MOHAMED ZAYED A
RA2211003050091

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
TIRUCHIRAPPALLI CAMPUS

COMPUTER NETWORK

1.) Distance Vector Routing Protocol :-

The distance Vector Routing Protocol is a dynamic routing protocol that determines the best path to a destination based on the distance in terms of hop from the source. It uses the Bellman-Ford algorithm to calculate the shortest path between nodes in a network.

* Distance Vector table :

Each router maintains a table containing the distance to every known destination

2. Link state Routing.

The Link State Routing Protocol is a dynamic routing Protocol that uses a different approach than distance vector Routing. It maintains a complete map of the network topology by understanding the state of each in the network. The key features,

* Link State Advertisements: Each router periodically sends LSA's, which contain information about it directly connected neighbors and the cost of the links to those neighbors.

* TOPology Database: Each router builds a topology database based on the received LSA's from all other routers.

* Shortest path calculation:

using Dijkstra's algorithm, each router calculates the shortest path to every other router in the network.

* Efficient updates:- when there is a change in the network (eg. a link goes down), only the affected LSA's are updated and flooded to the network.

* Loop-free Routing: Since each router independently calculates the shortest path based on the same network map, the routing is inherently loop-free.

3. Path vector Routing.

Path vector routing is a dynamic routing Protocal commonly used in large-scale networks like the Internet, Particularly in Border Gateway Protocal. It helps determine the best Path between autonomous systems rather than individual routers.

The main features include:

* Path vector Information: Each routing update contains the full Path that the route has traversed to reach the destination.

* Autonomous System (AS) Boundaries: Path vector routing operates at the level of AS, where each AS can be seen as a large network or organization with its own internal routing Policies.

* Loop Prevention:- By including the entire Path in the routing update, routers can easily detect routing loops.

* Routing updates: when the topology changes, routers only send updates to neighbors about the affected routes rather than the entire routing table.

4. RIP version 1 and version 2:

Routing Information Protocol (RIP) is a distance vector routing protocol used in smaller networks. RIP has two versions, with several key differences:

* Routing updates format:
  - RIP version 1 : uses classful routing, meaning it does not send subnet mask information with its routing updates.
  - RIP version 2 : supports classes routing by including the subnet mask in routing updates, allowing for variable length subnet masking (VLSM) and supporting more flexible IP addressing.

* Broadcast Vs Multicast:
  - RIPv1 : Sends routing updates using broadcast (255.255.255.255). This can lead to ~~ex~~ excessive traffic on the network, as all devices receive the updates, even if they are not running RIP.

* Support for VLSM and CIDR:
  - RIPv1 : Does not support VLSM or CIDR
  - RIPv2 : Supports VLSM and CIDR.

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
TIRUCHIRAPPALLI CAMPUS

5. ALOHA Protocol :-

ALOHA is a simple communication Protocol used for medium access control (MAC) in a shared network. It was developed to allow multiple devices to transmit data over a shared communication channel without a central controller. The key purpose of ALOHA is to manage access to the shared medium and reduce collisions, where multiple devices try to transmit simultaneously.

Types of ALOHA :-

* Pure ALOHA :
  - In Pure ALOHA, a device can transmit data at any time without checking whether the channel is free. This increases the chance of collisions, as two or more devices may transmit simultaneously.
  - when a collision occurs, the affected devices wait for a random back off period before trying to retransmit.

* Slotted ALOHA :- Device can only transmit at the beginning of a time slot
* maximum theoretical efficiency of 36.8%.

6. CSMA Protocols:-

Carrier sense multiple Access (CSMA) is a network access protocol used to minimize collisions in a shared communication channel. In CSMA, a device "listens" to the channel before transmiting data to check if it is currently free. If the channel is idle, the devices transmits; if it is busy, the device waits until it becomes free.

* 1-Persistent CSMA:

- In 1-Persistent CSMA, a device continuosly monitors the channel and transmits as soon as it becomes idle, with a Probability of 1

* Non-Persistent CSMA:

- a device checks the channel before transmitting. It waits for a random amount of time before rechecking the Channel.

* P-Persistent CSMA:

- The Protocol is used in time-slotted networks. It transmits with a probability of 'p' in the current time slot or it desers the transmission to the next time slot with a Probability of '1-p'

7. Stop and wait ARQ Protocol:

Stop and wait Automatic repeat Request (ARQ) is a fundamental error control Protocol used in data communication to ensure reliable data transmission. It operates by sending one frame at a time and waiting for an acknowledgment (ACK) from the receiver before sending the next frame. Here's how it works.

1. Basic Working mechanism:

- In the stop-and-wait ARQ Protocol, the sender transmits a single data frame to the receiver.
- After sending the frame, the sender waits for an acknowledgment (ACK) from the receiver, confirming that the frame was received correctly.

2. Handling Lost or Corrupted:

- If the ACK is not received within a specified timeout Period, the sender assumes the frame was either lost or corrupted during transmission.

3. Error Detection:

- To detect transmission errors, mechanisms like checksums or cyclic redudancy checks (CRC) are used.

8. Sliding window Protocol :-

The sliding window Protocol is a flow control and error control technique used in data communication to manage the transmission of multiple frames between a sender and a receiver. It allows for efficient use of network resources by sending multiple frames before needing an acknowledgment for the first one.

- working mechanism:
  -> The Protocol uses a window size that determines the number of frames the sender can transmit without waiting for an acknowledgment.
  -> The sender maintains a window of frames, which represents the frames that have been sent but not yet acknowledged.

- Flow control :-
  -> The receiver also has a window size, which indicates the number of frames it can receive and buffer before sending an acknowledgment.

- Error-Control :-
  -> The sliding window Protocol incorporates mechanisms to handle errors using acknowlegments and retransmissions

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
TIRUCHIRAPPALLI CAMPUS

9. Single-Bit Parity:-

Single-bit Parity is a simple error detection mechanism that adds an extra bit to a binary data unit to ensure that the total number of 1s in the data is either odd or even.

Types of Parity:

- Even Parity: The Parity bits is set such that the total number of 1s in the data is even.
- odd Parity: The Parity Parity bit is set so that the total number of 1s is odd.

How it detects Errors:-

when data is transmitted, the Sender calculates the parity and sends it along with the data. Upon receiving the data, the receiver recalculates the parity. If the calculated parity does not match the received parity bit, an error is detected.

Ex:-

- original data: 1011001
  -> Even Parity, since there are 4 ones, the Parity will be 0
- Transmitted data: 10110010
- received data : 10110011

10. Checksum method :-

The checksum method is an error detection technique used in data transmission where a value is calculated from the data being sent. This value is then transmitted along with the data. The receiver performs the same calculation to verify the integrity of the data.

- Data segmentation: The data is divided into equal-sized segments
- checksum calculation: The values of these segments are summed to create a checksm. Depending on the protocol, the checksum might be calculated by taking the one's complement or two's complement of the sum.
- transmission : The original data along with the computed checksum is sent to the receiver.
- verification :-

Upon receiving the data, the receiver recalculates the checksum from the received data segments and compares it to the received checksum. If they match, the data is considered error-free; if not, an error is dected.

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
TIRUCHIRAPPALLI CAMPUS

11. Cyclic Redundancy check (CRC)

Cyclic Redundancy check (CRC) is an error-detecting code used to detect accidental changes to raw data in digital networks and storage devices. It is based on Polynomial division and is widely used in network communications, file storage, and other applications where data integrity is critical.

How CRC works:

*. Polynomial Representation:

- Data is treated as a Polynomial. Each bit of data represents a coefficient of a Polynomial, where the power of each term corresponds to the bit's position.

* Generator Polynomial:

- A Predefined Polynomial is used for division. This Polynomial is chosen based on the application and the level of error detection required.
- Augmented data is divided by the generator Polynomial using binary division.
- The original data and the CRC remainder are sent together. The CRC acts as a checksum.

12. Hamming Code:-

Hamming code is an error-detection and error-correction code the can detect up to two-bits errors or correct one-bit errors in data transmission. It was developed by Richard Hamming in the 1950's and is widely used in computer memory and communication systems.

Hamming code uses a series of Parity bits added to the data bits to form a codeword. The positions of the Parity bits are powers of two and they are used to check the bits in specific positions.

$$2^n \geq k + r + 1$$

Here, k is the number of bits, and r is the number of Parity bits.

- Position the data Parity Bits:-

  -> The Parity bits are placed in positions that are powers of 2, and the data bits are placed in the remaining positions.

- calculate Parity Bits:-

  -> Each Parity bit covers a specific set of bits. The Parity is calculated such that the total number of 1s in the bits covered by the Parity bit is even.

13. Open Shortest Path first (OSPF) protocol.

OSPF is a link-state routing protocol used in Internet networks to determine the best path for data transmission. It is defined in several RFCs, with the most notable being RFC 2328. OSPF is designed to efficiently manage routing within large and complex networks.

Key features of OSPF:-

* Link-state Protocol:- OSPF is a link-state Protocol, meaning it maintains a complete view of the network topology.

* Hierarchical Structure: OSPF uses a hierarchical design with areas. The backbone area is the central part of an OSPF network, and other areas connect to it, allowing for scalability and efficient routing.

* Dijkstra's Algorithm:-
OSPF use dijkstra's algorithm to calculate the shortest path to each destination

in the network. This ensures that routers can quickly determine the most efficient route for data transmission.

* Fast convergence:
  * OSPF quickly adapts to changes in the network, such as link failures or new routes, minimizing downtime and ensuring reliable data transmission.

14. Border Gateway Protocol (BGP)

The Border Gateway Protocol is a standardized exterior gateway protocol used to exchange routing information between autonomous systems (ASes) on the Internet. It is defined in several RFCs, with RFC 4271 being the most widely referenced. BGP is crucial for the functioning of the global Internet, enabling different networks to communicate and exchange routing information.

15. Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol designed to provide efficient and scalable routing within an autonomous systems (AS). EIGRP is classified as an advanced distance-vector protocol, combining features of both distance-vector and link-state routing protocols. It was developed to overcome the limitations of its predecessor, the Interior Gateway Routing Protocol (IGRP).

- Dual Algorithm :-

→ EIGRP uses the Diffusing update Algorithm to calculate shortest path to a destination. DUAL ensures loop-free routes and allows for rapid convergence when the network topology changes reducing the time it takes for routers to update their routing to update their routing tables.

16. IPv6:

- An IPV6 address is a 128-bit identifier for a network interface, expressed as eight groups of four hexadecimal digits, separated by colons. Each group represents 16 bits of the address.

ex: 2001:0db8:0000:0042:0000:8a2e:0370:7334

-> It has 128 bits (16 bytes)

-> Hexadecimal with colns

ex: 2001:0b8:0000:0042

-> Approximately 3.4 undecillion addresses.

-> More complex header, designed for efficiency and extensibility

-> No broadcast; Uses multicast instead

-> Stateless Address Autoconfiguration (SLAAC) and DHCPV6.

-> IPSec is mandatory.

17. TO Ken ring:-

A token ring network is a type of local area network (LAN) that uses a token-passing protocol for communication between devices. Developed by IBM in the 1980s, token ring networks operate in a physical star or logical ring topology and are known for their predictable performance and collision-free communication.

-> Token Passing:

- In a token ring network, devices are connected in a logical ring. A special control packet called a "token" circulates around the network. only the devices holding the token can transmit data. This ensures that there are no collisions during data transmission.

-> Accessing the Network:

- when a device wants to send data, it must wait until it receives the token. once it has the token, it can send its the network. The token is then passed to the next device in the ring.

18. Comparison of Static and Dynamic routing:

Routing protocols are essential for directing data packets through a network. Static and dynamic routing are two primary methods used for this purpose, each with its advantages and disadvantages.

Static routing:-

Static routing involves manually configuring routing tables on routers. The network administrator specifies the paths for data packets, and these paths remain constant unless manually changed.

-> manual configuration, simplicity, no overhead, predictable performance.

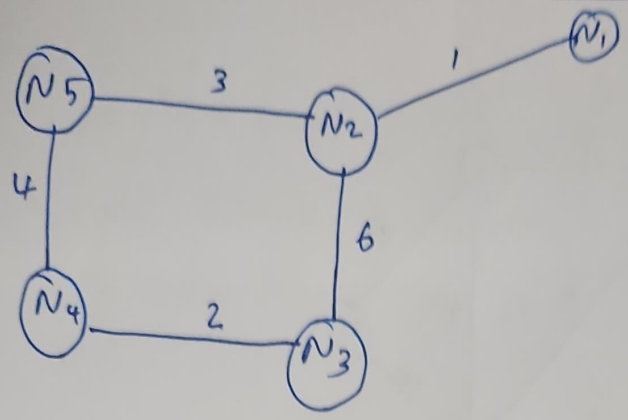
Dynamic routing:-

Dynamic routing uses protocols that automatically adjust routing tables based on network conditions and topology changes. Routers communicate with each other to exchange routing information.

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

TIRUCHIRAPPALLI CAMPUS

1.



As soon as N_2-N_3 reduces to 2, both N_2 and N_3 instantly updates their distance to N_3 and N_2 to 2 respectively.

So, N_2 : (1, 0, 2, 7, 3) , N_3 : (7, 2, 0, 2, 6) becomes this.

After this starts first round of update in which each node shares its table with their respective neighbors ONLY.

N1 : (0, 1, 7, 8, 4),

N_2 : (1, 0, 2, 7, 3),

N3 : (7, 2, 0, 2, 6),

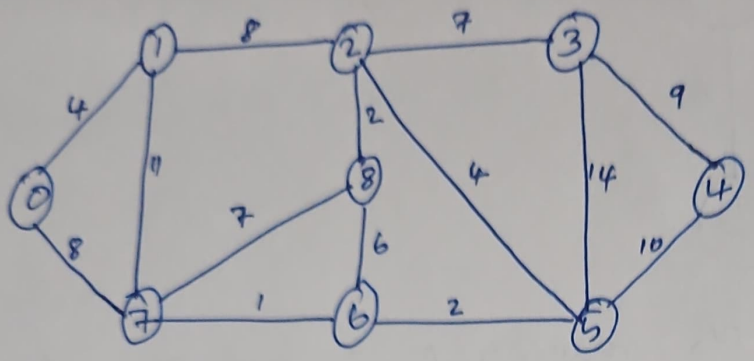
N_4 : (8, 7, 2, 0, 4),

N_5 : (4, 3, 6, 4, 0).

SEE at this time all the entries are old Except in N_2 and N_3 where value changes to 2 instead of 6.

N_3 receives tables from N_2 : (1, 0, 2, 7, 3) and N_4 (8, 7, 2, 0, 4). using this only original N_3 (7, 2, 0, 2, 6) updates to N_3 (3, 2, 0, 2, 5).

2.



The given graph does not contain any negative edge.

Examples:

Input: Src=0, The graph isShown below.

Output: 0 4 12 19 21 11 9 8 14

Explanation: The distance from 0 to 1 = 4

The minimum distance from 0 to 2 = 12. 0 -> 1 -> 2

The minimum distance from 0 to 3 = 19. 0 -> 1 -> 2 -> 3

The minimum distance from 0 to 4 = 21. 0 -> 7 -> 6 -> 5 -> 4

The minimum distance from 0 to 5 = 11. 0 -> 7 -> 6 -> 5

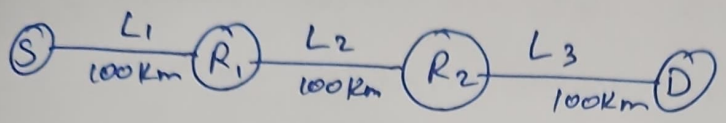
The minimum distance from 0 to 6 = 9. 0 -> 7 -> 6

The minimum distance from 0 to 7 = 8. 0 -> 7

The minimum distance from 0 to 8 = 14. 0 -> 1 -> 2 -> 8

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
TIRUCHIRAPPALLI CAMPUS

3.



TP from S to R_1 = Distance / Link Speed = 105/108 = 1ms

Total Propogation delay to travel from S to D

= 3 * 1 ms = 3ms

Total transmission delay for 1 Packet

= 3 * Number of Bits / Bandwidth

=> 3 * (1000/106)

= 3 ms.

The first packet will take 6ms to reach D. While first Packet was reaching D, other packets must have been processing in parallel. So D will receive remaining packets 1 Packet per 1ms from R2. So remaining 999 Packets will take 999ms.

so, 999+6 = 1005 ms

Propagation time = $\frac{100Km}{10^8 m/s}$ = 1 milli second

transmission time for a Packet = $\frac{1000 \text{ bits}}{10^6 \text{ bits/sec}}$ = 1 milli second.

1ms (Ts at Sender) + 1m (TP from Sender to R_1) + 1ms (T_2 at R_1) + 1m (TP from R_1 to R_2) + 1ms (T_2 at R_2) + 1ms (TP from R_2 to destination) = 6 ms

=> 1000 = 6ms + 999ms => 1005 ms.

4. Consider a CSMA/CD network that transmits data at a rate of 100 mbPS cable with no repeaters. If the minimum frame size required for this network is 1250 bytes, what is the signal speed (km/sec) in the cable?

B = 10^8 bits/sec

d = 1km

Round trip distance = 2km

$\therefore \frac{1250 \times 8}{10^8} = \frac{2}{\text{speed}}$

$\therefore \text{speed} = \frac{2 \times 10^8}{10^4} = 2 \times 10^4$

5. Frame size S >= 2BL/P

Where,

Cable length L = 1km = 1000 m

Propagation speed P = 2×10^8 m/sec

Bandwidth = 1 GbPS = 10^9 bps.

See this for details of above formula

S >= (2 * 10^9 * 1000) / (2×10^8)

= 10000 bits

10 4bits/8 = 1250 bytes.

6. In general sliding window ARQ scheme, the sending process sends a number of frames without worrying about receiving an ACK packet from the receiver. The sending window size in general is N and receiver window is 1. This means it can transmit N frames to its peer before receiving an ACK. The receiver keeps track of the sequence number with each ACK it sends. But in case of the question the sender window size is N and receiver is M so the receiver will accept M frames instead of 1 frame in general. Thus sending M sequence numbers attached with the acknowledgement. Hence, for such a scheme to work properly we will need a total of M + N distinct sequence numbers.