1.

a) What is a computer network? Describe the Network Criteria. [3 marks]

Ans: A **computer network** is a collection of interconnected devices (computers, servers, routers, etc.) that can communicate and share resources such as files, applications, or internet access. These devices are connected through communication links, either wired (e.g., coaxial, fiber optics) or wireless (e.g., radio, satellite).

To ensure efficient and effective networking, three essential criteria must be satisfied:

1. **Performance**: This refers to how well a network performs under load and is measured in terms of:
    - **Throughput**: the amount of data transmitted in a given time.
    - **Delay (Latency)**: the time it takes for data to travel from source to destination.

2. **Reliability**: It defines the dependability of the network, including:
    - Frequency of failure
    - Time taken to recover from failure
    - Network robustness under unexpected conditions

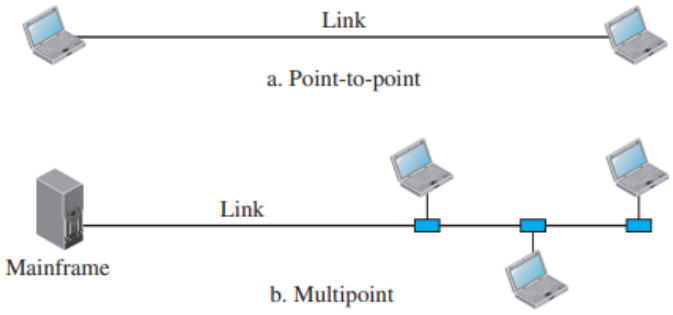
3. **Security**: It refers to protecting data from:
    - Unauthorized access (confidentiality)
    - Modification (integrity)
    - Disruptions or data loss (availability)

b) What are the advantages of a MultiPoint connection over a P2P connection? [2 marks]

Ans: A **point-to-point connection** provides a dedicated communication link between two devices. It is simple but resource-intensive when many devices are to be connected.

A **multipoint connection** (or multidrop) allows multiple devices to share a single link.

Figure 1.3 *Types of connections: point-to-point and multipoint*



Advantages of multipoint connections:

1. **Resource Efficiency**: Requires fewer cables and interfaces than multiple point-to-point links.
2. **Cost Reduction**: Lower hardware and installation costs due to shared infrastructure.
3. **Simplified Topology**: Easier setup for environments like LANs where many devices need to communicate over a common channel

c) Define protocol and Standards in Computer networks. [3 marks]

Ans: A **protocol** is a set of rules and conventions that define how data is transmitted and received across a network. Examples include TCP, IP, HTTP, FTP. It governs aspects such as:

- Data formatting
- Error detection and correction
- Synchronization and addressing

- A **standard** ensures interoperability between different devices and technologies by providing a formal specification of a protocol. Standards are defined by organizations like:
  - **ISO (International Organization for Standardization)**
  - **IEEE (Institute of Electrical and Electronics Engineers)**

- **IETF (Internet Engineering Task Force)**

Standards can be classified as

1. **De Facto:** by convention
2. **De Jure:** by law/regulation

In essence, **protocols** are the rules, and **standards** ensure those rules are followed uniformly across vendors and technologies.

d) What do you mean by ARPANET? Describe the physical topology of computer networks. [4 marks]

Ans: **ARPANET** (Advanced Research Projects Agency Network) was the first operational packet-switching network and the predecessor of the modern Internet. Developed in the late 1960s by the U.S. Department of Defense, ARPANET connected major academic and research institutions and demonstrated the feasibility of internetworking.

- **Physical topology** refers to the physical layout of devices and cables in a network. Common topologies include:

Topology	Description
Mesh	Every device is connected to every other device. Offers redundancy and fault tolerance.
Star	All devices connect to a central hub. Failure of the hub disables the network.
Bus	All devices are connected to a single backbone cable. Simple but prone to congestion.
Ring	Devices are connected in a circular chain. Data flows in one direction. Failure in one link can affect the whole network.

Each topology affects the performance, scalability, and fault tolerance of the network differently.

2.

a) In the Go-Back-N protocol, the size of the send window can be $2^m - 1$, while the size of the receive window is only 1. How can flow control be accomplished when there is a big difference between the size of the send and receive windows? Briefly Explain. [5 marks]

Ans: In the **Go-Back-N ARQ (Automatic Repeat reQuest)** protocol, the sender can send multiple frames before needing an acknowledgment, while the receiver only accepts frames in order.

- **Sender Window Size**: In Go-Back-N, the sender uses a sliding window of size $2^m - 1$, where m is the number of bits in the sequence number field. This allows the sender to send multiple frames before waiting for an acknowledgment.

- **Receiver Window Size**: The receiver window is **always 1**. It only accepts the next expected frame and discards any out-of-order frames.

Why This Works:

- Flow control is achieved by limiting the sender's ability to transmit beyond a window of unacknowledged frames.
- Even though the receiver accepts only one frame at a time, the large sender window ensures pipeline efficiency.
- If a frame is lost or has an error, all subsequent frames are discarded and retransmitted—ensuring reliability at the cost of potential redundancy.

Conclusion: The difference in window sizes is a design choice for simplicity at the receiver and throughput optimization at the sender.

b) What is the Socket address? Compare between TCP and UDP Protocol. [4 marks]

Ans: A **socket address** is a combination of an **IP address** and a **port number** that uniquely identifies a process on a host in a network. It enables the transport layer to deliver data to the correct application on a device.

$$Socket\ Address = IP\ Address + Port\ Number$$

For example, the socket address `192.168.1.1:80` refers to port 80 (commonly HTTP) on the device with IP address `192.168.1.1`.

Comparison between TCP and UDP:

Feature	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection Type	Connection-oriented	Connectionless

Reliability	Provides reliable delivery using ACKs and retransmission	No reliability; best-effort delivery
Order of Delivery	Ensures ordered data delivery	No guarantee of order
Flow and Congestion Control	Uses windowing and congestion control (e.g., slow start)	No such mechanisms
Overhead	Higher (due to headers and state maintenance)	Lower (minimal header)
Use Cases	Web browsing (HTTP), File transfer (FTP), Email (SMTP)	Streaming, DNS, VoIP

TCP is suited for applications that require **reliability**, while UDP is used where **speed and low overhead** are prioritized over guaranteed delivery.

c) What do you mean by loopback interface? An organization is assigned the block 2000:1456:2474:/48. What is the IPv6 address of an interface in the third subnet if the IEEE physical address of the computer is $(F5\text{-}A9\text{-}23\text{-}14\text{-}7A\text{-}D2)_{16}$? [3 marks]

Ans:

The **loopback interface** is a virtual interface that refers to the host itself. It is used for internal testing and communication within a host.

- **IPv4 loopback address:** `127.0.0.1`
- **IPv6 loopback address:** `0:0:0:0:0:0:0:1` or `::1`

No data sent to a loopback address ever leaves the host—it is looped back by the IP software stack.

Example 7.28

An organization is assigned the block 2000:1456:2474/48. What is the IPv6 address of an interface in the third subnet if the IEEE physical address of the computer is $(\mathbf{F5\text{-}A9\text{-}23\text{-}14\text{-}7A\text{-}D2})_{16}$?

Solution

The interface identifier for this interface is `F7A9:23FF:FE14:7AD2` (see solution to Example 7.27). If we add this identifier to the global prefix and the subnet identifier, we get:

```
2000:1456:2474:0003:F7A9:23FF:FE14:7AD2/128
```

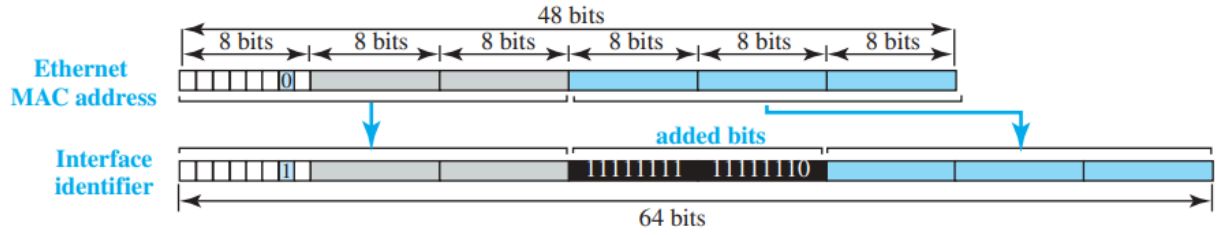
Given:

- IPv6 Block: `2000:1456:2474::/48`
- IEEE MAC Address: `F5-A9-23-14-7A-D2`
- Third subnet ⇒ we assume subnet ID: `0003`

Step 1: Convert MAC to EUI-64 Format

Split MAC into two halves and insert `FFFE` in the middle:

Figure 7.43 *Mapping for Ethernet MAC*



MAC: `F5-A9-23-14-7A-D2` ⇒ `F5A9:23FF:FE14::7AD2`

Step 2: Flip the 7th bit (Universal/Local bit):

- Original first byte = `F5` = `11110101`
- Flip 7th bit: `11110101` → `11110111` = `F7`

So the interface ID becomes:

Interface ID= `F7A9:23FF:FE14::7AD2`

Step 3: Combine with Subnet Prefix

The base prefix is `/48`, so the third subnet will be:

2000:1456:2474:0003::/64

Final IPv6 address:

2000 : 1456 : 2474:0003 : F7A9 : 23FF : FE14 : 7AD2

3.

a) You are given the following network address and subnet mask: [6 marks]
Network address: 192.168.10.0
Subnet mask: 255.255.255.252

i) How many subnets?
ii) How many hosts?
iii) What are the valid subnets?
iv) Fill in the table below

Meaning	Subnet 1	Subnet 2	Subnet 3	Subnet 4	Subnet 5	Subnet 6
Subnet address	192.168.10.0	192.168.10.4	192.168.10.8	192.168.10.12	192.168.10.16	192.168.10.20
First valid host						
Last valid host						
Broadcast address						

Ans:

Network Address: 192.168.10.0

Subnet Mask: 255.255.255.252 = /30

Total address bits: 32

Host bits = 32−30=2

i) Number of Subnets

If the original address is considered as part of a Class C network (/24), then:

$$Number\ of\ subnets\ = \frac{2^{(30-24)}}{1} = 2^6 = 64\ subnets$$

ii) Number of Hosts per Subnet

$$Number\ of\ hosts\ per\ subnet\ = 2^2 - 2 = 2\ hosts$$

The subtraction of 2 accounts for the **network address** and the **broadcast address**, which cannot be assigned to hosts.

iii) Valid Subnets

Since the block size =2^2 = 4, subnets increase in steps of 4:

- Subnet 1: 192.168.10.0
- Subnet 2: 192.168.10.4
- Subnet 3: 192.168.10.8
- Subnet 4: 192.168.10.12
- Subnet 5: 192.168.10.16
- Subnet 6: 192.168.10.20

iv) Fill in the Table

Meaning	Subnet 1	Subnet 2	Subnet 3	Subnet 4	Subnet 5	Subnet 6
Subnet Address	192.168.10.0	192.168.10.4	192.168.10.8	192.168.10.12	192.168.10.16	192.168.10.20
First Valid Host	192.168.10.1	192.168.10.5	192.168.10.9	192.168.10.13	192.168.10.17	192.168.10.21
Last Valid Host	192.168.10.2	192.168.10.6	192.168.10.10	192.168.10.14	192.168.10.18	192.168.10.22
Broadcast Address	192.168.10.3	192.168.10.7	192.168.10.11	192.168.10.15	192.168.10.19	192.168.10.23

b) If the data link layer can detect errors between hops, why do you think we need another checking mechanism at the transport layer in the OSI model? [3 marks]

Ans: The **data link layer** provides **hop-by-hop error detection**, which means it checks for errors between directly connected devices, such as from one router to the next.

However, data in a typical network traverses **multiple intermediate nodes** before reaching its final destination. Errors may occur:

- During transmission across a hop where error detection failed
- During queuing and processing at intermediate routers
- Due to misrouting or incorrect reassembly of packets

The **transport layer** (particularly TCP) offers **end-to-end error detection** using checksums that are verified **only at the source and the final destination**. This guarantees that data is **correct, complete, and ordered** when delivered to the application layer.

Without this layer, errors that occur after successful data link layer checks could go undetected, compromising data integrity.

c) How can NAT help in addressing depletion? Explain with necessary diagrams. [3 marks]

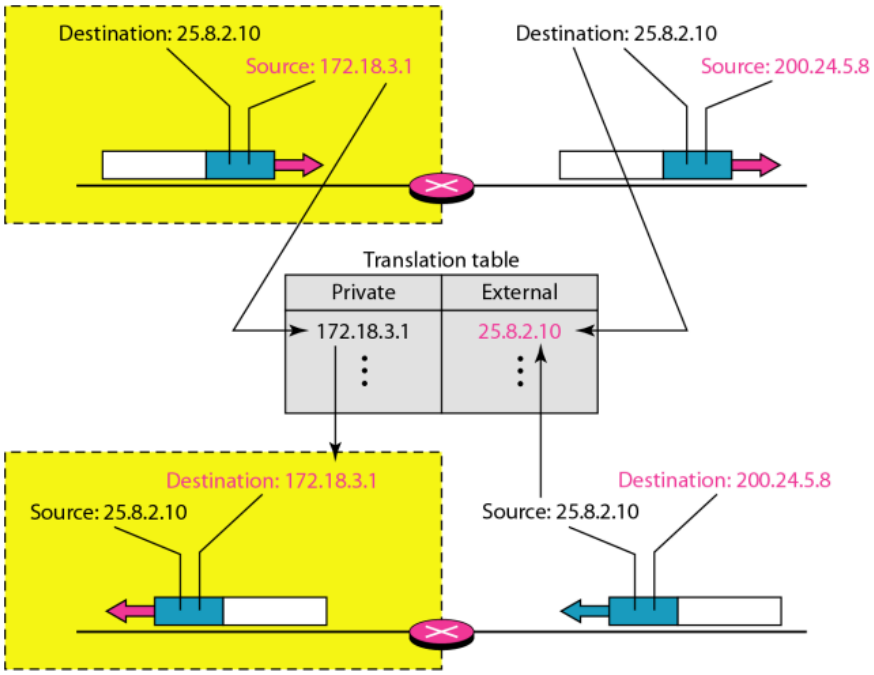
Ans: **Network Address Translation (NAT)** allows private IP addresses (used within internal networks) to be mapped to a public IP address when accessing external networks, such as the Internet.

Role in Address Depletion:

IPv4 uses a 32-bit address space, which limits the number of unique public IP addresses. NAT helps by:

- Allowing **multiple devices** within a private network to share a **single public IP**
- Conserving public address space by utilizing **private IP ranges** (e.g., 192.168.x.x)
- Internal hosts use private IPs.
- NAT router translates private IPs to public IP using port numbers (Port Address Translation).
- Responses are translated back correctly to the internal host.

Figure 19.12 *NAT address translation*



4.

a) What is Cryptography? Distinguish between passive and active attacks. [3 marks]

Ans: **Cryptography** is the science and art of transforming information to ensure secure communication. Its goal is to make messages unintelligible to unauthorized users, thereby protecting confidentiality and integrity. Traditionally, cryptography only involved encryption and decryption, but modern cryptography includes **symmetric-key**, **asymmetric-key**, and **hashing mechanisms**.

Passive vs Active Attacks:

Criteria	Passive Attack	Active Attack
Nature	Observational	Intrusive
Objective	To gather information without altering data	To modify, disrupt, or fabricate communication
Detection	Hard to detect	Easier to detect
Examples	Snooping, traffic analysis	Masquerading, replay, modification, DoS

- **Passive Attacks** threaten *confidentiality*. Example: Snooping on a message.
- **Active Attacks** threaten *integrity* and *availability*. Example: Tampering with or resending a message.

b) What are the differences between message confidentiality and message integrity? Can you have one without another? Use the additive cipher with k=5 to encrypt the plaintext "BU". Then decrypt the message to get the original plaintext. [4 marks]

Ans:

Message Confidentiality: It ensures that the content of a message remains inaccessible to unauthorized users during storage or transmission. Confidentiality is achieved using encryption techniques such as symmetric-key or asymmetric-key ciphers.

Message Integrity: It ensures that the content of a message has not been altered—intentionally or unintentionally—during transmission or storage. This is typically achieved using cryptographic hash functions like **Message Digest (MD)** or **Hash-based Message Authentication Code (HMAC)**.

Additive Cipher:

An **additive cipher**, also known as a **Caesar cipher**, is a basic form of symmetric-key encryption. It belongs to the class of **monoalphabetic ciphers**, where each letter in the plaintext is shifted by a fixed number of positions in the alphabet.

- Let plaintext P, key K, and ciphertext C be values in modulo 26.
  Encryption: $C = (P + K) \ mod \ 26$
  Decryption: $P = (C - K) \ mod \ 26$

Example:
Encrypt "BU" using key = 5:

- B → G, U → Z
- Encrypted text: **GZ**

This cipher is simple but vulnerable to brute-force attacks since only 25 usable keys exist.

c) Consider sending 4000-byte IP datagram (including the 20 bytes IP header) into a link that has an MTU of 1200 bytes. Determine the values of the length field and the offset field in each fragment. [5 marks]

Ans: To fragment the packet, consider the following:

- **MTU = 1200 bytes**

- **IP header = 20 bytes** (standard)
- **Maximum payload per fragment = 1200 - 20 = 1180 bytes**
- All fragments (except the last) must have a payload that is a multiple of 8 bytes

Fragmentation Calculation:

Total data=4000 bytes

Usable payload per fragment=1180 bytes

Adjusted to nearest multiple of 8=1176 bytes

Fragment 1:

- **Offset: 000**
- **Payload: 1176 bytes (bytes 0 to 1175)**
- **M bit: 1**

Fragment 2:

- **Offset: 1176/8=147**
- **Payload: 1176 bytes (bytes 1176 to 2351)**
- **M bit: 1**

Fragment 3:

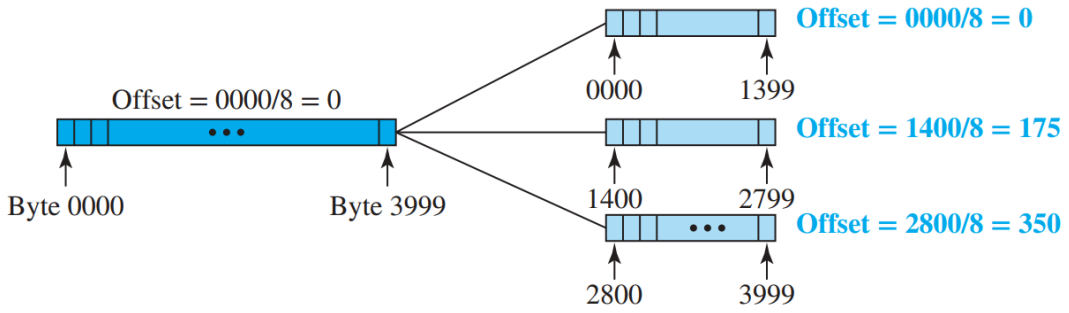
- **Offset: 2352/8=294**
- **Payload: 1176 bytes (bytes 2352 to 3527)**
- **M bit: 1**

Fragment 4:

- **Offset: 3528/8=441**
- **Remaining data: 4000−3528=472 bytes**
- **Payload: 472 bytes**

- **M bit: 0 (last fragment)**

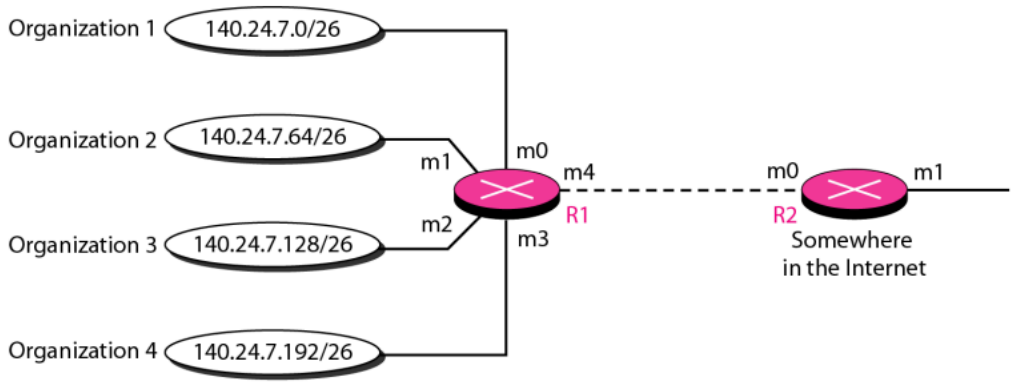
Figure 7.17 *Fragmentation example*



5.

a) Derive the routing table for the following Fig. 1. Can router R1 in Fig. 1 receive a packet with destination address 140.24.7.194? What will happen to the packet if this occurs? [6 marks]

Figure 22.7 *Address aggregation*



Ans:

Routing Table for Router R1:

Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/26	140.24.7.192	----------	m3
/0	0.0.0.0	Default	m4

Routing table for R1

Yes, router R1 can receive and forward a packet destined for 140.24.7.194

The router performs the following steps:

1. The first mask (/26) is applied to the destination address. The result is 140.24.7.192, which does match the corresponding network address. The next-hop address and the interface number m3 are passed to ARP for further processing.

b) Show abbreviations for the following IPv6 addresses:
i) 1234:0000:3456:0000:A058:0000:0000:F02F
ii) 0000:0001:0000:0000:0000:0000:56E2:24.120.12.90
[3 marks]

Ans:

i) 1234:0:3456:0:A058::F02F

ii) 0:1::56E2:24.120.12.90

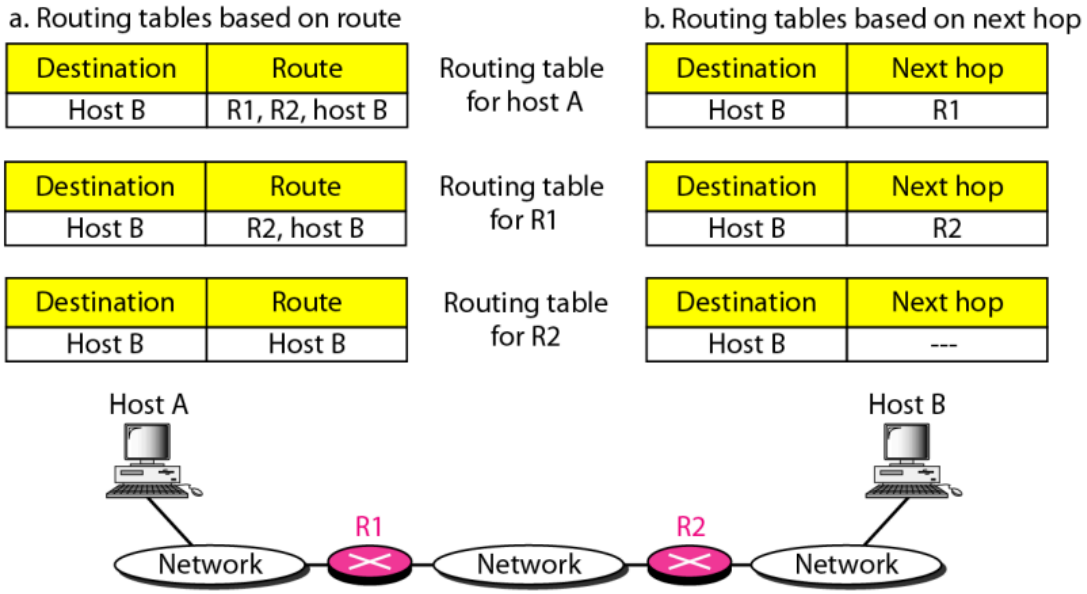
c) List three forwarding techniques and give a brief description of each. [3 marks]

Ans:

Route Method

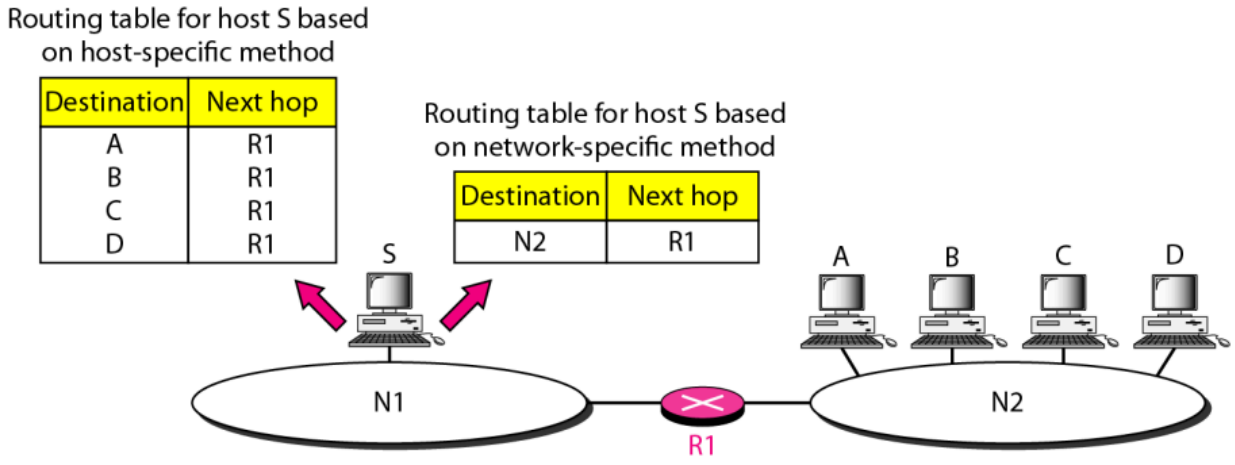
Next-Hop Method

Figure 22.2 *Route method versus next-hop method*



Network-Specific Method

Figure 22.3 *Host-specific versus network-specific method*



6.

a) What is Frame Relay? What is Frame Relay a better solution for connecting LANs than T-1 lines? [3 marks]

Ans:

b) What are the differences between IPv4 and IPv6 addressing? [3 marks]

Ans:

Feature	IPv4	IPv6
Address Length	32 bits (e.g., 192.168.1.1)	128 bits (e.g., 2001:0db8::1)
Address Format	Dotted decimal	Hexadecimal with colons
Address Space	$\approx 4.3 \times 10^9$ addresses	Vast: $\approx 3.4 \times 10^{38}$ addresses
Header Complexity	More complex (includes checksum)	Simplified header (no checksum field)
Security & Mobility	Optional (IPSec optional)	Built-in support for IPSec and mobility

c) Briefly define subnetting and supernetting. How do the subnet mask and supernet mask differ from a default mask in classful addressing? [3 marks]

Ans:

Subnetting:

- Divides a single network into multiple **smaller sub-networks**.
- Increases the **network portion** of the address by borrowing bits from the host part.
- Used to efficiently allocate address space within an organization.
- Increases number of 1s in the mask

Supernetting:

- Combines multiple **smaller networks** into a **larger address block**.
- Decreases the **network portion** and increases the **host portion**.
- Used in route aggregation and **Classless Inter-Domain Routing (CIDR)**.
- Decreases number of 1s in the mask

Type	Example (Class B)	Mask
Default Mask	128.10.0.0	255.255.0.0 (/16)
Subnet Mask	128.10.0.0/20	255.255.240.0
Supernet Mask	128.10.0.0/14	255.252.0.0

d) How does Frame Relay control congestion? What attributes are used for traffic control in Frame Relay? [3 marks]

Ans: Frame Relay uses **implicit congestion notification** by setting bits in the frame header:

1. **FECN (Forward Explicit Congestion Notification):** Set by switches in the forward path to inform the receiver of congestion.
2. **BECN (Backward Explicit Congestion Notification):** Sent back to the sender to indicate congestion in the return path.

These bits notify endpoints to **reduce the transmission rate** temporarily.

Traffic Control Attributes:

1. **CIR (Committed Information Rate):** Guaranteed minimum bandwidth over a time interval.
2. **Bc (Committed Burst Size):** Maximum bits allowed to be sent within a time frame without being discarded.
3. **Be (Excess Burst Size):** Additional bits allowed beyond Bc, not guaranteed to be delivered during congestion.

These parameters are negotiated during setup and monitored for **conformance** using a **leaky bucket algorithm**.

7.

a) What is the RSA algorithm? Alice wants to send a message to Bob. Then Bob needs to select keys. Suppose, Bob chose p=7 and q=13 in the RSA algorithm. Now, find the value of d. Also, encrypt the message "CSE" using Bob's public key so that he can only decrypt. For simplicity, do the encryption and decryption character by character. [5 marks]

Ans: The RSA algorithm is a public-key cryptographic system based on the mathematical difficulty of factoring large prime numbers. It uses two keys: a **public key** for encryption and a **private key** for decryption. The keys are generated using two large prime numbers and modular arithmetic.

To send a secure message using RSA, the sender encrypts the message using the receiver's **public key**, and only the receiver, who possesses the **private key**, can decrypt it. Below are the steps Bob performs to generate his keys and allow Alice to encrypt a message for him.

RSA Algorithm

Euclidean Alg.

Two positive integers a and b.

$a = bq + r \quad 0 \le r < b$

$b = r(q_1) + r_1 \quad 0 \le r_1 < r$

$r = r_1(q_2) + r_2 \quad 0 \le r_2 < r_1$

⋮

continue until remainder is zero

$r_{i-2} = r_{i-1} q_i + r_i \quad 0 \le r_i < r_{i-1}$

$r_{i-1} = r_i q_{i+1} + 0$

Example: Input 34, 55

$55 = 34(1) + 21$

$34 = 21(1) + 13$

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

$\gcd(55, 34) = 1$

The last nonzero remainder is the gcd. So, $\gcd(a,b) = r_i$

RSA Key Selection

Step-1: $p = 11, q = 5, n = p \times q;\ n = 11 \times 5 = 55$

Step-2: Calculate the totient of RSA modules.

$$\varphi(n) = (p-1)(q-1)$$
$$= (11-1)(5-1) = 40$$

* The totient function/ Euler's totient function, is defined as the number of positive integers that are positively prime to (i.e., do not contain any factor in common with) where 1 is counted as being relatively prime to all numbers.

Step-3: select a number, e, that is relative prime to the totient and is $1 < e < \varphi(n)$. (e is public)

So, 3, 7, 9, 11, 13, 17 ----- .

We have chosen, $e = 7$ co-prime of $\varphi(n)$

e, n → public
φ, d → secret

Extended Eucl. Alg. useful when a and b are coprime (or gcd is 1)

Step-4: Calculating d using the following equation.

$d \times e = 1 \bmod \varphi(n)$ (or $d \times e \bmod \varphi(n) = 1$)

$d(7) = 1 \bmod 40$ (or $d(7) \bmod 40 = 1$)

Use ~~Extended~~ Euclidean Alg. to solve this:

$40x + 7y = 1$

$40 = 5(7) + 5$

$7 = 1(5) + 2$

$5 = 2(2) + 1$

$2 = 2(1) + 0$

We stop at the last non-zero remainder, then use the extended Euclidean Alg.

Back substitute:

$5 = 2(2) + 1$

$1 = 5 - 2(2)$

$1 = 5 - 2(7 - 1(5))$

$= (5) - 2(7) + 2(5)$

$= 3(5) - 2(7)$

$= 3(40 - 5(7)) - 2(7)$

$= 3(40) - 15(7) - 2(7)$

$= 3(40) - 17(7)$

$\therefore d = 40 - 17 = 23$. (if negative)

if 17 was positive then $d = 17$

private				public	
p	q	φ(n)	d	n	e
11	5	40	23	55	7

Now encryption and decryption

Alice

message: HIDE

$c = p^e \bmod n$

First encrypt H, numerical representation of H is 7

So, $p = 7$

$c = 7^7 \bmod 55$

$= 28$ (is the ciphertext of H)

Similarly

for $I = 8^7 \bmod 55 = 2$

$D = 3^7 \bmod 55 = 42$

$E = 4^7 \bmod 55 = 49$

Bob

ciphertext: 28, 2, 42, 49

$p = c^d \bmod n$

$28 = 28^{23} \bmod 55 = 7 = H$ [see Fast exponential modular arithmetic]

$2 = 2^{23} \bmod 55 = 8 = I$

$42 = 42^{23} \bmod 55 = 3 = D$

$49 = 49^{23} \bmod 55 = 4 = E$

So, our plaintext = HIDE

b) What is Digital Signature? How can it be implemented to provide message integrity service? [4 marks]

Ans: A **Digital Signature** is a cryptographic technique that allows the recipient of a message to verify both the **authenticity** of the sender and the **integrity** of the message. It is the digital equivalent of a handwritten signature or stamped seal but is much more secure due to cryptographic properties.

In digital communication, ensuring **message integrity** means confirming that the message has not been altered during transit. A digital signature achieves this using a **hash function** combined with the sender's **private key**. The process involves:

1. The sender computes a hash (digest) of the original message using a secure hashing algorithm (e.g., SHA-256).
2. This digest is then **encrypted with the sender's private key** to create the digital signature.
3. The signature is attached to the message and sent to the receiver.
4. Upon receiving the message, the receiver:
    - Decrypts the signature using the sender's **public key** to retrieve the original hash.
    - Hashes the received message independently.
    - Compare both hashes. If they match, the message is unaltered and the sender is authenticated.

This mechanism ensures:

- **Integrity** (message hasn't changed),
- **Authentication** (sender is verified),
- And sometimes **non-repudiation** (sender cannot deny the message later).

c) The following shows the IPv6 datagram format. Compare it with IPv4 datagram format. [3 marks]

IPv6 Datagram Header:

Version	**Traffic Class**	**Flow Label**
Payload Length	**Next Header**	**Hop Limit**
Source Address (128 bits)		

Destination Address (128 bits)

Ans:

Figure 7.13 *IP datagram*

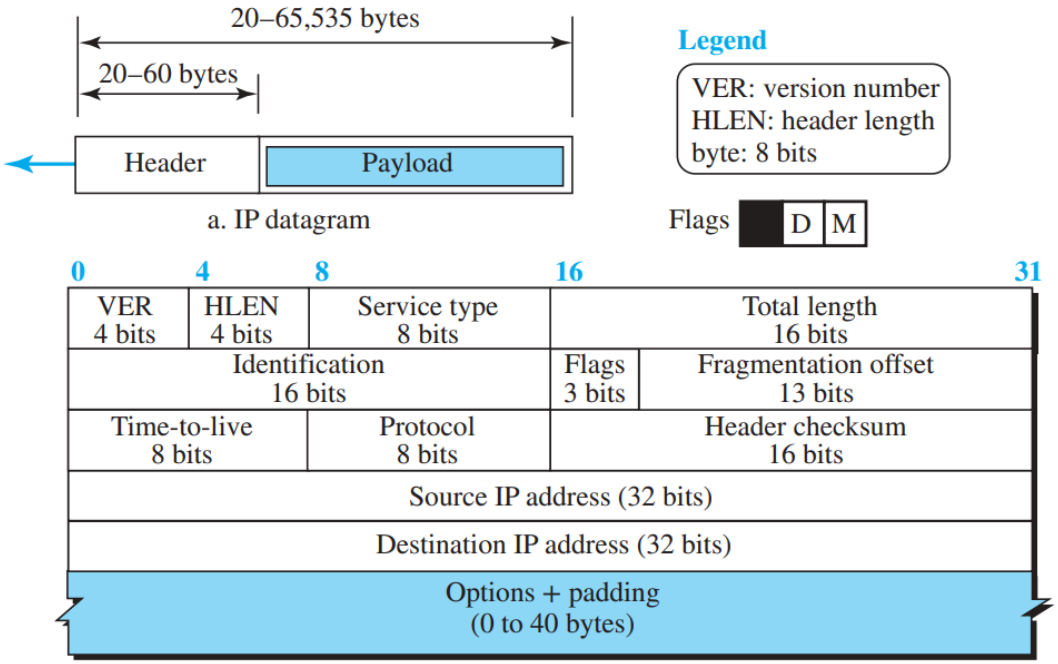


Table 20.9 ***Comparison between IPv4 and IPv6 packet headers***

Comparison
1. The header length field is eliminated in IPv6 because the length of the header is fixed in this version.
2. The service type field is eliminated in IPv6. The priority and flow label fields together take over the function of the service type field.
3. The total length field is eliminated in IPv6 and replaced by the payload length field.
4. The identification, flag, and offset fields are eliminated from the base header in IPv6. They are included in the fragmentation extension header.
5. The TTL field is called hop limit in IPv6.
6. The protocol field is replaced by the next header field.
7. The header checksum is eliminated because the checksum is provided by upper-layer protocols; it is therefore not needed at this level.
8. The option fields in IPv4 are implemented as extension headers in IPv6.

8.

a) Describe the shift cipher and transposition ciphers with example. [4 marks]

Ans: The **Shift Cipher**, also known as the **Caesar Cipher** or **Additive Cipher**, is a form of **monoalphabetic substitution cipher** where each letter in the plaintext is replaced by a letter a fixed number of positions down the alphabet. For example, with a key of 3, "A" becomes "D", "B" becomes "E", and so on. Encryption is performed using the formula:

$$C = (P + k) mod\ 26$$

where C is the ciphertext letter, P is the plaintext letter (as a number from 0–25), and k is the shift value.

Example: Encrypting "HELLO" with k=3:
H → K, E → H, L → O, L → O, O → R
Result: **KHOOR**

In contrast, a **Transposition Cipher** does not change the actual letters of the message, but rather **rearranges their positions** according to a predetermined system. It preserves the frequency of characters but disguises the message by reordering.

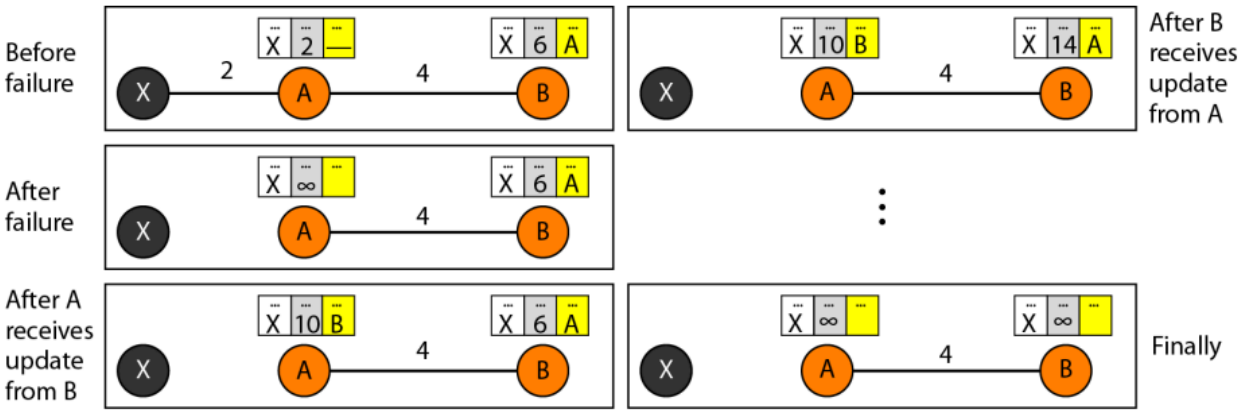
Example: For the plaintext "NETWORK", using a transposition key (say, reversing every two letters), we get:
Original: NE TW OR K
Transposed: EN WT RO K
Result: **ENWTROK**

Transposition ciphers are stronger when combined with substitution ciphers, forming more complex encryption schemes such as product ciphers.

b) What do you mean by the "Two-Node Loop Instability" problem with distance vector routing? Explain with necessary diagrams. Also, provide a solution to the problem. [4 marks]

Ans: The **Two-Node Loop Instability** problem occurs in **distance vector routing** when two routers continuously update their routing tables with incorrect distances due to a broken link, causing an endless loop and **count-to-infinity** behavior.

Figure 22.17 *Two-node instability*



If the actual path to network X fails, but A and B still share outdated information, they will **keep increasing the hop count to X** believing the other has a valid route, forming a **loop**.

This behavior continues until the hop count reaches a predefined maximum (e.g., 16 in RIP), at which point the route is considered unreachable.

A common solution is **Poisoned Reverse**, where a router advertises an infinite metric (e.g., 16) to its neighbor if it routes traffic to a network via that neighbor. For instance, if B routes to X via A, B tells A that its distance to X is ∞, thus preventing A from routing back through B. This technique breaks the loop by preventing mutual reinforcement of incorrect paths.

c) Write short notes on (any two): [4 marks]
i) Packet Switching
ii) Circuit Switching
iii) HTTP
iv) FDDI

Ans:

i) Packet Switching: Packet switching is a method of data communication where the data is divided into small units called **packets**, each of which is routed independently through the network. Unlike circuit switching, it does not reserve a dedicated path; instead, it uses a **store-and-forward mechanism** where routers temporarily store packets before forwarding them to the next hop. This allows for better bandwidth utilization and supports **bursty and dynamic traffic** patterns. The Internet primarily uses packet switching protocols such as IP, making it scalable and robust for modern data communication.

ii) Circuit Switching: Circuit switching is a communication method where a **dedicated communication path** is established between the sender and receiver for the entire duration of the session. This path remains reserved, even if no data is being transmitted. It is commonly used in traditional **telephone networks**, where a call occupies a fixed circuit. The main advantages are guaranteed bandwidth and low delay during transmission. However, it is inefficient for data networks due to idle time when no data is transmitted, leading to poor utilization of network resources.

iii) HTTP (Hypertext Transfer Protocol): HTTP is a protocol used at the **application layer** for accessing resources on the World Wide Web. It follows a **client-server model**, where the client (usually a browser) sends an HTTP request to the server, and the server responds with the requested content, such as HTML documents, images, or files. HTTP is **stateless**, meaning it does not retain session information between transactions. The standard HTTP uses TCP as its transport layer protocol, and its secure variant, **HTTPS**, ensures encrypted communication using SSL/TLS. HTTP is essential for enabling web browsing, REST APIs, and much of Internet-based communication.

iv) FDDI (Fiber Distributed Data Interface): FDDI is a high-speed **LAN protocol** that uses fiber optic cables to connect devices in a ring topology. It operates at speeds of **100 Mbps** and is based on the **token passing** access method. FDDI typically uses two rings—**a**

primary ring for data and **a secondary ring** for redundancy. In case of a failure in the primary ring, the secondary ring can be used to maintain communication. It provides a high degree of reliability and was historically used in backbone networks and environments requiring fault tolerance, though it has largely been replaced by Ethernet technologies in modern systems.
