Networking Knowledge Base.

1. Name two technologies by which you would connect two offices in remote locations.

Two technologies that would connect two offices in remote locations are VPN and Cloud computing.

2. What is internetworking?

Internetworking is a combination of two words, inter and networking which implies an association between totally different nodes or segments.
This connection area unit is established through intercessor devices akin to routers or gateways.
The first term for associate degree internetwork was interconnected.
This interconnection is often among or between public, private, commercial, industrial, or governmental networks.
Thus, associate degree internetwork could be an assortment of individual networks,
connected by intermediate networking devices, that function as one giant network.
Internetworking refers to the trade, products, and procedures that meet the challenge of making and administering Internet works.

3. Name of the software layers or User support layer in the OSI model.

Application layer
Presentation layer
Session layer

4. Name the hardware layers or network support layers in the OSI model.

Network layer
Datalink layer
Physical layer

5. Define HTTPS protocol?

The full form of HTTPS is a Hypertext transfer protocol secure. It is an advanced version of the HTTP protocol.
Its port number is 443 by default. It uses SSL/TLS protocol for providing security.

6. Name some services provided by the application layer in the Internet model?

Some services provided by the application layer in the Internet model are as follows:

Mail services
Directory services

File transfer
Access management
Network virtual terminal

7. In which OSI layer is the header and trailer added?

At the Data link layer trailer is added and at the OSI model layer 6,5,4,3 added header.

8. What happens in the OSI model, as a data packet moves from the lower to upper layers?

In the OSI model, as a data packet moves from the lower to upper layers, headers get removed.

9. What happens in the OSI model, as a data packet moves from the upper to lower layers?

In the OSI model, as a data packet moves from the upper to lower layers, headers are added. This header contains useful information.

10. What is a zone-based firewall?

A Zone-based firewall is an advanced method of stateful firewall. In a stateful firewall, a stateful database is maintained in which the source IP address, destination IP address, source port number, and destination port number are recorded. Due to this,
only the replies are allowed i.e. if the traffic is Generated from inside the network then only the replies (of inside network traffic) coming
from outside the network are allowed.

Cisco IOS router can be made firewall through two methods:

By using CBAC: create an access list and apply it to the interfaces keeping in mind what traffic should be allowed or denied and in what direction.
This has an extra overhead for the administrator.
Using a Zone-based firewall.
For more details please refer Zone-based firewall article.

11. What is a server farm?

A server farm is a set of many servers interconnected together and housed within the same physical facility.
A server farm provides the combined computing power of many servers by simultaneously executing one or more applications or services.
A server farm is generally a part of an enterprise data center or a component of a supercomputer. A server farm is also known as a server
cluster or computer ranch.

12. Name the three means of user authentication.

There is biometrics (e.g. a thumbprint, iris scan), a token, or a password.
There is also two-level authentication, which employs two of those methods.

13. What is Confidentiality, Integrity & Availability?

The CIA triad can be broadly defined as:

Confidentiality – means information is not disclosed to unauthorized individuals, entities, or processes.
For example, if we say I have a password for my Gmail account but someone saw it while I was doing login into my Gmail account.
In that case, my password has been compromised and Confidentiality has been breached.

Integrity – means maintaining the accuracy and completeness of data. This means data cannot be edited in an unauthorized way.
For example, if an employee leaves an organization then in that case data for that employee in all departments like accounts, should be updated to reflect the status to JOB LEFT so that data is complete and accurate in addition, this is only authorized persons should be allowed to edit employee data.

Availability – means information must be available when needed. For example, if one needs to access information about a particular employee to check whether an employee has outstood the number of leaves, that case, it requires collaboration from different organizational teams like network operations, development operations, incident response, and policy/change management.
Denial of service attack is one of the factors that can hamper the availability of information.

14. What is VPN?

VPN stands for the virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet.
A Virtual Private Network is a way to extend a private network using a public network such as the Internet.
The name only suggests that it is a Virtual “private network” i.e. user can be part of a local network sitting at a remote location.
It makes use of tunneling protocols to establish a secure connection.

15. What is Symmetric and Asymmetric Encryption?

Symmetric Key Encryption: Encryption is a process to change the form of any message in order to protect it from reading by anyone.
In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure.
It also requires a safe method to transfer the key from one party to another.
Asymmetric Key Encryption: Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different keys to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower.
For more details please refer difference between symmetric and asymmetric encryption articles.

16. At what layer IPsec works?

An IPsec works on layer 3 of the OSI model.

17. What is a Tunnel mode?

This is a mode of data exchange wherein two communicating computers do not use IPSec themselves. Instead,
the gateway that is connecting their LANs to the transit network creates a virtual tunnel that uses the
IPSec protocol to secure all communication that passes through it.
Tunnel mode is most commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.
Tunnel mode is most commonly used to encrypt traffic between secure IPSec gateways, such as between the Cisco router and PIX Firewall

18. Define Digital Signatures?

As the name sounds are the new alternative to signing a document digitally.
It ensures that the message is sent to the intended use without any tampering by any third party (attacker).
In simple words, digital signatures are used to verify the authenticity of the message sent electronically.

OR

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

19. What is Authorization?

Authorization provides capabilities to enforce policies on network resources after the user has gained access to the network resources
through authentication. After the authentication is successful, authorization can be used to determine what resources is the user allowed to access
and the operations that can be performed.

20. What is the difference between IPS and a firewall?

The Intrusion Prevention System is also known as Intrusion Detection and Prevention System.
It is a network security application that monitors network or system activities for malicious activity.

The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it,
and attempt to block or stop it. Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because
both IPS and IDS operate network traffic and system activities for malicious activity. IPS typically records information related to observed events,
notifies security administrators of important observed events, and produces reports. Many IPS can also respond to a detected threat by attempting
to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment,
or changing the attack’s content. A firewall is a network security device, either hardware or software-based,
which monitors all incoming and outgoing traffic, and based on a defined set of security rules it accepts, rejects, or drops that specific traffic.

21. What is IP Spoofing?

IP Spoofing is essentially a technique used by hackers to gain unauthorized access to Computers.
Concepts of IP Spoofing were initially discussed in academic circles as early as 1980.
IP Spoofing types of attacks had been known to Security experts on the theoretical level.
It was primarily theoretical until Robert Morris discovered a security weakness in the TCP protocol known as sequence prediction.
Occasionally IP spoofing is done to mask the origins of a Dos attack. In fact, Dos attacks often mask the actual
IP addresses from where the attack has originated from.

22. What is the meaning of threat, vulnerability, and risk?

Threats are anything that can exploit a vulnerability accidentally or intentionally and destroy or damage an asset.
An asset can be anything people, property, or information. The asset is what we are trying to protect and a threat is what we are trying to protect against.
Vulnerability means a gap or weakness in our protection efforts.

Risk is nothing but an intersection of assets, threats, and vulnerability.

A+T+V = R

23. What is the main purpose of a DNS server?

DNS stands for Domain Name Server. It translates Internet domains and hostnames to IP addresses and vice versa.
DNS technology allows typing names into your Web browsers and your computer to automatically find that address on the Internet.
A key element of the DNS is a worldwide collection of DNS servers.
It has the responsibility of assigning domain names and mapping those names to Internet resources by designating an
authoritative name server for each domain.
The Internet maintains two main namespaces like Domain Name hierarchy and Internet protocol address space.

24. What is the protocol and port no of DNS?

Protocol – TCP/UDP

Port number- 53

25. What is the position of the transmission media in the OSI model?

In the OSI model, transmission media supports layer-1(Physical layer).

26. What is the importance of twisting in the twisted-pair cable?

The twisted-pair cable consists of two insulated copper wires twisted together. The twisting is important for minimizing electromagnetic radiation and external interference.

27. What kind of error is undetectable by the checksum?

In checksum, multiple-bit errors can not be undetectable.

28. Which multiplexing technique is used in the Fiber-optic links?

The wavelength division multiplexing is commonly used in fiber optic links.

29. What are the Advantages of Fiber Optics?

The advantages of Fiber Optics are mentioned below:

Bandwidth is above copper cables.
Less power loss and allows data transmission for extended distances.
The optical cable is resistant to electromagnetic interference.
Fiber cable is sized 4.5 times which is best than copper wires.
As the cable is lighter, and thinner, in order that they use less area as compared to copper wires.
Installation is extremely easy thanks to less weight.
Optical fiber cable is extremely hard to tap because they don’t produce electromagnetic energy. These optical fiber cables are very secure for transmitting data.
This cable opposes most acidic elements that hit copper wires also are flexible in nature.
Optical fiber cables are often made cheaper than equivalent lengths of copper wire.
Light has the fastest speed within the universe, such a lot faster signals.
Fiber optic cables allow much more cable than copper twisted-pair cables.
Fiber optic cables have how more bandwidth than copper twisted-pair cables.
30. Which of the multiplexing techniques are used to combine analog signals?
To combine analog signals, commonly FDM(Frequency division multiplexing) and WDM (Wavelength-division multiplexing) are used.

31. Which of the multiplexing techniques is used to combine digital signals?

To combine digital signals, time division multiplexing techniques are used.

32. Can IP Multicast be load-balanced?

No, The IP multicast multipath command load splits the traffic and does not load balance the traffic.
Traffic from a source will use only one path, even if the traffic far outweighs traffic from other sources.

33. What is CGMP(Cisco Group Management Protocol)?

CGMP is a simple protocol, the routers are the only devices that are producing CGMP messages.
The switches only listen to these messages and act upon them. CGMP uses a well-known destination MAC address (0100.0cdd.dddd) for all its messages.
When switches receive frames with this destination address, they flood it on all their interfaces Bluetoothso all switches in the network will receive CGMP messages.

Within a CGMP message, the two most important items are:

Group Destination Address (GDA)
Unicast Source Address (USA)
The group destination address is the multicast group MAC address, and a unicast source address is the MAC address of the host (receiver).

34. What is Multicast?

Multicast is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously.
Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers
at once across LANs or WANs. This process helps in minimizing the data frame of the network. For more details please read Multicasting in computer
network article.

35. What is the difference between Bluetooth and wifi?

Bluetooth Wifi
Bluetooth has no full form. While Wifi stands for Wireless Fidelity.
It requires a Bluetooth adapter on all devices for connectivity.
Whereas it requires a wireless adapter Bluetooth for all devices and a wireless router for connectivity.
Bluetooth consumes low power.   while it consumes high power.
The security of BlueTooth is less in comparison to the number of wifi. While it provides better security than BlueTooth.
Bluetooth is less flexible means these limited users are supported. Whereas wifi supports a large number of users.
The radio signal range of BlueTooth is ten meters. Whereas in wifi this range is a hundred meters.
Bluetooth requires low bandwidth. While it requires high bandwidth.

36. What is a reverse proxy?

Reverse Proxy Server: The job of a reverse proxy server is to listen to the request made by the client and redirect to the particular web server which is present
on different servers. This is also used to restrict the access of the clients to the confidential data residing on particular servers.
For more details please refer to what is proxy server article.

37. What is the role of address in a packet traveling through a datagram network?

The address field in a datagram network is end-to-end addressing.

38. Can a routing table in the datagram network have two entries with the same destination address?

No. routing tables in the datagram network have two entries with the same destination address,
not possible because the destination address or receiver address is unique in the datagram network.

39. What kind of arithmetic is used to add data items in checksum calculation?

To add data items in checksum calculations, one’s complement arithmetic is used.

40. Define piggybacking?

Piggybacking is used to improve the efficiency of the bidirectional protocols.

When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B;
when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

41. What are the advantages and disadvantages of piggybacking?

Advantages of Piggybacking:

The major advantage of piggybacking is the better use of available channel bandwidth.

Disadvantages of Piggybacking:

The major disadvantage of piggybacking is additional complexity and if the data link layer waits too long before transmitting the acknowledgment,
then re-transmission of the frame would take place.

42. Which technique is used in byte-oriented protocols?

Byte stuffing is used in byte-oriented protocols. A special byte is added to the data section of the frame
when there is a character with the same pattern as the flag.

43. Define the term OFDM?

Orthogonal Frequency Division Multiplexing (OFDM):

It is also the multiplexing technique that is used in an analog system.
In OFDM, the Guard band is not required and the spectral efficiency of OFDM is high which oppose to the FDM. In OFDM,
a Single data source attaches all the sub-channels.

44. What is a transparent bridge?

Transparent Bridge:
A transparent bridge automatically maintains a routing table and updates tables in response to maintaining changing topology.
The transparent bridge mechanism consists of three mechanisms:

Frame forwarding
Address Learning
Loop Resolution
The Transparent bridge is easy to use. Install the bridge and no software changes are needed in the hosts. In all the cases,
transparent bridges flooded the broadcast and multicast frames.

45. What is the minimum size of the icmpV4 packet what is the maximum size of the icmpv4 packet?

Minimum size ICMPv4 packet = 28 bytes
Maximum size ICMPv4 packet = 2068 bytes
46. Why do we OSPF a protocol that is faster than our RIP?
OSPF stands for Open Shortest Path First which uses a link-state routing algorithm. This protocol is faster than RIP because:
Using the link-state information which is available in routers,
it constructs the topology of Bluetooth which Bluetooth the topology determines the routing table for routing decisions.
It supports both variable-length subnet masking and classless inter-domain routing addressing models.
Since it uses Dijkstra’s algorithm, it computes the shortest path tree for each route.
OSPF (Open Shortest Path First) is handling the error detection by itself and it uses multicast addressing for routing in a broadcast domain.

47. What are the two main categories of DNS messages?

The two categories of DNS messages are queries and replies.

48. Why do we need the pop3 protocol for e-mail?

Need of POP3: The Post Office Protocol (POP3) is the most widely used protocol and is supported by most email clients.
It provides a convenient and standard way for users to access mailboxes and download messages.
An important advantage of this is that the mail messages get delivered to the client’s PC and they can be read with or without accessing the web.

49. Define the term Jitter?

Jitter is a “packet delay variance”.
It can simply mean that jitter is considered a problem when different packets of data face different delays
in a network and the data at the receiver application is time-sensitive, i.e. audio or video data. Jitter is measured in milliseconds(ms).
It is defined as an interference in the normal order of sending data packets.

50. Why Bandwidth is important to network performance parameters?

Bandwidth is characterized as the measure of data or information that can be transmitted in a fixed measure of time.
The term can be used in two different contexts with two distinctive estimating values. In the case of digital devices,
the bandwidth is measured in bits per second(bps) or bytes per second. In the case of analog devices, the bandwidth is measured in cycles per second,
or Hertz (Hz).
Bandwidth is only one component of what an individual sees as the speed of a network.
True internet speed is actually the amount of data you receive every second and that has a lot to do with latency too.

51. How do I Identify When an IP Address is Private or Public?

You can identify private IP addresses by checking if they fall within the reserved ranges (e.g., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

52. How To Get an IP Address from Domain Name?

Answer: We can get an IP address from a domain name using ping commands and nslookup command.For this, use command-line tools like PING
or nslookup to get the IP address.
Run the commands “PING example.com” or “nslookup example.com” on command prompt or terminal window.

53. Which Diffie Hellman Group is Most Secure?

The most secure Diffie-Hellman group is currently considered to be Group 24 (2048-bit ECP) or higher, offering stronger encryption and resistance to attacks.
Apart from that the security of a Diffie-Hellman (DH) group depends on the size and type of the underlying prime numbers or elliptic curves used.

54. How Flow Control is Achieved in TCP?

In computer networks, reliable data delivery is important.
The Transmission Control Protocol guarantees in-order and error-free data transfer using flow control.
This is to prevent the sender from flooding the receiver so as to make sure it can work efficiently in turn.
TCP utilizes a sliding window protocol for flow control.
The receiver advertises a window size, indicating the number of bytes its buffer can hold.
The sender transmits data segments up to this advertised window.

55. How To Find Your Port Number ?

We can find port number using command line Tool, and using resource monitor. By utilizing the tools like ‘Netstat’ we can troubleshoot
and monitor our system and network,
and also gain the insights into network security, and identify any processes using specific ports.
It will help us in managing and securing our system efficiently.