GENERAL

1. Internet API is a set of rules that the sending program must follow so that the Internet can deliver the data to the destination program.
2. UDP is used together with IP when small amounts of information are involved, but it uses fewer system resources than TCP.
3. When configuring email clients, an Internet address for an SMTP server must be entered.
4. File Transfer Protocol (FTP) provides a method for copying files over a network from one computer to another.
5. The Open System Interconnection (OSI) model defines a networking framework to implement protocols in layers, with control passed from one layer to the next.
6. The Network Layer manages the mapping between these logical addresses and physical addresses. In IP networking, this mapping is accomplished through the Address Resolution Protocol (ARP).
7. To test the IP stack on your local host, you would ping the IP address 127.0.0.1.
8. A switch keeps a record of the MAC addresses of all the devices connected to it.
9. The UDP HEADER identifies the destination port and a reply port.
10. TCP/IP allows a packet to be sent without waiting for the ACKNOWLEDGEMENT of the previous packet.
11. A 10/100 Mbps hub must share its BANDWIDTH with each and every one of its ports.
12. A router is typically connected to at least two networks, commonly two LOCAL AREA NETWORKS(LANs) or WIDE AREA NETWORKS(WANs) or a LAN and its ISP'S network.
13. TRACEROUTE is a Computer Network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an (IP) network.
14. A PROTOCOL defines the format and the order of messages exchanged between two or more communicating entities.
15. The TCP/IP CHECKSUM is used to detect corruption of data over a TCP or IPv4 connection.
16. CONGESTION in a network may occur when the load on the network is greater than the capacity of the network.
17. HTTP Protocol allows exchange of HTML and WEB DATA.
18. Address Resolution Protocol (ARP) is a protocol for mapping an INTERNET PROTOCOL ADDRESS(IP) to a PHYSICAL MACHINE ADDRESS that is recognized in the local network.
19. UDP does not guarantees datagram delivery.
20. The socket type used by TCP is SOCK_STREAM.
21. With UDP, one party can overflow the other, which results in lost packets.
22. The connect system call is normally called by the client process in order to connect to a server process.
23. All the hosts from the same network can physically reach each other without an intervening router.
24. A network address can be determined based on an IP address from the network and the netmask.
25. Always, in a class of addresses, the first and last IP addresses are reserved.
26. 172.16.0.0/12 refers to a private address space.
27. When NAT is involved, the local network uses just one IP address as far as outside world is concerned.
28. The number of IP addresses allocated for each subnet block has to be a power of 2.
29. There is no routing based on MAC addresses.
30. A proxy server acts as an intermediary for requests from clients seeking resources from other servers.
31. The combination DNS server = default gateway is possible.
32. A collection of computers (PCs, Workstations) and other devices interconnected represent a computer network.
33. Hosts (computers), links (coaxial cable, twisted pair, optical fiber, radio, satellite), switches/routers (intermediate systems) are all components of a computer system.
34. Big endian means 'most significant byte first', while little endian means 'least significant byte first'.
35. SOCK_DGRAM is used for UDP connections.
36. The optical fiber cable theoretically has unlimited bandwidth.
37. Every domain name that is not already in use is not free to claim as your own.
38. Port forwarding is a use of NAT.
39. MAC addressed are guaranteed to be unique.
40. The natural mask for a class C address is 255.255.255.0.
41. The natural mask for a class B address is 255.255.0.0.
42. The natural mask for a class A address is 255.0.0.0.

43. You can only divide the network into powers of 2. If you have x IP addresses, you will have the smallest power of 2 greater than x.
44. To access a web browser, you start from your computer, go through the default gateway, reach the DNS server (which gives you the domain name for the site), return through the default gateway back to the computer, and then go to the site (web) through the default gateway where you find its IP in the DNS table. Basically, the default gateway is before and after each component.
45. It is necessary to have a separate subnet for each department, and it is necessary to know from where the internet is accessed so that you can have different addresses for each department based on IP.
46. The maximum number of hosts for a class C network is 254.
47. The maximum number of networks in a class A network is 126.
48. In TCP/IP there are 4 layers.
49. Class B address of IP address has Network 14, Host 16.
50. Class D is the multicast IP addresses class.
51. TCP header contains the following entries: Source Port, Destination Port, Sequence Number, Acknowledgement Number, Flags, Data Offset, Checksum, Urgent Pointer
52. Protocols involved in sending an email are SMTP, POP3, HTTP.
53. The length of the TCP header is 20.
54. A checksum is a 16-bit field used on the header and data to check for errors.
55. A routing table contains interface, netmask, destination address, gateway.
56. Throughput is the quantity of data over quantity of time which we send at a given time through a transmission channel.
57. Traceroute shows all IPs of the routers parsed until the current IP.
58. A congestion window is a sender impose window implemented to avoid overrunning some routers in the middle of the network path.
59. The networks can be classified on the types of transmission as circuit switching and packet switching.
60. Class A is the IP address class that can have 64000 subnets with 64000 hosts/subnet.
61. A web server can run on ports different than 80.
62. Two computers from the Internet can have the same IP address if they use private IP addresses.
63. UDP sockets are based on messages, not on a connection.
64. IP/RIP is a distance-vector routing protocol.
65. DHCP can be set up on a router.
66. TCP and UDP can use the same port at the same time.
67. ICMP Echo and Reply are used by Ping in order to determine if a host is up.
68. A TCP header is larger than a UDP header by 12 bytes.
69. UDP length = IP length – IP header's length -UDP header length

SWITCH

1. A switch has a lot of ports.
2. A switch understands MAC addresses.
3. A switch is more performant than a hub.
4. A switch can transport UDP packets.
5. A switch can transport TCP packets.
6. A switch can transport IP packets.

HUB

1. A hub doesn't understand MAC addresses.
2. A hub has many ports.

MAC ADDRESS

1. The MAC address is represented on 6 groups of 2 hexa digits.
2. The MAC address is represented on 6 bytes.

3. The MAC address can be changed.
4. The MAC address is represented on 12 hexa digits.
5. All the network cards don't have the same MAC address (Media Access Control Address and also known as Ethernet physical address).

LEVEL LINK TRANSPORT APPLICATION NETWORK

1. IP is on the Network Layer.
2. SSH is on the Application Layer.
3. HTTP is on the Application Layer.
4. SMTP is on the Application Layer.
5. DNS is on the Application Layer.
6. FTP is on the Application Layer.
7. TCP is on the Transport Layer
8. UDP is on the Transport Layer.

NETWORK ADDRESS

1. If the IP address has all 1s in the host portion (last 8 bits) of the address, it is likely a broadcast address.
2. A broadcast address can't be a network address.
3. Addresses that start with 127 or 0 can't be network addresses.
4. Network addresses are typically assigned to the first address in a subnet, which is reserved for identifying the network itself.
5. To determine if an IP address is not the first address in a subnet, you can perform a bitwise AND operation between the IP address and the inverted subnet mask. If the result of the operation is not equal to the network address, then the IP address is not the first address in the subnet.
6. If the IP address has the host portion (last 8 bits) of the address a number that it is divisible with the numbers of possible addresses, it is likely a network address.
7. The network address can be computed with the broadcast address and the netmask.
8. The network address can't be computed with the broadcast address and the IP address.
9. The network address can be computed with the IP address and the netmask.

PRIVATE ADDRESSES

1. CLI comes from Command Line Interface.
2. ARP means Address Resolution Protocol.
3. MAC means Media Access Control.
4. DNS means Domain Name System.
5. Two computers from the Internet can't have the same IP address if they have the same MAC address.
6. Not all the IP addresses in the class 172.0.0.0/8 are private.
7. Not all the IP addresses from the class 10.0.0.0/6 are private.
8. Not all the IP addresses from the class 172.0.0.0/12 are private.
9. Not all the IP addresses in the class 192.168.0.0/8 are private.
10. All the IP addresses from the class 172.16.0.0/12 are private.
11. All the IP addresses in the class 192.168.0.0/16 are private.
12. All the IP addresses from the class 10.0.0.0/16 are private.
13. All the IP addresses from the class 10.0.0.0/8 are private.
14. All the IP addresses from the class 10.0.0.0/8 are private.
15. All the IP addresses from the class 172.16.0.0/12 are private.
16. All the IP addresses from the class 10.0.0.0/16 are private.

TOPOLOGIES

1. There are several standard network topologies: Star, Bus, Ring, Mesh, Tree.

PROTOCOLS

1. DNS uses the UDP protocol.

2. HTTP uses the TCP protocol.

CONNECTION-ORIENTATION

1. UDP is not connection-oriented.
2. TCP is connection-oriented.

DEFAULT GATEWAY

1. The dimension of an IP address class has to be a power of 2.
2. The dimension of a network is 2^n, where n is the number of 0's in the netmask.

COMPUTER

1. A computer can have more network cards.
2. A computer can have more IP addresses.
3. A computer can't have 2 gateways.
4. 2 computers from the Internet can't have the same IP address if they have the same MAC address.
5. A computer is connected to a switch through a Straight-Through cable.
6. 2 computers from the same network both physically and logically can have different default gateways.
7. A router is connected to a computer with a Cross-Over cable.

SERVER

1. A web server can run on ports different than 80.
2. The DNS server configured on a computer can be in the same network with the computer.
3. A DNS server can be default gateway.
4. More websites can be hosted on the same web server.

NETMASK

1. The netmask can't contain 0 bits embedded with 1 bits.
2. 0.0.0.0 represents a valid netmask.
3. A network with the netmask 255.255.255.0 can have max. 254 computers.
4. The netmask of a network with 512 IP addresses is /23.
5. The netmask can't be determined using the IP address and the network address.
6. The netmask can't be determined using the IP address and the broadcast address.
7. The netmask can be computed using the broadcast address and the network address.
8. A netmask is a binary number on 32 bits.
9. There are other types of sockets besides TCP and UDP.
10. There are more computers with the address 127.0.0.1.
11. The address 127.0.0.1 can't be a broadcast address neither a network address.
12. 127.0.0.1 can be configured on a system as default gateway.
13. 127.0.0.1 can't be configured on a system as a DNS server.
14. The localhost is 127.0.0.1 (also known as loopback address).
15. UDP is sometimes faster than TCP.
16. TCP is sometimes faster than UDP.
17. TCP is safer than UDP.
18. The accept() call is mandatory in any TCP server.
19. The accept() call can be used in any TCP server.
20. The accept() call is not mandatory in any TCP client.
21. The recvfrom() call reads data from the UDP server.
22. The recvfrom() call doesn't send data to the TCP server.
23. The recvfrom() call doesn't send data to the TCP client.
24. The recvfrom() call doesn't send data to the UDP client.
25. The recvfrom() call reads data from the UDP client.

26. The connect() call can’t be used in UDP clients.
27. The connect() call can be used in TCP clients.
28. The connect() call is mandatory in any TCP client.
29. The sendto() call sends data to the UDP client.
30. The sendto() call sends data to the UDP server.
31. The listen() call is not mandatory in any TCP client.
32. The listen() call can be used in any TCP server.
33. The bind() call can be used in UDP clients.
34. The bind() call can be used in TCP clients.
35. The bind() call is mandatory in any TCP server.
36. The bind() call is mandatory in any UDP server.
37. LAN is not a global network.
38. The subnetwork address for the station with an IP address is determined by setting all host bits to 0.
39. Mobile phones can’t connect to the internet without a network card.
40. The IP address can’t be determined using the network address and the netmask.
41. UDP doesn’t wait for the confirmation that the packets were received.
42. The routers use the IP addresses to transfer frames to other networks.
43. A wireless access point has a limited area coverage.
44. More websites can be hosted on the same web server.
45. TCP waits for the confirmation that the packets were received.
46. An IP address is a unique identifier for every computer in an IP network.
47. The network card transfers data to other computers.
48. A UDP socket is created with the parameters AF_INET and SOCK_DGRAM.
49. The DNS service runs on the UDP port 53.
50. A TCP socket is created with the parameters AF_INET and SOCK_STREAM.
51. HTTPS transfers encrypted data.
52. A network card can have more IP addresses.
53. The broadcast address can be computed using the network address and the netmask.
54. The broadcast address can be computed using the IP address and the netmask.
55. The network card can be external.
56. The BUS topology consists of a single cable which connects in series all the computers from the network.