**Topic: Networking Interview Questions**

**Q #1) What is a Network?**

**Answer:** Network is defined as a set of devices connected to each other using a physical transmission medium.

**For Example,** A computer network is a group of computers connected with each other to communicate and share information and resources like hardware, data, and software. In a network, nodes are used to connect two or more networks.

**Q #2) What is a Node?**

**Answer:** Two or more computers are connected directly by an optical fiber or any other cable. A node is a point where a connection is established. It is a network component that is used to send, receive and forward the electronic information.

A device connected to a network is also termed as Node. Let’s consider that in a network there are 2 computers, 2 printers, and a server are connected, then we can say that there are five nodes on the network.



**Q #3) What is Network Topology?**

**Answer:** Network topology is a physical layout of the computer network and it defines how the computers, devices, cables, etc are connected to each other.

**Q #4) What are Routers?**

**Answer:** The router is a network device that connects two or more network segments. It is used to transfer information from the source to the destination.

Routers send the information in terms of data packets and when these data packets are forwarded from one router to another router then the router reads the network address in the packets and identifies the destination network.

**Q #5) What is the OSI reference model?**

**Answer: O**pen **S**ystem **I**nterconnection, the name itself suggests that it is a reference model that defines how applications can communicate with each other over a networking system.

It also helps to understand the relationship between networks and defines the process of communication in a network.

**Q #6) What are the layers in OSI Reference Models? Describe each layer briefly.**

**Answer: Given below are the seven layers of OSI Reference Models:**

**a) Physical Layer (Layer 1):** It converts data bits into electrical impulses or radio signals. **Example:** Ethernet.

**b) Data Link Layer (Layer 2):** At the Data Link layer, data packets are encoded and decoded into bits and it provides a node to node data transfer. This layer also detects the errors that occurred at Layer 1.

**c) Network Layer (Layer 3):** This layer transfers variable length data sequence from one node to another node in the same network. This variable-length data sequence is also known as **“Datagrams”**.

**d) Transport Layer (Layer 4):** It transfers data between nodes and also provides acknowledgment of successful data transmission. It keeps track of transmission and sends the segments again if the transmission fails.



**e) Session Layer (Layer 5):** This layer manages and controls the connections between computers. It establishes, coordinates, exchange and terminates the connections between local and remote applications.

**f) Presentation Layer (Layer 6):** It is also called as “Syntax Layer”. Layer 6 transforms the data into the form in which the application layer accepts.

**g) Application Layer (Layer 7):** This is the last layer of the OSI Reference Model and is the one that is close to the end-user. Both end-user and application layer interacts with the software application. This layer provides services for email, file transfer, etc.

**Q #7) What is the difference between Hub, Switch, and Router?**

**Answer:**

|  |  |  |
| --- | --- | --- |
| **Hub** | **Switch** | **Router** |
| Hub is least expensive, least intelligent and least complicated of the three. It broadcast all data to every port which may cause serious security and reliability concern | Switches work similarly like Hubs but in a more efficient manner. It creates connections dynamically and provides information only to the requesting port | The router is smartest and most complicated out of these three. It comes in all shapes and sizes. Routers are similar like little computers dedicated for routing network traffic |
| In a Network, Hub is a common connection point for devices connected to the network. Hub contains multiple ports and is used to connect segments of LAN | Switch is a device in a network which forwards packets in a network | Routers are located at gateway and forwards data packets |

**Q #8) Explain TCP/IP Model**

**Answer:** The most widely used and available protocol is TCP/IP i.e. Transmission Control Protocol and Internet Protocol. TCP/IP specifies how data should be packaged, transmitted and routed in their end to end data communication.

**There are four layers as shown in the below diagram:**



**Given below is a brief explanation of each layer:**

 **Application Layer**: This is the top layer in the TCP/IP model. It includes processes that use the Transport Layer Protocol to transmit the data to their destination. There are different Application Layer Protocols such as HTTP, FTP, SMTP, SNMP protocols, etc.

 **Transport Layer**: It receives the data from the Application Layer which is above the Transport Layer. It acts as a backbone between the host’s system connected with each other and it mainly concerns about the transmission of data. TCP and UDP are mainly used as Transport Layer protocols.

 **Network or Internet Layer**: This layer sends the packets across the network. Packets mainly contain source & destination IP addresses and actual data to be transmitted.

 **Network Interface Layer**: It is the lowest layer of the TCP/IP model. It transfers the packets between different hosts. It includes

encapsulation of IP packets into frames, mapping IP addresses to physical hardware devices, etc.

**Q #9) What is HTTP and what port does it use?**

**Answer:** HTTP is HyperText Transfer Protocol and it is responsible for web content. Many web pages are using HTTP to transmit the web content and allow the display and navigation of HyperText. It is the primary protocol and port used here is TCP port 80.

**Q #10) What is HTTPs and what port does it use?**

**Answer:** HTTPs is a Secure HTTP. HTTPs is used for secure communication over a computer network. HTTPs provides authentication of websites that prevents unwanted attacks.

In bi-directional communication, the HTTPs protocol encrypts the communication so that the tampering of the data gets avoided. With the help of an SSL certificate, it verifies if the requested server connection is a valid connection or not. HTTPs use TCP with port 443.

**Q #11) What are TCP and UDP?**

**Answer: Common factors in TCP and UDP are:**

 TCP and UDP are the most widely used protocols that are built on the top of the IP protocol.

 Both protocols TCP and UDP are used to send bits of data over the Internet, which is also known as ‘packets’.

 When packets are transferred using either TCP or UDP, it is sent to an IP address. These packets are traversed through routers to the destination.

**The difference between TCP and UDP are enlisted in the below table:**

|  |  |
| --- | --- |
| **TCP** | **UDP** |
| TCP stands for Transmission Control Protocol | UDP is stands for User Datagram Protocol or Universal Datagram Protocol |
| Once the connection is setup, data can be sent bi-directional i.e. TCP is a connection oriented protocol | UDP is connectionless, simple protocol. Using UDP, messages are sent as packets |
| The speed of TCP is slower than UDP | UDP is faster compared to TCP |
| TCP is used for the application where time is not critical part of data transmission | UDP is suitable for the applications which require fast transmission of data and time is crucial in this case. |
| TCP transmission occurs in a sequential manner | UDP transmission also occurs in a sequential manner but it does not maintain the same sequence when it reaches the destination |
| It is heavy weight connection | It is lightweight transport layer |
| TCP tracks the data sent to ensure no data loss during data transmission | UDP does not ensure whether receiver receives packets are not. If packets are misses then they are just lost |

**Q #12) What is a Firewall?**

**Answer:** Firewall is a network security system that is used to protect computer networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.

The firewall consists of a hardware device, software program or a combined configuration of both. All the messages that route through the firewall are examined by specific security criteria and the messages which meet the criteria are successfully traversed through the network or else those messages are blocked.



Firewalls can be installed just like any other computer software and later can be customized as per the need and have some control over the access and security features. “

Windows Firewall” is an inbuilt Microsoft Windows application that comes along with the operating system. This “Windows Firewall” also helps to prevent viruses, worms, etc.

**Q #13) What is DNS?**

**Answer:** Domain Name Server (DNS), in a non-professional language and we can call it an Internet’s phone book. All the public IP addresses and their hostnames are stored in the DNS and later it translates into a corresponding IP address.

For a human being, it is easy to remember and recognize the domain name, however, the computer is a machine that does not understand the human language and they only understand the language of IP addresses for data transfer.

There is a “Central Registry” where all the domain names are stored and it gets updated on a periodic basis. All Internet service providers and different host companies usually interact with this central registry to get the updated DNS details.

**For Example**, When you type a website www.softwaretestinghelp.com, then your Internet service provider looks for the DNS associated with this domain name and translates this website command into a machine language – IP address – 151.144.210.59 (note that, this is the imaginary IP address and not the actual IP for the given website) so that you will get redirected to the appropriate destination.

**This process is explained in the below diagram:**



**Q #14) What is the difference between a Domain and a Workgroup?**

**Answer:** In a computer network, different computers are organized in different methods and these methods are – Domains and Workgroups. Usually, computers which run on the home network belong to a Workgroup.

However, computers that are running on an office network or any workplace network belong to the Domain.

**Their differences are as follows:**

|  |  |
| --- | --- |
| **Workgroup** | **Domain** |
| All computers are peers and no computer has control over another computer | Network admin uses one or more computer as a server and provide all accesses, security permission to all other computers in a network |
| In a Workgroup, each computer maintains their own database | The domain is a form of a computer network in which computers, printers, and user accounts are registered in a central database. |
| Each computer has their own authentication rule for every user account | It has centralized authentication servers which set the rule of authentication |
| Each computer has set of user account. If user has account on that computer then only user able to access the computer | If user has an account in a domain then user can login to any computer in a domain |
| Workgroup does not bind to any security permission or does not require any password | Domain user has to provide security credentials whenever they are accessing the domain network |
| Computer settings need to change manually for each computer in a Workgroup | In a domain, changes made in one computer automatically made same changes to all other computers in a network |
| All computers must be on same local area network | In a domain, computers can be on a different local network |
| In a Workgroup, there can be only 20 computers connected | In a domain, thousands of computers can be connected |

**Q #15) What is a Proxy Server and how do they protect the computer network?**

**Answer:** For data transmission, IP addresses are required and even DNS uses IP addresses to route to the correct website. It means without the knowledge of correct and actual IP addresses it is not possible to identify the physical location of the network.

Proxy servers prevent external users who are unauthorized to access such IP addresses of the internal network. It makes the computer network virtually invisible to external users.