IT 694 Computer Networks: ***Solution***

Final Examination, Last Year

Que.1: briefly describe ARP protocol? why is an ARP query sent within broadcast frame? why is an ARP response sent within frame with specific destination MAC address?

Answer: ARP protocol is a network protocol that is used to find the MAC address of a device from its known IP address. It works by sending requests and responses over the network.

An ARP request is sent within a broadcast frame because the sender does not know the MAC address of the receiver, so it needs to ask all devices on the network. The broadcast frame has a special MAC address of FF: FF:FF:FF:FF:FF that means it is for everyone.

An ARP response is sent within a unicast frame with a specific destination MAC address because the receiver knows the MAC address of the sender, so it can reply directly to it. The unicast frame has the MAC address of the sender as the destination address. The response contains the MAC address of the receiver, which the sender can use for future communication.

Que.2: we discussed an outline of derivation of the efficiency of slotted ALOHA. For N active nodes, and probability of transmission p, derive the expression for efficiency. Find the value of p that maximize the expression. What is this expression as N approaches infinity?

Answer: Slotted ALOHA is a random access protocol used in computer networks to allow multiple nodes to transmit data over a shared channel. The efficiency of Slotted ALOHA is defined as the fraction of slots in which successful transmissions occur.

For N active nodes, the probability that a node transmits successfully in a given slot is p(1-p)^(N-1). The first term p represents the probability that the node transmits in the slot, while the second term (1-p)^(N-1) represents the probability that the other N-1 nodes do not transmit in the same slot.

The probability that a slot is successful is the probability that exactly one node transmits in that slot. Therefore, the probability of success is Np(1-p)^(N-1).

The efficiency is then given by the ratio of the number of successful transmissions to the total number of slots:

Efficiency = Np(1-p)^(N-1) / N = p(1-p)^(N-1)

To find the value of p that maximizes the efficiency, we can take the derivative of the expression for efficiency with respect to p and set it to zero:

d/dp (p(1-p)^(N-1)) = (1-p)^(N-1) - Np(N-1)(1-p)^(N-2) = 0

Simplifying and solving for p, we get:

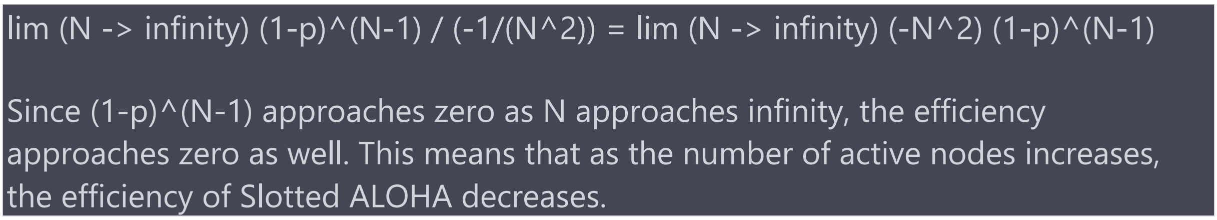
p = 1/N

This means that the maximum efficiency occurs when the probability of transmission is equal to 1/N.

As N approaches infinity, we can use the limit to find the expression for efficiency:

lim (N -> infinity) p(1-p)^(N-1)

Using L'Hopital's rule, we can take the derivative of the numerator and denominator with respect to N:



lim (N -> infinity) (1-p)^(N-1) / (-1/(N^2)) = lim (N -> infinity) (-N^2) (1-p)^(N-1)

Since (1-p)^(N-1) approaches zero as N approaches infinity, the efficiency approaches zero as well. This means that as the number of active nodes increases, the efficiency of Slotted ALOHA decreases.

Que 3: Briefly describe the routing protocol based on (a) DV-distance vector and (b) LSP - Link state packets. Give a reason Why LSP based protocol is preferred over DV in the internet.

Answer: Routing protocols are used to determine the best path for data packets to travel through a network. There are two common types of routing protocols: Distance Vector (DV) and Link State Packet (LSP).

(a) DV (Distance Vector) Protocol:

In the Distance Vector protocol, each node maintains a table that contains information about its own neighbors and the distances to all other nodes in the network. Periodically, each node sends its table to its neighbors, and each node updates its own table based on the information received from its neighbors. This process continues until all the tables in the network converge.

Advantages:
- Simple to implement and configure
- Uses less bandwidth as it only needs to transmit the distance vectors.

Disadvantages:
- Slow convergence, as each node has to wait for its neighbors to update their tables before it can update its own table.
- The network can become unstable, as the distance vectors can oscillate and create loops.
- The protocol does not take into account the quality of the link between two nodes.

(b) LSP (Link State Packet) Protocol:

In the Link State Packet protocol, each node maintains a complete map of the network, which includes the node's ID, its neighbors, and the quality of the links to its neighbors. Each node floods the network with its own link state information, which is used by all nodes to calculate the shortest path to each destination node.

Advantages:
- Faster convergence, as each node has a complete map of the network and can immediately calculate the shortest path to each destination node.
- More accurate, as it takes into account the quality of the link between two nodes.
- The protocol is more stable, as it uses a shortest-path algorithm that guarantees a loop-free topology.

Disadvantages:
- Uses more bandwidth, as each node needs to transmit its own link state information.
- Requires more memory and processing power to maintain the map of the network.

Why LSP based protocol is preferred over DV in the internet:

In the internet, the LSP protocol is preferred over the DV protocol for several reasons. The internet is a large and complex network, with many nodes and links. The DV protocol can suffer from slow convergence and instability, which can lead to network failures. The LSP protocol, on the other hand, is more stable and can handle larger networks with more nodes and links. It also provides more accurate and efficient routing, as it takes into account the quality of the link between two nodes.

Moreover, the LSP protocol is better suited to handle network changes, such as link failures or node failures. When a link fails in the network, the LSP protocol can quickly update the map and calculate the shortest path to each destination node. The DV protocol, on the other hand, can take longer to converge and can potentially create loops in the network.

In summary, the LSP protocol is preferred over the DV protocol in the internet because it is more stable, efficient, and can handle larger and more complex networks with greater accuracy.

Que 4: Router switching element to forward packets. Describe switching via (a) Memory, (b) bus, and (c) interconnection network. How do these how these architectures compare to each other? - Give Reasons

Answer: Switching is the process of forwarding packets from the input ports of a router to the output ports based on the destination address in the packet header. There are different types of switching architectures, including memory-based, bus-based, and interconnection network-based switching.

(a) Memory-Based Switching:
In memory-based switching, incoming packets are stored in the router's memory, and the forwarding decision is made by the router's CPU. The CPU looks up the destination address in the packet header and searches the router's forwarding table to find the appropriate output port. The packet is then copied from the memory to the output port. Memory-based switching is simple and inexpensive, but it is not suitable for high-speed networks because the CPU processing time is slow.

(b) Bus-Based Switching:
In bus-based switching, the incoming packets are buffered in the input ports of the router. The forwarding decision is made by a shared bus that connects all the input and output ports of the router. When a packet arrives at an input port, it is placed in a buffer, and the forwarding decision is made by the shared bus. The packet is then forwarded to the output port determined by the bus. Bus-based switching is fast and can handle high-speed networks, but it is expensive and can suffer from congestion due to the shared bus.

(c) Interconnection Network-Based Switching:
Interconnection network-based switching uses a network of switches to forward packets from input ports to output ports. The switches are interconnected to form a network, and the forwarding decision is made by the switches based on the destination address in the packet header. The switches can be programmed to implement different forwarding algorithms, such as shortest path routing or load balancing. Interconnection network-based switching is fast, scalable, and can handle high-speed networks, but it is also expensive and requires complex routing algorithms.

Comparison of Switching Architectures:
Memory-based switching is simple and inexpensive, but it is not suitable for high-speed networks. Bus-based switching is fast and can handle high-speed networks, but it is expensive and can suffer from congestion due to the shared bus. Interconnection network-based switching is fast, scalable, and can handle high-speed networks, but it is also expensive and requires complex routing algorithms. Therefore, the choice of switching architecture depends on the network requirements, such as speed, cost, and scalability.

Que.5: Many Organization provide NAT protocol to provide outward connectivity to a large number of internal nodes even though they have only few global ip addresses. Using a clear example, explain the working of NAT

Answer: Network Address Translation (NAT) is a protocol used to enable communication between networks with overlapping IP addresses by mapping private IP addresses to public IP addresses. It allows a single public IP address to be used for multiple private devices within a network, thus conserving public IP addresses.

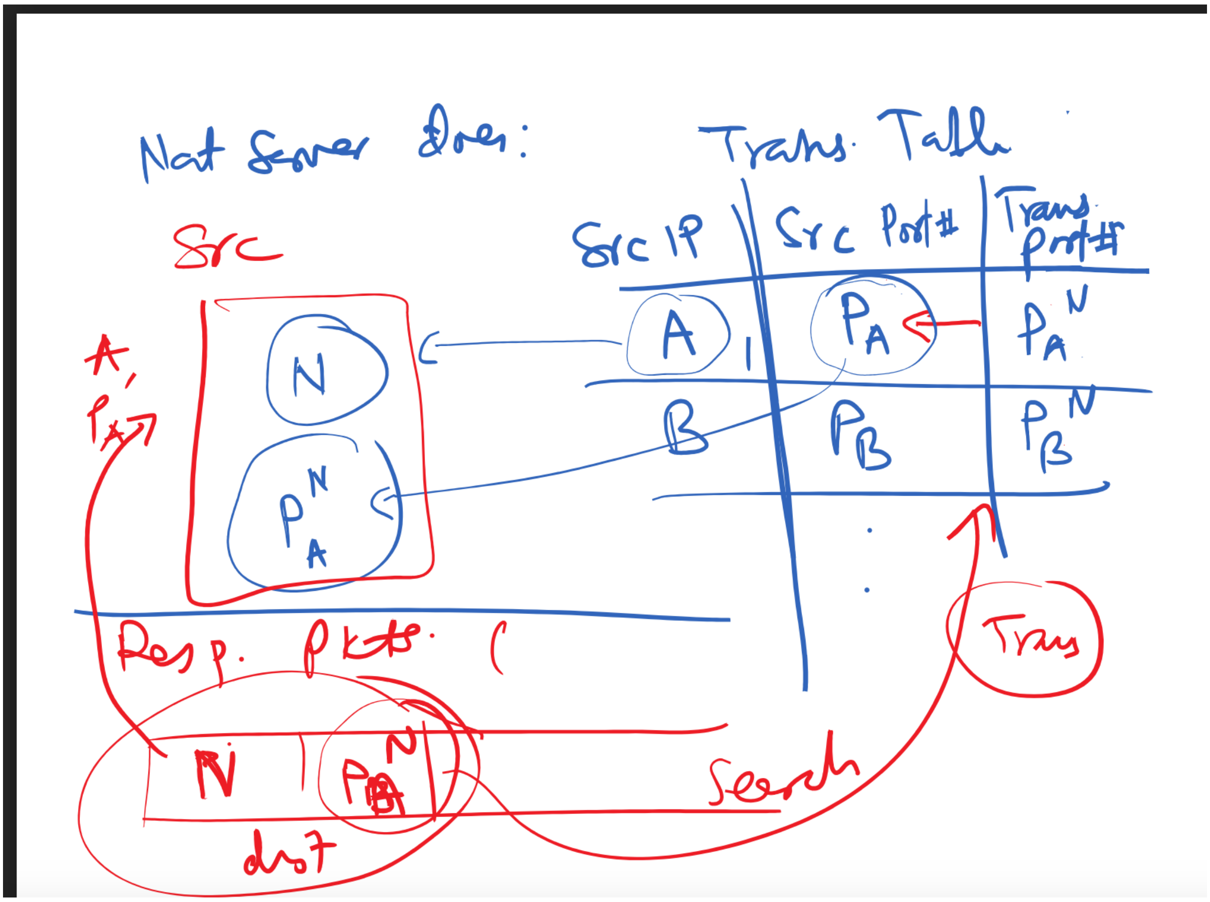
Let's consider an example of a company that has a private network consisting of several computers and devices with private IP addresses (e.g., 192.168.1.x). This network is connected to the internet via a router that has a single public IP address provided by the Internet Service Provider (ISP).

When a computer from the private network wants to access a website on the internet, it sends a request to the router with its source IP address, which is a private IP address. The router then changes the source IP address of the request to its own public IP address and forwards the request to the internet. The website responds to the router's public IP address, and the router receives the response. It then changes the destination IP address of the response from its public IP address to the private IP address of the requesting computer and forwards the response to that computer.

Here's a diagram to illustrate the process:

```
+-------------+    Private network with private IP addresses (e.g., 192.168.1.x)
|   Computer  |
+-------------+
      |
      |  Request with private IP source address
      V
+-------------+    Router with public IP address provided by ISP
|    Router   |
+-------------+
      |
      |  Request with public IP source address
      V
+-------------+    Internet
|   Website   |
+-------------+
      |
      |  Response with public IP destination address
      V
+-------------+    Router with public IP address provided by ISP
|    Router   |
+-------------+
      |
      |  Response with private IP destination address
      V
+-------------+    Private network with private IP addresses (e.g., 192.168.1.x)
|   Computer  |
+-------------+
```

This process allows the private network to access the internet with a single public IP address, as the router changes the IP addresses of the requests and responses as they pass through it. This way, a large number of internal nodes can have outward connectivity even though there are only a few global IP addresses available.



Que 6: Show the main fields in TCP and Briefly Describe these main fields. How does TCP manage connection between two nodes? Use diagram to show establishments and termination of connections.

Answer: TCP (Transmission Control Protocol) is a reliable transport layer protocol used in the Internet Protocol (IP) suite. It provides a connection-oriented communication between two hosts over an IP network. TCP breaks the data into segments, sends them to the destination, and reassembles them in the correct order at the receiving end. The main fields in a TCP header are:

- Source and destination port numbers: These fields identify the endpoints of the connection.
- Sequence number: This field is used to keep track of the number of bytes sent in each segment, and to acknowledge the receipt of data.
- Acknowledgment number: This field acknowledges the receipt of data and specifies the next expected sequence number.
- Data offset: This field specifies the size of the TCP header.

- Control flags: These are bits that control the behavior of the TCP protocol, such as SYN, ACK, FIN, RST, URG, and PSH.
- Window size: This field specifies the amount of data that the sender is willing to accept before receiving an acknowledgment from the receiver.
- Checksum: This field is used to detect errors in the TCP segment.
- Urgent pointer: This field indicates the urgent data in the segment.

TCP **manages connections** between two nodes using a three-way handshake process. The handshake process is used to establish a connection between two hosts and is initiated by the sender. The process involves the following steps:

1. SYN: The sender sends a SYN (synchronize) segment to the receiver, indicating its initial sequence number.

2. SYN-ACK: The receiver sends a SYN-ACK (synchronize-acknowledge) segment to the sender, acknowledging the receipt of the SYN and indicating its own initial sequence number.

3. ACK: The sender sends an ACK (acknowledge) segment to the receiver, acknowledging the receipt of the SYN-ACK and indicating its next sequence number.

Once the connection is established, data transfer can begin. When the data transfer is complete, a four-way handshake process is used to **terminate** the connection. The process involves the following steps:

1. FIN: The sender sends a FIN (finish) segment to the receiver, indicating that it has finished sending data.

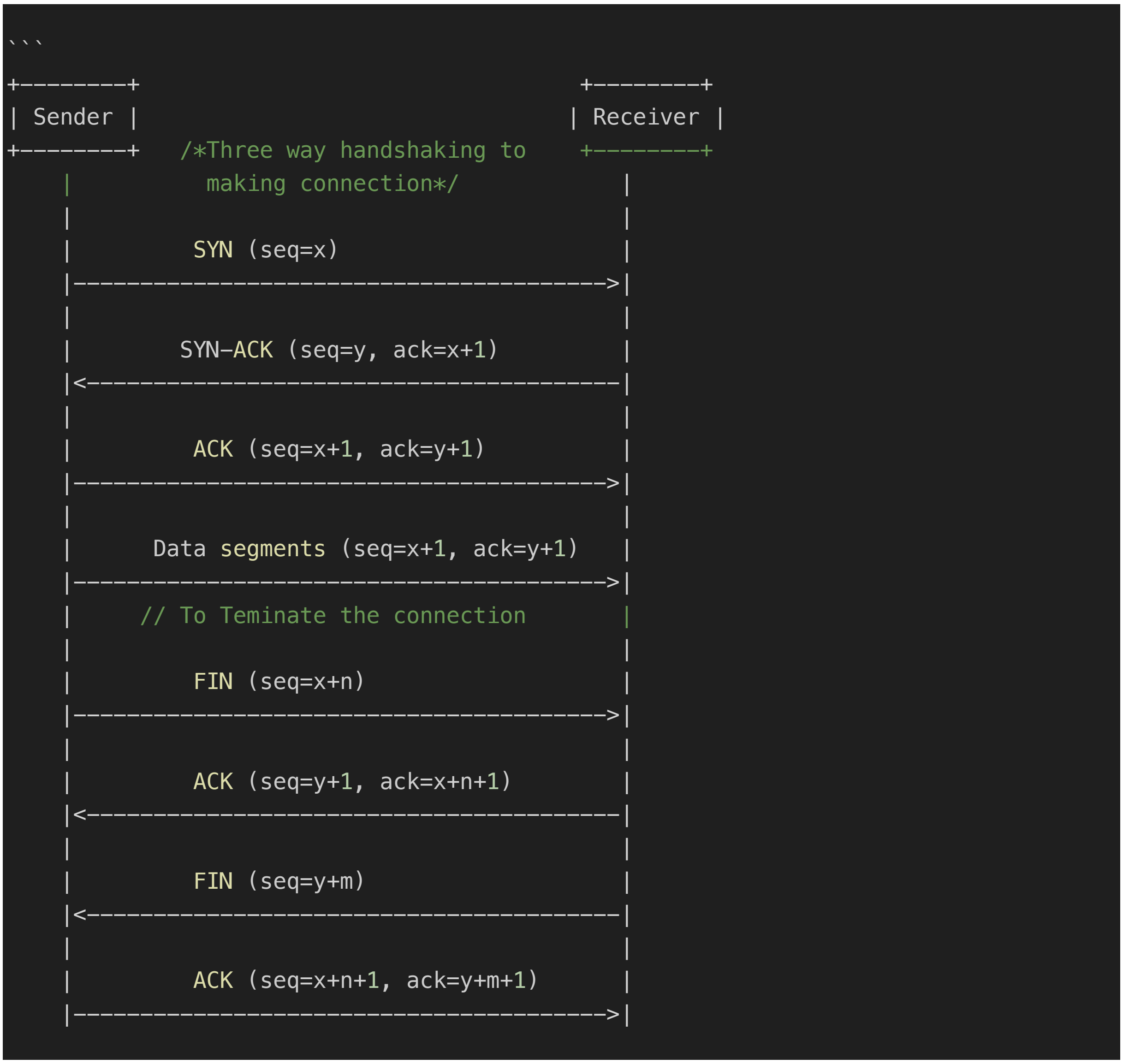
2. ACK: The receiver sends an ACK (acknowledge) segment to the sender, acknowledging the receipt of the FIN.

3. FIN: The receiver sends a FIN segment to the sender, indicating that it has finished sending data.

4. ACK: The sender sends an ACK segment to the receiver, acknowledging the receipt of the FIN.

The connection is terminated once both hosts have sent and received FIN and ACK segments.

The diagram below illustrates the establishment and termination of a TCP connection between two nodes:



~~~
```
+---------+                                +---------+
| Sender |                                | Receiver |
+---------+  /*Three way handshaking to    +---------+
    |          making connection*/            |
    |                                         |
    |         SYN (seq=x)                     |
    |---------------------------------------->|
    |                                         |
    |        SYN-ACK (seq=y, ack=x+1)         |
    |<----------------------------------------|
    |                                         |
    |         ACK (seq=x+1, ack=y+1)          |
    |---------------------------------------->|
    |                                         |
    |      Data segments (seq=x+1, ack=y+1)   |
    |---------------------------------------->|
    |     // To Teminate the connection       |
    |                                         |
    |         FIN (seq=x+n)                   |
    |---------------------------------------->|
    |                                         |
    |         ACK (seq=y+1, ack=x+n+1)        |
    |<----------------------------------------|
    |                                         |
    |         FIN (seq=y+m)                   |
    |<----------------------------------------|
    |                                         |
    |         ACK (seq=x+n+1, ack=y+m+1)      |
    |---------------------------------------->|
~~~

Que 7 & 8: Do it yourself