Assignment 3:Get ready to embark on this exhilarating treasure hunt. You have uncovered a magic ancient scroll that has the following crossword puzzle. Solve the crossword puzzle to find clues. These clues will then have to be used along with the Wireshark capture given to you to find mystical paths hidden on the Internet. There are totally 4 paths, each hidden with a treasure- which are questions on networking. If you answer these questions, you'll obtain the invaluable treasure of knowledge along with assignment points.

Objective 1: Complete the crossword puzzle below to retrieve the hints required to complete Objective 1. Use these hints to direct yourself to the paths containing the questions. These paths are hidden in the Wireshark file uploaded on canvas (assignment3_wireshark_capture.pcap). Use the hints from the crossword to retrieve the paths to your assignment questions.

Path 1: **[15 Points + 5 Extra Credit]** Hint: 14 Down

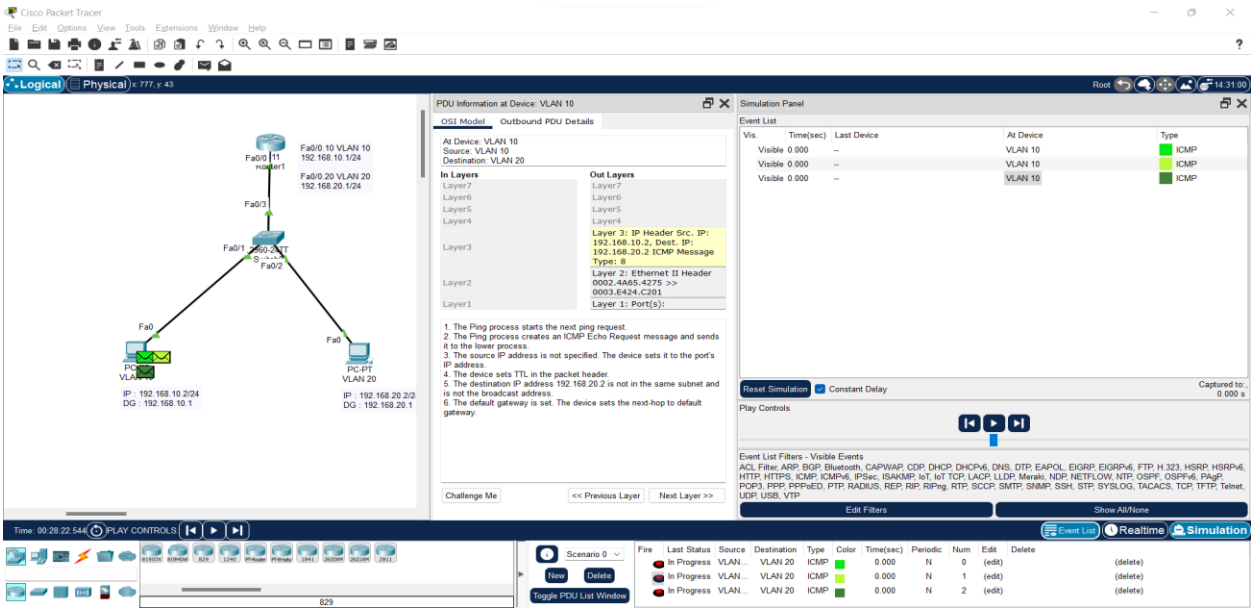
Question 1 : What needs to be done to establish communication between Host 1 in VLAN 10 and Host 2 in VLAN 20. Explain in detail about the steps involved. **[10 points]**

Step 1: Configure the host1 with 192.168.10.2/24, DG : 192.168.10.1. And host2 with 192.168.10.2/24, DG : 192.168.10.1

Step 2 : Configure the switch with VLAN 10, 20 and access port using the following commands

```
Switch(config)#vlan 10
Switch(Config)# #int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#end
```

```
Switch(config)#vlan 20
Switch(Config)# #int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
```



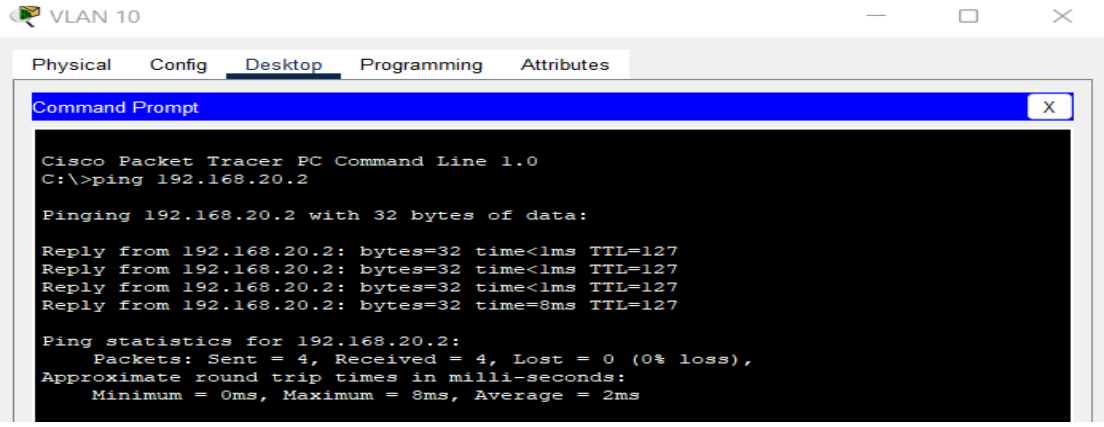
Step 3: Configure the Trunk port on Switch using the following command

```
Switch(config)#int fa0/3
Switch(config-if)#no shutdown
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#exit
```

Step 4: Configure the Router with sub-interfaces and encapsulation to allow the connectivity between VLAN 10 configured on Host1 and VLAN 20 configured on Host2

```
Router(config)#int fa0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed to up
Router(config-if)#exit
Router(config)#int fa0/0.10
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.10, changed
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#
Router(config)#int fa0/0.20
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.20, changed
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit
```

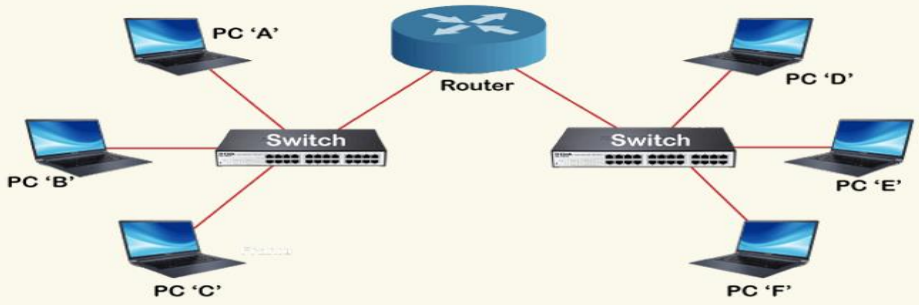
Step 5:: After configuring the switch, Router-on-stick check the communication using "ping"/"Tracert" command



Question 2: List some differences between TCP and UDP **[5 points]**

TCP	UDP
Requires an established connection to transmit data (connection should be closed once transmission is complete)	Connectionless protocol with no requirements for opening, maintaining, or terminating a connection
Data will be able to sequence	Unable to sequence the Data
Can guarantee delivery of data to the destination router	Cannot guarantee delivery of data to the destination
Retransmission of lost packets is possible	No retransmission of lost packets
Extensive error checking and acknowledgment of data	Basic error checking mechanism using checksums
Does not support Broadcasting	Does support Broadcasting
Used by HTTPS, HTTP, SMTP, POP, FTP, etc	Video conferencing, streaming, DNS, VoIP, etc

Question 3 (Extra Credit): What is the difference between a collision domain and a broadcast collision domain. Please indicate the number of collision domains and broadcast domain from the below picture. **[5 points]**

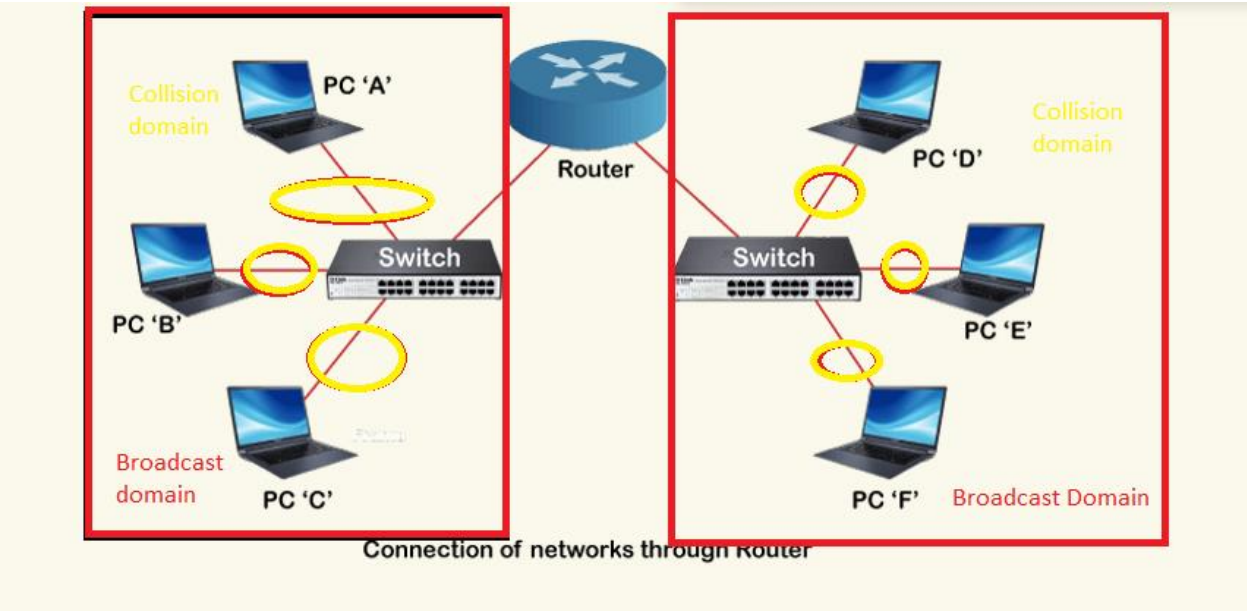


Connection of networks through Router

Ans:: Difference b/w a collision and broadcast domain

Collision Domain	Broadcast Domain
A collision domain is the part of a network where packet collisions can occur. A collision occurs when two devices send a packet at the same time on the shared network segment. The packets collide and both devices must send the packets again, which reduces network efficiency	A broadcast domain is the domain in which a broadcast is forwarded. A broadcast domain contains all devices that can reach each other at the data link layer (OSI layer 2) by using broadcast. All ports on a hub or a switch are by default in the same broadcast domain
Switches will break in the collision domain.	Switches will never break in the broadcast domain.
Every port on a router are in the separate broadcast domains.	All ports on a switch or a hub likely to be in the same broadcast domain.

There is 2 broadcast domains and 6 collision domains



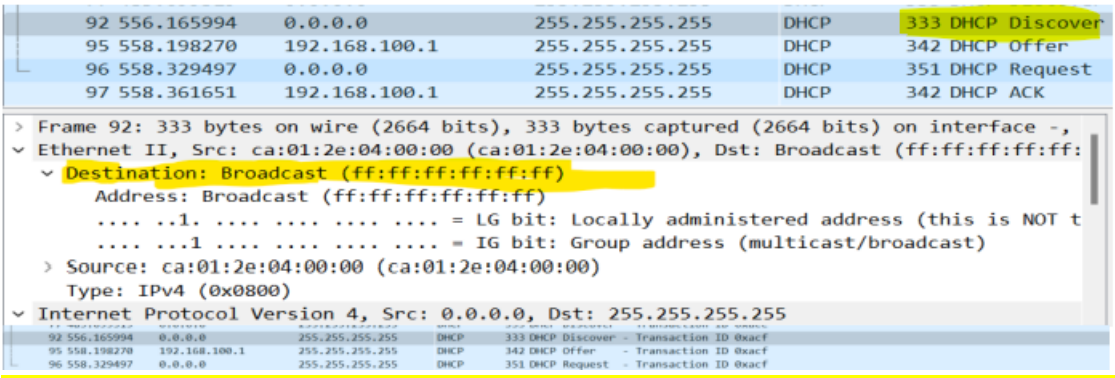
Path 2: **[20 Points]** Hint: 4 Down

Question 4: Explain the process by which a host obtains an IP address dynamically (Hint: DORA) **[10 points]**

Ans: The technique used by which host obtains IP address dynamically is called DORA process.

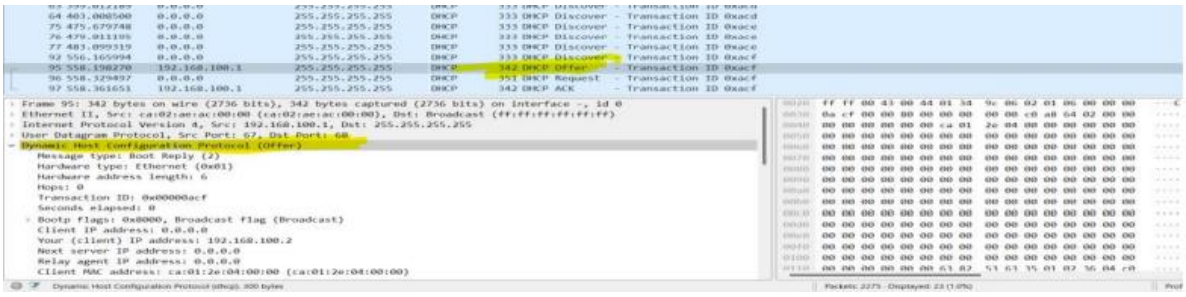
The DORA process used by DHCP to assign IP address works in four steps

DHCP Discover: a DHCP client sends out a DHCP Discover message to find a DHCP server on the network that can allocate a unique IP address. This message contains an identifier, also known as a media control address (MAC), that uniquely identifies the client. It also includes other parameters, such as subnet mask, domain name and DNS. This is a broadcast message that reaches all the nodes in a network



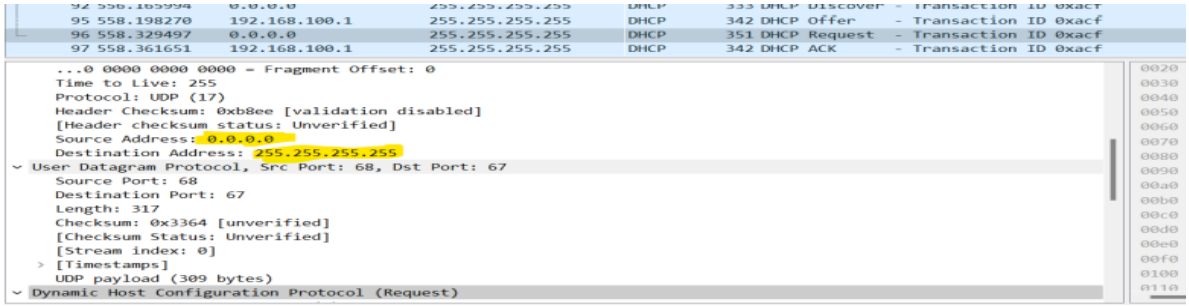
the client is not aware of the server's IP address, so the destination IP is 255.255.255.255. Since the client does not have an IP address yet, its source IP is 0.0.0.0

DHCP Offer: The DHCP server receives the message sent by the DHCP client. After receiving this message, the DHCP server replies to the DHCP client with a DHCP Offer message. The intent of this message is to lease an IP address to the client. The message contains an IP address the client can use,along with its lease time, network config parameters.



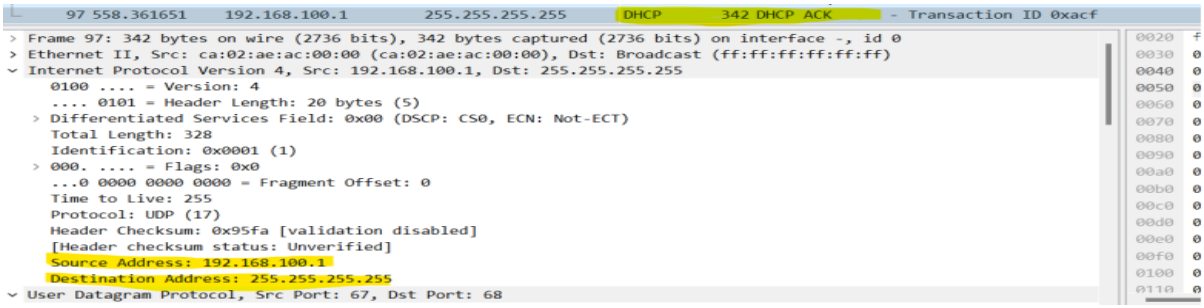
Here, the destination IP address is 255.255.255.255 since the client does not have an IP yet. The source MAC address is the MAC address of the DHCP server and the destination MAC address is the MAC address of the DHCP client

DHCP Request: The DHCP client sends a DHCP Request message after receiving the DHCP Offer message from the server. Since there are multiple DHCP servers sending offer messages to the client, the DHCP client selects the one that reaches it first. Later, the client sends out a broadcast message to confirm that it accepts the IP address assigned by the DHCP.



The default IP lease duration is eight days. Here, the source IP address is 0.0.0.0 as the DHCP server has not yet assigned an IP address to the client. The destination is 255.255.255.255

DHCP Acknowledge: the DHCP server sends a DHCP Acknowledge message to the client after receiving the DHCP Request message. In the message, it sends the IP address and other network configurations essential for the client. After assigning the IP address to a client, the server registers this IP along with the lease time. It does not provide this IP address to any other client. The source IP address is the IP address of the DHCP server. The destination IP address is 255.255.255.255 since it is a broadcast message in the network layer.



Question 5: Explain the differences between a distance-vector protocol and a link-state protocol. Give examples of each and justify your answer. **[10 points]**

Distance-vector Routing	Link-state Routing
No flooding, small packets and local sharing require less bandwidth.	More bandwidth required to facilitate flooding and sending large link state packets.
Uses Bellman-Ford algorithm.	Uses Dijkstra's algorithm.
Less traffic.	More network traffic when compared to Distance Vector Routing.
Updates table based on information from neighbours, thus uses local knowledge.	It has knowledge about the entire network, thus it uses global knowledge.
Persistent looping problem exists.	Only transient loop problems.
Based on least hops.	Based on least cost.
Updation of full routing tables.	Updation of only link states.
Less CPU utilisation.	High CPU utilisation.
Uses broadcast for updates.	Uses multicast for updates.
Moderate convergence time.	Low convergence time
Follows no Hierarchial Strcuture	Follows Hierarchial Structure
RIP - Routing Information Protocol and IGRP - Interior Gateway Routing Protocol	OSPF - Open Shortest Path First Protocol

Example Distance-Vector:

In the network shown below, there are three routers, A, B, and C, with the following weights − AB =2, BC =3 and CA =5.

Step 1 − In this DVR network, each router shares its routing table with every neighbor. For example, A will share its routing table with neighbors B and C and neighbors B and C will share their routing table with A.

Form A	A	B	C
A	0	2	3
B			
C			
Form B	A	B	C
A			
B	2	0	1
C			

Form C	A	B	C
A			
B			
C	3	1	0

Step 2 − If the path via a neighbor has a lower cost, then the router updates its local table to forward packets to the neighbor. In this table, the router updates the lower cost for A and C by updating the new weight from 4 to 3 in router A and from 4 to 3 in router C.

Form A	A	B	C
A	0	2	3
B			
C			
Form B	A	B	C
A			
B	2	0	1
C			
Form C	A	B	C
A			
B			
C	3	1	0

Step 3 − The final updated routing table with lower cost distance vector routing protocol for all routers A, B, and C is given below

Router A			
Form A	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0
Router B			
Form B	A	B	C
A	0	2	3
B	2	0	1
C	3	1	0
Router C			
Form C	A	B	C
A	0	2	3
B	2	0	1
C	3	1	

Link state example: **if** a packet needs to be transmitted from the Router-1 to Router-2, then it can follow two paths.

1. Directly from Router-1 to Router-2, the cost of this traveling is 6.
2. It can also go from Router-1 to Router-2, via path: Router-1 --> Router-3 --> Router-2. The cost of this traveling is (2 + 3) = 5.
3. So, the data packet will be sent from the second path i.e., Router-1 --> Router-3 --> Router-2

Path 3: **[15 Points + 10 Extra Credit]** Hint: 3 Down

Question 5: Explain the TCP 3-way handshake process. [10 points]

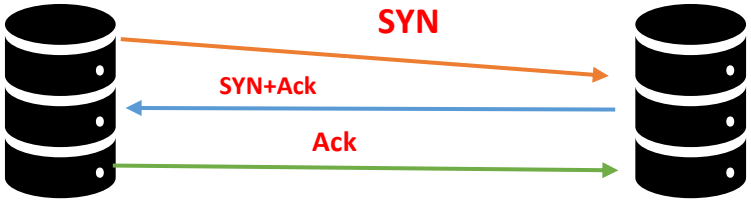
TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts. Three-way handshake process is designed in such a way that both ends help you to initiate, negotiate, and separate TCP socket connections at the same time. It allows you to transfer multiple TCP socket connections in both directions at the same time.

TCP Message types:

Message	Description
Syn	Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.
ACK	Helps to confirm to the other side that it has received the SYN.
SYN-ACK	SYN message from local device and ACK of the earlier packet.
FIN	Used to terminate a connection.

TCP Three-Way Handshake Process

TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server:



Step 1: In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.

Step 2: In this step server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.

Step 3: In this final step, the client acknowledges the response of the Server, and they both create a stable connection will begin the actual data transfer process. After the data transmission process is over, TCP automatically terminates the connection between two separate endpoints.

Question 6: What are Routers, Hubs, Switches, Bridges and Firewalls? **[5 points]**

Ans: Routers, Hubs, Switches, and Bridges are all devices connecting two or more devices together that are present in the same or different networks

Hub	A Hub is a layer-1 device and operates only in the physical network of the OSI Model**.** Since it works in the physical layer, it mainly deals with the data in the form of bits or electrical signals. A Hub is mainly used to create a network and connect devices on the same network only
	A Hub is not an intelligent device, it forwards the incoming messages to other devices without checking for any errors or processing it. It does not maintain any address table for connected devices. It only knows that a device is connected to one of its ports
	A Hub uses a half-duplex mode of communication. It shares the bandwidth of its channel with the connecting devices. It has only one collision domain, so there are more chances of collision and traffic on the channel. A hub is connected in limited network size

Bridge:

Bridge	A bridge is a layer-2 network connecting device, i.e., it works on the physical and data-link layer of the OSI model. It interprets data in the form of data frames. In the physical layer, the bridge acts as a Repeater which regenerates the weak signals, while in the data-link layer, it checks the MAC(Media Access Control) address of the data frames for its transmission
	A bridge connects the devices which are present in the same network. It is mainly used to segment a network to allow a large network size. It has two types of port - incoming and outgoing. It uses the incoming port to receive the data frames and outgoing port to send the data frames to other devices. It has two collision domains, so there is still a chance of collision and traffic in the data transmission channel
	Bridge is a Repeater with filtering capability. It means that it can discard the faulty data frames and will allow only the errorless data frames in the network. Also, it can check the destination MAC address of a frame and decides the port from which the frame should be sent out

Switch	A switch is a layer-2 network connecting device, i.e., it works on the physical and data-link layer of the OSI model. It interprets data in the form of data frames. A switch acts as a multiport bridge in the network. It provides the bridging functionality with greater efficiency

	A switch maintains a Switch table which has the MAC addresses of all the devices connected to it. It is preferred more over the hub, as it reduces any kind of unnecessary traffic in the transmission channel. A switch can connect the devices only in the same network. It uses the full-duplex mode of communication and saves bandwidth. The switch table keeps on updating every few seconds for better processing.
	A Switch is an intelligent device with filtering capabilities. It can discard the faulty data frames and will allow only the errorless data frames in the network.A Switch can have 8/6/24/48 ports. The data transmission speed is slow in a switch(around 10-100 Mbps). Also, it has only one broadcasting domain

Router	A Router is a layer-3 network connecting device, i.e., it works on the physical, data-link and network layer of the OSI model. It interprets data in the form of data packets. It is mainly an internetworking device, which can connect devices of different networks(implementing the same architecture and protocols).
	Router is the Gateway of a network.connecting two devices of different networks, the connecting device should implement an Internet Protocol(IP) address. So, the Router has a physical and logical(Internet Protocol) address for each of its interfaces
	A router does not perform addressing. It can have 2/4/8 ports for connecting the devices. It can control both the collision domain(inside the network) and the broadcast domain(outside the network). It has a fast data transmission speed(up to 1 Gbps). A Router can be a Wireless Router, Core Routers, Edge Routers, Virtual Routers, etc

Firewall	A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
	Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
	A firewall can be hardware, software, software-as-a service (SaaS), public cloud, or private cloud (virtual).

Question 7 (Extra Credit):

Each of the college departments have the corresponding number of usable hosts as mentioned below. Use 172.16.10.0/24 as the base subnet, assign IP subnets for each of the departments while using the most efficient use of the address space. Indicate the network address, broadcast address and valid host range for each subnets assigned to earn full points **[10 points]**

- Engineering: 64
- Accounting: 30
- Management: 25
- Sales: 8

We need to create 4 subnets and the largest subnet must support 64 host addresses. In order to create the four needed subnets, you would need to use 2 bits from the Class B host bits. Two bits would only allow you four subnets (2^2). Hence,

Network Address	Host Range	Broadcast
Sales(netA): 172.16.10.0/24	host address range 1 to 10	172.16.10.255
Management(netB): 172.16.10.11/24	host address range 11 to 26	172.16.10.255
Accounting(netc): 172.16.10.27/24	host address range 27 to 58	172.16.10.255
Engineering(netD): 172.16.10.59/27	host address range 59 to 124	172.16.10.255

Path 4: **[20 Points + 5 Extra Credit]**

Hint: 9 Across

Question 8: What happens when you type an URL in the web browser? Explain in detail the complete packet flow process. (Hint: ARP, DNS, TCP, HTTP) **[20 points]**

Requesting for IP Address – DHCP Request Message

The network related action taken by laptop is to run DHCP protocol to obtain an IP address from local DHCP server in the router along with other required information. The operating system of laptop creates a DHCP request message and puts in the UDP. This UDP segment with a request for IP address message is then placed in IP datagram with Broadcast IP destination address -- 255.255.255.255 and Source IP Address -- 0.0.0.0

DHCP and Ethernet Frame

The IP datagram with DHCP request message is then placed in the Ethernet Frame with destination MAC address: FF: FF: FF: FF: FF: FF. This datagram is broadcasted to all devices hoping to get connected to the DHCP server. The Ethernet Frame that is broadcasted containing the DHCP message is the first packet sent to the outside world from the laptop to the Ethernet Switch. Switch broadcasts all the frames in the outgoing ports, including routers port**.** The router gets the Ethernet frame broadcasted having the Dynamic Host Configuration Protocol request on its interface.

- The IP datagram is extracted from the frame.
- The IP destination address indicated that datagram should be taken care by the protocols in the upper layer

DHCP Ack and Switching

The DHCP server within router can allocate data within the CIDR(Classless Inter-Domain Routing) range. Here, the IP addresses are within the ISP's private addresses that are specifically allocated for the DHCP server to give away. DHCP ACK Message with IP address and DHCP server IP is sent through the router. This info is put into a UDP segment which is put inside an IP datagram.

- Source MAC – Ethernet's IP
- Destination MAC – Laptop's MAC Address.
- The DHCP ACK frame is sent by the router to the switch.
- Since switch can do self-learning and had already received the Ethernet frame, the switch forwards the frame to output leading to laptop

IP Forwarding

Laptop receives Ethernet frame containing DHCP ACK.IP datagram is extracted from Ethernet frame.UDP segment is extracted from IP datagram. DHCP ACK message from UDP segment. And then this data is installed in the IP forwarding table. Now Laptop would send the information to outside world with this default gateway.

DNS Query Message

The laptop then creates a DNS query message with the Website in the question section of the message.DNS message is placed in the UDP segment. Destination port – 53.UDP segment is placed within IP datagram with an IP destination address.DNS server address returned in the DHCP ACK message.Source IP – Default gateway. Laptop puts the question in Ethernet frame which is sent to the gateway router. Even though DNS knows the IP address of the IP address through DHCP ACK, It doesn't know the MAC address**.**

Hence it requests to use *ARP -- Address Resolution Protocol*.

ARP Protocol and ARP Query and Reply

Laptop creates ARP query. Target IP address – Default gateway address. Places ARP messages and the Destination address is Broadcasted. Ethernet frame is sent to switch. And the frame is sent to all connected devices. The gateway router receives the frame containing ARP query and replies with its MAC Address corresponding to its IP Address. Laptop receives the frame containing ARP reply. Extracts MAC address of gateway router. Now the Laptop addresses the Ethernet frame with DNS query to gateway router's MAC address.

- Destination Address – IP of the DNS server.
- Destination MAC address – Gateway routers address.

The frame is sent to switch which delivers the frame to the gateway router.

Network to Network

The gateway router receives the frame and extracts IP datagram containing DNS query. The destination address is noted. The data is sent to the leftmost router in the ISP's network. IP datagram is placed inside link layer frame and send to the left most router. The router in the leftmost gets the frame, extracts the IP datagram, examines destination, determines outgoing interface towards DNS server from its forwarding table. Then Uses intra-domain routing protocol such as BGP

DNS Resource Record and IP address extraction

The IP datagram with DNS query arrives DNS server. And DNS server extracts query message, looks up for domain name, finds DNS resource record, this contains the IP address of the **website**. And then DNS server forms the DNS reply message by doing Hostname to IP mapping. Places it in the UDP segment in IP datagram to Laptop. The laptop then extracts IP address of **Website** and is ready to connect to the **Website's** server.

Three Way TCP Handshake

Laptop has the IP address of **Website**. It can create a TCP socket to send HTTP GET message. The laptop must perform a TCP three-way handshake.

TCP SYN segment with destination port 80 inside IP datagram.

- Destination IP address – **Website's** IP address.
- Destination MAC Address – Gateway router's address.
- Sends the frame to switch.

The routers inside private NW, ISP NW and **Website's** NW forwards the TCP SYN towards **Website** using forwarding table in each router. BGP determined the forwarding table in the intra-domain link between ISP and **Website** networks.

Eventually, the datagram with TCP SYN message arrives at **Website**. TCP SYN message is extracted from datagram and sent to welcome socket with port 80.A TCP connection between **Website's** HTTP server and Laptop is initiated. TCP SYN-ACK segment is generated inside link layer frame and sent to its first-hop router. The datagram with TCP SYN-ACK segment is forwarded through all the networks and reached the Ethernet card of the laptop.

HTTP GET Message With socket in laptop ready to send bytes to Website. Browser creates an HTTP GET message. With URL to be fetched. HTTP GET is written into a socket. GET request is the TCP segment payload. TCP is placed in IP datagram and delivered to Website.

HTTP Response Message The HTTP server at Website reads the GET message and creates HTTP response and places the web page in the HTTP response message.

- Sends into the TCP socket.

Web Browser Rendering The reply message datagram is forwarded through all the networks and then arrives at the laptop. And the website with the URL gets rendered.

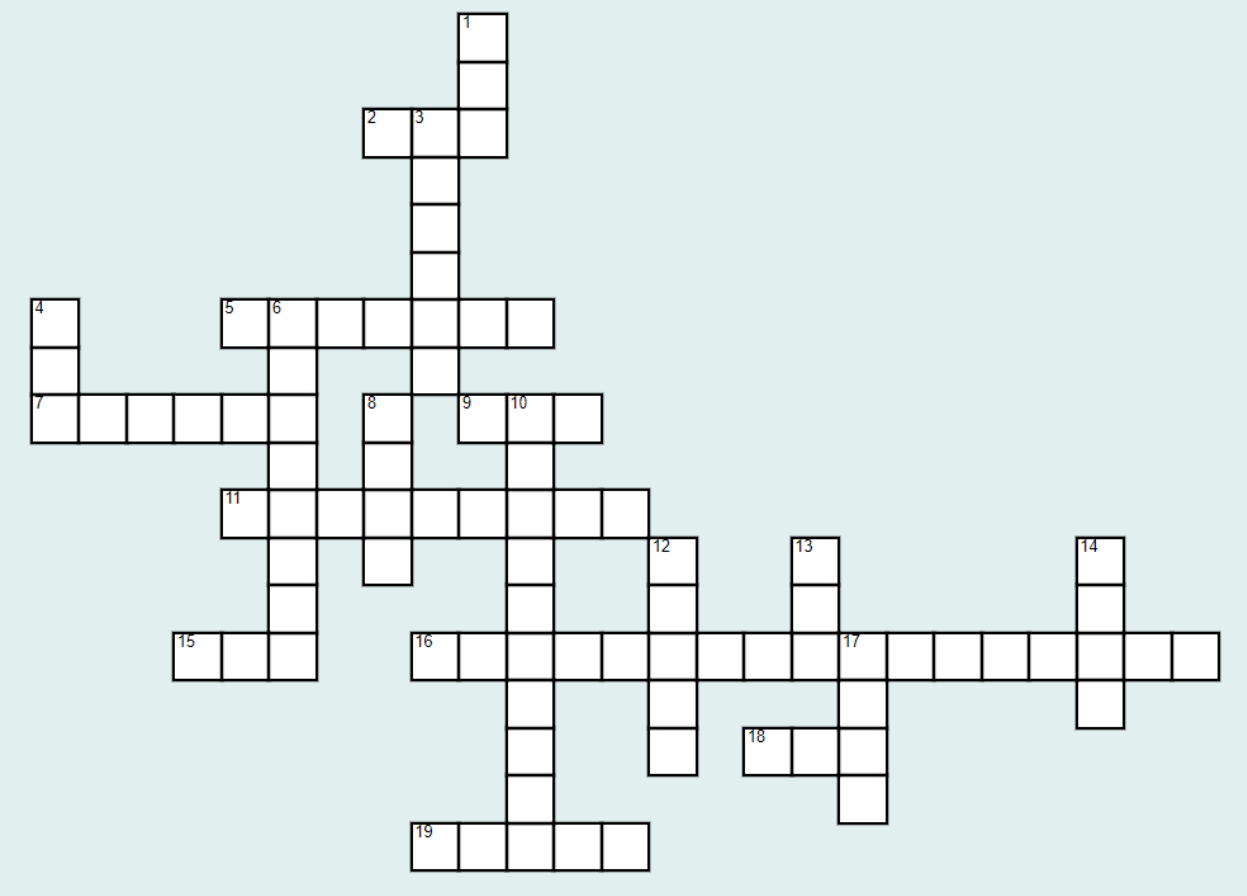
Question 9 (Extra Credit): List the network address, broadcast address, and valid host address range for the IP address 198.22.45.173/26? Also, Indicate the subnet mask in dotted decimal notation. **[5 points]**

The host range, Network and Braodcast Address of the above Ip address 198.22.45.173/26

IP Address:	198.22.45.173/26
Network Address:	198.22.45.128
Usable Host IP Range:	198.22.45.129 - 198.22.45.190
Broadcast Address:	198.22.45.191
Subnet Mask:	255.255.255.192
Wildcard Mask:	0.0.0.63
Binary Subnet Mask:	11111111.11111111.11111111.11000000
IP Class:	C
CIDR Notation:	/26
IP Type:	Public

Network Address	Usable Host Range	Broadcast Address:
198.22.45.0	198.22.45.1 - 198.22.45.62	198.22.45.63
198.22.45.64	198.22.45.65 - 198.22.45.126	198.22.45.127
198.22.45.128	198.22.45.129 - 198.22.45.190	198.22.45.191
198.22.45.192	198.22.45.193 - 198.22.45.254	198.22.45.255

Crossword [30 points]



Hints for completing the crossword:

Across

2 Avoids layer-2 loops

STP

5 PDU of the transport layer

Segment

7 Networking device that operates at the data- link layer of the protocol stack

Switch

9 Uses two TCP ports for communication – FTP

11 DHCP discover is a _____ message

Broadcast

15 Field in an IP header that prevents L3 loops

TTL :: Time to Live

16 Most preferred routes in the routing table (2 words)

Directly Connected

18 Glues the internet together

BGP

19 DNS message for converting a domain-name to IP address

Query

Down:

1 Protocol used to obtain the MAC address

ARP

3 Uses port 23

Telnet

4 Uses port 53

DNS

6 Wireshark was earlier known as?

Ethereal

8 Separates broadcast on a switch

VLAN

10 Utility that records route from source to destination

Traceroute

12 Uses a secure, reliable protocol on port 443

HTTPS

13 Is 48-bits in length

MAC

14 Uses port 80

HTTP

17 Routing protocol that uses both link-state and distance-vector algorithm

OSPF