Department of Computer Science and Engineering

Assignment – II

Subject: Computer Networks (U23CD602)

Class: B.E. — VI Semester, CSE_A2

Academic Year: 2025–2026

Date of Assignment: 12-04-2026
Date of Submission: 13-04-2026
Maximum Marks: 10

Name: Mohammed Ufraan

Roll No: 160923733152

Contents

Collision-Free Protocol and CSMA/CD

Question	What is a Collision-Free protocol? Explain in detail CSMA/CD technique.
Marks	2
Course Outcome (CO)	CO2
Taxonomy Level	BTL2 (Understand)

A **collision-free protocol** is a Medium Access Control (MAC) protocol that ensures no two stations ever transmit simultaneously on a shared channel. Unlike contention-based protocols (ALOHA, CSMA), collision-free protocols use controlled access mechanisms such as token passing, bitmap protocols, or binary countdown to eliminate collisions entirely, resulting in predictable and efficient channel utilization.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

CSMA/CD is the foundational access method used in wired Ethernet (IEEE 802.3). While not strictly collision-free, it minimizes collision impact through detection and recovery. It allows multiple stations to share a channel and handles collisions as they occur.

Working Principle:

- **Carrier Sense:** Before transmitting, a station first listens to the channel. If the medium is busy, it defers transmission until the channel is idle.
- **Multiple Access:** All stations share the same physical medium; any station can attempt to transmit when the channel is free.
- **Collision Detection:** While transmitting, the station continuously monitors the channel. If the detected signal differs from the transmitted signal, a collision has occurred and transmission is immediately aborted.
- **Jamming Signal:** After aborting, a 48-bit jam signal is broadcast to ensure all stations are aware of the collision.
- **Binary Exponential Backoff:** Each colliding station waits a random backoff time drawn from an exponentially growing range before retrying. After k collisions, the wait is chosen from $\{0, 1, \ldots, 2^k - 1\}$ slot times.

Advantages and Limitations:

CSMA/CD significantly reduces wasted bandwidth compared to Pure ALOHA and works well under light to moderate traffic loads. However, it is unsuitable for

wireless networks due to the hidden terminal problem and the physical impossibility of detecting collisions while transmitting over a wireless medium. Modern switched Ethernet has largely made CSMA/CD obsolete by providing dedicated point-to-point links per host.

Multiple Access Protocols: Pure ALOHA and Slotted ALOHA

Question	Explain in detail about Multiple Access Protocols (Pure Aloha and Slotted Aloha).
Marks	2
Course Outcome (CO)	CO2
Taxonomy Level	BTL2 (Understand)

Multiple Access Protocols define rules for how multiple stations share a single common communication channel without centralized control. They are essential in broadcast networks such as LANs and satellite links where simultaneous transmissions would interfere with each other.

1. Pure ALOHA

Pure ALOHA, developed at the University of Hawaii, is the simplest random access protocol.

- A station transmits a frame whenever it has data, without checking whether the channel is busy.
- If a collision occurs (another station transmitted at the same time), the frames are destroyed.
- After a random wait time, the station retransmits the frame.
- The **vulnerable period** is **2T** (two frame times), since a collision can occur if any other station transmits within one frame time before or after.
- **Maximum throughput:** $S = 0.184$ (18.4%) at offered load $G = 0.5$.

2. Slotted ALOHA

Slotted ALOHA improves on Pure ALOHA by introducing time synchronization.

- Time is divided into discrete slots, each equal to one frame transmission time.
- Stations are only permitted to begin transmission at the start of a slot.
- This constraint halves the vulnerable period to **T** (one frame time), cutting collision probability significantly.
- **Maximum throughput:** $S = 0.368$ (36.8%) at offered load $G = 1$, exactly double that of Pure ALOHA.
- Requires a global clock or synchronization mechanism across all stations.

Comparison Table:

Feature	**Pure ALOHA**	**Slotted ALOHA**
Transmission time	Any time	Start of slot only
Vulnerable period	2T	T
Max throughput	18.4%	36.8%
Synchronization	Not required	Required
Complexity	Simpler	Slightly more complex

Differences Between IPv4 and IPv6

Question	State the differences between IPv6 and IPv4 protocol in detail.
Marks	2
Course Outcome (CO)	CO3
Taxonomy Level	BTL2 (Understand)

IPv4 (Internet Protocol version 4) has been the backbone of the internet since the 1980s. However, the exhaustion of its 32-bit address space led to the development of **IPv6** (Internet Protocol version 6), which offers a vastly larger address space along with several architectural improvements.

Feature	**IPv4**	**IPv6**
Address Length	32-bit	128-bit
Address Space	≈ 4.3 billion addresses	$\approx 3.4 \times 10^{38}$ addresses
Notation	Dotted decimal (e.g., 192.168.1.1)	Hexadecimal with colons (e.g., 2001:0db8::1)
Header Size	20–60 bytes (variable, options allowed)	Fixed 40 bytes
Fragmentation	Done by routers and the sender	Done by sender only; routers do not fragment
Header Checksum	Present	Removed (handled by transport layer)
NAT	Required due to address scarcity	Not needed; every device gets a unique address
Security (IPSec)	Optional extension	Mandatory part of the protocol
Broadcast	Supported	Not supported; replaced by multicast and anycast
Address Configuration	Manual or DHCP	Stateless auto-configuration (SLAAC) or DHCPv6
QoS Support	Limited (DSCP/ToS field)	Built-in Flow Label field for QoS

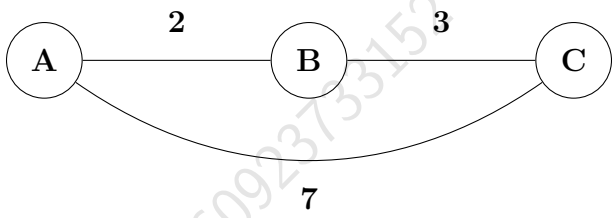
The fixed header size in IPv6 simplifies router processing, while the elimination of the checksum field at the IP layer reduces per-hop overhead. These changes collectively make IPv6 more efficient and scalable for modern networks.

Distance Vector Routing Algorithm

Question	Draw a subnet graph and develop the routing table using the distance vector routing algorithm. State the drawbacks of distance vector routing algorithm.
Marks	2
Course Outcome (CO)	CO3
Taxonomy Level	BTL2 (Understand)

The **Distance Vector Routing** algorithm (based on the Bellman-Ford equation) is a distributed routing algorithm where each router maintains a table of the best known distance to every destination and the link to use to get there. Routers periodically share their tables with direct neighbors and update their own tables accordingly.

Subnet Graph



The network has three routers A, B, C. Direct link costs: A–B = 2, B–C = 3, A–C = 7. The optimal path from A to C is via B (cost = 5), not the direct link (cost = 7).

Routing Table After Convergence

Router	To A	To B	To C
A	0 (self)	2 (via B)	5 (via B)
B	2 (via A)	0 (self)	3 (via C)
C	5 (via B)	3 (via B)	0 (self)

Drawbacks of Distance Vector Routing

- **Count-to-infinity problem:** When a link fails, bad news propagates very slowly as routers increment distances one hop at a time, potentially looping until infinity.
- **Slow convergence:** After any topology change, multiple update cycles are needed before all routers agree on correct paths, during which routing loops

may occur.

- **High bandwidth consumption:** Each router periodically broadcasts its entire routing table to all neighbors, which becomes expensive as the network scales.
- **No global view:** Routers only know next-hop information; they have no knowledge of the complete network topology, making loop detection difficult.

Need for Routing Algorithms

Question	What is the need for routing algorithm?
Marks	2
Course Outcome (CO)	CO3
Taxonomy Level	BTL2 (Understand)

A **routing algorithm** is the logic embedded in routers that determines the best path for forwarding packets from a source to a destination across a network of interconnected nodes. In any real-world network, multiple paths exist between endpoints, and conditions such as link failures, congestion, and topology changes occur continuously. Routing algorithms address these challenges systematically.

Key Reasons for Routing Algorithms

- **Optimal Path Selection:** Networks contain multiple possible routes between any two nodes. Routing algorithms evaluate metrics such as hop count, link bandwidth, propagation delay, and congestion to select the most efficient path.
- **Fault Tolerance and Reliability:** When a router or link fails, routing algorithms automatically detect the failure and recalculate alternative paths, ensuring continuous packet delivery without manual intervention.
- **Load Balancing:** Traffic can be intelligently distributed across multiple available paths to prevent any single link from becoming a bottleneck, thereby improving overall network throughput.
- **Scalability:** The internet spans billions of devices across millions of networks. Routing algorithms such as OSPF and BGP are designed to scale to this level, ensuring packets can still reach any destination efficiently.
- **Dynamic Adaptation:** Network conditions change constantly due to congestion, new links, or failures. Routing algorithms adapt in real time, updating forwarding tables to reflect the current state of the network.
- **Support for QoS:** Advanced routing algorithms can prioritize traffic flows based on quality of service requirements, ensuring time-sensitive data (e.g., VoIP, video) is delivered with minimal delay.

Without routing algorithms, it would be impossible to deliver packets reliably across large heterogeneous networks like the internet, where no static or manually configured path can account for the dynamic nature of real-world network infrastructure.