changing each 1 to 0 and each 0 to 1
  - The number of addresses can be found by complementing the mask, interpreting it as a decimal number, and adding 1 to it.

Example

A classless address is given as 167.199.170.82/27. We can find the number of addresses, first and last addresses as follows.

Mask of : 167.199.170.82/**27** ⟶ **11111111 11111111 11111111 11100000**

167.199.170.82/**27** ⟶ **10100111 11000111 10101010 01010010**

AND **11111111 11111111 11111111 11100000**

First Address **10100111 11000111 10101010 01000000**

167.199.170.82/**27** ⟶ **10100111 11000111 10101010 01010010**

OR **00000000 00000000 00000000 00011111**

Last Address **10100111 11000111 10101010 01011111**

Complement of the mask 00000000 00000000 00000000 00011111 = 31 in decimal

number of addresses = 31 +1 = 32 addresses

Exercise

- IP address 190.36.80.55/26
  - What's the binary representation?
  - What's the network address?
  - What's the broadcast address?
  - How many host addresses in the block?
  - First and the last node address in the block?

Overview of IP

- **Internet Protocol (IP)** – host-to-host network-layer delivery protocol for the Internet with following properties
  - connectionless service – each packet is handled independently (possibly along different path)
  - best-effort delivery service
    1) does its best to deliver packet to its destination, but with no guarantees
    2) limited error control – only error detection, corrupted packets are discarded
    3) no flow control
  - must be paired with a reliable transport- (TCP) and/or application- layer protocol to ensure reliability

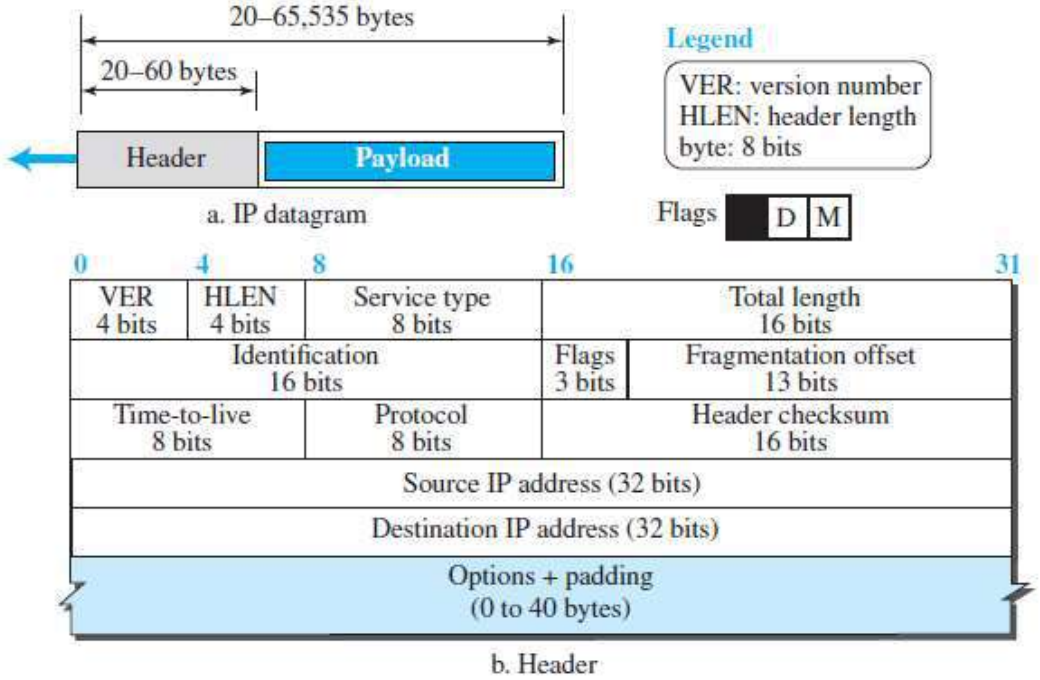
IP Versions

- IPv4 – version currently in wide use (1981)
- IPv6 – new version of IP created to correct some of significant problems of IPv4 such as exhaustion of address space (1996), continues to gain significant traction due to Internet of Things (IoT)
- Mobile IP – enhanced version of IPv4 – supports IP in mobile environments (1996)

IPv4 Datagram Format

Datagram-IP packet: variable length packet consisting of header & data

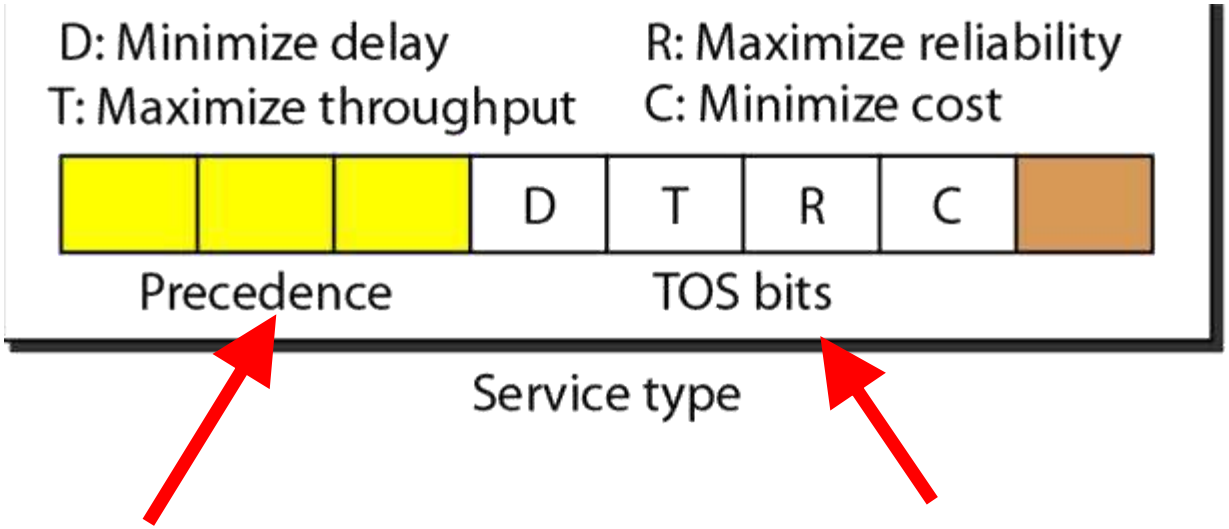
- **Header** – 20 to 60 bytes in length, contains information essential to routing and delivery
- **Data** – length determined by Maximum Transmission Unit (MTU) of link layer protocol (theoretically between 20 to 65536 bytes)



IPv4 Datagram Format

- **Version Number** (4-bit field) specifies IP protocol version of the datagram (IPv4 or IPv6)
  - different version of IP use different datagram formats
  - by looking at version number router can determine how to interpret remainder of datagram
- **Header Length** (4-bit field) defines total length of datagram header in 4-byte words
  - when there are no options header length is 20 bytes (HLEN=5)
- **Differentiated Service** (8-bit field) allows different types of datagrams to be distinguished from each other based on their associated / requested QoS
  - • e.g. datagrams particularly requiring low delay, high throughput, or reliability

IPv4 Datagram Format

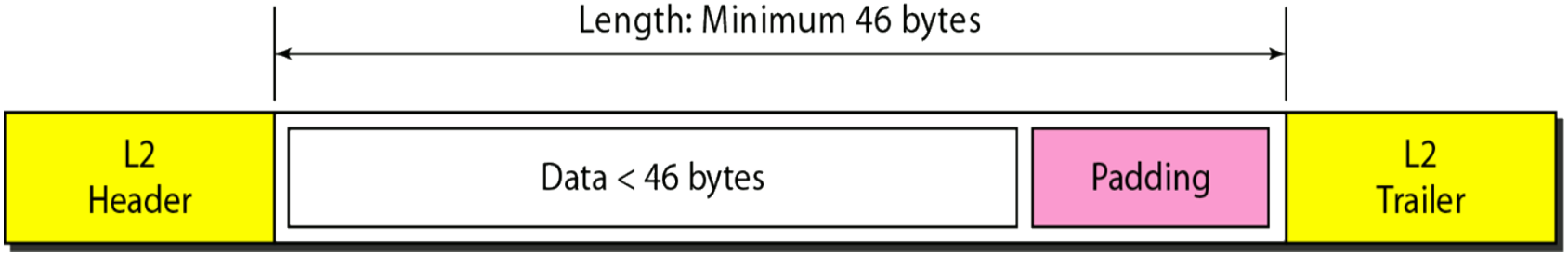


Precedence defines the priority of datagram in case of congestion. If a router is congested and needs to discard some datagrams, those datagrams with lowest precedence are discarded first.
Network management datagrams have the highest precedence

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

IPv4 Datagram Format

- **Total Length** (16-bit field) – defines total datagram length in bytes, including header
  - 16 bits ⇒ maximum size = 65,535 bytes
  - some physical networks are not able to encapsulate a datagram of 65,535 bytes, so datagram must be fragmented to be able to pass through those networks
  - some physical networks have restriction on minimum size of data that can be encapsulated in a frame, so datagram must be padded (e.g. Ethernet min size of data – 46 bytes)



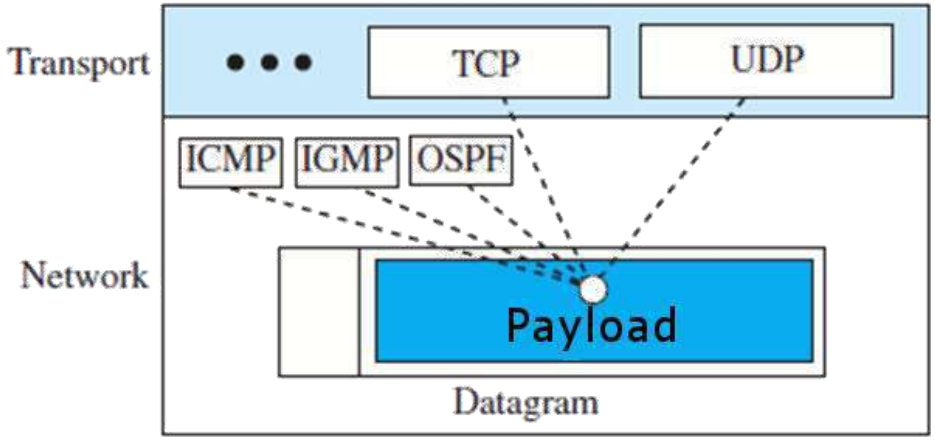
IPv4 Datagram Format

- **Identifier**(16bits)**, Flags**(3bits)**, Fragmentation Offset** (13 bits): These three fields are related to the fragmentation of the IP datagram when the size of the datagram is larger than the underlying network can carry.

- **Time-To-Live (TTL)** (8-bit field): controls max number of hops visited by datagram and/or time spend in the network
  - field is decremented by one each time datagram is processed by a router – when TTL reaches 0, datagram must be dropped.
  - ensures that
    1. datagram does not circulate/loop forever, or
    2. to limit its journey (e.g. LAN only: TTL = 1)

IPv4 Datagram Format

- **Protocol** (8-bit field) indicates specific transport-layer protocol to which data portion of this IP datagram should be passed
  - used only at final destination to facilitate demultiplexing process
  - protocol number is glue that binds network & transport layer, while port number is glue that binds transport & application layer
  - values: 1 – ICMP, 2 – IGMP, 6 – TCP, 17 – UDP, 89 – OSPF



Some protocol values

ICMP	01
IGMP	02
TCP	06
UDP	17
OSPF	89

IPv4 Datagram Format

- **Header Checksum: (**16-bit field) – aids in detecting errors in header only!
  - checksum must be recomputed & stored again at each router as TTL and some options fields may change
  - routers discard datagrams for which an error is detected
    - If destination IP addr is corrupted, datagram may be delivered to incorrect host
    - If protocol field is corrupted, datagram may be delivered to the wrong protocol
    - If fragmentation fields are corrupted, datagram can't be assembled at dest.
  - checksum calculation:
    1) divide header into 16-bit (2-byte) sections – checksum field itself is set to 0
    2) sum all sections using 1s complement arithmetic

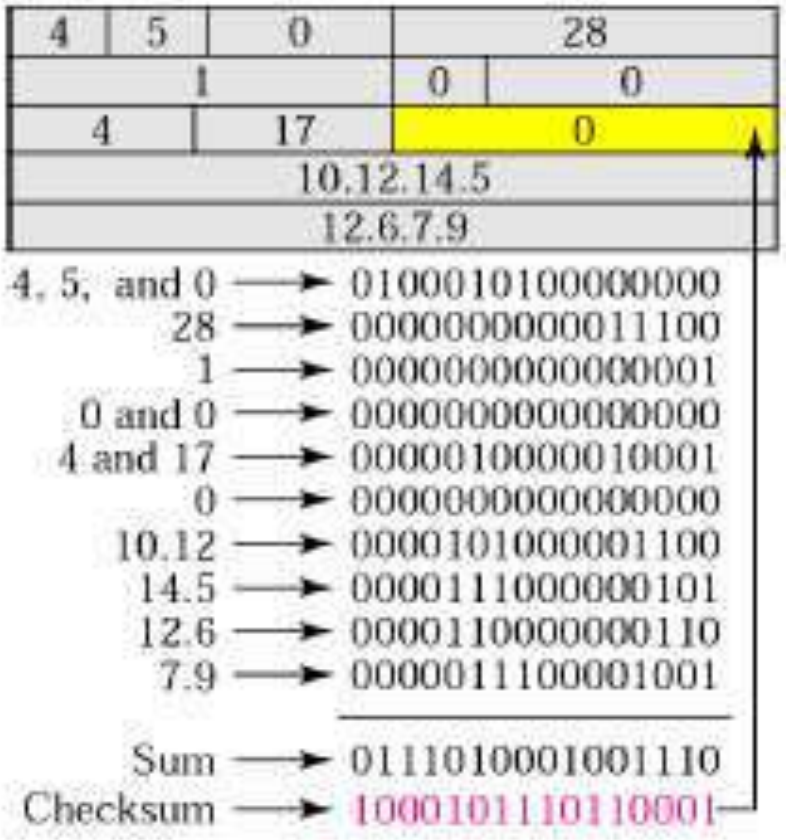
IPv4 Datagram Format

Example of checksum calculation in IPv4

Each intermediate router must:

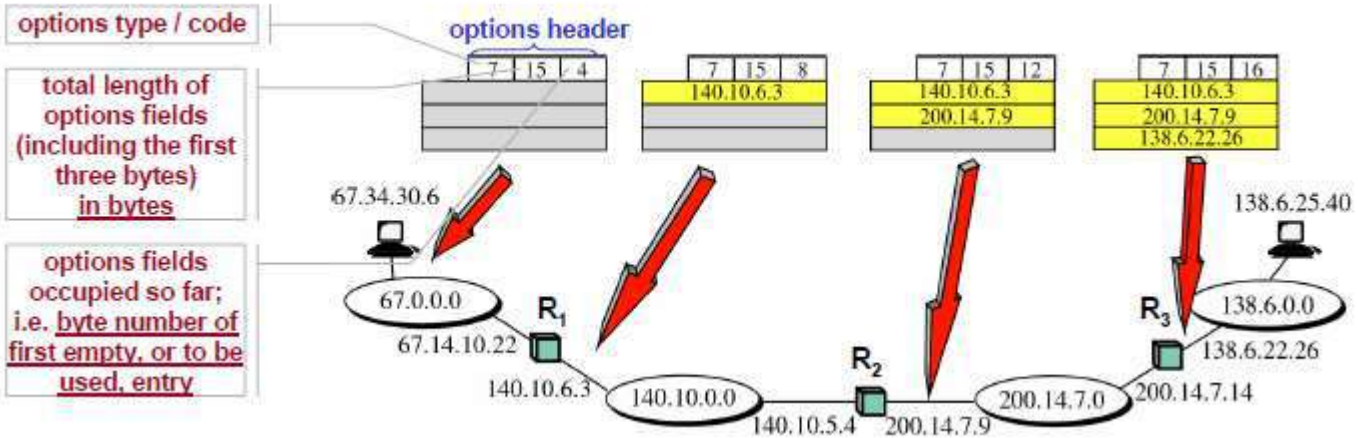
1) verify / recompute checksum on every incoming packet

2) compute checksum for every outgoing packet



IPv4 Datagram Format

- **Source and Destination IP Addresses** (32-bit fields): must remain unchanged until IP datagram reaches its final destination
- **Options** (32-bit field(s)) not required for every datagram! allows expansion of IP header for special purposes
  - (a) Record Route option – used to trace route that datagram takes source creates empty fields for IP addresses – up to 9 (40 bytes options – 4 bytes option header) / 4 bytes for IP address
  - each router that processes datagram inserts its outgoing IP address



IPv4 Datagram Format: Examples

An IP packet has arrived with the first 8 bits as shown: 01000010

The receiver discards the packet. Why?

Solution:

There is an error in this packet. The 4 left-most bits (0100) show the version, which is correct. The next 4 bits (0010) show the header length, which means (2 × 4 = 8), which is wrong. The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

In an IP packet, the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet?

Solution:

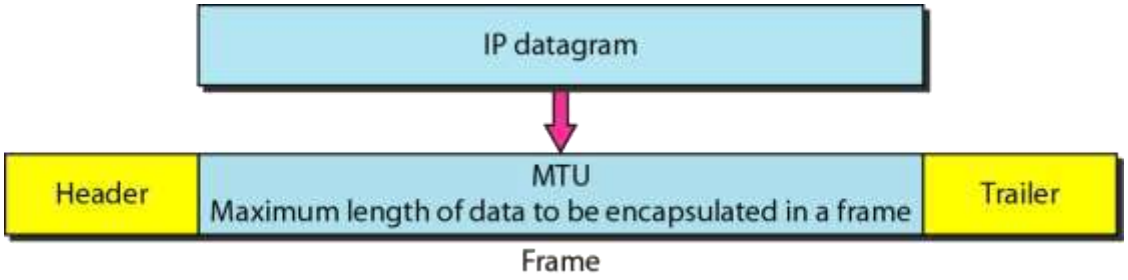
The HLEN value is 8, which means the total number of bytes in the header is 8x4 or 32 bytes. The first 20 bytes are the main header, the next 12 bytes are the options.

IP Datagram Fragmentation

- A datagram can travel through different networks.
- Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame.
- The format and size of the received frame depends on the protocol used by the physical network through which the frame has just traveled.
- The format and size of the sent frame depends on the protocol used by the physical network through which the frame is going to travel.

IP Datagram Fragmentation

- **Maximum Transfer Unit (MTU):** maximum amount of data that link-layer frame can carry = hard limit on IP datagram length.
- MTU differs from one data-link layer protocol to another
  A. Token Ring (4 Mbps): MTU = 4,464 bytes
  B. Ethernet: MTU = 1,500 bytes
  C. PPP: MTU = 296 bytes



Hard limit on IP datagram size is not a problem. What is a problem is that each of the links along the route between sender and receiver can use different link-layer protocols, and each of these protocols can have different MTUs.

IP Datagram Fragmentation

- **IP Datagram Fragmentation** – process of dividing datagram into smaller fragments that meet MTU requirements of underlying data-link layer protocol.
  - Datagram can be fragmented by source host or any other router in the path; however reassembly of datagram is done only by destination host! – parts of a fragmented datagram may take different routes !!!
  - Once fragmented datagram may be further fragmented if it encounters network with even smaller MTU
  - When a datagram is fragmented, each fragment gets its own header with most fields repeated, but some changed
  - Host or router that fragments datagram must change values of three fields: flags, fragmentation offset and total length

IP Datagram Fragmentation

- **Identification:** (16-bit field) uniquely identifies datagram originating from source host
  - to guarantee uniqueness, IP uses counter to label each datagram
  - when IP sends a datagram, it copies current counter value to identification field, and increments counter by one
  - when datagram is fragmented, identification field is copied into all fragments
  - identification number helps destination in reassembling datagram
    - all fragments with same identification value should be assembled into one datagram

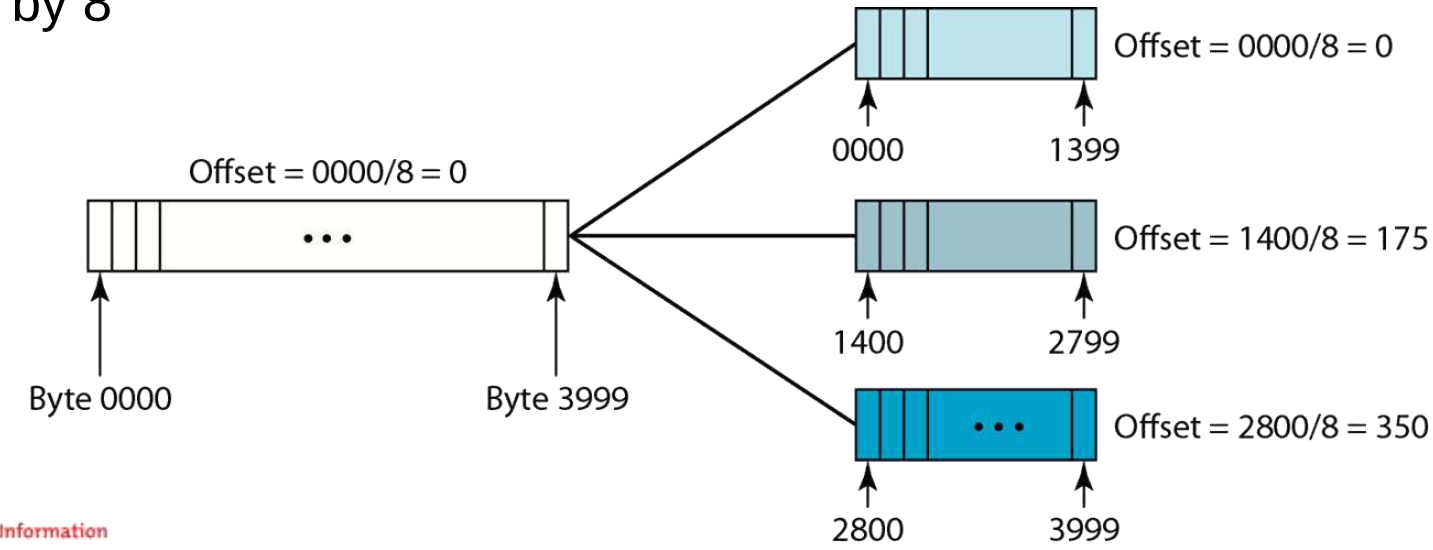
IP Datagram Fragmentation

- **Flags**: (3-bit field)
  - 1st bit is reserved
  - 2nd bit is called “do not fragment” bit
    - if its value is 1, machine must NOT fragment datagram
    - if fragment cannot pass through physical network router discards packet and sends ICMP error message back to source host
  - 3rd bit is called “more fragment” bit
    - if its value is 1, datagram is not last fragment – there are more fragments after this one
    - if its value is 0, this is last or only fragment

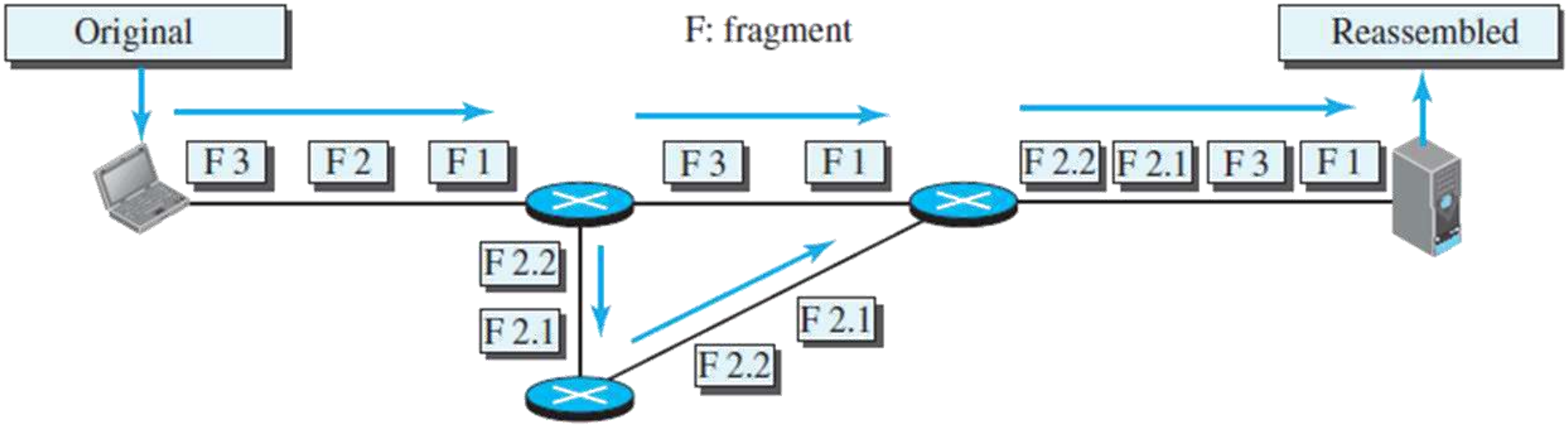
D: Do not fragment
M: More fragments

IP Datagram Fragmentation

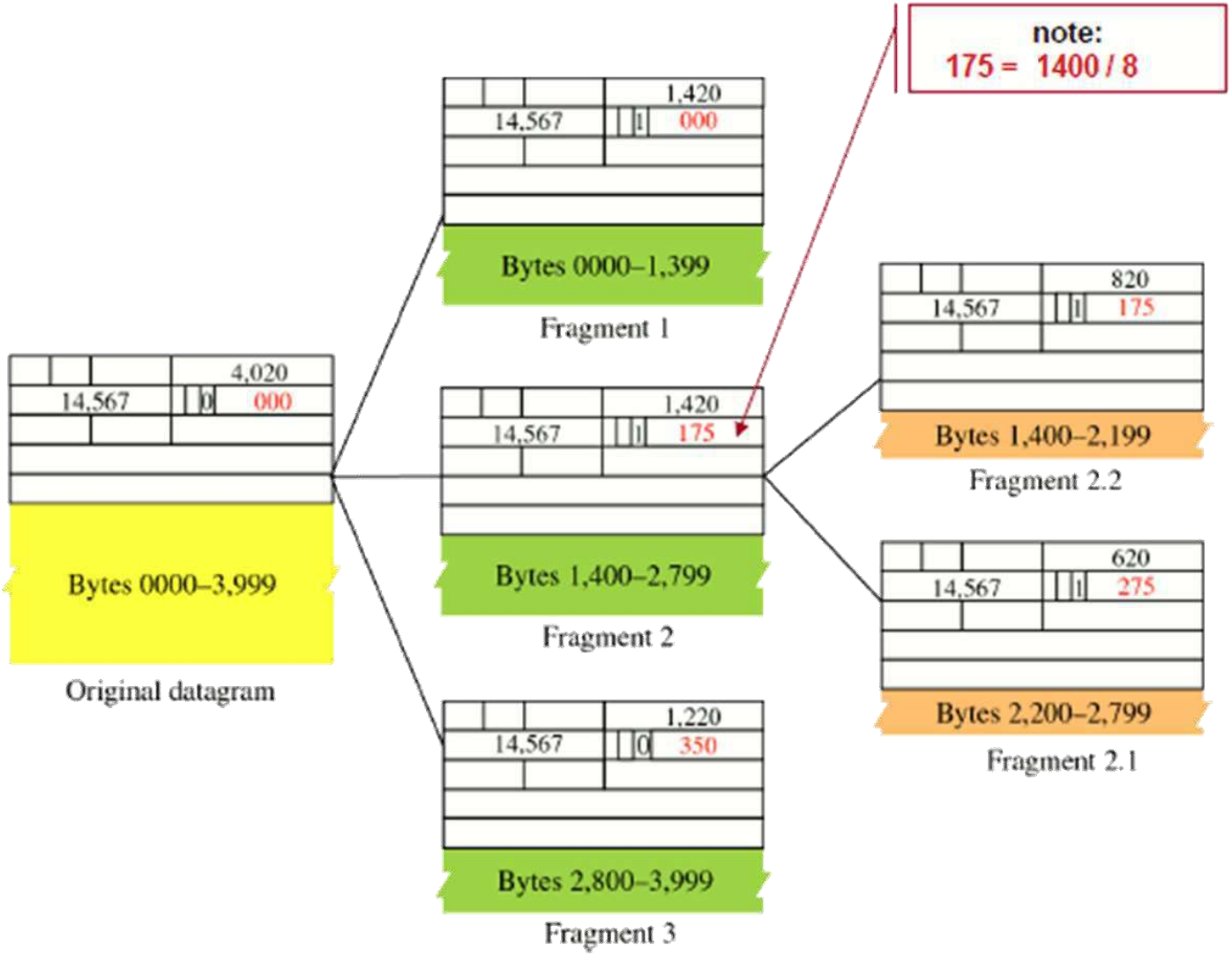
- **Fragmentation Offset** (13-bit field) shows relative position of fragment's data with respect to whole datagram
  - The offset is measured in units of 8 bytes – this is done because offset field is only 13 bits long and otherwise could not represent sequences greater than 8191
  - this forces hosts and routers to choose fragment sizes divisible by 8



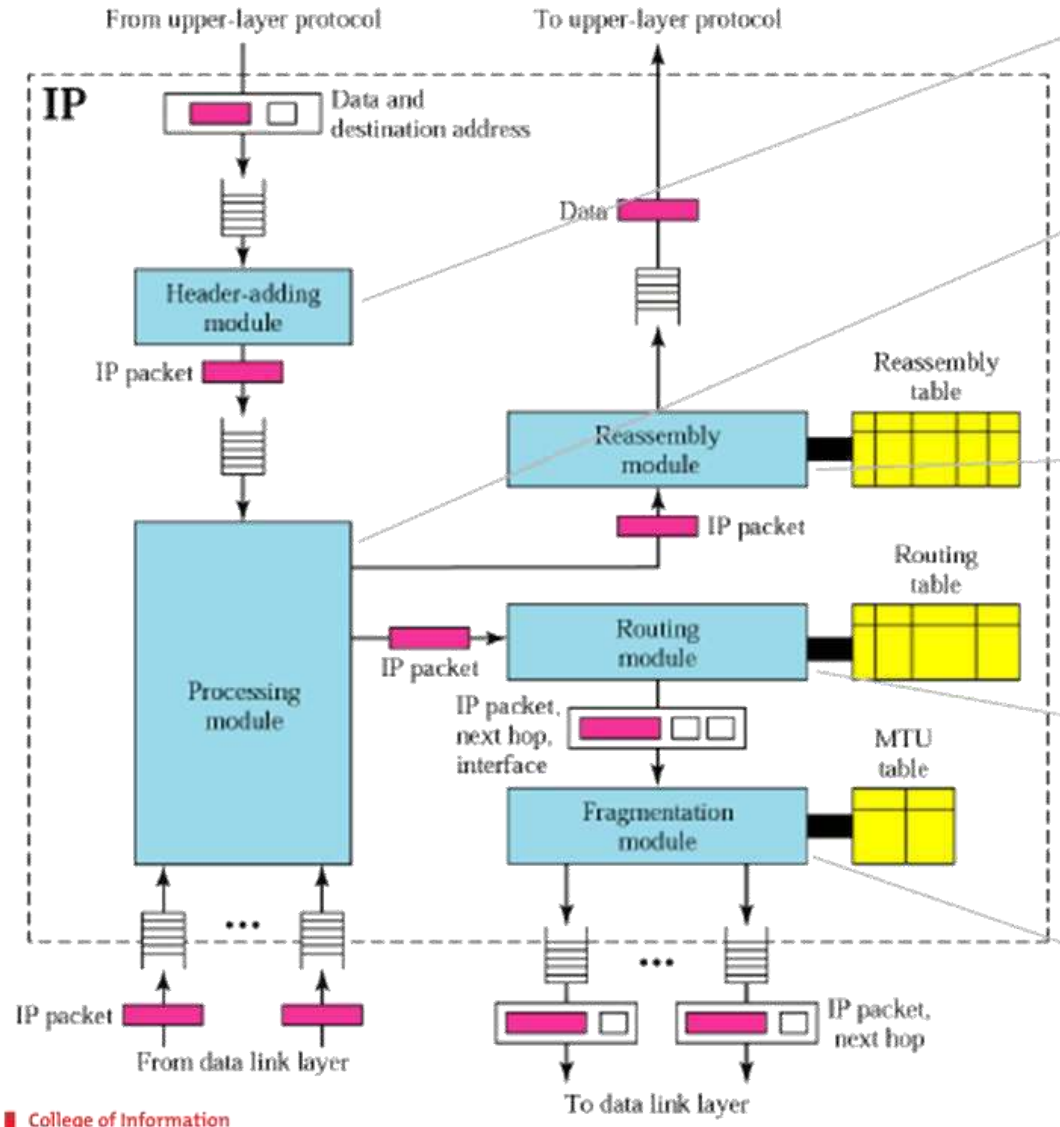
IP Datagram Fragmentation



IP Datagram Fragmentation



IP Datagram Processing



Header-adding module
encapsulates the data from the transport-layer protocol by adding the IP header

Processing module
1) checks if destination IP address = host IP address
2) decrements TTL by 1
(done only at router-nodes)

Reassembly module
orders and reassembles the fragments belonging to the same datagram. Reassembly table keeps track of received fragments

Routing module
finds the IP address of the next station along with the interface number to which the packet should be sent.

Fragmentation module
consults MTU table to find the MUT for the specific interface number.

ICMPv4

- IPv4 has no error-reporting or error-correcting mechanism

- IP lacks a mechanism for host and management queries
  - A host may need to determine if a router or another host is alive
  - A network manager may need information from another host or router

- **The Internet Control Message Protocol version 4** (ICMPv4) was designed to compensate for the above two deficiencies

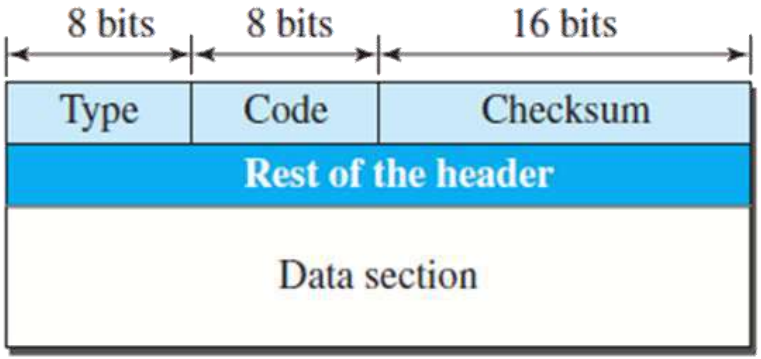
ICMPv4 Messages

- ICMP messages are divided into two broad categories: error-reporting messages and query messages

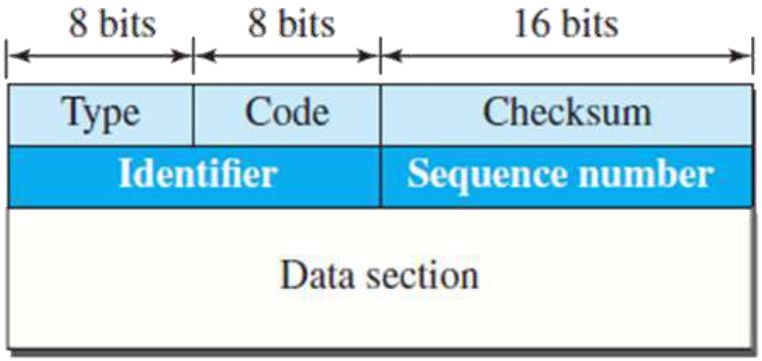
  - The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet

  - The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

ICMPv4 Message Format



Error-reporting messages



Query messages

Type and code values

Error-reporting messages

03: Destination unreachable (codes 0 to 15)
04: Source quench (only code 0)
05: Redirection (codes 0 to 3)
11: Time exceeded (codes 0 and 1)
12: Parameter problem (codes 0 and 1)

Query messages

08 and 00: Echo request and reply (only code 0)
13 and 14: Timestamp request and reply (only code 0)

Summary

- We discussed:
  - Introduction
  - Network Layer Responsibilities
  - Packetization
  - Routing and Forwarding
  - Packet Switching
  - IP4 Addressing
  - IPv4 Datagram format, fragmentation, processing
  - ICMPv4
- That concludes discussion on the network layer!