Homework 4

CH4 homework

Please complete these and submit to e-learning. All must be handwritten. Write, scan as pdf, submit.

1. Within this chapter, name a layer-3 device. **Router**
2. Why is that device in Q1 called a layer-3 device? **Because it only checks information (decapsualte) up to layer 3, to get the destination address.**
3. Explain the 2 main functions of the network layer.

   To move packets from a sending host to a receiving host, the network-layer uses 2 important functions ➔Forwarding & Routing

   - **Forwarding ➔ the transfer of a packet from an incoming link to an outgoing link within a *single router***
   - **Routing ➔ interactions all of a network's routers (via routing protocols/algorithms) to determine the best paths to destination node.**

```
     172.16.0.0/16 is variably subnetted, 8 subnets, 3 masks
O       172.16.224.0/23 [110/65] via 172.16.230.5, 00:00:13, Serial2/0
O       172.16.226.0/23 [110/129] via 172.16.230.5, 00:00:13, Serial2/0
C       172.16.228.0/24 is directly connected, FastEthernet1/0
O       172.16.229.0/24 [110/65] via 172.16.230.14, 00:00:13, Serial3/0
O       172.16.230.0/30 [110/128] via 172.16.230.5, 00:00:13, Serial2/0
C       172.16.230.4/30 is directly connected, Serial2/0
C       172.16.230.8/30 is directly connected, FastEthernet0/0
C       172.16.230.12/30 is directly connected, Serial3/0
```

Figure 1

4. Figure 1 shows a forwarding table of a router. Refer to Figure 1 to answer the following questions.
   a. What routing algorithm is being used here? **OSPF**
   b. Can you tell how many subnets are in the network topology from the information on the routing table? How many? **8 subnets**
   c. If a packet with a destination address of 172.16.227.123 arrives at the router, which output port will it be sent to? **Serial2/0**
   d. If a packet with a destination address of 172.16.231.2 arrives at the router, which output port will it be sent to? **None, it will be dropped.**
5. If an IP address (200.20.226.5/21) is given, find the subnet's network and broadcast address. Show your workings. **NA = 200.20.224.0, BA = 200.20.255.255**
6. Organization is given network address 188.192.192.0/22. Subnet using VLSM for 5 departments A (100 hosts), B (210 hosts), C (80 hosts), D (40hosts), E (10 hosts). All hosts mentioned here are usable host.
   a. Show your workings clearly and present final results in a subnet addressing table.**Note: table header shown below.*
   b. Calculate all the unused hosts in each subnet.

Subnet	Hosts Needed	Hosts Available	Unused hosts	Network Address	Subnet Mask (Slash format)	Subnet Mask (dotted decimal format)	Usable address Range	Broadcast

The network 188.192.192.0/22 has 1022 hosts.
Your subnets need 440 hosts.

NAME	HOSTS NEEDED	HOSTS AVAILABLE	UNUSED HOSTS	NETWORK ADDRESS	SLASH	MASK	USABLE RANGE	BROADCAST
2	210	254	44	188.192.192.0	/24	255.255.255.0	188.192.192.1 - 188.192.192.254	188.192.192.255
1	100	126	26	188.192.193.0	/25	255.255.255.128	188.192.193.1 - 188.192.193.126	188.192.193.127
3	80	126	46	188.192.193.128	/25	255.255.255.128	188.192.193.129 - 188.192.193.254	188.192.193.255
4	40	62	22	188.192.194.0	/26	255.255.255.192	188.192.194.1 - 188.192.194.62	188.192.194.63
5	10	14	4	188.192.194.64	/28	255.255.255.240	188.192.194.65 - 188.192.194.78	188.192.194.79

7. With respect to DHCP, answer the following questions.
   a. What is DHCP? Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on IP networks to automatically assign IP addresses and other network configuration settings to devices (such as computers, smartphones, printers, etc.) on the network.
   b. How does DHCP works?

      DHCP Discovery (Client): A device (client) sends a broadcast message (DHCPDISCOVER) to find a DHCP server.

      DHCP Offer (Server): The DHCP server responds with an offer (DHCPOFFER) that includes an available IP address and other network settings.

      DHCP Request (Client): The client requests to lease the offered IP address by sending a DHCPREQUEST message to the server.

      DHCP Acknowledgment (Server): The server acknowledges (DHCPACK) the request, confirming the lease of the IP address and providing the configuration details.

   c. What is the benefit of DHCP?

      Simplifies network management.

      Reduces the risk of configuration errors.

      Supports dynamic changes in the network (e.g., adding new devices without manual intervention).

   d. When configuring DHCP, what portion of the subnetwork address is used for distribution?

When configuring DHCP, the portion of the **subnetwork address** that is used for distribution is the range of **usable IP addresses** within that subnet. This range **EXCLUDES**:

- **The Network Address**: This is the first address in the subnet, which identifies the subnet itself (e.g., in 192.168.1.0/24, the network address is 192.168.1.0).
- **The Broadcast Address**: This is the last address in the subnet, which is used to send broadcast messages to all devices within the subnet (e.g., in 192.168.1.0/24, the broadcast address is 192.168.1.255).
- In this subnet, the DHCP server can distribute IPs from 192.168.1.1 to 192.168.1.254, but the **administrator typically reserves certain IPs** for:
  i. Static IP addresses (e.g., for servers, printers, or routers).
  ii. Reserved IPs (e.g., for future expansion or specific devices).

e. What is the lease time for an IP address, and what happens when it expires? Additionally, what occurs if the lease expires while the host is still actively using the address?

The **lease time** is the duration for which a DHCP server assigns an IP address to a client. It defines how long the client can use the assigned IP address before it must either renew the lease or stop using it.

What Happens When the Lease Time Ends?

1. **If the Host is No Longer Active or Offline:**
   - The DHCP server reclaims the IP address.
   - The IP address is returned to the available pool and can be reassigned to another device.
2. **If the Host is Still Using the IP Address:**
   - The client must **renew the lease** before it expires to continue using the IP address. The renewal process is handled automatically by the DHCP client.

How DHCP Lease Renewal Works:

The lease renewal process occurs in stages:

1. **T1 Timer: Renewal Request (50% of Lease Time):**
   - When 50% of the lease time has passed, the DHCP client sends a **DHCPREQUEST** message directly to the DHCP server to renew the lease.
   - If the server responds with a **DHCPACK**, the lease is renewed, and the timer resets.

2. **T2 Timer: Rebinding (87.5% of Lease Time):**

   - If the client does not receive a response from the server at 50% (T1), it waits until 87.5% of the lease time has passed.
   - At this stage, the client broadcasts the **DHCPREQUEST** to all DHCP servers on the network, trying to renew the lease from any available server.

3. **Lease Expiration:**

   - If no response is received from the DHCP server(s) by the time the lease expires, the client must stop using the IP address.
   - The client will then start the DHCP process again (DORA: Discover, Offer, Request, Acknowledge) to obtain a new IP address.

8. With regards to Network Address Translation (NAT), answer the following questions.
   a. What is NAT? **Network Address Translation (NAT)** is a method used in networking to modify the IP address information in packet headers while in transit, allowing a single device (such as a router or firewall) to act as an intermediary between a local (private) network and the broader public internet. NAT is widely used to enable devices in a private network to share a single public IP address.
   b. What is the purpose of NAT?
   - **Conserve Public IP Addresses**: Private networks can use a single public IP address to connect multiple devices to the internet, reducing the need for a large number of public IPs.
   - **Improve Security**: Devices in the private network are not directly exposed to the public internet, as their private IPs are hidden behind the NAT device.
   - **Facilitate Communication**: Allows devices using private IP addresses (e.g., 192.168.0.0/24) to access resources on the public internet.
   c. How does NAT works?

   When a device inside a private network communicates with the internet, NAT performs the following:

   - **Translation of Private to Public IP**:
     - The NAT device replaces the private IP address (source) in outgoing packets with its own public IP address.
     - It keeps track of the translation in a table.
   - **Translation of Public to Private IP**:
     - When a response is received, NAT uses the table to map the public IP address back to the original private IP address and forwards the packet to the corresponding device.

9. Given N=5000, RTT = 150ms, C = 5Gbps, how much is average buffer size B?
   a. Following rule of thumb.
   b. Following recent recommendations.

Parameters:

- $N = 5000$ (number of flows)
- $RTT = 150\,\text{ms} = 0.15\,\text{s}$
- $C = 5\,\text{Gbps} = 5 \times 10^9\,\text{bits/sec}$

Part a. Following Rule of Thumb

The rule of thumb suggests that the buffer size B should be:

$$B = C \times RTT$$

Substituting the values:

$$B = (5 \times 10^9)\,\text{bits/sec} \times 0.15\,\text{sec}$$

$$B = 750 \times 10^6\,\text{bits} = 750\,\text{Mb}$$

So, the **average buffer size** following the rule of thumb is $750\,\text{Mb}$.

Part b. Following Recent Recommendations

Recent research (e.g., Data Center Networking) suggests using a buffer size proportional to $\frac{RTT \times C}{\sqrt{N}}$.
The formula is:

$$B = \frac{RTT \times C}{\sqrt{N}}$$

Substituting the values:

$$B = \frac{(5 \times 10^9) \times 0.15}{\sqrt{5000}}$$

First, calculate $\sqrt{5000}$:

$$\sqrt{5000} \approx 70.71$$

First, calculate $\sqrt{5000}$:

$$\sqrt{5000} \approx 70.71$$

Now compute B:

$$B = \frac{750 \times 10^6}{70.71}\,\text{bits}$$

$$B \approx 10.6 \times 10^6\,\text{bits} = 10.6\,\text{Mb}$$

So, the **average buffer size** following recent recommendations is $10.6\,\text{Mb}$.

10. If a file with a size 6000bytes is sent to destination through a link with and MTU of 1500bytes, explain the fragmentation process that happens here. ***Please use the fragmentation table as given in class.*

Fragmentation Process:

MTU and Fragment Size:

- MTU is the largest size of a packet that can be sent over the network without needing to be fragmented. Here, MTU = 1500 bytes.

- The size of the data that can be carried in each fragment is calculated by subtracting the IP header size (usually 20 bytes for IPv4) from the MTU:

$$\text{Fragment data size} = 1500 \text{ bytes} - 20 \text{ bytes} = 1480 \text{ bytes}$$

Number of Fragments Needed:

- The total file size is 6000 bytes. To determine the number of fragments, we divide the file size by the fragment data size:

$$\text{Number of fragments} = \left\lceil \frac{6000 \text{ bytes}}{1480 \text{ bytes}} \right\rceil = \lceil 4.05 \rceil = 5 \text{ fragments}$$

Fragmentation Details:

Fragment#	Bytes in fragment	ID	Offset	Flag (MF)
1	1480 bytes of data + 20 bytes IP header = 1500 bytes total	xx	0	1
2	1480 bytes of data	xx	185	1
3	1480	xx	370	1
4	1480	xx	555	1
5	Remaining 80 bytes of data	xx	740	0

Fragment Assembly:

At the destination, the fragments are reassembled based on the offset values to recreate the original 6000-byte file.

Summary:

- The file is fragmented into 5 parts to accommodate the MTU of 1500 bytes.

- Each fragment includes a 20-byte IP header.

- Fragments are sent with the appropriate offsets and are reassembled at the destination.

This ensures that the file can be transmitted over the network link despite the MTU limitation.

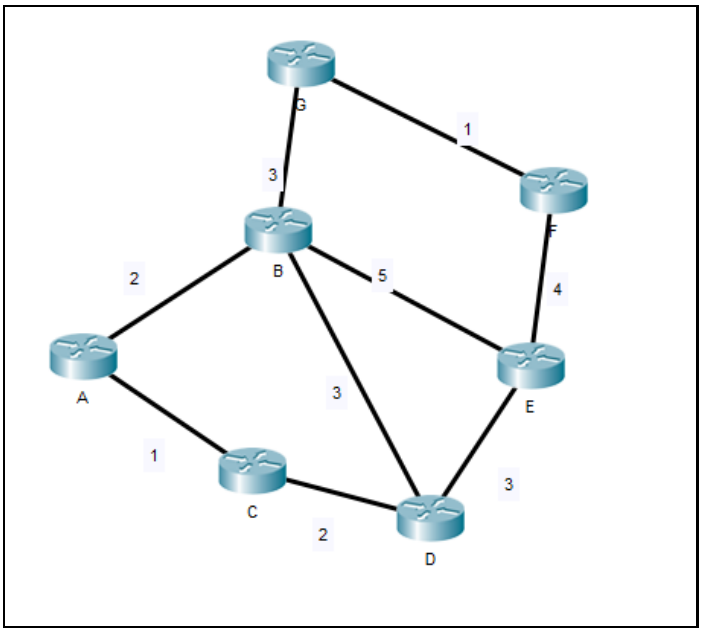


Figure 2

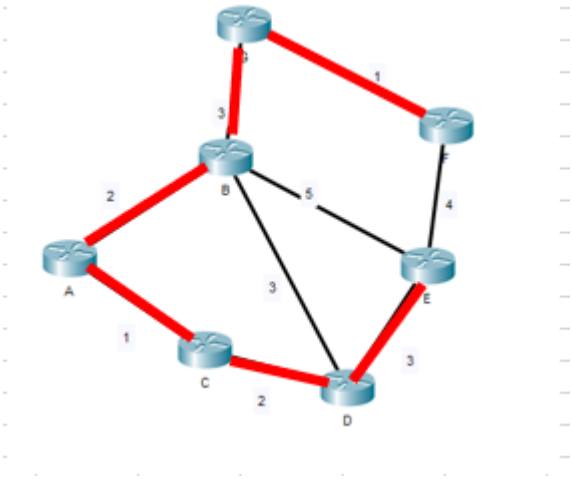
11. Given the network topology in Figure 2, answer the following questions. Show your workings.
    a. Create the forwarding table, using Djikstra algorithm (for Link State routing) for the source router A.

Construct least cost path table

	DJIKSTRA												
		Distance from A	Previous Router										
STEP	N'	D(B), p(B)		D(C), p(C)		D(D), p(D)		D(E), p(E)		D(F), p(F)		D(G), p(G)	
0	A	2	A	1	A	INF	INF	INF	INF	INF	INF	INF	INF
1	AC					3	C						
2	ACB							6	C			5	B
3	ACBD												
4	ACBDG									6	G		
5	ACBDGE												
6	ACBDGEF												

Forwarding table

DESTINATION	LINK
B	A-B
C	A-C
D	A-C
E	A-C
F	A-B
G	A-B



b. Create the forwarding table, using Bellman-Ford algorithm (for Distance Vector routing) for the source router A. **forwarding table here means for the whole network.*

BELLMAN-FORD - only directly connected

min of all path to V	cost to neighbor V from U	cost from neighbor v to dest. V

$d_A(B)$

DEST	BEST	c(A,B) + $d_B(B)$		c(A,C) + $d_C(B)$	
A to B	A-B	2	0	1	3
		2		4	

$d_A(C)$

DEST	BEST	c(A,B) + $d_B(C)$		c(A,C) + $d_C(C)$	
A to C	A-C	2	3	1	0
		5		1	

$d_A(E)$

DEST	BEST	c(A,B) + d_B(D)		c(A,C) + d_C(D)	
A to D	A-C	2	3	1	2
		5		3	

d_A(B)

DEST	BEST	c(A,B) + d_B(E)		c(A,C) + d_C(E)	
A to E	A-C	2	5	1	5
		7		6	

d_A(F)

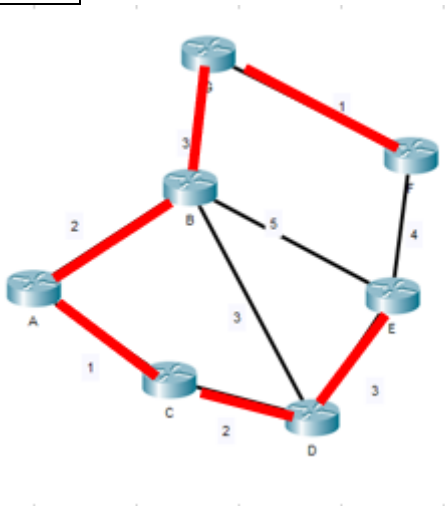
DEST	BEST	c(A,B) + d_B(F)		c(A,C) + d_C(F)	
A to F	A-B	2	4	1	9
		6		10	

d_A(G)

DEST	BEST	c(A,B) + d_B(G)		c(A,C) + d_C(G)	
A to G	A-B	2	3	1	6
		5		7	

Forwarding table

DESTINATION	LINK
B	A-B
C	A-C
D	A-C
E	A-C
F	A-B
G	A-B



12. Why was UDP chosen for SNMP instead of TCP? Explain your answer.

SNMP extras : Why UDP and not TCP?

The Simple Network Management Protocol (SNMP) was designed to facilitate the management and monitoring of network devices, such as routers, switches, servers, and more. The decision to use UDP (User Datagram Protocol) instead of TCP (Transmission Control Protocol) as the transport protocol for SNMP was made based on several considerations:

- **Lower Overhead**: UDP is a connectionless protocol with less overhead compared to TCP. It doesn't have the inherent reliability mechanisms such as acknowledgments, retransmissions, and flow control, which makes it lightweight. SNMP, being a protocol that primarily deals with small, non-critical messages (like status updates, queries, and notifications), can benefit from the reduced complexity and overhead offered by UDP.
- **Real-Time Monitoring**: SNMP often deals with real-time monitoring and data collection tasks. UDP's lack of handshaking and acknowledgment mechanisms means it operates faster and suits scenarios where immediate data retrieval is crucial. While UDP doesn't guarantee delivery, for SNMP, the periodic nature of data collection often mitigates the need for guaranteed delivery of every message.
- **Stateless Communication**: UDP is stateless, meaning each datagram is treated as an independent entity. This aligns well with SNMP's model, where each request-response cycle is independent. With SNMP, a manager sends a request (Get, Set, etc.), and the agent responds with the requested information. There is no need for maintaining a connection state between manager and agent, making UDP's stateless nature fitting for this purpose.
- **Efficiency in Certain Network Conditions**: In environments where occasional packet loss or less critical information transfer is acceptable, UDP can be more efficient. For example, in networks with low latency and low error rates, UDP can perform well without the overhead of TCP's reliability mechanisms.

However, it's essential to acknowledge that while UDP offers advantages in terms of simplicity and speed, it lacks the reliability features provided by TCP. SNMP versions, such as SNMPv3, have added security features like authentication and encryption, compensating for UDP's lack of inherent security.

--END - -