1. For each of the following applications, determine whether TCP or UDP is used as the transport layer protocol and explain the reason(s) for your choice

a) File Transfer
b) Watching a real time streamed video
c) Web browsing
d) A Voice over IP (VoIP) telephone conversation
e)YouTube video

Ans:

a) File Transfer – TCP
FTP protocol uses TCP, a connection oriented protocol for reliability, to ensure integrity of the file being transmitted

b) Watching a real time streamed video – UDP
UDP is faster and has lower overhead (as there is no need for establishing any connection, or any flow control mechanisms or retransmission attempts). It doesn't matter if a few packets in between get dropped.

c) Web browsing – TCP
HTTP is the standard protocol for web browsing, which uses connection oriented protocol TCP as the transport layer for a reliable connection between the client and the server. Required so that the files, images, web pages which we get from the remote host should not be dropped on the way and it should be delivered in order to the HTTP client

d) A Voice over IP (VoIP) telephone conversation – UDP**
Real time communications services such as VoIP do not require a completely reliable transport layer protocol. This allows UDP to be better suited. Errors like packet loss usually only have minor impacts on the audio output. It is much better to drop a packet and have a few milliseconds of silence than to have seconds of lag within a conversation.

e) YouTube video – TCP
YouTube buffers videos so that they can be watched again, rewound, paused etc. , and thus a reliable transmission protocol like TCP is needed. So if there's a missing packet which causes a glitch in the video, TCP will let the packet to be retransmitted. YouTube also adjusts video quality based on network congestion, and this can be detected by TCP.

2. (a) How was the original definition of an Ethernet frame updated by IEEE 802.1Q to permit the use of Virtual Local Area Networks (VLANs)?

(b) What is SPF and what is used for? Suppose you are the domain administrator for the domain test.com. How will you use SPF to prevent incoming mails from a domain **abc.com**, unless they originate from an IPv4 address between 192.128.0.1 and 192.128.255.255.

Ans:

(a) 802.1Q does not encapsulate the original frame. Instead, for Ethernet frames, it adds a 32-bit field between the source MAC address and the Type/length fields of the original frame.

1. A **16-bit Tag protocol identifier (TPID):** set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame.

2. A **16-bit Tag control information (TCI)** which further consists of

a) A **3-bit Priority code point (PCP**) used to prioritize class of service given to traffic

b) A **1-bit Drop eligible indicator (DEI)** used separately or in conjunction with PCP to indicate

frames eligible to be dropped in case of congestion in the network
c) A **12-bit VLAN identifier (VID)** specifying the VLAN to which the frame belongs.

(b) Sender Policy Framework(SPF) is a mechanism through which a DNS TXT record is created for a given mail domain, containing a list of valid IP addresses - When a mail needs to be accepted from a particular domain, the MTA checks if the IP is valid for that domain.
SPF prevent spammers from sending messages with forged "From addresses". If the SPF record created in the mail exchanger for test.com domain is as follows:
abc.com TXT "v=spf1 ip4:192.128.0.1/16 -all"
Then, the mail exchanger for test.com domain will allow mails from abc.com only if the IP address of the originating mail in the address range between 192.128.0.1 and 192.128.255.255.

3. (a) In the figure 1 below, N1 to N6 are six nodes (routers). The numbers on the edges(links) indicate the cost to traverse the path from one node to another in a particular direction. Using Djikstra's algorithm, find the least cost route from node 2 to node 6

Ans:

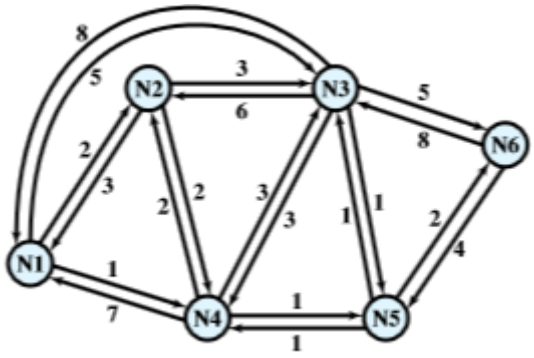

Figure 1

(b) Among the MAC protocols, CSMA/CD and CSMA/CA, which do you think is suitable for wireless networks and why ? Show any two differences between CSMA/CD and CSMA/CA

Ans:

	M	L(1)	Path	L(3)	Path	L(4)	Path	L(5)	Path	L(6)	Path
1	{2}	3	2-1	3	2-3	2	2-4	∞	—	∞	—
2	{2, 4}	3	2-1	3	2-3	2	2-4	3	2-4-5	∞	—
3	{2, 4, 1}	3	2-1	3	2-3	2	2-4	3	2-4-5	∞	—
4	{2, 4, 1, 3}	3	2-1	3	2-3	2	2-4	3	2-4-5	8	2-3-6
5	{2, 4, 1, 3, 5}	3	2-1	3	2-3	2	2-4	3	2-4-5	5	2-4-5-6
6	{2, 4, 1, 3, 5, 6}	3	2-1	3	2-3	2	2-4	3	2-4-5	5	2-4-5-6

It is evident that the least cost path is 2-4-5-6

4. Consider this home network setup.
R1 : Internet connectivity router with a Ethernet 8-port LAN.
with IP 192.168.1.1
R1's DHCP range is set as all IPs above 192.168.1.100
with subnet mask 255.255.248.0
W1 : Wireless Access Point connected via wired Ethernet LAN to R1.
PC1 : Computer PC1 connected directly to R1 via wired Ethernet LAN
with a static IP. 192.168.1.4
PC2 : Computer PC1 connected directly to R1 via wired Ethernet LAN
with a static IP. 192.168.1.5
M1 : Mobile1 connected via 802.11 Wifi to W1 though IP is
dynamically allocated by R1 as 192.168.1.100
M2 : Mobile1 connected via 802.11 Wifi to W1 though IP is
dynamically allocated by R1 as 192.168.1.101

A) What is the IP to ping from PC2, if it wants responses
from all devices on the network.

B) If there is a SFTP-fileserver running in PC1 and is M1 and M2 are
downloading some files from PC1.
What happens if R1 is switched off ? Reason out your answer.
C) What happens if W1 is switched off ? Reason out your answer.
D) Is the fileserver running in PC1 accessible by others outside the network.
If not how to make it accessible.
Show the packet flow on how the access is achieved.
E) What is the maximum number of devices that could be connected
to this network via DHCP ?

Ans:

A) 192.168.7.255 -- Broadcast IP
B) Nothing happens if R1 is switched off, the download will continue
C) If W1 is switched off, the download will get interrupted
as the mobile's connectivity via Wifi is lost.
D) No. PC1's IP is a private IP and hence it is not accessible to
outside world. A static public IP set on the router R1 +
proper port forwarding done at the router R1 will make
PC1's file server accessible to the external world.
E) 2046 - 255 - 100 = 1691
Note 2046 is the maximum hosts for this network but given
that DHCP starts only from 192.168.1.100, the above calculation results.

F) The problem is not then with the Internet or the website per-se.
As it is not accessible from both M1 and M2, most likely problem
in the wifi connection or more possibly the DNS setting in DHCP.

5. A 10MB file was being downloaded from a website in the browser.
Suddenly when about 4 MB had got downloaded, it got interrupted due to bad network.
Much later when the network came back, the file download automatically resumed from the 4 MB. How did this magic happen ? Explain with HTTP headers/messages.

Ans:

This is HTTP's bytes + ranges header at work.

In the HTTP request when trying to download again, the browser sends
an extra header
Range: bytes=4194304-
and possibly another header 'If-Range: "etag of the resource"

6. I clicked a link in a webpage which had this URL:
http://www.imagescontent1.servers.net/images/global-state.img.jpg
and it opened in a new browser tab, and loaded and displayed the image subsequently.
But when I looked at the Address Bar the URL had changed to
http://www.1.newserv.servers.net/images/global-state.img.jpg
What is going on here? Explain with HTTP headers/messages.

Ans:

This is HTTP Redirect mechanism at work.
the server www.imagescontent1.servers.net is redirecting via response
302 Found or
301 Moved permanently or
301 Moved temporarily
and Location header as
Location: http://www.1.newserv.servers.net/images/global-state.img.jp