NAME: SAAD UR REHMAN

ID: 15608

SEMESTER: 3rd

SUBJECT: Advance Computer Networks (MS EE)

Sessional Assignment 2020

Q1: Differentiate between a Hub, Switch and Router?

Hub Vs. Switch:

A hub works on the physical layer (Layer 1) of OSI model while Switch works on the data link layer (Layer 2). Switch is more efficient than the hub. A switch can join multiple computers within one LAN, and a hub just connects multiple Ethernet devices together as a single segment. Switch is smarter than hub to determine the target of the forwarding data. Since switch has a higher performance, its cost will also become more expensive.

Switch Vs. Router:

In the OSI model, router is working on a higher level of network layer (Layer 3) than switch. Router is very different from the switch because it is for routing packet to other networks. It is also more intelligent and sophisticated to serve as an intermediate destination to connect multiple area networks together. A switch is only used for wired network, yet a router can also link with the wireless network. With much more functions, a router definitely costs higher than a switch.

Hub Vs. Router:

As mentioned above, a hub only contains the basic function of a switch. Hence, differences between hub and router are even bigger. For instance, hub is a passive device without software while router is a networking device, and data transmission form in hub is in electrical signal or bits while in router it is in form of packet.

Q2: What does a backbone network means?

A backbone is the part of the computer network infrastructure that interconnects different networks and provides a path for exchange of data between these different networks. A backbone may interconnect different local area networks in offices, campuses or buildings. When several local area networks (LAN) are being interconnected over a considerable area, the result is a wide area network (WAN), or metropolitan area network (MAN) if it happens to serve the whole city. On a large scale, a backbone is a set of pathways to which other large networks connect for long distance communication. Various networking technologies work together as connection points or nodes, and are connected by different mediums for transporting data like optical fiber, traditional copper and even wireless technology like microwave and satellites. The traditional notion of a backbone is a bundle of wires, which serves the multiple networks

as the main super highway for data. The idea remains the same, but the execution has become more diverse. Of course the capacity of the backbone is supposed to be greater than that of the networks it serves.

Q3: Explain the protocols used at different TCP/IP layers?

A protocol is a set of rules that govern how systems communicate. For networking they govern how data is transferred from one system to another.

What is a Protocol Suite:

A protocol suite is a collection of protocols that are designed to work together.Before TCP/IP became the de-facto standard other protocol suites like IPX and SPX were common (Novell).

Protocol Stacks:

It is possible to write a single protocol that takes data from one computer application and sends it to an application on another computer.- A Single stack Protocol The problem with this approach is that it very inflexible, as any changes require changing the entire application and protocol software. The approach used in networking is to create layered protocol stacks. Each level of the stack performs a particular function and communicates with the levels above and below it. This layered arrangement is not confined to networking, and how it works is probably best understood if you compare it to real life example.

Let's take an example of a parcel service between two offices.

The task is simple – send parcels between people in each office.

We will divide the task into two distinct processes as follows:

1. Take a package, wrap it and address it.
2. Send it to the destination

at the receiving end

1. Receive the package
2. Deliver it to the recipient

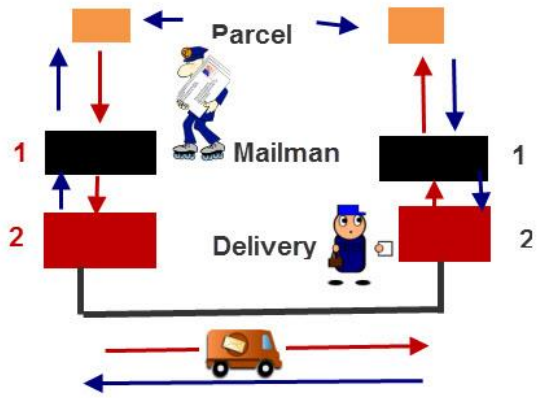
Typically you would have an internal mail man that:

1. Collects the parcels from the senders and takes then to a mail dispatch room.
2. The parcels are placed in a van by the dispatcher and then driven to the remote office.

At the remote office

1. The parcels are received by the dispatcher and placed into a tray for the mail man
2. The mail man collects the parcels and delivers them to the recipients,

Here is a simple diagram to illustrate the process:

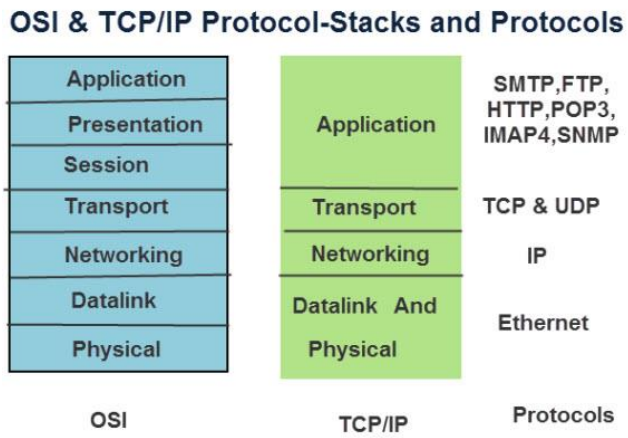


Layered System Example

The OSI and TCP/IP Networking Models

All networking courses teach the 7 layer OSI model.

It is important to understand that this model provides for a conceptual framework, and no modern protocols implement this model fully.



Q4: What is anonymous FTP?

Anonymous FTP is a method of giving users access to an FTP server without having to provide any credentials to the server. Sometimes anonymous FTP requires a general username and password which anyone could use and does not identify individuals. Anonymous FTP is usually only for retrieving files. This is a common method for downloading public files via the file transfer protocol.

Q5: What is subnet mask?

A subnet mask is a number that defines a range of IP addresses available within a network. A single subnet mask limits the number of valid IPs for a specific network. Multiple subnet masks can organize a single network into smaller networks (called sub networks or subnets). Systems within the same subnet can communicate directly with each other, while systems on different subnets must communicate through a router.
A subnet mask hides (or masks) the network part of a system's IP address and leaves only the host part as the machine identifier. It uses the same format as an IPv4 address — four sections of one to three numbers, separated by dots. Each section of the subnet mask can contain a number from 0 to 255, just like an IP address. For example, a typical subnet mask for a Class C IP address is:

255.255.255.0

In the example above, the first three sections are full (255 out of 255), meaning the IP addresses of devices within the subnet mask must be identical in the first three sections. The last section of each computer's IP address can be anything from 0 to 255. If the subnet mask is defined as 255.255.255.0, the IP addresses 10.0.1.99 and 10.0.1.100 are in the same subnet, but 10.0.2.100 is not.

A subnet mask of 255.255.255.0 allows for close to 256 unique hosts within the network (since not all 256 IP addresses can be used). If your computer is connected to a network, you can view the network's subnet mask number in the Network control panel (Windows) or System Preference (macOS). Most home networks use the default subnet mask of 255.255.255.0. However, an office network may be configured with a different subnet mask such as 255.255.255.192, which limits the number of IP addresses to 64.

Large networks with several thousand machines may use a subnet mask of 255.255.0.0. This is the default subnet mask used by Class B networks and provides up to 65,536 IP addresses (256 x 256). The largest Class A networks use a subnet mask of 255.0.0.0, allowing for up to 16,777,216 IP addresses (256 x 256 x 256).

Q6: What is NAT?

Stands for "Network Address Translation." NAT translates the IP addresses of computers in a local network to a single IP address. This address is often used by the router that connects the computers to the Internet. The router can be connected to a DSL modem, cable modem, T1 line, or even a dial-up modem. When other computers on the Internet attempt to access computers within the local network, they only see the IP address of the router. This adds an extra level of security, since the router can be configured as a firewall, only allowing authorized systems to access the computers within the network.

Once a system from outside the network has been allowed to access a computer within the network, the IP address is then translated from the router's address to the computer's unique address. The address is found in a "NAT table" that defines the internal IP addresses of computers on the network. The NAT table also defines the global address seen by computers outside the network. Even though each computer within the local network has a specific IP address, external systems can only see one IP address when connecting to any of the computers within the network.

To simplify, network address translation makes computers outside the local area network (LAN) see only one IP address, while computers within the network can see each system's unique address. While this aids in network security, it also limits the number of IP addresses needed by companies and organizations. Using NAT, even large companies with thousands of computers can use a single IP address for connecting to the Internet.

Q7: Differentiate between TCP and UDP?

Differences between TCP and UDP

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
1. TCP is a connection-oriented protocol. **2**. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
3. TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
4. TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
5. Sequencing of data is a feature of Transmission Control Protocol (TCP). This means that packets arrive in-order	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.

TRANSMISSION CONTROL PROTOCOL (TCP)	USER DATAGRAM PROTOCOL (UDP)
at the receiver.	
6. TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
7. Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
8. TCP has a (20-80) bytes variable length header.	UDP has a 8 bytes fixed length header.
9. TCP is heavy-weight.	UDP is lightweight.
10. TCP doesn't supports Broadcasting.	UDP supports Broadcasting.
11. TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.

Q8: What is RIP and its key features?

Routing Information Protocol (RIP):

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

Hop Count:

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP:

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. This is also known as routing on rumors.

RIP V1	RIP V2	RIPNG
Sends update as broadcast	Sends update as multicast	Sends update as multicast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9	Multicast at FF02::9 (RIPng can only run on IPv6 networks)
Doesn't support authentication of update messages	Supports authentication of RIPv2 update messages	–
Classful routing protocol	Classless protocol, supports classful	Classless updates are sent

Q9: Explain what is a firewall?

Firewall defined:

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

How does a firewall work:

Firewalls carefully analyze incoming traffic based on pre-established rules and filter traffic coming from unsecured or suspicious sources to prevent attacks. Firewalls guard traffic at a computer's entry point, called ports, which is where information is exchanged with external devices. For example, "Source address 172.18.1.1 is allowed to reach destination 172.18.2.1 over port 22."

Think of IP addresses as houses, and port numbers as rooms within the house. Only trusted people (source addresses) are allowed to enter the house (destination address) at all—then it's further filtered so that people within the house are only allowed to access certain rooms (destination ports), depending on if they're the owner, a child, or a guest. The owner is allowed to any room (any port), while children and guests are allowed into a certain set of rooms (specific ports).

Q10: What is NOS?

Network operating system is an operating system designed for the sole purpose of supporting workstations, database sharing, application sharing and file and printer access sharing among multiple computers in a network. Certain standalone operating systems, such as Microsoft Windows NT and Digital's OpenVMS, come with multipurpose capabilities and can also act as network operating systems. Some of the most well-known network operating systems include Microsoft Windows Server 2003, Microsoft Windows Server 2008, Linux and Mac OS X.The salient features of network operating systems are:

- Basic operating system features support like protocol support, processor support, hardware detection and multiprocessing support for applications
- Security features like authentication, restrictions, authorizations and access control
- Features for file, Web service, printing and replication
- Directory and name services management
- User management features along with provisions for remote access and system management
- Internetworking features like routing and WAN ports
- Clustering capabilities

Common tasks associated with network operating systems include:

- User administration
- System maintenance activities like backup
- Tasks associated with file management
- Security monitoring on all resources in the network
- Setting priority to print jobs in the network

Q11: What is Denial of Service (DoS)?

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected. Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle. There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- Buffer overflow attacks – the most common DoS attack. The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks
- ICMP flood – leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.
- SYN flood – sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Other DoS attacks simply exploit vulnerabilities that cause the target system or service to crash. In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system, so that it can’t be accessed or used.

An additional type of DoS attack is the Distributed Denial of Service (DDoS) attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack to a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once. The distribution of hosts that defines a DDoS provides the attacker multiple advantages:

- He can leverage the greater volume of machine to execute a seriously disruptive attack
- The location of the attack is difficult to detect due to the random distribution of attacking systems (often worldwide)
- It is more difficult to shut down multiple machines than one
- The true attacking party is very difficult to identify, as they are disguised behind many (mostly compromised) systems

Modern security technologies have developed mechanisms to defend against most forms of DoS attacks, but due to the unique characteristics of DDoS, it is still regarded as an elevated threat and is of higher concern to organizations that fear being targeted by such an attack.

Q12: What is piggybacking?

In reliable full - duplex data transmission, the technique of hooking up acknowledgments onto outgoing data frames is called piggybacking.

Why Piggybacking:

Communications are mostly full – duplex in nature, i.e. data transmission occurs in both directions. A method to achieve full – duplex communication is to consider both the communication as a pair of simplex communication. Each link comprises a forward channel for sending data and a reverse channel for sending acknowledgments. However, in the above arrangement, traffic load doubles for each data unit that is transmitted. Half of all data transmission comprise of transmission of acknowledgments.

So, a solution that provides better utilization of bandwidth is piggybacking. Here, sending of acknowledgment is delayed until the next data frame is available for transmission. The acknowledgment is then hooked onto the outgoing data frame. The data frame consists of an **ack** field. The size of the **ack** field is only a few bits, while an acknowledgment frame comprises of several bytes. Thus, a substantial gain is obtained in reducing bandwidth requirement.

Working Principle:

Suppose that there are two communication stations X and Y. The data frames transmitted have an acknowledgment field, **ack** field that is of a few bits length. Additionally, there are frames for sending acknowledgments, ACK frames. The purpose is to minimize the ACK frames.

The three principles governing piggybacking when the station X wants to communicate with station Y are:

1. If station X has both data and acknowledgment to send, it sends a data frame with the **ack** field containing the sequence number of the frame to be acknowledged.
2. If station X has only an acknowledgment to send, it waits for a finite period of time to see whether a data frame is available to be sent. If a data frame becomes available, then it piggybacks the acknowledgment with it. Otherwise, it sends an ACK frame.
3. If station X has only a data frame to send, it adds the last acknowledgment with it. The station Y discards all duplicate acknowledgments. Alternatively, station X may send the data frame with the **ack** field containing a bit combination denoting no acknowledgment

Q13: What is DNS?

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1:: c629:d7a2 (in IPv6).

How does DNS work:

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it's important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user's computer apart from the initial request.

There are 4 DNS servers involved in loading a webpage:

DNS recursor - The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.

Root name server - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.

TLD name server - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This name server is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is "com").

Authoritative name server - This final name server can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative name server is the last stop in the name server query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

Q14: What is OSPF?

Open Shortest Path First (OSPF) protocol States:

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR). OSPF terms

1. Router I'd – It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. Router priority – It is a 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.
3. Designated Router (DR) – It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.
4. Backup Designated Router (BDR) – BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

Q15: What is a ping?

Ping is a command-line utility, available on virtually any operating system with network connectivity that acts as a test to see if a networked device is reachable.
The ping command sends a request over the network to a specific device. A successful ping results in a response from the computer that was pinged back to the originating computer.

What does Ping stand for:

According to the author, the name Ping comes from sonar terminology. In sonar, a ping is an audible sound wave sent out to find an object. If the sound hits the object, the sound waves will reflect, or echo, back to the source. The distance and location of the object can be determined by measuring the time and direction of the returning sound wave.

Similarly, the ping command sends out an echo request. If it finds the target system, the remote host sends back an echo reply. The distance (number of hops) to the remote system can be determined from the reply, as well as the conditions in-between (packet loss and time to respond). While the author of the ping utility said the name of the program was simply based on the sound of sonar, others sometimes say that Ping is an acronym for Packet Internet Groper.

Q16: In a network that contains two servers and twenty workstations, where is the best place to install an Anti-Virus program?

You need AT LEAST three levels of security.

A good firewall. This can stop intrusions, malware, unauthorized access, etc. before they reach the workstations.

Antivirus software on the servers and at the endpoint workstations. This software should be centrally managed to keep end users updated constantly and to minimize user meddling with the settings. Good antivirus will also protect email clients.

Educated and aware users who: do not casually install downloaded programs; don't click on unknown links; don't fall for phishing emails, etc. Establish a strong password policy for all users. You should consider not giving your users Administrative rights on their accounts. They will complain that they cannot install what they need and your workload will increase but, I guarantee you, your entire environment will be more reliable and secure.

Remember: your computing environment is only as secure as your weakest link and non-compliant user.

Q17: What is the difference between CSMA/CD and CSMA/CA?

Difference between CSMA/CA and CSMA/CD

CSMA/CD:
CSMA/CD stands for Carrier Sense Multiple Access / Collision Detection is a network protocol for carrier transmission. It is operated in the medium access control layer. It senses of the shared channel is busy for broadcasting and interrupt the broadcast until the channel is free. In CSMA/CD collision is detected by broadcast sensing from the other stations. Upon collision detection in CSMA/CD, the transmission is stopped and a jam signal is send by the stations and then station waits for a random time context before retransmission.

CSMA/CA:
CSMA/CD stands for Carrier Sense Multiple Access / Collision Avoidance is a network protocol for carrier transmission. Like CSMA/CD it is also operated in the medium access control layer. Unlike CSMA/CD(that is effective after a collision) CSMA / CA is effective before a collision.

Let’s see the difference between CSMA/CA and CSMA/CD:-

CSMA/CD	CSMA/CA
1. CSMA / CD are effective after a collision.	Whereas CSMA / CA is effective before a collision.
2. CSMA / CD are used in wired networks.	Whereas CSMA / CA is commonly used in wireless networks.
3. It only reduces the recovery time.	Whereas CSMA/ CA minimizes the possibility of collision.
4. CSMA / CD resend the data frame whenever a conflict occurs.	Whereas CSMA / CA will first transmit the intent to send for data transmission.
5. CSMA / CD are used in 802.3 standards.	While CSMA / CA is used in 802.11 standard.
6. It is more efficient than simple CSMA (Carrier Sense Multiple Access).	While it is similar to simple CSMA (Carrier Sense Multiple Access).

Q18: What is RSA Algorithm?

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a

large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

Let's say you want to tell your friend a secret. If you're right next to them, you can just whisper it. If you are on opposite sides of the country, that obviously won't work. You could write it down and mail it to them, or use the phone, but each of these communication channels is insecure and anyone with a strong enough motivation could easily intercept the message.

If the secret was important enough, you wouldn't risk writing it down normally–spies or a rogue postal employee could be looking through your mail. Likewise, someone could be tapping your phone without your knowledge and logging every single call you make.

One solution to prevent eavesdroppers from accessing message contents is to encrypt it. This basically means to add a code to the message which changes it into a jumbled mess. If your code is sufficiently complex, then the only people who will be able to access the original message are those who have access to the code.

If you had a chance to share the code with your friend beforehand, then either of you can send an encrypted message at any time, knowing that you two are the only ones with the ability to read the message contents. But what if you didn't have a chance to share the code beforehand?

This is one of the fundamental problems of cryptography, which has been addressed by public-key encryption schemes (also known as asymmetric encryption) like RSA.

Under RSA encryption, messages are encrypted with a code called a public key, which can be shared openly. Due to some distinct mathematical properties of the RSA algorithm, once a message has been encrypted with the public key, it can only be decrypted by another key, known as the private key. Each RSA user has a key pair consisting of their public and private keys. As the name suggests, the private key must be kept secret.

Public key encryption schemes differ from symmetric-key encryption, where both the encryption and decryption process use the same private key. These differences make public key encryption like RSA useful for communicating in situations where there has been no opportunity to safely distribute keys beforehand.

Symmetric-key algorithms have their own applications, such as encrypting data for personal use, or for when there are secure channels that the private keys can be shared over.

Q19: What are the components of Protocol?

In the era of Computer and Mobile technologies, computer network technology is growing at a very fast speed and frequency. Billions of electronic devices and gadgets are operating to make this happen. These devices are designed and manufactured by different manufacturers. They may have been developed using different hardware and software resources. Due to this, they are unable to establish a connection and communicate with each other for sharing data and other information. Hence, to resolve this problem, we need protocols. Protocols provide us with a medium and set of rules to establish communication between different devices for the exchange of data and other services.

Protocols:

Protocols are a fundamental aspect of digital communication as they dictate how to format, transmit and receive data. They are a set of rules that determines how the data will be transmitted over the network.

It can also be defined as a communication standard followed by the two key parties(sender and receiver) in a computer network to communicate with each other.

It specifies what type of data can be transmitted, what commands are used to send and receive data, and how data transfers are confirmed.

In simple terms, a protocol is similar to a language. Every language has its own rules and vocabulary. Protocols have their own rules, specifications, and implementations. If two people share the same language, they can communicate very easily and effectively. Similarly, two hosts implementing the same protocol can connect and communicate easily with each other. Hence, protocols provide a common language for network devices participating in data communication.

Protocols are developed by industry-wide organizations. The ARPA (Advanced Research Project Agency) part of the US Defense program was the first organization to introduce the concept of a standardized protocol. Support for network protocols can be built into the software, hardware, or both. All network end-users rely on network protocols for connectivity.

Protocols use a specific model for their implementation like the OSI (Open System Interface) Model, TCP/IP (Transmission Control Protocol / Internet Protocol) Model, etc. There are different layers (for instance, data, network, transport, and application layer, etc.) in these models, where these protocols are implemented.

Combining all these, we can say that protocol is an agreement between a sender and a receiver, which states how communication will be established, and how to maintain

& release it. It is the communication between entities in different systems, where entities can be a user application program, file transfer package, DBMS, etc., and systems can be a remote computer, sensor, etc.

Levels of a Protocol:

There are mainly three levels of a protocol, they are as follows:

Hardware Level: In this level, the protocol enables the hardware devices to connect and communicate with each other for various purposes.

Software Level: In the software level, the protocol enables different software to connect and communicate with each other to work collaboratively.

Application Level: In this level, the protocol enables the application programs to connect and communicate with each other for various purposes.

Hence protocols can be implemented at the hardware, software, and application levels.

Types of Protocols

Protocols can be broadly divided into the following two types:

Standard Protocols:

Proprietary Protocols:

Let's learn one by one:

Standard Protocols:

A standard protocol is a mandated protocol for all devices. It supports multiple devices and acts as a standard.

Standard protocols are not vendor-specific i.e. they are not specific to a particular company or organization. They are developed by a group of experts from different organizations.

These protocols are publicly available, and we need not pay for them.

Some of the examples of Standard Protocols are FTP, DNS, DHCP, SMTP, TELNET, TFTP, etc.

Proprietary Protocols:

Proprietary protocols are developed by an individual organization for their specific devices. We have to take permission from the organization if we want to use their protocols.

It is not a standard protocol and it supports only specific devices. We may have to pay for these protocols.

Q20: What is Tunnel mode?

Tunneling is a protocol that allows for the secure movement of data from one network to another. Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation. The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.

Tunneling is also known as port forwarding.

In tunneling, the data are broken into smaller pieces called packets as they move along the tunnel for transport. As the packets move through the tunnel, they are encrypted and another process called encapsulation occurs. The private network data and the protocol information that goes with it are encapsulated in public network transmission units for sending. The units look like public data, allowing them to be transmitted across the Internet. Encapsulation allows the packets to arrive at their proper destination. At the final destination, de-capsulation and decryption occur.

There are various protocols that allow tunneling to occur, including:

Point-to-Point Tunneling Protocol (PPTP): PPTP keeps proprietary data secure even when it is being communicated over public networks. Authorized users can access a private network called a virtual private network, which is provided by an Internet service provider. This is a private network in the “virtual” sense because it is actually being created in a tunneled environment.

Layer Two Tunneling Protocol (L2TP): This type of tunneling protocol involves a combination of using PPTP and Layer 2 Forwarding.

Tunneling is a way for communication to be conducted over a private network but tunneled through a public network. This is particularly useful in a corporate setting and also offers security features such as encryption options.