PART I - 25 x 1 marks = 25 marks

1. What is the ARP Cache timeout in Windows 7 OS? Reasonable approximation is allowed but justify the reasoning behind choosing such a value.

   ANSWER :

   ARP cache is integrated with Neighbor discovery mechanism in Windows. Roughly about 45 seconds to 1 minute. Reachability check fail and timeout triggers a ARP cache entry deletion.

2. I asked my Internet Service Provider (ISP) for some static IPs. They responded that I have been allocated 129.22.8.32/29. How many IPs can I setup/provision in my network ?

   ANSWER :

   8 IPs are available 129.22.8.32, .33, thro' 129.22.8.39

3. Below is an Hexadecimal dump of an UDP datagram captured. Find the source UDP Port.
   e2 a7 14 eb 00 20 74 9e 0e ff 00 00 00 01 00 00 00 00 00 00 06 69 73 61 74 61 70 00 00 01 00 01

   ANSWER :

   e2 a7 is the source port and is 58023 in decimal

4. Apply the standard byte stuffing mechanism on this input data and show the transmitted stream.
   B A ESC C A ESC FLAG C A

   ANSWER :

   ESC and FLAG data has to be byte stuffed.
   Transmitted stream : B A ESC ESC C A ESC ESC ESC FLAG C A

5. State two Protocols as in IP Header Protocol Field other than TCP and UDP.

   ANSWER :
   ICMP, IGMP, SCTP, etc.

6. In the case of a fragmented IP Packet transmission, the last fragment loss is worse than the first fragment loss. True/False. Validate your claim.

   ANSWER :

   False. Any fragment loss is just the same. Equally Bad.

7. What is the time it takes for a jumbo frame of 32 KBytes to be sent by endpoint A on to a link where the frame transmission is 2 Mbps ?

   ANSWER :

   It will take (32 x 1024 x 8) / (2 x 1024 x 1024) = 1/8 second

8. What would you suggest to set as a best possible firewall rule to block ping ?

   ANSWER :

   Block ICMP Traffic will get 0.5 mark credit.

   The question is very specific - only Ping ICMP - Echo Request and Echo Reply based on the ICMP code should be blocked. - 1 mark credit.

9. I need to send a 10 MB file over to another system in the same LAN. Assuming I am using a 10Mbps LAN connection what is the best transfer time I can achieve in ideal network conditions ? Figure in TCP/IP overhead.

   ANSWER :

   If no TCP/IP overhead, the best time is 8 seconds. (10 MB / 10 Mb)
   But as the question asks for TCP/IP overhead we are looking at approx. 20 + 20 = 40 bytes extra.
   Assuming LAN MTU of 1500 bytes, max size of a frame on the wire can have only 1460 payload.
   10 MB / 1460 = 10 x 1024 x 1024 / 1460 = 7183 frames approx.
   Extra metadata on the wire = 7183 x 40 = 287320 bytes
   Extra time = (287320 x 8) / (10 x Mb) =~ 0.2 seconds

   So Best transfer time = 8.2 seconds

10. Give an example for HTTP ' HTTP/1.1 302 Moved Temporarily' message and its typical use.

    ANSWER :

    302 Moved Temporarily is usually send by the server to REDIRECT a incoming request. sample response:

```
HTTP/1.1 302 Moved Temporarily
Server: Apache/1.1
Location: http://newdomain.com/newpage
Transfer-Encoding: chunked
Date: Thu,  30 Jan 2014 04:25:45 GMT
```

11. If the same source and destination port is used by two different processes A and B in the same machine, and A uses TCP and B uses UDP, what problems would arise ? Will it work? If so how?

ANSWER :

No issues should arise. It should work.
A network flow is usually uniquely identified by the five parameters - Src Port, Src IP, Dest Port, Dest IP and Protocol. So as long as the at least one parameter is different, it should work, though quite rare to see such a flow in actuality.

12. CSMA/CD is not an effective MAC protocol in Wireless. True/False. Validate.

ANSWER :

True. Due to heavy signal attenuation and differing range in Wireless, Collision Detection does not suffice. Rather to have an effective MAC protocol/mechanism, Collision Avoidance has to be chosen/employed.

13. A Layer 2 protocol is running a Go-back-N scheme with window size of 20 frames. The maximum end-to-end delay on the medium is about 500ms. What do you propose as the transmission timer value on the sender for effective line utilization ?

ANSWER:

Transmission timeout should be a little greater than Round trip time on the link/line.
So, a good transmission timer should be slightly more than 2 x 500 ms = 1 second, say 1.1 second. This will avoid premature timeouts/retransmissions.

*** Note: This metric is independent of the Window size!**

14. A Layer3 router typically has many network interfaces for its operation. Can I say my machine which has both Ethernet and Wifi connectivity is in also a router ? Why ? Why not ? Validate.

ANSWER :

NO. A multihomed machine - having many network interfaces - does not perform the same functions as a IP router. A laptop/machine having both Ethernet and Wifi is only providing multiple reachability endpoints for that particular machine., but does not indulge in routing for other hosts as done by the IP router. And also most likely, IP Router also run Routing protocols to discover and maintain routes to far destinations which the machine does not do.

15. Give an example in the TCP/IP stack where Layering is violated.

ANSWER :
A Layer should be self contained in its internal implementation and should not be dependent on other layers's internals for its proper functioning. If that is not the case, it is termed as a Layering violation. In TCP/IP, the UDP Checksum is arrived at by looking into IP Header source and destination IP. This is probably there for end-to-end checks to avoid misrouted packets coming in and being interpreted/processed, but whatever be the reasoning behind it, it is a layering violation as UDP which is Layer 4 has to look into internal data of IP Protocol which is Layer 3.

16. Why is it considered that PASV Mode FTP as firewall friendly?

ANSWER :

ACTIVE Mode FTP requires the Server to open a TCP connection to the client for data transfer., whereas this is not the case in PASV Mode FTP. Typically, in enterprise environments, incoming TCP connections to random ephemeral ports will be blocked in the firewall, so ACTIVE mode FTP does not work, but PASV Mode FTP will still work. Hence the term firewall friendly !

17. Consider a DHCP based LAN setup with many machines. Is it possible the DHCP server to be running on a different device than the default router. ? Yes/No. Validate.

ANSWER :

YES. DHCP mechanism typically is integrated in the router, but it is also possible that DHCP runs in a separate machine altogether for load/performance reasons than the default router. In that case the big question is how would an endpoint/machine know what is the default router's IP Address. DHCP Offer message carries a field called the Gateway Address which contains the default router's IP Address.

* Not mentioning DHCP Offer message has the Gateway Address field will get 0 mark credit

18. List out two advantages of CSMA over Token mechanism as a MAC protocol.

ANSWER :
1. CSMA is a distributed protocol and does not need any kind of centralized authority at any point of time for the protocol to work effectively. Token mechanisms typically need a token issuing authority which may change time to time but definitely a centralized mechanism and is bound to cause issues with performance bottlenecks.
2. CSMA adapts much better than Token based mechanisms when new nodes are added to the link.

19. https is a mechanism where server authenticates the client. Yes/No. Validate.

ANSWER :

NO. Actually it is the other way around. Client authenticates whether it is talking to the correct server by looking at the veracity of the Server SSL certificate in https.

20. A UDP based sender application is sending data to a remote application, and gets the destination IP correctly but the port is wrong. How would the sender application know this issue, typically ?

ANSWER :

Well, UDP has no acknowledgements, so the Sender Application will not be able to get that UDP datagram did not reach the receiver from UDP layer - Layer 4, but from the Application protocol - Layer 5 - it is running. eg. If it is sending data to the remote application and is expecting a Layer 5 reply and never gets it, it may indicate to the sender application that something is not ok. One other way is that, the sender may get ICMP Port Unreachable errors from the remote side if ICMP is turned on, in which case, the sender app. may get a matching error code in the socket.

21. The Domain a.root-servers.net maps to IPv4 IP: [198.41.0.4]. Can you state a point of significance ?

ANSWER :

There are 13 root DNS servers in the world (entire Internet). They are lettered a.root-servers.net, b., c., thro' m.root-servers.net. All their IPs are load-balanced throughout the world in different geographical zones operated by entities like Verisign, RIPE, Netnod, etc. A root node server is the top most in the DNS Zone hierarchy and which is where the query will start eg. if trying to look for www.sinclair.tregart.com, the root servers will house the .com zones and will be able to point the DNS request to tregart.com's name server. As DNS resolution is hierarchical, root servers should be always available for proper functioning of the Internet.

22. 1990s saw a raise in the occurrences of TCP SYN flooding, which caused downtime for many websites. Outline briefly the background of this problem.

ANSWER :

When a endpoint A wants to initiate a connection to another endpoint B, it sends out a TCP SYN Packet/Segment., which usually contains the connection setup details - TCP Start Sequence number, Max. Segment Size (MSS) value, other TCP options eg. SACK, etc. So when the TCP SYN is received by the remote side - endpoint B, it has to be processed and some memory has to be allocated to hold these information and then a reply SYN + ACK is sent back to the endpoint A as a reply. Now as can be seen, sending many TCP SYNs from many machines to a particular host can make the host go down as all memory/connections get used up. This Distributed Denial of Service (DDOS) attack was launched many a time against websites which was termed as TCP SYN Attacks or TCP SYN Flooding.

23. SMTP RFC 5321 states that a line with an dot (period) character is treated as the end of the message. How would then email messages which contain empty lines or lines with a dot character alone be handled ?

    ANSWER :

    Well, this is called ESCAPING or BYTE/BIT/DATA Stuffing.
    If a line with a dot character alone is seen in the email message, SMTP Clients send a line with two dots (..) to indicate to the SMTP Server, that it is not the end of the message, rather it is part of the message.

24. I have a subnet mask 255.255.255.248 set up in my machine with IP 10.5.5.20? What IP address should I ping to, so that I get response from all machines on my LAN subnet.

    ANSWER :

    This is called Broadcast Ping. As can be seen the Subnet Address is got by Bitwise ANDing the subnet mask with the given IP.
    10.5.5.20 ----------> 10. 5.5. 00010100
    255.255.255.248 - Binary -----> 255.255.255. 11111000
    ----------> 10.5.5. 00010000 --> 10.5.5.16
    There are 255 - 248 = 7 IP Addresses in this subnet
    10.5.5.17, .18, .19, .20, .21, .22 and the last one is the **Broadcast IP - 10.5.5.23**

    So issuing a ping to 10.5.5.23 will most likely evince a response from all LAN subnet machines.

25. As TCP Sequence numbers wrap around, how would a TCP endpoint know about segments with same sequence numbers arriving delayed ?

    ANSWER :

    Well, not all sequence numbers would be considered valid by the receiving endpoint in TCP. Only if the packet coming in has a sequence number within the expected Sequence number window, it will be processed. Moreover, given that the sequence number field in TCP is 32 bits, it would take about 4GB of data transmitted successfully before the sequence number wraps around which even in LAN scenario with about 1 Gbps ethernet would take about 32 seconds.

PART II - 7 x 5 marks = 35 marks

26. Write a HTTP parser in C/C++/Java to handle an incoming data from a TCP socket to handle HTTP GET message and send out a proper response. Parser need not handle other type of HTTP Messages, but should fail gracefully when presented with other type of messages. List out the steps in the parsing mechanism in pseudocode and then show the C/C++/Java code snippet.

ANSWER :

Steps:

1. As data is going to be read from a TCP Socket, until a complete HTTP message is received, it cannot be parsed. So there needs to be a buffer into which TCP socket read() data would go into directly.
2. HTTP Message consists of HTTP Header part and Payload - HTTP Body. Given that the parser only needs to read HTTP GET messages, which usually does not have a HTTP Body.
3. As HTTP is a text based protocol, every line in the header is delimited by CR LF ie. '\r\n' And the entire Header is delimited from the body by Double CRLF that is '\r\n\r\n'. So the parser has to look for these characters to identify the end of a line.
4. Within a line, every HTTP Header has the format Header Field : Header Field value. So, here the first occurrence of the COLON (:) signifies the end of the Http Header field name and what follows tills the CRLF is the field value.
5. As this parser is for the server side, interestingly the FIRST Line in the Incoming HTTP Request is called a Request Line and would be of the form eg. GET /hello.php&device=desktop HTTP/1.1. So the Request line parsing has to be different from the other header lines.
6. Process the GET and anything else a error response can be returned in this case. 403 Forbidden, etc.
7. Return a 200 OK with the other relevant fields for the incoming GET request.

27. Assume my machine is 192.168.1.40 setup on a LAN where all Internet traffic from browser goes via a HTTP Proxy server 140.100.140.100 and the default router on the LAN is 192.168.1.1and the DNS server is running on 192.168.1.2. Show all the steps while establishing a login session via my machine's Google Chrome browser - which has system proxy settings setup - to a website https://abcd.com. Is this a secure connection ? Reason out your stand.

ANSWER :

Steps (most probable)

1. ARP to find out the default router MAC address
2. DNS server is in the LAN subnet (valid assumption) looking at the IP address 192.168.1.2 - So ARP Request is send out to find out the DNS Server MAC Address
3. ARP Replies received
4. DNS REquest created to find out the domain abcd.com and sent to DNS server via UDP.
5. DNS Reply most likely with the IP Address of abcd.com 100.100.100.100 received.
6. Proxy server is running on an Public IP and the protocol here is https.
7. https via proxy will require end to end connection done first before data transmission.
8. Browser sends a HTTP Connect message to the proxy server, but before this, a TCP Connection needs to be established from 192.168.1.40 and proxy server 140.100.140.100, which is a TCP SYN packet encapsulated inside a IP Packet which is sent via the router.

9. Most likely the TCP SYN gets a TCP SYN+ACK response and the 3 way handshake of TCP gets done and the connection is set up.

10. Now the Browser's first HTTP Connect message is sent out to the Proxy Server via the established TCP Connection.

11. Browser sees the domain abcd.com and connects to it by initiating a TCP connection from the proxy server to the abcd.com ie. 140.100.140.100 to 100.100.100.100. Note: As the DNS resolution is required only at the webserver level, Steps 4 and 5 above may not be required from the client side. But once again, depends on the browser !

12. Once 2nd TCP connection from Proxy server to abcd.com is set up, the Proxy server responds back to the browser (192.168.1.40) with HTTP 202 Connected message.

13. Note this is a split TCP model, but the HTTP session is end-to-end which makes https secure even when going via Proxy server. The proxy server cannot snoop into the Browser traffic.

14. Now Https SSL/TLS negotiation gets started which is end-to-end from my machine browser to abcd.com webserver. All data sent by my browser via TCP Connection 1 will be forwarded by the Proxy server to TCP Connection 2 and vice-versa. Note most likely, as my machine is in a LAN subnet, the router 192.168.1.2 may have to do NAT mechanism to make the TCP Connection 1 between my browser and the Proxy server work in the first place.

15. Once the TLS negotiation is done, all data is encrypted with the agreed key and my machine - browser - sends out the HTTP Get Request

28. I sent a UDP Packet to an IP 50.50.50.50 and UDP port 5050 with data payload of 40040 bytes. Sender side UDP source port was 65423 and my system IP was 192.168.1.38. Show the IP Fragments that will be sent on the wire with the relevant IP headers if the path MTU is 1500.

ANSWER :

Path MTU is 1500, which is the biggest Ethernet frame that would be sent out, so assuming there were no IP Options, IP Header would take away 20 bytes.
UDP Header is 8 bytes, so the total IP Payload is 40048 bytes.

So 40048 bytes is split into 'p' IP fragments each not more than size 1480 - as each fragment will have a 20 byte header.

40048/1480 =~ approx. 27.43

27 Fragments each of size 1480 with 20 byte header
And the last 28th Fragment will be the remaining data 40048 - (1480 x 27) = 88 bytes.

All 27 Fragments will have the IP Flag - More Fragments bit set to 1 and Total Length = 1500 in the IP Header
The last 28th Fragment will have More Fragments bit set to 0. and Total Length = 108 bytes.

All 28 IP Fragments will have the same value in the IP Header Identification field so that the receiver can identify all these fragments as the same and reassemble accordingly. eg. 5555

Fragment Offset field in the IP Header will be adjusted for every packet accordingly.
ie. 1st Fragment : 0
2nd Fragment : 1480
3rd Fragment : 2960

4th Fragment : 4440
...
27th Fragment : 38480
28th Fragment : 39960

29. Show the list of steps in a machine being booted up and trying to acquire a new IP address via DHCP. Assume relevant aspects and state your assumptions clearly.

ANSWER :

DHCP Messages have to be shown - at least with the common details like lease time, gateway address, - DHCP OFFER, DHCP Discover, DHCP Request etc.

Mention of DHCP running on top of UDP with ports 68 and 67 is required.

DHCP Request messages is usually broadcasting so that other machines in LAN get to know the new IP/machine.

DHCP Ack from the Router offering the IP address is also typically broadcasted in the LAN.

Only explaining the idea of sending a broadcast query on the LAN and receiving the IP will max. get 1 mark credit. English only answers are not entertained. Answers need to talk technically.

30. Assume a 64kbps link is setup between Earth station and a Mars rover. The distance from Earth to Mars is approximately 56 Gm, and data travels over the link at the speed of light (3×10^8 m/sec.).
i. Calculate the minimum RTT on the link.
ii. What is the effective maximum data that can be on the pipe at any instance of time?
iii. The Mars rover's camera takes pictures of its surroundings and sends them to Earth. How quickly can a picture reach Earth station, assuming each image is of 6 MB in size.

ANSWER :

i. Minimum RTT of link is 2 x propagation delay on link
prop. delay = (56 x 10 ^ 9) / (3 x 10 ^ 8) = 187 seconds
RTT = 2 x 187 = 374 seconds ----------> 1 mark

ii. Max data in the pipe = delay x bandwidth = 187 x (64 x 10 ^3) bits = 1496 KB = **1.496 MB**
as more than would mean too many retransmissions or drops or ineffective transmission.

iii. transmission time for 6 MB image = (6 x 10 ^ 6) x 8 / (64 x 10^3) = 786 seconds
Now total time to reach earth = transmission time + prop.delay = 786 + 187 = 973 seconds.

So the best time for the entire image to reach earth = 973 seconds = ~ 16 minutes