NAME: FASEEH MUNIR SUFI

ID: 15606

SEMESTER: 3rd

SUBJECT: Advance Computer Networks (MS EE)

Sessional Assignment 2020

Q1: Differentiate between a Hub, Switch and Router?

Hub vs Switch vs Router:

In network equipment and devices, data is usually transmitted in the form of a frame. When a frame is received, it is amplified and then transmitted to the port of the destination PC (Personal Computer). The big difference between hub and switch is in the method in which frames are being delivered.

In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Additionally, a 10/100Mbps hub must share its bandwidth with each and every one of its ports. In comparison, a switch keeps a record of the MAC (Media Access Control) addresses of all the devices connected to it. With this information, a network switch can identify which system is sitting on which port. So when a frame is received, it knows exactly which port to send it to, without significantly increasing network response times. In addition, unlike a hub, a 10/100Mbps switch will allocate a full 10/100Mbps to each of its ports. So regardless of the number of PCs transmitting, users will always have access to the maximum amount of bandwidth.

Q2: What does a backbone network means?

A backbone or core is a part of computer network that interconnects various pieces of network, providing a path for the exchange of information between different LANs or sub networks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than the networks connected to it.

A diagram of a typical nationwide network backbone.

A large corporation that has many locations may have a backbone network that ties all of the locations together, for example, if a server cluster needs to be accessed by different departments of a company that are located at different geographical locations. The pieces of the network connections (for example: Ethernet, wireless) that bring these departments together is often mentioned as network backbone. Network congestion is often taken into consideration while designing backbones.

One example of a backbone network is the Internet backbone. Backbones are primarily used in medium to large-sized networks, such as those occupying a building or a group of buildings on a campus. Backbone cabling should have the highest bandwidth of any cabling in your network, since backbones are used to join together hubs, switches, and routers, linking departmental LANs or sub networks into building-wide or campus-wide internetworks. In buildings, backbone cabling often refers to the vertical cabling running through the rises or elevator shafts that connects the hubs and switches in each floor's wiring closet.

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

n computer science, the concept of network layers is a framework that helps to understand complex network interactions. There are two models that are widely referenced today: OSI and TCP/IP. The concepts are similar, but the layers themselves differ between the two models.

What are the network layers:

While TCP/IP is the newer model, the Open Systems Interconnection (OSI) model is still referenced a lot to describe network layers. The OSI model was developed by the International Organization for Standardization. There are 7 layers:

Physical (e.g. cable, RJ45)

Data Link (e.g. MAC, switches)

Network (e.g. IP, routers)

Transport (e.g. TCP, UDP, port numbers)

Session (e.g. Syn/Ack)

Presentation (e.g. encryption, ASCII, PNG, MIDI)

Application (e.g. SNMP, HTTP, FTP)

People have come up with tons of mnemonic devices to memorize the OSI network layers. One popular mnemonic, starting with Layer 7, is "All People Seem To Need Data Processing." But one that I'm partial to, which starts with Layer 1, is "Please Do Not Throw Sausage Pizza Away."

The TCP/IP model is a more concise framework, with only 4 layers:

Network Access (or Link)

Internet

Transport (or Host-to-Host)

Application (or Process)

One mnemonic device for the TCP/IP model is “Armadillos Take in New Ants.”

Network Layers and Functions

For the OSI model, let’s start at the top layer and work our way down.

Layer 7 (Application): Most of what the user actually interacts with is at this layer. Web browsers and other internet-connected applications (like Skype or Outlook) use Layer 7 application protocols.

Layer 6 (Presentation): This layer converts data to and from the Application layer. In other words, it translates application formatting to network formatting and vice versa. This allows the different layers to understand each other.

Layer 5 (Session): This layer establishes and terminates connections between devices. It also determines which packets belong to which text and image files.

Layer 4 (Transport): This layer coordinates data transfer between system and hosts, including error-checking and data recovery.

Layer 3 (Network): This layer determines how data is sent to the receiving device. It’s responsible for packet forwarding, routing, and addressing.

Layer 2 (Data Link): Translates binary (or BITs) into signals and allows upper layers to access media.

Layer 1 (Physical): Actual hardware sits at this layer. It transmits signals over media.

The TCP/IP model, sometimes referred to as a protocol stack, can be considered a condensed version of the OSI model.

Layer 1 (Network Access): Also called the Link or Network Interface layer. This layer combines the OSI model’s L1 and L2.

Layer 2 (Internet): This layer is similar to the OSI model’s L3.

Layer 3 (Transport): Also called the Host-to-Host layer. This layer is similar to the OSI model’s L4.

Layer 4 (Application): Also called the Process layer, this layer combines the OSI model’s L5, L6, and L7.

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.

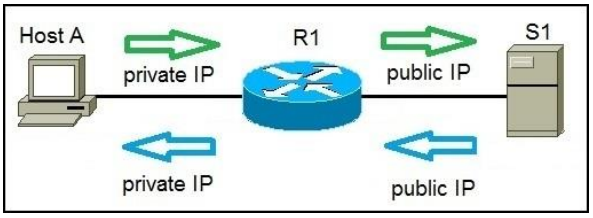
A subnet mask of 255.255.255.0 allows for close to 256 unique hosts within the network (since not all 256 IP addresses can be used). If your computer is connected to a network, you can view the network's subnet mask number in the Network control panel (Windows) or System Preference (macOS). Most home 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?

NAT (Network Address Translation) is a process of changing the source and destination IP addresses and ports. Address translation reduces the need for IPv4 public addresses and hides private network address ranges. This process is usually done by routers or firewalls.

An example will help you understand the concept:



Host A request a web page from an Internet server. Because Host A uses private IP addressing, the source address of the request has to be changed by the router because private IP addresses are not routable on the Internet. Router R1 receives the request, changes the source IP address to its public IP address and sends the packet to server S1. Server S1 receives the packet and replies to router R1. Router R1 receives the packet, changes the destination IP addresses to the private IP address of Host A and sends the packet to Host A.

There are three types of address translation:

Static NAT – translates one private IP address to a public one. The public IP address is always the same.

Dynamic NAT – private IP addresses are mapped to the pool of public IP addresses.

Port Address Translation (PAT) – one public IP address is used for all internal devices, but a different port is assigned to each private IP address. Also known as NAT Overload.

Q7: Differentiate between TCP and UDP?

TCP:

TCP stands for Transmission Control Protocol. It is the most commonly used protocol on the Internet.

When you load a web page, your computer sends TCP packets to the web server's address, asking it to send the web page to you. The web server responds by sending a stream of TCP packets, which your web browser stitches together to form the web page and display it to you. When you click a link, sign in, post a comment, or do anything else, your web browser sends TCP packets to the server and the server sends TCP packets back. TCP is not just one way communication — the remote system sends packets back to acknowledge it is received your packets.

TCP guarantees the recipient will receive the packets in order by numbering them. The recipient sends messages back to the sender saying it received the messages. If the sender does not get a correct response, it will resend the packets to ensure the recipient received them. Packets are also checked for errors. TCP is all about this reliability — packets sent with TCP are tracked so no data is lost or corrupted in transit. This is why file downloads do not become corrupted even if there are network hiccups. Of course, if the recipient is completely offline, your computer will give up and you will see an error message saying it can not communicate with the remote host.

UDP:

UDP stands for User Datagram Protocol — a datagram is the same thing as a packet of information. The UDP protocol works similarly to TCP, but it throws all the error-checking stuff out. All the back-and-forth communication and deliverability guarantees slow things down.

When using UDP, packets are just sent to the recipient. The sender will not wait to make sure the recipient received the packet — it will just continue sending the next packets. If you are the recipient and you miss some UDP packets, too bad — you can not ask for those packets again. There is no guarantee you are getting all the packets and there is no way to ask for a packet again if you miss it, but losing all this overhead means the computers can communicate more quickly.

UDP is used when speed is desirable and error correction is not necessary. For example, UDP is frequently used for live broadcasts and online games.

Q8: What is RIP and its key features?

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employ the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support.

RIP implements the split horizon, route poisoning and hold down mechanisms to prevent incorrect routing information from being propagated.

In RIPv1 routers broadcast updates with their routing table every 30 seconds. In the early deployments, routing tables were small enough that the traffic was not significant. As networks grew in size, however, it became evident there could be a massive traffic burst every 30 seconds, even if the routers had been initialized at random times.

In most networking environments, RIP is not the preferred choice for routing as its time to converge and scalability are poor compared to EIGRP, OSPF, or IS-IS. However, it is easy to configure, because RIP does not require any parameters, unlike other protocols.

RIP uses the User Datagram Protocol (UDP) as its transport protocol, and is assigned the reserved port number 520

Features of RIP:

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?

Introduction:

A firewall is a system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules. In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate communication to flow freely. In most server infrastructures, firewalls provide an essential layer of security that, combined with other measures, prevent attackers from accessing your servers in malicious ways.

This guide will discuss how firewalls work, with a focus on stateful software firewalls, such as iptables and Firewall, as they relate to cloud servers. We'll start with a brief explanation of TCP packets and the different types of firewalls. Then we'll discuss a variety of topics that a relevant to stateful firewalls. Lastly, we will provide links to other tutorials that will help you set up a firewall on your own server.

Types of Firewalls:

Let's quickly discuss the three basic types of network firewalls: packet filtering (stateless), stateful, and application layer.

Packet filtering, or stateless, firewalls work by inspecting individual packets in isolation. As such, they are unaware of connection state and can only allow or deny packets based on individual packet headers.

Stateful firewalls are able to determine the connection state of packets, which makes them much more flexible than stateless firewalls. They work by collecting related packets until the connection state can be determined before any firewall rules are applied to the traffic.

Application firewalls go one step further by analyzing the data being transmitted, which allows network traffic to be matched against firewall rules that are specific to individual services or applications. These are also known as proxy-based firewalls.

In addition to firewall software, which is available on all modern operating systems, firewall functionality can also be provided by hardware devices, such as routers or firewall appliances. Again, our discussion will be focused on stateful software firewalls that run on the servers that they are intended to protect.

Q10: What is NOS?

Short for network operating system, NOS is the software that allows multiple computers to communicate, share files and hardware devices with one another. Earlier versions of Microsoft Windows and Apple operating systems were not designed for single computer usage and not network usage. As computer networks started to emerge and be used more frequently, network operating systems began to be developed.

The first network operating system was Novell NetWare, released in 1983. After Netware, other network operating systems were released, including Banyan VINES and Microsoft Windows NT. Some examples of other network operating systems include Windows 2000, Microsoft Windows XP, Sun Solaris, and Linux.

Q11: What is Denial of Service (DoS)?

A "denial of service" or DoS attack is used to tie up a website's resources so that users who need to access the site cannot do so. Many major companies have been the focus of DoS attacks. Because a DoS attack can be easily engineered from nearly any location, finding those responsible can be extremely difficult.

A bit of history: The first DoS attack was done by 13-year-old David Dennis in 1974. Dennis wrote a program using the “external” or “ext” command that forced some computers at a nearby university research lab to power off.

DoS attacks have evolved into the more complex and sophisticated “distributed denial of service” (DDoS) attacks. The biggest attack ever recorded — at that time — targeted code-hosting-service GitHub in 2018. Attackers include hacktivists (hackers whose activity is aimed at promoting a social or political cause), profit-motivated cybercriminals, and nation states.

How a DoS attack works

Unlike a virus or malware, a DoS attack doesn’t depend on a special program to run. Instead, it takes advantage of an inherent vulnerability in the way computer networks communicate.

Here’s an example. Suppose you wish to visit an e-commerce site in order to shop for a gift. Your computer sends a small packet of information to the website. The packet works as a “hello” – basically, your computer says, “Hi, I’d like to visit you, please let me in.”

When the server receives your computer’s message, it sends a short one back, saying in a sense, “OK, are you real?” Your computer responds — “Yes!” — and communication is established.

The website’s homepage then pops up on your screen, and you can explore the site. Your computer and the server continue communicating as you click links, place orders, and carry out other business.

In a DoS attack, a computer is rigged to send not just one “introduction” to a server, but hundreds or thousands. The server — which cannot tell that the introductions are fake — sends back its usual response, waiting up to a minute in each case to hear a reply. When it gets no reply, the server shuts down the connection, and the computer executing the attack repeats, sending a new batch of fake requests.

DoS attacks mostly affect organizations and how they run in a connected world. For consumers, the attacks hinder their ability to access services and information.

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:

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.

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.

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?

A Brief History of the DNS:

Thirty years ago, when the Internet was still in its infancy when you wanted to visit a website you had to know the IP address of that site. That's because computers are and were only able to communicate using numbers.

This is an IP address: 127.33.54.200.

It's long, hard to remember, and we (humans, I presume) are not robots. We needed a way to translate computer-readable information into human-readable. And it had to be fast, lightweight, and scalable.

In the early 1980's, Paul Mockapetris came up with a system that automatically mapped IP addresses to domain names.. and the DNS was born. This same system still serves as the backbone of the modern Internet, today.

And yet, only a small subset of the world knows that it exists, and an even smaller group understand what it does. The real problem is that the people that need to know how it works and could actually benefit from this knowledge… don't take the time to learn.

How Does It Work

Before we get into how you can use the DNS, we need to understand how the system works. We already know that it maps IP addresses to domain names, but where is this information stored? On name servers!

Name servers store DNS records which are the actual file that says "this domain" maps to "this IP address". So is there a room somewhere that has all the name servers and DNS records for every site on the Internet? No… that would be ridiculous.

They are actually distributed all around the world. These name servers are called the root name servers and instead of storing every domain ever, they store the locations of the TLD (top level domains).

TLD's are the two or three character like .com that end a domain name. Each TLD has their own set of name servers that store the information that says who is authoritative for storing the DNS records for that domain.

The authoritative name server is typically the DNS provider or the DNS registrar (like Go Daddy that offers both DNS registration and hosting). And here we can find the DNS record that maps example.com to the IP address 127.66.122.88.

Q14: What is OSPF?

Open Shortest Path First (OSPF) protocol States:

OSPF is a Link State protocol that's considered may be the most famous protocol among the Interior Gateway Protocol (IGP) family, developed in the mid 1980's by the OSPF working group of the IETF.

When configured, OSPF will listen to neighbors and gather all link state data available to build a topology map of all available paths in its network and then save the information in its topology database, also known as its Link-State Database (LSDB). Using the information from its topology database. From the information gathered, it will calculate the best shortest path to each reachable subnet/network using an algorithm called Shortest Path First (SFP) that was developed by the computer scientist *Edsger W. Dijkstra* in 1956. OSPF will then construct three tables to store the following information:

Neighbor Table: Contains all discovered OSPF neighbors with whom routing information will be interchanged

Topology Table: Contains the entire road map of the network with all available OSPF routers and calculated best and alternative paths.

Routing Table: Contain the current working best paths that will be used to forward data traffic between neighbors.

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?

CSMA CA vs CSMA CD:

Carrier Sense Multiple Access or CSMA is a Media Access Control (MAC) protocol that is used to control the flow of data in a transmission media so that packets do not get lost and data integrity is maintained. There are two modifications to CSMA, the CSMA CD (Collision Detection) and *CSMA CA (Collision Avoidance)*, each having its own strengths.

CSMA operates by sensing the state of the medium in order to prevent or recover from a collision. A collision happens when two transmitters transmit at the same time. The data gets scrambled, and the receivers would not be able to discern one from the other thereby causing the information to get lost. The lost information needs to be resent so that the receiver will get it.

CSMA CD operates by detecting the occurrence of a collision. Once a collision is detected, CSMA CD immediately terminates the transmission so that the transmitter does not have to waste a lot of time in continuing. The last information can be

retransmitted. In comparison, CSMA CA does not deal with the recovery after a collision. What it does is to check whether the medium is in use. If it is busy, then the transmitter waits until it is idle before it starts transmitting. This effectively minimizes the possibility of collisions and makes more efficient use of the medium.

Another difference between CSMA CD and CSMA CA is where they are typically used. CSMA CD is used mostly in wired installations because it is possible to detect whether a collision has occurred. With wireless installations, it is not possible for the transmitter to detect whether a collision has occurred or not. That is why wireless installations often use CSMA CA instead of CSMA CD.

Most people do not really have to deal with *access control protocols* as they work behind the scenes in order for our devices to work together. CSMA CD has also fallen out of favor with modern wired networks as they were only necessary with hubs and not with modern switches that route the information instead of broadcasting it.

Summary:

1. CSMA CD takes effect after a collision while CSMA CA takes effect before a collision.
2. CSMA CA reduces the possibility of a collision while CSMA CD only minimizes the recovery time.
3. CSMA CD is typically used in wired networks while CSMA CA is used in wireless networks.

Q18: What is RSA Algorithm?

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and distinct from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". The acronym RSA is the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, which was not declassified until 1997.

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of the prime numbers can decode the message. Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.

RSA is a relatively slow algorithm, and because of this, it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys

for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

Q19: What are the components of Protocol?

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.

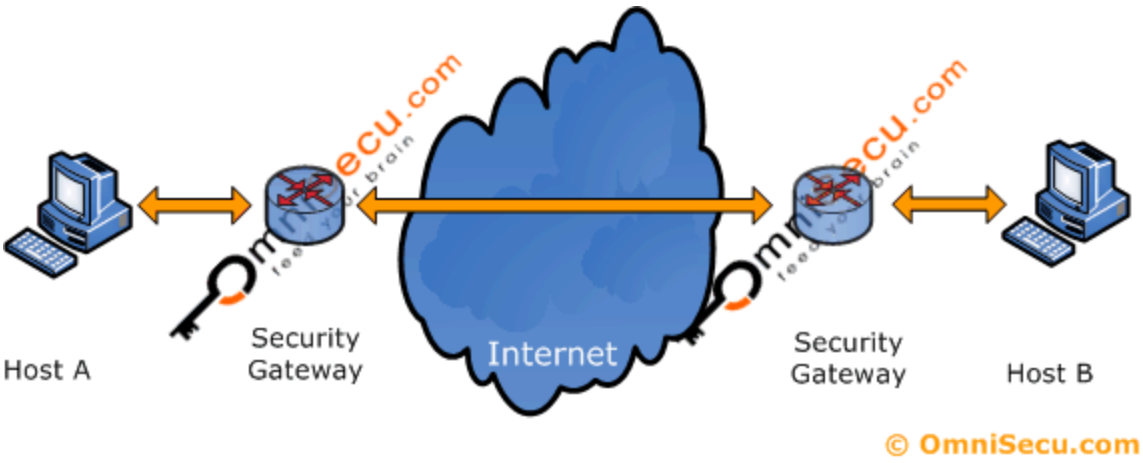
Hence protocols can be implemented at the hardware, software, and application levels.

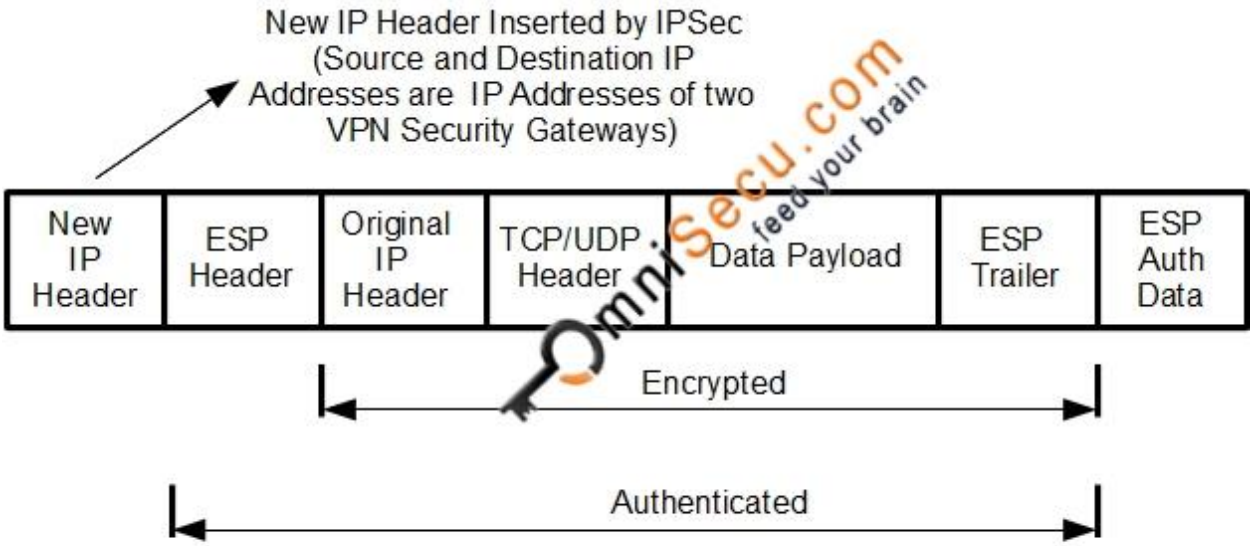
Q20: What is Tunnel mode?

IPsec can be used to create VPN Tunnels to end-to-end IP Traffic (also called as IPsec Transport mode) or site-to-site IPsec Tunnels (between two VPN Gateways, also known as IPsec Tunnel mode).

IPsec Tunnel mode: In IPsec Tunnel mode, the original IP packet (IP header and the Data payload) is encapsulated within another packet. In IPsec tunnel mode the original IP Datagram from is encapsulated with an AH (provides no confidentiality by encryption) or ESP (provides encryption) header and an additional IP header. The IP addresses of the newly added outer IP header are that of the VPN Gateways. The traffic between the two VPN Gateways appears to be from the two gateways (in a new IP datagram), with the original IP datagram is encrypted (in case of ESP) inside IPsec packet.

IPsec Tunnel mode is most widely used to create site-to-site IPsec VPN.

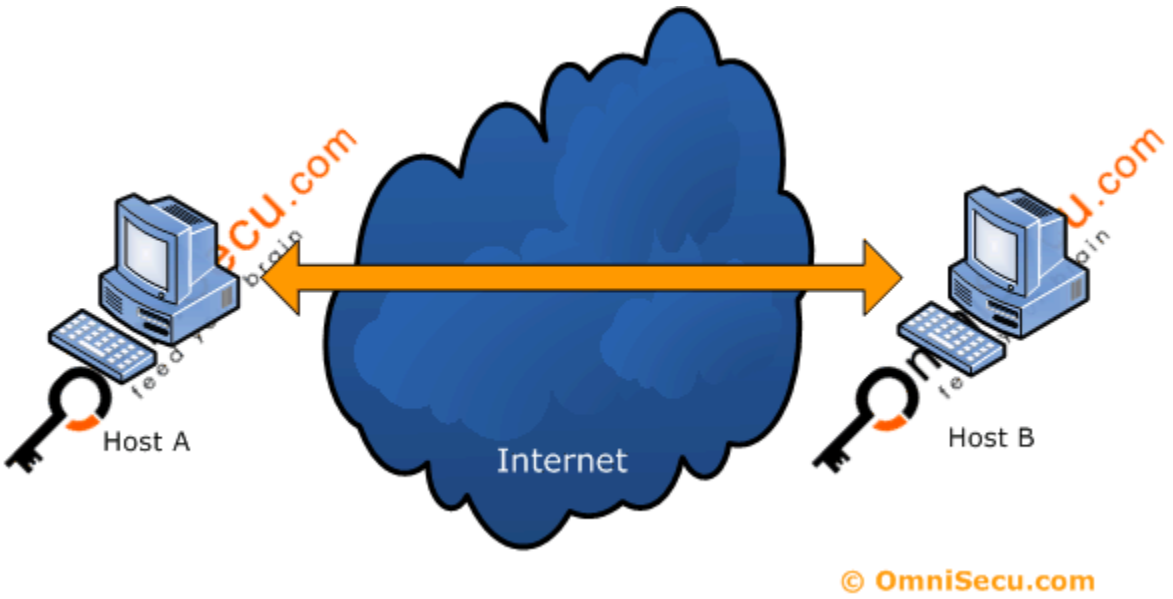




IPSec – Tunnel Mode

IPsec Transport mode: In IPsec Transport mode, only the Data Payload of the IP datagram is secured by IPsec. IP Header is the original IP Header and IPsec inserts its header between the IP header and the upper level headers.

IPsec Transport mode can be used when encrypting traffic between two hosts or between a host and a VPN gateway.



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.