Introduction to Networking

Overview

The dictionary defines the word networking as "a group or system of interconnected people or things." Similarly, within the computer world, the term network means two or more connected computers which will share resources like data and applications, office machines, an online connection, or some combination.
The main task is to supply participants with one platform for exchanging data and sharing resources. This task is so essential that many aspects of lifestyle and therefore the times would be unimaginable without networks. Here's a real-life example: during a typical office, every workstation has its computer. Without a network of computers, it might be difficult for a team to figure on a project since there would be no commonplace to share or store digital documents and knowledge, and team members wouldn't be ready to share specific applications.

Overview of Network Components

The following list describes the network components depicted and, therefore, the functions they serve:

- **Client:** The term client defines the device an end-user uses to access a network. This device could be a workstation, laptop, smartphone with wireless capabilities, or a spread of other end-user terminal devices.
- **Server:** A server, because the name suggests, serves up resources to a network. These resources might include e-mail access provided by an e-mail server, sites provided by an internet server, or files available on a digital computer.

Network Architecture

A way to categorize networks is predicated on where network resources reside. An example of a client/server network may be a collection of PCs, all sharing files on a centralized server. However, if those PCs had their OS (OS) (for example, Microsoft Windows 8 or Mac OS X) configured for file sharing, they might share files from one another's hard drives. Such an appointment would be a peer-to-peer network because the peers (the PCs during this example) make resources available to other peers.

❖ Peer-to-Peer Networks

Peer-to-peer networks allow interconnected devices (for example, PCs) to share their resources. Those resources might be, for instance, files or printers. As an example of a peer-to-peer network, consider Figure 1, where each peer can share files on their hard drives shared with the opposite peers within the network.

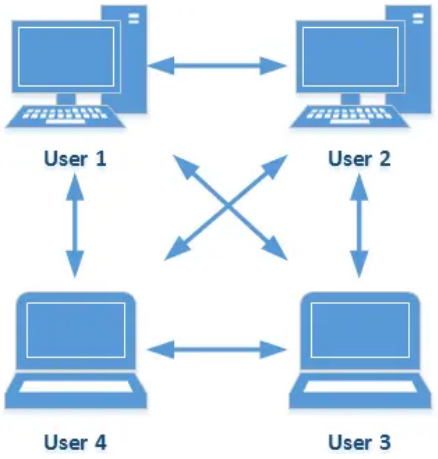

Figure 1: Peer to Peer

❖ Client-Server Networks

Client/server may be a model of interaction during which a program sends an invitation to a different program and awaits a response. The requesting program is named a client; the answering program is called a server. Although the client/server model is often used between programs during a single computer, the term typically refers to a network. A client-server network may have quite one server, each dedicated to handling a selected function.

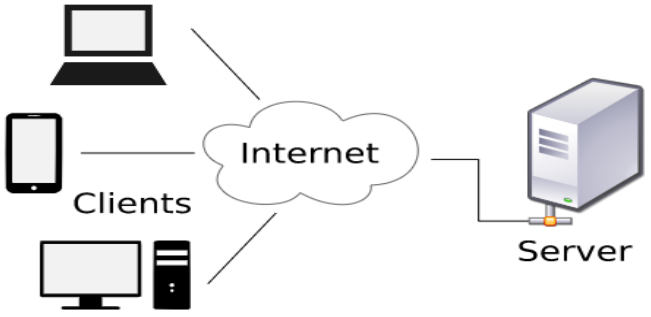

Figure 2: Client/Server Architecture

Topologies

Overview

The configuration, or topology, of a network is vital to determining its performance. Topology is the way a network is arranged, including the physical or logical description of how links and nodes are found to relate to every other. It maps how different nodes on a network--including switches and routers--are placed and interconnected, as well as how data flows. Diagramming the locations of endpoints and repair requirements helps determine the most precise placement for every node to optimize traffic flows. A well-planned topology enhances the user experience and allows administrators to maximize performance while fulfilling business needs. When the proper topology is chosen for a business's needs, it's easier to locate faults, troubleshoot and fixes problems, and share resources across networks.

Type of Physical Topologies

The physical topology refers to the particular connections (wires, cables, etc.) of how the network is arranged. Setup, maintenance, and provisioning tasks require insight into the physical network. The subsequent are some of the physical topologies:

Bus topology

As depicted in Figure 1, it typically uses a single cable running throughout, requiring connectivity. Early Ethernet networks commonly relied on bus topologies.

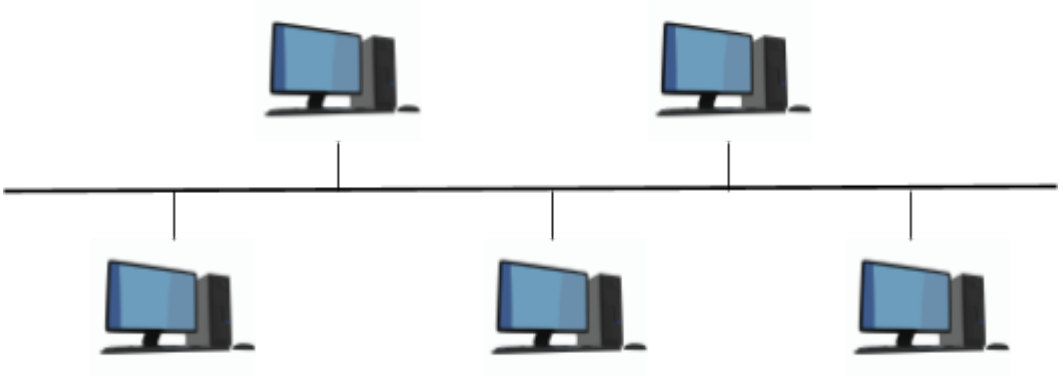

Figure 1: Bus Topology

Every device connected to this structure requires a network segment. One network segment may be a single collision domain, which suggests that each one device connected to the bus might attempt to gain access to the bus at an equivalent time, leading to a condition referred to as a collision. Table 1-1 identifies a number of characteristics, benefits, and disadvantages of the bus.

Characteristics	**Benefits**	**Drawbacks**
One cable is used per network segment.	Less cable is required to put in a bus, as compared with other topologies.	Because one cable is operating per network segment, the cable becomes a possible single point of failure.
To maintain the cable's electrical characteristics appropriately, the line requires a terminator (of a selected resistance) at each end of the cable.	Counting on the media operating by the bus, a bus is often less costly.	Troubleshooting a bus is often tricky because problem isolation might require an inspection of multiple network taps to make sure they either have an endpoint connected or they're correctly terminated.
Bus topologies were popular in early Ethernet networks.	Installation of a network supported by a bus is more superficial than another topology, requiring extra wiring to be installed.	Adding devices to a bus might cause an outage for other users on the bus.
Network components tap directly into the cable via a connector like a T connector or a vampire tap.	Not Applicable	A fault condition existing on one device on the bus can impact the performance of other devices on the bus.

Table 1

Ring topology

Figure 2 offers an example of a ring topology, where traffic flows circularly around a closed network loop (that is, a ring). Typically, this topology sends data, during a single direction, to every connected device successively until the intended destination receives the info. Token Ring networks typically relied on the same topology, although the ring may need been the topology, whereas physically, the topology was a star.

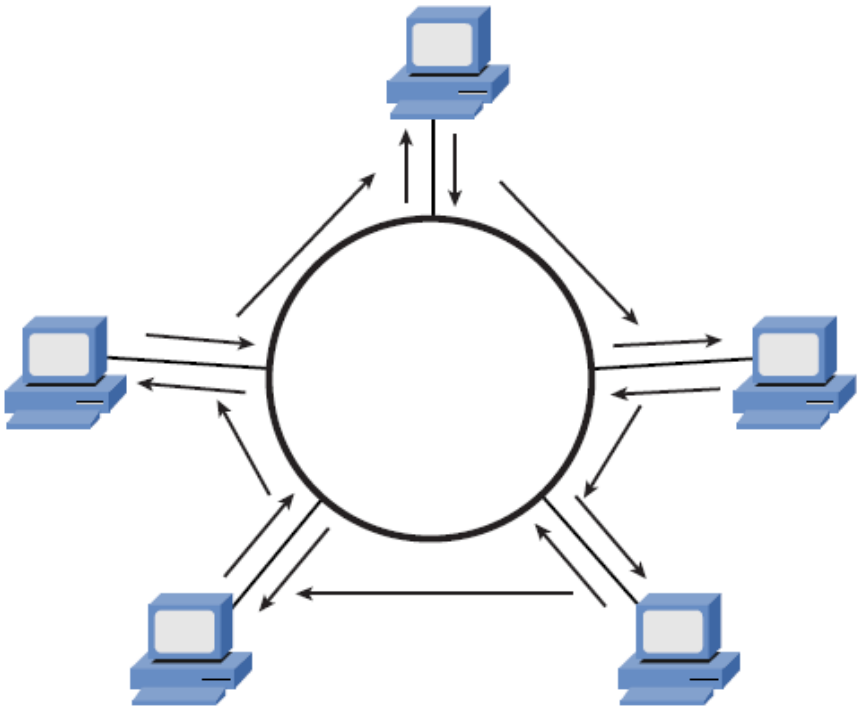

Figure 2: Ring Topology

The method of transferring data within the ring structure is named token passing. A token may be a particular sequence of bits containing control information. Owning the ticket allows a network device to transfer data to the network. There's just one token in each network. The sending computer removes the token from the ring and sends the requested data within the circle. Each computer forwards the info until the packet finds the pc that matches the info address. The receiving computer then sends a message that the information has been received back to the sending computer. After verification, the sending computer creates a replacement token and releases it to the network.

Because this topology allows devices on the ring to require turns transmitting, contention for media access wasn't dragged because it was for a bus. If the crew was broken at any point, data would stop flowing. Table 2 identifies a number of the primary characteristics, benefits, and disadvantages of a hoop topology.

Characteristics	**Benefits**	**Drawbacks**
Devices are interconnected by connecting to one ring or, in some cases (for example, FDDI), a dual ring.	A double ring topology adds a layer of fault tolerance. Therefore, if a cable break occurred, connectivity to all or any devices might be restored.	An opportunity when one ring topology is employed leads to a network outage for all devices connected to the ring.
Each device includes both a receiver (for the incoming cable) and a transmitter (for the outgoing line).	Troubleshooting is simplified in a cable break because each device contains a repeater. When the repeater on the far side of a cable break doesn't receive any data within a particular amount of your time, it reports a fault condition (typically within the sort of an indicator light on a network interface card [NIC]).	Rings have scalability limitations. Specifically, it features a maximum length and a maximum number of attached stations. Once either of those limits is exceeded, one ring might be divided into two interconnected rings. A network maintenance window might get to be scheduled to perform this ring division.
Each device on the ring repeats the signal it receives.		Because this network must be a complete loop, the quantity of cable required for a ring is usually above the quantity of line needed for a bus topology serving an equivalent Several devices.

Table 2

Star topology

Star topology may be where each piece of a network is attached to a central node (often called a hub or switch). The attachment of those network pieces to the main component is visually represented during a form, almost like a star.
Computers aren't connected to at least one another in a star but are all connected to a central hub or switch. When a computer sends data to other computers on the network, it's sent along the cable to a central hub or control, determining which port it must send the info through for it to succeed in the right destination.

Figure 3: Star Topology

Characteristics	Benefits	Drawbacks
Devices have independent connections back to a central device (for example, a hub or a switch).	A cable break only impacts the device connected via the broken cable and not the whole topology.	More cable is required for a star, as against bus or ring topologies because each device requires its line to attach back to the central device.
Star topologies are commonly used with Ethernet technologies	Troubleshooting is comparatively simple because a central device within the star acts because the aggregation point of all the connected devices.	Installation can take longer for a star than against a bus or ring topology because more cable runs have to be installed.

Table 3

Mesh topology

A mesh may be a network setup where each computer and network device is interconnected with each other. This topology setup allows for many transmissions to be distributed, albeit one among the connections goes down. It's a topology commonly used for wireless networks. Below may be a visual example of an accessible computer found out on a web employing a mesh.

Each computer not only sends its signals but also relays data from other computers. This sort of topology is costly as It's challenging to determine the connections of the mesh. During a mesh, every node features a point-to-point connection to the opposite node. The links within the mesh are often wired or wireless.

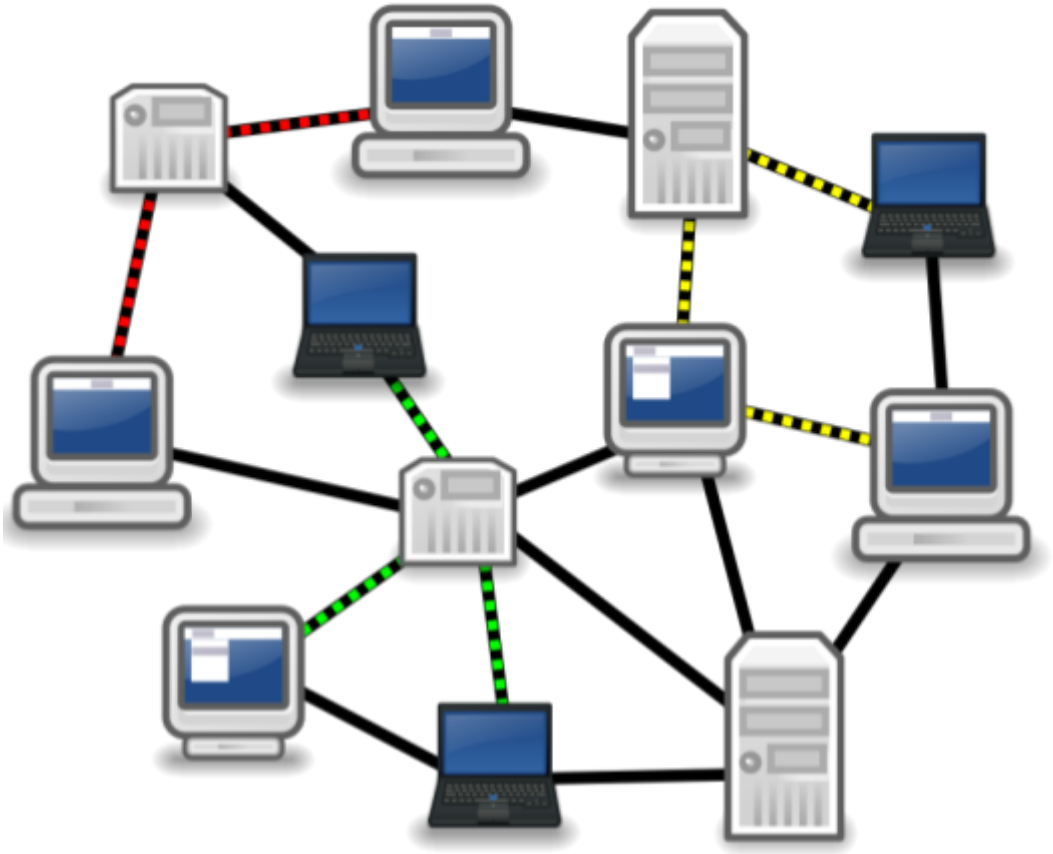

Figure 4: Mesh Topology

Mesh network topologies create multiple routes for information to travel among connected nodes. This approach increases the resilience of the network just in case of a node or connection failure. More extensive mesh networks may include multiple routers, switches, and other devices, which operate as nodes. A mesh network can consist of many wireless mesh nodes, which allows it to span an outsized area.

Characteristics	Benefits	Drawbacks
Selected sites (that is, areas with frequent intersite communication) are interconnected via direct links, whereas sites with less regular contact can communicate via another site.	A partial-mesh topology provides optimal routes between selected sites with higher intersite traffic volumes while avoiding the expense of interconnecting every site to each other site.	A partial-mesh topology is a smaller amount fault-tolerant than a full-mesh topology.
A partial-mesh topology uses fewer links than a full-mesh topology and more links than a hub-and-spoke topology for interconnecting an equivalent number of places.	A partial-mesh topology is more redundant than a hub and spoke topology.	A partial-mesh topology is costlier than a hub-and-spoke topology.

Table 4

OSI Model

Overview

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the primary standard model for network interchanges, embraced by all significant PC and telecom organizations inside the 1980s. To raise and see how a particular innovation fits in, be that as it may, it assists with having a typical perspective against which different advancements from different merchants are frequently looked at. Understanding the OSI model additionally can help investigate organizations. One of the solitary standard methods of sorting the capacity of organization innovation is to state at what layer (or layers) of the OSI model that innovation works.

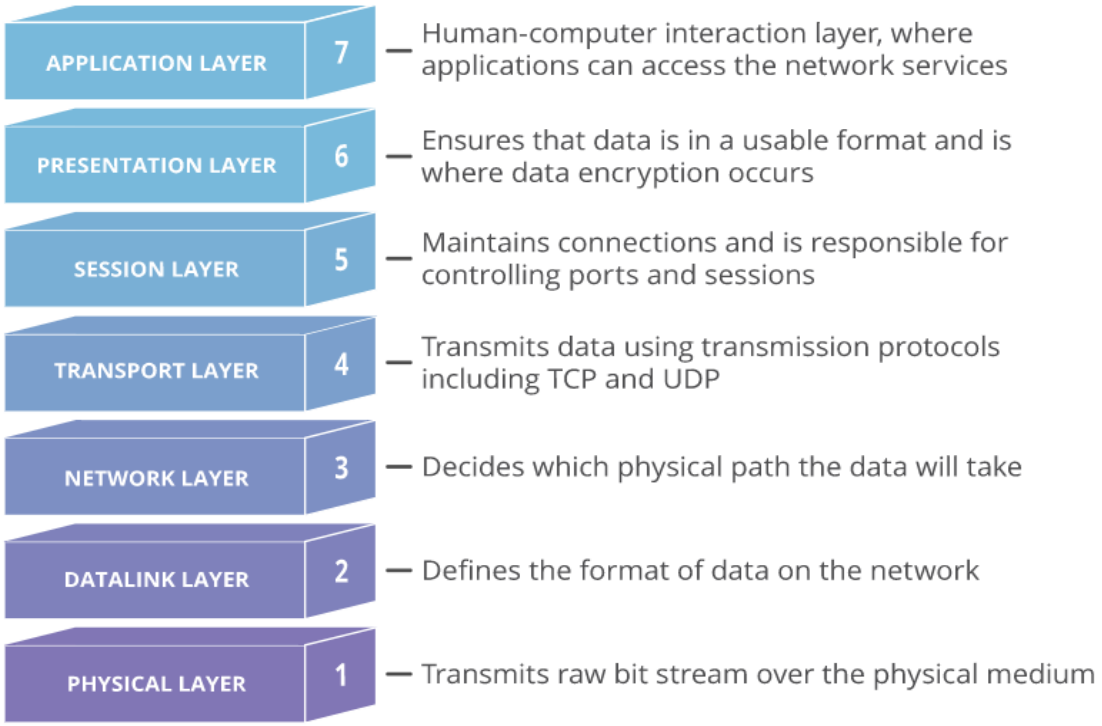

Figure 1: OSI Layer

Presently we should take apart each layer and look at its job and usefulness to comprehend the OSI model and its utilization. Before beginning, different mental aides are accessible to help with remembering these layers in their appropriate request. A down-top (that is, beginning at the absolute bottom of the stack with Layer 1 and managing your high to Layer 7) acrostic is:

Please Do Not Throw Sausage Pizza Away

The Physical Layer

At this layer, double articulations (that is, a progression of 1s and 0s). A twofold word is framed from **bits**, where a touch might be a solitary one or one 0. At upper layers, nonetheless, pieces are gathered into what's alluded to as a convention information unit or an information administration unit.

It characterizes electrical and actual determinations for gadgets. The virtual layer depicts the association between an apparatus and a transmission medium, similar to a copper or optical link. This incorporates the format of pins, voltages, link particulars, centers, repeaters, network connectors, have transport connectors, and the sky is the limit from there. The principle capacities and administrations performed by the actual layer are:

- **The portrayal of Bits:** Data during this layer comprises a surge of pieces. The pieces should be encoded into signals for transmission. It characterizes the kind of encoding, i.e., how 0's and 1's are changed to flag.
- **Information Rate:** This layer characterizes the speed of transmission, the number of pieces each second.
- **Synchronization:** It manages the synchronization of the transmitter and recipient. The sender and recipient are synchronized at bit level.
- **Interface:** The actual layer characterizes the transmission interface among gadgets and, in this way, the transmission medium.
- **Line Configuration:** This layer interfaces gadgets with the medium: Point to Point setup and Multipoint arrangement.

HUB

NIC

CABLE

Figure 2: Devices of Physica Layer

The Data Link Layer

This layer cares about bundling information into **frames** and sends, transmitting organization, performing mistake identification/rectification, distinguishing network gadgets with a location, and taking care of stream control. These cycles are aggregately referenced as information interface control.

Layer 2 of the OSI model comprises of two sublayers: the **Media Access Control** (MAC) sublayer and, along these lines, the **Logical Link Control** (LLC) sublayer. The MAC sublayer controls gadget connection. The LLC sublayer manages tending to and multiplexing. Actual Addressing for network associations exists at the information connect layer. The primary capacities and administrations performed by this layer are:

- **Framing:** Frames are the floods of pieces from the organization layer into reasonable informationThe Data Link Layer does this division of stream of bits.
- **Physical Addressing:** The Data Link layer adds a header to the casing to characterize the exact location of the sender or beneficiary of the edge if the edges are to be disseminated to various frameworks on the organization.
- **Flow Control:** Error control is accomplished by adding a trailer at the highest point of the edge. Duplication of designs is moreover forestalled by utilizing this system. Connection Layers add an apparatus to stop the proliferation of borders.
- **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of structures is also prevented by using this mechanism. Data Link Layers adds a means to avoid the recurrence of frames.
- **Access Control:** Protocols of this layer figure out which of the gadgets has authority over the connection at some random time when at least two devices are associated with an identical connection.

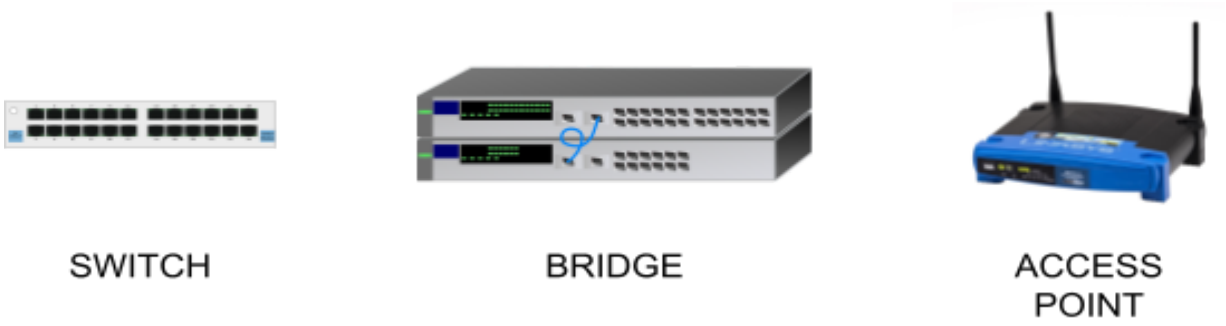

Figure 3: Devices of Data Link Layer

The information interface layer is selective from the contrary layers in that it's two sublayers of its own:

- **Media Access Control:** The MAC layer is obligated for moving information frames to and from one Network Interface Card (NIC) to an alternate across a common channel. This layer's usefulness is made into the organization connectors, consolidating a chronic number that recognizes the dealer and connector.
- **Logical Link Control:** The Logical Link Control (LLC) sublayer explains the data connection; along these lines, it controls the synchronization, stream control, and slip checking elements of the information interface layer. This layer can deal with association arranged transmissions (dissimilar to the MAC sublayer beneath it), albeit this layer can likewise offer connectionless support.

The Network Layer

This layer has two primary capacities. One is finishing sections into network **Packets** and reassembling them on the less than desirable end. The inverse is directing parcels by finding the most obvious way across an actual organization. This layer utilizes network addresses (commonly Internet Protocol addresses) to course parcels to an objective hub. The organization layer discovers the objective by using intelligent addresses, similar to IP (web convention). At this layer, switches are a fundamental part that will not work precisely in a real sense of course data where it should go between networks.

- The network layer breaks the more oversized parcels into little bundles.
- Association administrations are given, including network layer stream control, layer mistake control, and bundle succession control.
- **Logical Addressing** Sensible Addressing Physical Addressing carried out by the DL layer handles the issue of tending to locally. The Network layer adds a header

to the parcel coming from the upper layer that additionally incorporates consistent addresses of the sender and, subsequently, the collector.

- **Routing** When free organizations or connections are associated with make internetworks/broad organization, the directing devices(router or switches) course the parcels to their last objective. This is frequently perhaps the most capacity of the network layer.

As the connection layer manages the conveyance of the bundles between two frameworks on an identical organization, the organization layer essentially guarantees that each pack gets from its starting place to a definitive objective. It likewise partitions the active messages into parcels and gathers approaching bundles into messages for more elevated levels. The steering issue in broadcast networks is direct; along these lines, the organization layer usually is slight or non-existent. On the off chance that two PCs (framework) are associated with a close connection, there's no requirement for an organization layer. In any case, for good measure, if two frameworks ate joined to various networks(relationships) with interfacing gadgets between the networks(links), then, at that point, there's a necessity for the organization layer to achieve the source-to-objective conveyance. Devices for this layer:

Figure 4: Devices of Network Layer

The Transport Layer

This layer goes about as a line between the OSI model's upper and lower layers. It takes information moved inside the session layer and breaks it into **Segments** on the sending end. In particular, messages are taken from the upper (Layers 5–7) and are epitomized into pieces for transmission to the lower (Layers 1–3). Also, information streams from lower layers are decapsulated and shipped off Layer 5 (the meeting layer) or another upper layer, depending on the convention. It's obligated for reassembling the fragments on the less than desirable end, turning it back to information that the meeting layer will utilize.

- **Service Point Addressing:** Transport Layer header incorporates administration point address which is that the port location. This layer gets the message to the appropriate cycle on the pc, in contrast to Network Layer, which receives every bundle to the correct PC.
- **Division and Reassembling:** A message is parted into segments(that are communicable); each part contains a succession number, which empowers this layer to reassemble the message. The message is reassembled accurately upon landing in the objective and replaces bundles that were lost in transmission.
- **Association Control:** It incorporates two sorts:
    - Connectionless Transport Layer: Each fragment is viewed as an autonomous bundle and conveyed to the vehicle layer at the objective machine.
    - Association Oriented Transport Layer: The association is framed with the vehicle layer at the objective machine before conveying bundles.
- **Flow Control:** during this layer, stream control is performed end to complete rather than across one connection.
- **Error Control:** Error Control is performed end to wrap up during this layer to guarantee that the whole message shows up at the getting transport layer with no mistake. Blunder Correction is finished through retransmission.

Figure 5: Devices of Transport Layer

The Session Layer

This layer tracks the exchanges between PCs, which likewise are called **Sessions**. This layer sets up, controls, and finishes the concourses among area and distant applications. The Session Layer permits clients on various machines to decide dynamic

correspondence meetings between them. Its principal point is to characterize, keep up with and synchronize the cooperation between imparting frameworks. The meeting layer oversees and synchronizes the discussion between two separate applications. In the Session layer, floods of information are stamped and are sufficiently resynchronized so the closures of the messages aren't cut rashly, and information misfortune is kept away from.

- **Discourse Control:** This layer permits two frameworks to begin correspondence with each other fifty-fifty duplex or full-duplex.
- **Token Management:** This layer keeps two gatherings from endeavoring an identical essential activity at a comparable time.
- **Synchronization:** This layer permits a cycle to highlight designated spots, which are considered synchronization focuses on the stream of information. Model: If a framework sends a record of 800 pages, adding designated sites after every 50 pages are proposed. This guarantees that a fifty-page unit is effectively gotten and recognized. This is frequently gainful at the hour of the crash as though an accident occurs at pagination 110; there's no chance to retransmit one to100 pages.

GATEWAY

Figure 6: Devices of Transport Layer

The Presentation Layer

The show layer is responsible for the arranging of information being traded and protecting that information with **encryption**. This layer fundamentally acts because of the interpreter of the organization. Another name of the show layer is that the Syntax layer. The principal objective of this layer is to require care of the sentence structure and semantics of the information traded between two conveying frameworks.

This layer takes care that the data is sent in such that the recipient will comprehend the information(data) and be prepared to utilize the information. Languages(syntax) are frequently unique between the two conveying frameworks. Under this condition, the show layer plays an undertaking as an interpreter. To frame it workable for PCs with various information portrayals to talk, the data designs to be traded are frequently characterized in a theoretical manner.

- **Interpretation:** Before being sent, the information inside the characters and numbers ought to be changed to bitstreams. The show layer is obligated for interoperability between encoding techniques as various PCs utilize diverse encoding strategies. It deciphers information between the configurations the organization requires and subsequently the arrangement of the pc.
- **Encryption:** It completes encryption at the transmitter and decoding at the collector.
- **Compression:** It does information squeezing to downsize the data transfer capacity of the information to be sent. The primary job of information pressure is proportional back to the measure of pieces to be sent. It's significant in communicating interactive media like sound, video, text, and so on.

The Application Layer

The application layer gives application administrations to a network. An essential and frequently misconstrued idea is that end-client applications (for instance, Microsoft Word) don't live at the machine layer. The machine layer upholds administrations utilized by end-client applications. For example, email is an application layer administration that dwells at the apparatus layer. In contrast, Microsoft Outlook (an illustration of an email customer) is an end-client application that doesn't live at the machine layer. Another capacity of the machine layer is promoting accessible administrations.

- **Mail Services:** This layer gives the plan to Email sending and capacity.
- **Organization Virtual Terminal:** It permits a client to go online to an unfamiliar host. The apparatus makes programming copying of a terminal at the far off have. The client's PC converses with the product terminal, which progressively chats with the host and the reverse way around. Then, at that point, the distant host trusts it's speaking with one among its terminals and permits the client to go on the web.
- **Index Services:** This layer gives admittance to worldwide data about different administrations.

- **File Transfer, Access, and Management (FTAM):** it's a run-of-the-mill component to get to records and oversees them. Clients can get to documents on a remote PC and watch them. They will likewise recover documents from an unfamiliar PC.

The accompanying portrays the elements of the machine layer in extra detail:

- Application administrations: tests of the apparatus administrations living at the machine layer incorporate document sharing and email.
- Administration ad: Some applications' administrations (for instance, some organized printers) occasionally send promotions, spreading the word about the stock of their administration for different gadgets on the organization. Different administrations, notwithstanding, register themselves and their administrations with a brought together index (for instance, Microsoft Active Directory), which might be questioned by other organization gadgets looking for such administrations. structures

Interview Questions

Networking Basic

Q1. What is a node? (**Cisco**)

Answer: A node may be a point of connection within a network for systematic data transmission. A computer or printer, or other devices capable of sending and receiving data through a network is often called a node. Let's consider that there are two computers, two printers, and a server connected during a network; then we will say there are five nodes.

Q2. What exactly does one mean by a backbone network? (**Juniper**)

Answer: It is a network liable for assigning the info and, therefore, the route to different networks. Monitoring the channels, protocols, and bandwidth management is additionally the responsibility of a backbone network. It's due to this reason it's been named as a backbone network.

Q3. In data encapsulation, how each chunk knows about its destination? (**Cisco**)

Answer: Data encapsulation is an approach during which the info is split into smaller packets called chunks. All chunks have their source and destination address on them, which is how they reach their destination. It's necessary for network security that the chunk must contain its source address too.

Q4. What is the importance of the Physical Layer within the OSI model? (**Arista**)

Answer: Physical layer resembles the particular transfer of data from source to destination in bitstream – electrical impulse, light, or radio wave. In simple words, it accepts a frame from the info link layer and converts it into bits. It also receives bits from the physical medium and converts them into the structure.

Q5. What are the standards to see the network reliability? (**Dell**)

Answer: Network reliability means the power of the network to hold out the specified operation, like communication through a network. Network reliability plays a significant role in network functionality. The network monitoring systems and devices are the essential requirements for creating network reliability. The network monitoring system identifies the issues within the network while the network devices make sure that data should reach the excellent destination.

The following factors can measure the reliability of a network:

- **Downtime:** The downtime is defined because of the required time to recover.
- **Failure Frequency:** it's the frequency when it fails to figure the way it's intended.
- **Catastrophe:** It indicates that the network has been attacked by some unexpected event like fire or earthquake.

Classful Addressing

Overview

Classful addressing may be a concept that divides the available address space of IPv4 into five classes, namely A, B, C, D & E. Nowadays, this idea has become obsolete and has been replaced with classless addressing. IP addresses, before 1993, use the classful addressing where classes have a hard and fast number of blocks and every block features a fixed number of hosts. Each of those classes features a valid range of IP addresses. Types D and E are reserved for multicast and experimental purposes, respectively. The order of bits within the first octet determine the classes of IP address.

The IP Address

IP (Internet Protocol) Address is an address of your network hardware. It helps in connecting your computer to other devices on your Network and everyone over the planet. An IPv4 address may be a 32-bit address. However, instead of writing out each bit value, the address is usually written in dotted-decimal notation. Consider the IP address of 10.1.2.3. This address is written in dotted-decimal notation. Notice that the IP address is split into four separate numbers, separated by periods. Each number represents one-fourth of the IP address. Specifically, each number represents an 8-bit portion of the 32 bits within the address. Because each of those four divisions of an IP address represents 8 bits, these divisions are called octets.

All devices connected to an online connection have a singular IP address, which suggests billions of IP addresses are required. An IP address has information about how to reach a selected host, especially outside the LAN. An IP address may be a 32-bit unique address having an address space of 2^{32}. Generally, there are two notations during which IP address is written, dotted mathematical notation and sexadecimal notation. Addresses in IPv4 are 32-bits long. This enables for a maximum of 4,294,967,296 (2^{32}) unique addresses. Addresses in IPv6 are 128-bits, which allows for 3.4×10^{38} (2^{128}) unique addresses.

IPv4 address is split into two parts:

- **Network ID:** A network ID, within the world of Transmission Control Protocol/Internet Protocol or TCP/IP, is the portion of the TCP/IP address that identifies the Network for a given host, usually composed of three octets with dotted-decimal representation. The term "network ID" also can be applied in several ways to local network resources for user authentication. Still, the classic use of the time relates to the TCP/IP address itself, how that's wont to route information. Think of the Network ID because the suburb you reside in and therefore the Node ID your street therein suburb. You'll tell precisely where someone is that if you've got their suburb and street name. In the same way, the Network ID tells us which Network a specific computer belongs to. Therefore the Node ID identifies that computer from all the remainder that reside within the same Network.
- **Host ID:** The Host ID is the portion of an IP address that uniquely identifies a number on a given TCP/IP network. You discover the host ID by logically NANDing the binary sort of the IP address with the binary some the subnet mask for the Network. The opposite part of an IP address is the network ID, which specifies the Network to which the host belongs.

When writing a network address, or an IP address for that matter, Who must provide more detail than simply a dotted-decimal representation of an IP address's 32 bits. For instance, just being told that a tool has an IP address of 10.1.2.3 doesn't tell you the Network on which the IP address resides. To understand the network address, you would like to understand the subnet mask, which might be written in dotted-decimal notation or Lukasiewicz notation (also referred to as slash notation). Within the Example, where we have an IP address of 10.1.2.3 and an 8-bit subnet mask, the IP address might be written as 10.1.2.3 255.0.0.0 or 10.1.2.3 /8. Similarly, the network address might be written as 10.0.0.0 255.0.0.0 or 10.0.0.0 /8.

Classes of Addresses

Although an IP address (or a network address) needs subnet mask information to work out which bits represent the network portion of the lesson, there are default subnet masks with which you ought to be familiar. The default subnet mask for a given IP address is solely determined by the worth within the IP address's first octet.

Address Classes	Value in First Octet	Classful Mask	Slash Notation
Class A	1-126	255.0.0.0	/8
Class B	128-191	255.255.0.0	/16
Class C	192-233	255.255.255.0	/24
Class D	224-239	-	-
Class E	240-255	-	-

Table 1: Classes in IPv4

Class A Addresses

Class A addresses are for networks with a sizable amount of total hosts. Class A allows for 126 networks by using the primary octet for the Network ID. the primary bit is usually set and glued to zero during this octet. And next seven bits within the octet are ready to at least one, which then complete network ID. The 24 bits within the remaining octets represent the host's ID, allowing 126 networks and approximately 17 million hosts per Network. Class A network number values begin at one and end at 127. the category A format is as follows:

Network.Host.Host.Host

Class A network addresses are 1 byte long, with the primary little bit of the byte reserved and the seven remaining bits available for manipulation or address. As a result, the theoretical maximum number of sophistication A networks which will be created is 128. Why well, each of the seven-bit positions can either be a zero or one, and a couple of to the facility of seven gives you 128. The designers of the IP address scheme said that the primary little bit of the quick bite during a Class A network address should be off, or 0. this suggests Class A address must be between zero and 127 within the first byte, inclusive.

To complicate matters further, the Network of all zeros addresses is resolved by designating the default route. Additionally, the route address 127, reserved for diagnostics, cannot be used either, which suggests that you can only use the numbers 1 to 126to designate class eight network addresses. this means the particular number of usable classes in network addresses is 128 - 2 or 126.

Address	Function
Network addresses of all 0's.	They are interpreted to mean this Network or segment.
The network address of all 1's.	They are interpreted to mean all networks.
Network 127.0.0.1	Reserved for loopback test designated the localhost and allowed the host to send a test packet without generating network traffic.
Host address of all 0's.	They are interpreted to mean network addresses or any host on the precise Network.
Host address of all 1's.	Interpreted to mean all hosts on the precise Network; for instance, 126.255.255.255 means all hosts on network 126.
Entire IP address set to all 0's.	Employed by Cisco router to designate the default route could also mean any network.
entire IP address set to all 1's.	Broadcast to all or any hosts on the present Network is usually called once broadcast or limited broadcast.

Table 2: Classes A

Each class address has three bytes for the host address of the machine this suggests there are 2^{24} unique combinations and thus precisely that a lot of potential special hosting lessons for every class within the Network. Because host addresses with two partners of all zeros and ones are reserved, the particular maximum usable number of hosts for sophistication in-network is 2^{24} - 2, which equals 16,777,214.

Class B Addresses

In a class be network addresses, the primary two bytes are assigned to the network Addresses, and therefore, the remaining 2 bytes are used for host addresses. The format is as follows:

Network.Network.Host.Host

With a network address being two Bytes, we are left with 2^{16} unique combinations, but the web designers decided that each Class B network address should start with digit one, then 0. This leaves 14-bit positions available to control so. Wicked 16,384 unique class be network addresses. during a Class B network, the RFC state that the primary bit on the primary bite should be turned on, but the second bit always must be turned off if we turn the opposite six bits on all of them on we'll find the range for the category be Network:

10000000 = 128
10111111 = 191

As you'll see, a category B network is defined when the preceding byte is configured from 128 to 191.

Class C Addresses

The first octet of sophistication C IP addresses has its first 3 bits set to 110. Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for sophistication C is 255.255.255.x. Class C network addresses were for little organizations and used 3bytes for the Network and 1 byte for node addresses. Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses. Class C IP address format is:

Network.Network.Network.Host

In a class C network address, the primary three-bit positions are always the binary the calculation is as follows:
Three bytes, or 24 bits, minus three reserve positions, leave 21 positions. Hence, there are 2^{21}, or 20,97,152 possible C Class networks. The RFC defines the primary 2 bits of the primary update as always turned on for sophistication C networks, but the third bit will never get on. Here's the range for a category C network:

11000000 = 192
11011111 = 223

So if you see an IP address with a variety from 192 up to 223, you recognize it is a class C IP address. Each unique class C network has one byte to use for host addresses. This gets us to 2^8 or 256 minus the two reserved patterns for all zeros and ones for a complete of 254 available host addresses for every class C network. When deciding which network address class to use, you want to consider what percentage of local hosts there'll get on the Network and how many subnetworks will be within the organization. Therefore, if the organization is small and the Network will have fewer than 256 hosts, a category C address is perhaps sufficient. If the organization is large, then a category B or Class A address could be more appropriate.

Class D and E Addresses

Class D addresses are used for multicasting applications. Unlike the previous classes, this is often not used for "normal" networking operations. Class D addresses have their first three bits set to "1" and their fourth bit to "0". Class D addresses are 32-bit network addresses, meaning that each one of the values within the range of 224.0.0.0 – 239.255.255.255 are wont to identify multicast groups uniquely. There are no host addresses within the category D address space since all the hosts within a gaggle share the group's IP address for receiver purposes. Example for a category D IP address: **226.22.5.172.**

Class E networks are defined by having the primary four network address bits as 1. That encompasses addresses from 240.0.0.0 to 255.255.255.255. While this class is reserved, its usage was never defined. As a result, most network implementations discard these addresses as illegal or undefined. The exception is 255.255.255.255, which is employed as a broadcast address. For example, a category E IP address is **244.124.79.31.**

Class	Higher bits	Network address bits	Host address bits	No. of networks	No.of hosts per network	Range
A	0	8	24	2^7	2^{24}	0.0.0.0 - 125.255.255.255
B	10	16	16	2^{14}	2^{16}	128.0.0.0 - 191.255.255.255
C	10	24	8	2^{21}	2^8	192.0.0.0 - 223.255.255.255
D	1110	Reserved	Reserved	Reserved	Reserved	224.0.0.0 - 239.255.255.255
E	1111	Reserved	Reserved	Reserved	Reserved	240.0.0.0 - 255.255.255.255

Table 3: Classes Network Bits/ Host Bits

Private IP Addresses

Overview

The local address of the home router is set to the default dedicated IP address number. This is usually the equivalent address of the opposite model from that manufacturer and is often seen in the manufacturer's documentation. Your public IP address is the IP address that someone at the other end of your Internet activity will see (if they bother to find it). This is the only reason it is called a public IP address. The web works similarly, except that it guides your activities (emails, answers to Google queries, etc.) and forwards the emails to your computer address. If there is no public IP address, there is nothing you can do. It is your pass to the Internet.

In theory, your computer should have your unique IP address so that it only receives knowledge prepared for you. However, this is not how it works due to an important exception: computers on the network connect to the router and share an equivalent public IP address.

Range of Private IP Address

The organization that distributes IP addresses to the earth reserves various IP addresses for personal networks. In your simple home network, the router is in the middle, the computer is wired or wirelessly connected to it, and these networks are clustered. Once an internet connection is established through your internet service provider, your router sends internet activity to any computer connected to your router, which is the basis of a network innovation called Network Address Translation. (NAT).

- NAT can be a process where your router changes your private IP address to a public IP address so that you can send your traffic across the network and track changes in the process.
- When this information is returned to your router, it will reverse the change from a valid IP address to a personal IP address and forward the traffic to your computer.

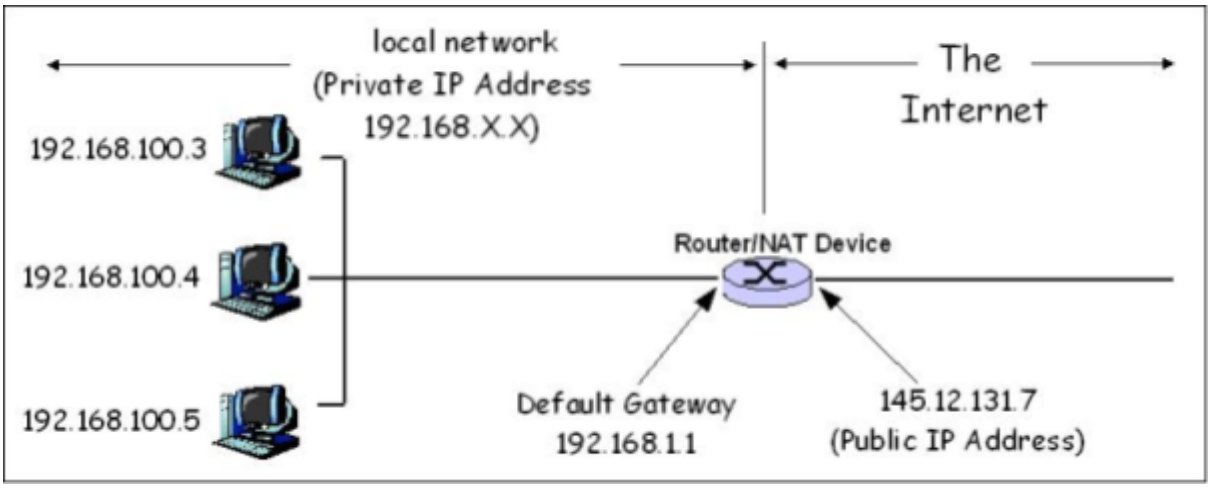

Figure 1: Private Network

Your private address is only used for your router, your network, and you. The range of remote addresses on the web does not need to be in sync with the rest of the earth and therefore does not need to be in sync with the Internet. The private address range is generally used by one address. Network administrators who use these personal addresses have more subnet space and more addresses than those assigned. The private IP address does my job for your home network. A single network typically uses these address blocks. Even if your neighbor uses the same course, it will not cause a problem because that is your network, not yours. You see, these private addresses are called non-routable addresses. Networks on the web only route Internet activity to your public IP address, not your IP.

- Class A: 10.0.0.0 — 10.255.255.255
- Class B: 172.16.0.0 — 172.31.255.255
- Class C: 192.168.0.0 — 192.168.255.255

Public IP Addresses

Overview

A public IP address is an IP address that can be accessed directly via the Web and assigned by your Internet Service Provider (ISP) to your network router. Your device also has a private IP; the IP remains hidden once it connects to the network through the router's public IP. Using a public IP address to connect to the Internet is like using a PO Box instead of providing your home address. It's a bit more secure but more noticeable. If the resource on your tenant is to be directly accessible from the network, it must have a public IP address. Depending on the type of resource, there may be other requirements. Certain types of resources in the lease are designed to be directly accessible from the Web and automatically include a public IP address. For example, NAT gateway or a general load balancer. What can now access other types of resources as long as they are configured? For example, the instance in your VCN.

Public IP Address

The public (external) IP address is assigned to each device connected to the Web, and each IP address is unique. Therefore, it is impossible to have two devices with the same public IP address. This addressing scheme allows widgets to "search" and exchange information online. The user cannot control the (public) IP address assigned to the device. Since the device is connected to the network, the network service provider will transfer a public IP address to the machine as soon as possible. This usually doesn't seem right. Public IP addresses are generally static, dynamic, or shared.

Static IP

Public static is sometimes referred to as private, meaning that the IP address never changes and is linked to a user, device, server, or website. A web service provider provides unique and constant IP addresses for different routers (they never change for each device). In this case, the router performs the NAT process instead of the ISP, so when the router sends or receives data from a remote host on the Web, the ISP is "transparent."

Most users do not need a static IP address, but when external devices, websites, or users must remember their IP address for continued use, a static IP address is essential.

For example, if you continuously need to access a tool remotely. Since the IP address never changes, you or other users only need to remember one IP address at any given time to be successful on the device.

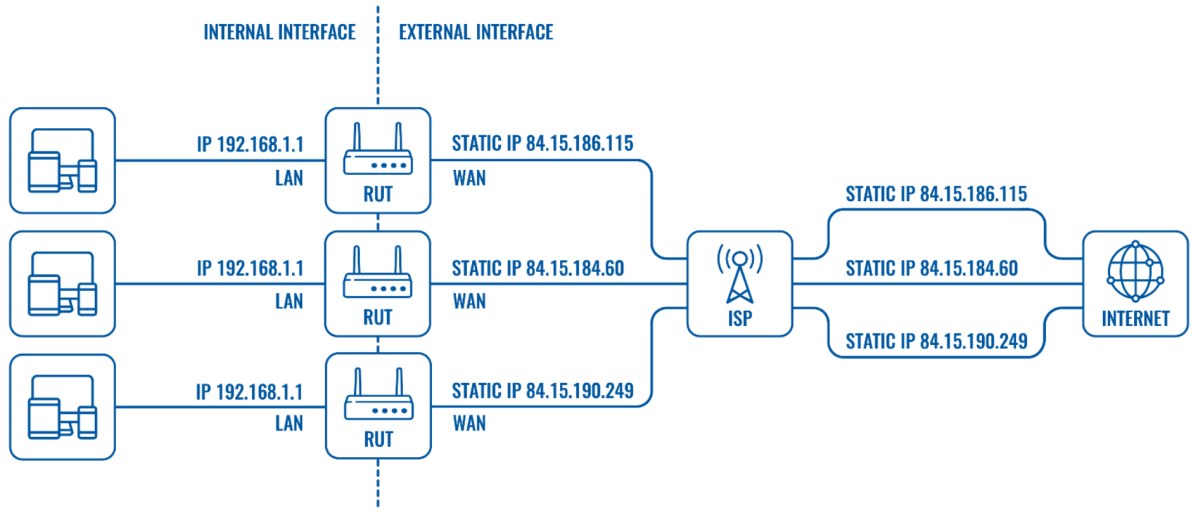

Figure 1: Static IP

Shared IP

Shared IP in some cases, an ISP can assign a public IP address to a group of users and then use NAT to isolate their traffic. We all know that multiple devices (even websites) can share a public IP address. The ISP provides the customer with a private WAN IP address and then uses NAT to distinguish which host a particular packet should be directed to. However, shared IP has a massive disadvantage because the owner of the tool or website is no longer the only entity responsible for its IP address. For example, if one of the multiple users with the same IP address commits some cybercrime so that IP address is blocked, what will also block all users using that IP. You can find more information about Network Address Translation (NAT) here.

Dynamic IP address

A dynamic public network means that the IP address may change from time to time (for example, once you lose the connection and reconnect, the ISP may change the address periodically). We all know that in the case of a dynamic IP address, the ISP provides a private WAN IP address for the router and then "translates" it to a public IP address when connecting to a remote host on the Web. The most significant difference with a static IP address is that the dynamic IP provided by the ISP is not permanent. They will change when the router disconnects and reconnects, re-registers with the network

operator, or in some cases, the ISP may periodically update the IP address. When it comes to remote access, dynamic IP complicates things because it is impossible to know the external IP address at any given time. Although the use of dynamic IP addresses for remote access is more complicated, it is not impossible; what can achieve it by using active DNS services (Service → Dynamic DNS). Naming services or DNS provide names for IP addresses (for example, www.google.com, www.facebook.com). Dynamic DNS will periodically rebind the IP address to the hostname. Therefore, when using dynamic DNS, you only need to remember the hostname to be successful on the selected device at any given time, although its IP address may change from time to time.

Ping, DHCP Client Address

DHCP Overview

Statically assigning IP address information to individual networked devices is often time-consuming, error-prone, and lacking scalability. Rather than static IP address assignments, many corporate networks dynamically set IP address parameters to their devices. An early option for performing this automatic assignment of IP addresses was Bootstrap Protocol (BOOTP for short). However, the foremost popular approach for dynamic IP address assignment is Dynamic Host Configuration Protocol (DHCP). DHCP offers a more robust solution to IP address assignment than the answer provided by BOOTP. DHCP doesn't require a statically configured database of MAC address to IP address mappings. Also, DHCP features a wide variety of options beyond introductory IP address, subnet mask, and default gateway parameters. For instance, a DHCP server can educate a DHCP client about the IP address of a WINS server, or maybe an administrator-defined parameter (for example, the IP address of a TFTP server from which a configuration file might be downloaded). A protocol rendered obsolete by BOOTP and DHCP is Reverse Address Resolution Protocol (RARP).

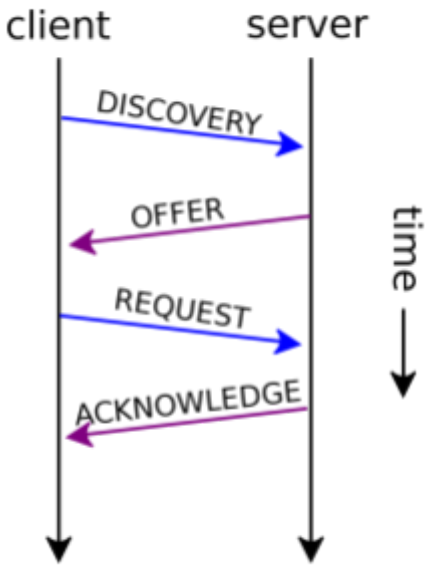

Figure 1: DHCP Request

Ping Overview

Ping may be a command-line utility available on virtually any OS with network connectivity that tests to ascertain if a networked device is reachable. The ping command sends an invitation over the network to a selected device. A successful ping leads to a response from the pc that was pinged back to the originating computer. A ping is employed to verify connectivity at an IP level to a second TCP/IP device. It does this by transmitting Internet Control Message Protocol (ICMP) Echo Request messages and waits for a return message. Unless modified, the ping command will send 4 requests by default in Windows. What percentage of responses get returned and the way long it takes for the round-trip provide essential information, such as:

- Bytes sent and received
- Packets sent, received, and lost
- Approximate round-trip time (in milliseconds)

The ping is initiated several times to check consistency within the connection. Here's what a successful ping request would return when connecting to a router. A Ping measures the time it takes for packets sent from the local host to a destination computer and back. The Ping tool measures and records the round-trip time of the package and any losses along the way. DomainTools' Ping service offers Ping information to display in a graphical and arranged manner available directly from the DomainTools website. This tool tests the essential connectivity of domains and IP addresses. Use this tool for troubleshooting purposes and to check response times.

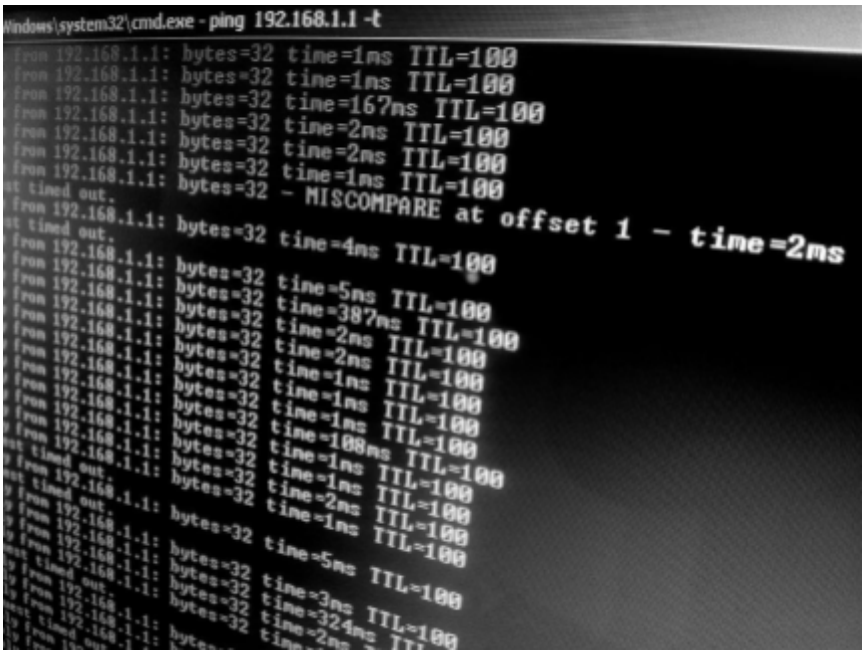

Figure 2: Ping Request

Subnetting

Overview

A subnet or subnet can be a network within the network. Subnets make the web more efficient. Through subnetting, network traffic can be transmitted over a shorter distance without going through unnecessary routers to reach the destination successfully. Imagine that Alice mails a letter to Bob, who lives in a small town near her home. For Bob to receive the letter as soon as possible, it must be sent from Alice's post office to Bob's city post office, and then to Bob. If the letter were first sent to a post office a few miles away, it could take longer for Alice's letter to succeed Bob. Like mail, the network will be more efficient when the message is spread as directly as possible. When a network receives data packets from another web, it classifies and routes these data packets by subnet so that the data packets do not reach the destination through inefficient routes.

When the IP system was first introduced, it quickly became apparent that although it is now much easier to find the selected network, it is now also challenging to send the knowledge packet to the machine you want to be on the web. This becomes especially obvious when the network becomes large enough to support a business because network performance becomes more significant. Subnets help solve this problem by dividing the network into smaller parts, reducing congestion. The data packet is ready to flow to the destination and avoid human bottlenecks. For logical reasons (firewalls, etc.) or physical requirements (smaller broadcast domains, etc.), companies can use IP subnets to divide more extensive networks. In other words, routers use subnets to form routing options.

The purpose of subnetting

Consider the number of assignable IP addresses in the various IP address categories shown in Table 1. Remember that the host bits of an IP address cannot be all zeros (representing a network address) or all ones (representing a directed broadcast address). Therefore, the number of IP addresses that who can assign in a subnet is generally determined by the following formula, where h is the number of host bits during the subnet mask:

Number of IP addresses that can be assigned during the subnet = $2^h - 2$,

Address Class	Assignable IP Addresses
Class A	16,777,214 ($2^{24} - 2$)
Class B	65,534 ($2^{16} - 2$)
Class C	254 ($2^8 - 2$)

Table 1: Assignable IP Addresses

Suppose you decide to use a class B private IP address (for example, 172.16.0.0/16) as your internal IP address. For performance reasons, you may not want to support up to 65,534 hosts in a single broadcast domain. Therefore, the best practice is to use this network address and subnet the network (thus expanding the number of network bits in the network subnet mask) to other subnets.

Calculate the number of subnets created

To determine the number of subnets created by adding bits to the classful mask, you can use the following formula, where s is the number of bits rendered:

Number of subnets made = 2^s

For example, Suppose you use a 28-bit subnet mask to subnet the 192.168.1.0 network, and you want to calculate the percentage of subnets created. First, determine the percentage of borrowed bits that you have acquired. Remember that the number of bits rendered is the number of bits that exceed the classful mask during the subnet mask. In this case, because the value of the leading octet in the network address is 192, you will conclude that this is usually a class C network. Also, as you may recall, a class C network has 24 bits in its subnet mask with class (that is, default). Because you now have a 28-bit subnet mask, the number of rendered bits is generally calculated as follows:

number of borrowed bits = bits in a custom subnet mask-bits in a classful subnet mask

number Borrowed bits = 28 - 24 = 4

Now, if you only know you have four borrowed places, you will increase the install from 2 to 4 (2^4, or 2 * 2 * 2 * 2), which equals 16. Based on this calculation, you can conclude that dividing into 192.168.1.0/24 subnets with a 28-bit subnet mask results in 16 subnets.

Calculate the number of obtainable hosts

Suppose you want to calculate the number of available hosts IP addresses in one of the 192.168.1.0/28 subnets. First, you need to calculate the number of host bits in the subnet mask. Since it recognizes that the IPv4 address consists of 32 bits, it will subtract the number of bits in the subnet mask (28 in this example) from 32 to calculate the number of host bits:

host bits = 32-host bits Count the number of bits in the subnet mask
number of bits in the host = 32-28 = 4

Now you only know the number of host bits. You will apply it to the above formula, where h is the number of host bits in the subnet mask:

The number of IP addresses that can be allocated in the subnet = 2^h-2
The number of IP addresses that can be allocated in the subnet = 24-2 = 16-2 = 14

Through this calculation, you will conclude that 192,168.1.0 / 28 Each of these subnets has 14 available IP addresses.

Host Bit	Supported Hosts
2	2
3	6
4	14
5	30
6	62
7	126
8	254
9	510

10	1022
11	2046
12	4094

Table 2: The number of hosts supported by a given number of specific host bits

Figuring New IP Address Ranges

Since you basically can figure the number of subnets made upheld a given number of acquired pieces, the ensuing coherent advance is to compute the IP address ranges making up those subnets. for instance, on the off chance that you took the 172.25.0.0/16 and subnetted it with a 24-bit subnet veil, the subsequent subnets would be as per the following:

172.25.0.0/24

172.25.1.0/24

172.25.2.0/24

...

172.25.255.0/24

Let's consider how such a calculation is performed. Notice in the previous example that you count by 1 in the third octet to calculate the new networks. To determine in what octet you start counting and by want increment you count, a new term needs to be defined. The interesting octet is the octet containing the last 1 in the subnet mask.

Example:

A 27-bit subnet veil is applied to an organization address of 192.168.10.0/24. To compute the made subnets, you'll play out the ensuing advances:

1. The subnet cover (in parallel) is 11111111.11111111.11111111.11100000. The intriguing octet is the fourth octet on the grounds that the fourth octet contains the final remaining one inside the subnet.
2. The decimal worth of the fourth octet inside the subnet veil is 224 (11100000 in decimal). Along these lines, the square size is 32 (256 – 224 = 32).
3. The first subnet is 192.168.10.0/27 (the worth of the principal 192.168.10.0 organization with the acquired pieces [the initial three pieces inside the fourth octet] set to 0).
4. Tallying by 32 inside the intriguing octet (the fourth octet) permits you to ascertain the excess subnets:

192.168.10.0
192.168.10.32
192.168.10.64
192.168.10.96
192.168.10.128
192.168.10.160
192.168.10.192
192.168.10.224

Since you know the subnets made from a classful organization given a subnet cover, an ensuing consistent advance is to work out the usable addresses inside those subnets. Review that you can't dole out an IP address to a device if all the host bits inside the IP address are set to 0 on the grounds that an IP address with all host bits set to 0 is that the location of the subnet itself. Also, you can't appoint an IP address to a device if all the host bits inside the IP address are set to 1 on the grounds that an IP address with all host bits set to 1 is the coordinated transmission address of a subnet. By barring the organization and coordinated transmission addresses from the 192.168.10.0/27 subnets (as recently determined), the usable addresses are displayed in Table 3 not really settled.

Subnet Address	Directed Broadcast Address	Usable IP Addresses
192.168.10.0	192.168.10.31	192.168.10.1–192.168.10.30
192.168.10.32	192.168.10.63	92.168.10.33–192.168.10.62
192.168.10.64	192.168.10.95	192.168.10.65–192.168.10.94
192.168.10.96	192.168.10.127	192.168.10.97–192.168.10.126
192.168.10.128	192.168.10.159	192.168.10.129–192.168.10.158
192.168.10.160	192.168.10.159	192.168.10.161–192.168.10.190
192.168.10.192	192.168.10.223	192.168.10.193–192.168.10.222
192.168.10.224	192.168.10.255	192.168.10.225–192.168.10.254

Table 3: Usable IP Address Ranges for the 192.168.10.0/27 Subnets

Supernetting

Overview

Supernetting is to add a network to create a more extensive network (supernet or supernet). Let us consider the basic definition of an IP (network) address: it consists of a network part and a host ID. For subnetting, we "borrow" bits from the host ID to create a smaller network. In contrast, we extract bits from the network part for supernets to develop a more extensive network. Supernets are usually used to route advertisements. However, it has other uses, such as building access control lists (ACLs), combining multiple static routes into one, etc.

Supernetting is mainly used for route summarization, combining the routes of multiple networks with similar network prefixes into one routing entry. The routing entry points to an excellent network that spans all networks. This continuously significantly reduces the dimensionality of the routing table and the metric of routing updates exchanged by the routing protocol. Combine multiple IP network addresses into one IP address. Supernetting minimizes the number of routing table entries in CIDR, which also targets the internal network.

The purpose of Supernetting

The primary purpose of the supernet is to reduce the dimension of the routing table in the router. For example, instead of having eight separate routes (pointing to the equivalent next hop), a router can have an aggregate way of eight independent ways. This is usually important for the following reasons:

- It can save memory and processing resources on the routing device. They have little storage space for routing tables, and their throughput to view routing tables is also low.
- Provides network stability because fluctuations in a specific part of the network will not extend to all or any aspect of the web. That is, the changes are usually isolated.

In addition to the benefits of the routing table, it also helps prevent IP address depletion through classless inter-domain routing (CIDR). Basically, instead of distributing the Class B network to everyone who needs the equivalent of a Class C network, you can now use variable-length prefixes (like / 19, / 21, etc.) to add these Class C networks as efficiently

as possible. Finally, you will use supernets to expand the number of addresses available on the network. For example, you would add four / 24 networks (each with 254 public IP addresses) to create a / 22 network (with 1022 available IP addresses).

Rules of Supernetting

Supernet rules are the same as subnetting. Super grids are counted in the order of 2, 2, 4, 8, 16, etc.; Once you create a supernet, you want to make sure it only covers what you want to add network, not less. Less is better, so avoid routing problems.

- Make sure the network is continuous (defined as "adjacent or together in order").
- Determine the number of networks to be added and make sure the number is two.
- The value of the leading non-public octet in the first (lowest) IP address block in the list of networks to be added is compared to the number of networks to be added (plus the order of 2). The value of the non-public leading octet must be A multiple of the number of networks to be aggregated. For example, 16 is a multiple of 8 but 8 is not a multiple of 16.

Interview Questions

IPV4 Addressing

Q1. What are the different particular IP addresses? **(Cisco)**

Answer: Below are multiple unique IP addresses and Their roles:

IP Address	Description
127.0.0.1	Loopback Address
0.0.0.0	Non-routable addresses describing invalid or unknown destinations
255.255.255.255	Limited Broadcast address
xxx.255.255.255 xxx.xxx.255.255 xxx.xxx.xxx.255	Directed broadcast address

Q2. What is a private IP? What is the range set for private IP? **(Dell)**

Answer: A dedicated IP address is a series of non-Internet IP addresses used on the internal network. Private IP addresses are provided by network devices (such as routers) through network address translation. The range for private IP addresses are:
Class A: 10.0.0.0 — 10.255.255.255
Class B: 172.16.0.0 — 172.31.255.255
Class C: 192.168.0.0 — 192.168.255.255

Q3. How is Public IP different from private IP? Can we access other networks Using their public IP? **(Cisco)**

Answer: Your private IP address exists in the specified remote IP address range reserved by the Internet Assigned Numbers Authority and should not appear on the Internet. There are millions of private networks globally, and all of these networks contain devices assigned personal IP addresses within these ranges. Yes, that is how the Internet works; we access other systems using their public IPs.

Q4. What is Ping utility? What protocol does ping work on and on which layer of the OSI model? **(Arista)**

Answer: Ping is a command-line utility used on almost any operating system with a network connection to test whether it can access networked devices. The ping command sends a request to a specific device over the network. A successful ping will cause the computer to ping the original computer to respond. Ping works using ICMP protocol and works on layer 3.

Q5. What is the Process of DHCP? How does it work?

Answer: Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically configure devices on an IP network, allowing them to use network services, such as DNS, NTP, and any communication protocol based on UDP or TCP. The DHCP server dynamically assigns IP addresses and other network configuration parameters to each device on the network to communicate with other IP networks.
The following factors can measure the reliability of a network:

- **Discover:** The client discovers DHCP
- **Offers:** The DHCP server provides a set of IPs for the client to choose any
- **Request:** The client selects an IP and asks for a DHCP confirmation
- **Acknowledgment:** The DHCP server sends a DHCP ACK execution confirmation to the client.

Q6. Your router has the following IP address on Ethernet0: 172.16.2.1/23. Which of the following can be a valid host ID on the LAN interface connected to the router? **(Wipro)**

Answer: 172.16.2.255. The IP address of the E0 interface router is 172.16.2.1/23, which is 255.255.254.0. This makes the block size of the third octet 2. The router interface is on

subnet 2.0, and the broadcast address is 3.255 because the next subnet is 4.0. The valid host range is 2.1 to 3.254. The router is using the first valid host address in the content.

Q7. What is the maximum number of IP addresses assigned to a host on the local subnet using a subnet mask of 255.255.255.224? **(TCS)**

Answer: 30. A / 27 (255.255.255.224) has 3 bits on and 5 bits off. This provides eight subnets, each with 30 hosts. Is it essential to use this mask with class A, B, or C network addresses? Not at all. The number of host bits will never change.

Q8. How many subnets and hosts do the network address 172.16.0.0/19 provide? **(Infosys)**

Answer: 8 subnets, 8,190 hosts each. The CIDR address of /19 is 255.255.224.0. This is a Class B address, so it has only three subnet bits, but it provides 13 host bits or eight subnets, each with 8,190 hosts.

Flow Control Policies of DLL

Overview

On the network, the sender sends information, so the receiver receives the information. But assuming that the sender can receive and process the data faster than the receiver, then the information will be diverted. Flow control methods will help ensure this. The flow control method will ensure that the sender only sends notifications that the receiver can receive and process. Flow control tells the sender what percentage of data needs to be sent to the receiver not to be lost. This mechanism allows the sender to wait for confirmation before sending subsequent data.

An ideal network should be prepared to ensure that knowledge is transferred to the target host without errors in the DLL(Data Link Layer). The system must ensure that the information received is the same as the information transmitted for many applications. Many factors will eventually change the information and can corrupt the transmitted bits. Data is often destroyed during transmission. Some applications often require error detection and correction. Some applications can tolerate a small number of errors. For example, random audio or video transmission errors can also be accepted, but in text messages, equivalent errors are unacceptable.

Stop and Wait Protocol

In this protocol, the sender will send one frame to the receiver at a time. The sender will stop and wait for confirmation from the receiver. This time (the time between sending the message and receiving the confirmation) is the sender's timeout, so the sender is completely inactive during this period. When the sender acknowledges receipt (ACK), it will send the following packets to the receiver and wait for the confirmation again; this process will continue because the sender has information to send. The following figure will help understand this:

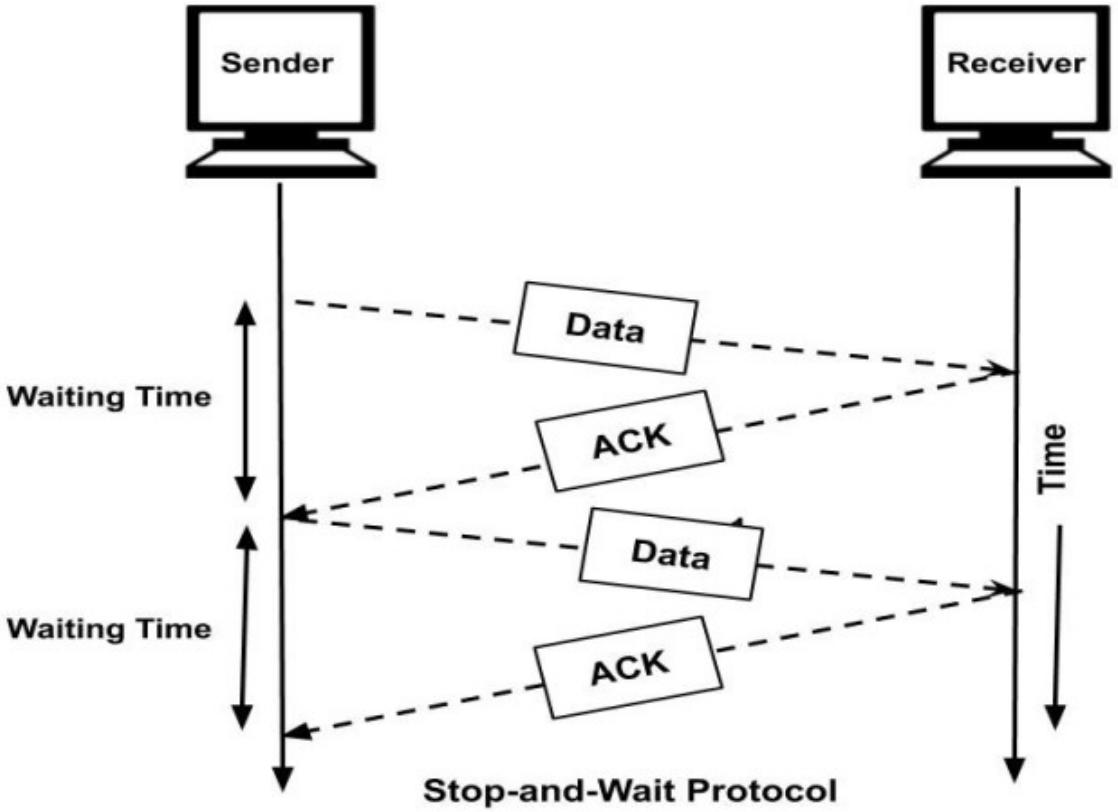

Figure 1: Stop and Wait Protocol

Suppose that any frame sent is not received by the receiver and is lost. Therefore, the receiver will not send an acknowledgment because it has not received any frames. In addition, the sender will not send subsequent frames because it will wait for an acknowledgment of an earlier frame that it has shipped. Therefore, there is often a stalemate here. To avoid any such situation, there is a timeout timer. The sender will wait for this fixed time to receive the confirmation, and if it does not receive the ack, it will resend the frame. It allows us to assume that the channel is noisy and can introduce errors in the data transmitted through it. Channel noise can damage the frames, or they can drift completely. Let's understand this through simple steps:

- The sender first transmits a frame, then stops the transmission and waits for confirmation from the receiver.
- If a positive acknowledgment is received (meaning the receiver is ready to receive subsequent frames), go to step 1 above.
- If a negative acknowledgment (NACK) is received (the receiver cannot receive subsequent frames), it waits for a positive acknowledgment (ACK) from the receiver.

Go Back N ARQ

Go back was introduced because the "stop and wait protocol" is not efficient because the sender can only send one data packet at a time and must wait for the next frame to be transmitted until the previous frame is recognized. In this way, the stop-and-wait protocol wastes channel bandwidth and even increases the trigger delay. This is usually because the stop and wait protocol does not use the concept of pipes. A pipeline can be a general concept in which post-task processing starts before the end of the previous task. In the network, the idea of pipes specifies that the source can send several frames before acknowledging the main transmission frame. The sliding window is an imaginary box in the transmitter and receiver. This window also keeps the frame in transmission as the receiving endpoint and provides an upper limit on the number of frames transmitted before an acknowledgment is obtained. The range that the sender pays attention to is called the sending window, and the range that the receiver gives priority to is called the receiving window.

Figure 2: Sliding Window

GoBackN ARQ, the sender's dimension is N, so the receiver's window size is usually 1.

- The use of cumulative acknowledgments in this protocol means that the receiver maintains an identification timer; whenever the receiver receives a replacement frame from the sender, it starts the replacement identification timer. When the

timer expires, the receiver sends a cumulative acknowledgment of all structures that the receiver did not recognize at that time.

- It should be noted that the new confirmation timer will only start after receiving the replacement frame, and the old confirmation timer will not start after the timeout.
- If the receiver receives a corrupted frame, it silently discards it, so the sender will retransmit the correct frame after the timeout timer expires. Therefore, the receiver silently discards corrupted frames. By silently discarding, we mean: "Only reject the frame, and take no action on the frame."
- If the confirmation timer expires, it is assumed that there is only one frame left for confirmation. In this case, the receiver sends a separate acknowledgment of the frame.
- If the receiver receives messy frames, it just discards all frames.
- If the sender does not receive any confirmation, the entire frame window will be retransmitted.
- Use of GoBackN ARQ protocol results in retransmission of lost frames

Selective Repeat ARQ

The function of the selective repetition protocol is that it allows the receiver to accept and buffer the packets following the damaged or missing packages and then only retransmit the boxes that are lost or damaged in the network channel during transmission. This protocol is similar to the GoBackN ARQ protocol or an improved version of GBN ARQ. The difference is that a buffer is used here, and both the receiver and the sender maintain a size window. This selective repetition sometimes works best when network links are generally unreliable. Because here, in this case, retransmission tends to occur more frequently. Selective frame retransmission is much more efficient than full-frame retransmission. Selective retransmission also requires a full-duplex channel to transmit packets uniformly. And feedback/confirmation.

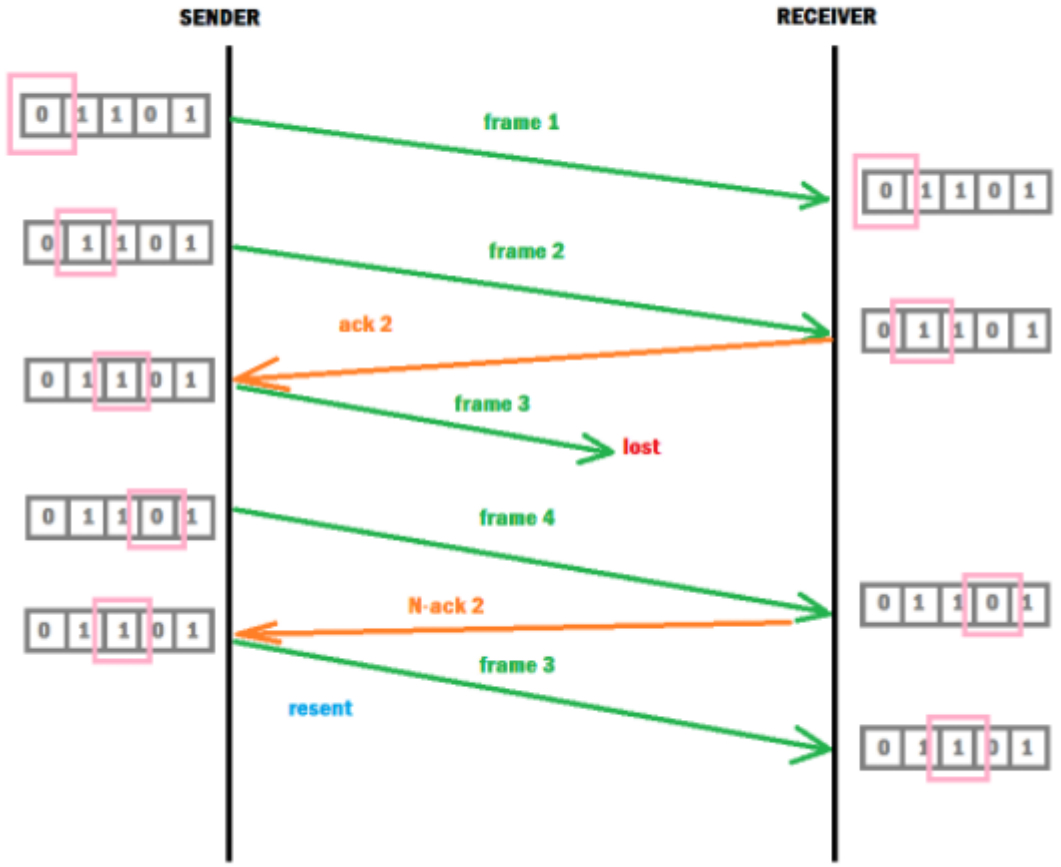

Figure 3: Selective Repeat

Now, in the above figure, the sender first sends frame 1 (i.e., 0), the receiver immediately recognizes the frame, and then sends frame 2, which is also recognized. We will see that frame3 is lost during transmission and cannot succeed at the receiver, but the next frame, i.e., frame4, is transmitted and accepted by the receiver. Then the receiver sends a negative confirmation, thanks to the sender for only transmit and send frame3 again Instead of retransmitting all frames starting from frame3 (this happens in GoBackN ARQ). The efficiency of the selective repeat protocol is the same as that of the GoBackN ARQ protocol.

efficiency = N / (1 + 2a)

where a = propagation delay / transmission delay

buffer = N + N

serial number = N (sender) + N (receiver)

Error Control Policies

Overview

Error control in the link layer can detect and retransmit information lost or damaged during the knowledge transmission process. Any reliable system must have mechanisms to detect and correct such errors. Error detection and correction occur at the transport layer and link layer. Error control is the technique of detecting and correcting knowledge blocks in the communication process. In other words, it checks the reliability of characters at the bit level and the packet level. By performing proper error checking on-site, you can ensure that the data sent and received are the same because the communication channel is often very unreliable in many cases.

Error handling includes error detection and correction. It primarily allows the receiver to inform the sender of any damaged or lost frames during transmission and then coordinate to retransmit them. The term link-layer error control refers mainly to the method of error detection and retransmission. Error handling is implemented particularly in a simple way when an error is detected during the exchange.

Parity

In transmitting data from the transmitter to the receiver, electrical noise corrupts the transmit signal. If the noise is significant, it will change the logic level of the movement, thus introducing errors in the transmitted signal. Parity is an additional 0 or 1 bit added to the first signal and does not detect errors. There are two methods of checking for equality, even and odd. In the even parity checking method, the value of the bit is selected so that the total number of ones (including parity) in the transmit signal is even.

Similarly, for odd parity, the value of the bit is chosen so that the total number of units is odd. For example, for the next byte, 11010000, the even check will be 1, which will make the total number of ones in the signal an exact number, so the odd review will be 0, which will make the total number of ones in the call is an odd number. It will determine if an error occurred during transmission by calculating the parity of the received byte and comparing the generated equality with the transmitted equality. Parity can only detect strange mistakes. If a large number of errors occur, the calculated

parity will match the transmitted parity. In addition, the parity check method only allows error detection; errors cannot be corrected because it does not provide a way to determine which bit is wrong.

Whenever a message is transmitted, it will be disturbed by noise, or data may be corrupted. To avoid this, we use error detection codes, which are additional data added to a given digital message to help us detect whether an error occurred during message transmission. A simple example of an error detection code is a redundancy check. Another method called cyclic redundancy check codes involves dividing the message into blocks. Then each block is treated as a binary number and separated by a predetermined number. The rest of this department is sent because the error verification number at the end of the message can verify the accuracy.

Checksum

The checksum can be a value representing the number of bits during the transmission of a message and is used by IT professionals to detect advanced errors in data transmission. Before dispatch, each knowledge or file is usually assigned a checksum value after executing a cryptographic hash function. The term checksum is sometimes called a hash sum or hash value. The way they work is to provide information about the transmission to the receiving party to ensure that the full scope of knowledge is fully delivered. The value of the checksum itself is usually an extended string of letters and numbers, such as a fingerprint of a file or set of files, used to indicate the number of bits contained in the transmission. If the checksum value calculated by the top user is slightly different from the first checksum value of the file, it can remind all parties in the transmission that the file has been corrupted or tampered with by a third party. From there, the recipient can investigate what went wrong or try to download the file again. The standard protocol used to determine the checksum number is the Transmission Control Protocol (TCP) and the User Map Protocol (UDP). TCP generally tracks transmitted knowledge packets more reliably, but UDP may also help avoid slowing down TRM.

The idea of a cryptographic checksum or hash function may seem complicated and may not be worth the effort. The checksum is not challenging to know or create.

Checksum Use Case

Suppose you download a massive software update, a service pack. This may be a huge file, and it will take a few minutes or longer to download. After downloading, how do I know that the file has been downloaded successfully? What if a few bits are lost during the download process, so the file you immediately get to your computer is not exactly

what you expected? Applying an update to a program that may not be the same as how the developer created it can cause you big problems. This is where you can get comfortable comparing the checksum. Assuming that the website where you downloaded the file provides checksum data next to the file to be downloaded, you will use a checksum calculator to provide the checksum of the downloaded file. The checksum can also be used to verify that the file you downloaded from somewhere other than the first source is a legitimate file from the first. Just compare the hash you created with the hashes available at the start of the file.

Cyclic Redundancy Check

Cyclic Redundancy Check (CRC) can be a technique used to detect errors in digital data. As a checksum, CRC generates a fixed-length data set that supports the construction of larger files or data sets. In terms of its use, CRC can be a hash function used to detect accidental changes in raw computer data that are commonly used in storage devices such as digital telecommunications networks and hard drives. The system was invented by W. Wesley Peterson in 1961 and developed by the CCITT (Comité Consultatif International Telegraphique et Telephonique). The cyclic redundancy check is quite simple to implement in hardware and can be easily analyzed mathematically. CRC is one of the most advanced technologies and is usually used to detect common transmission errors.

In Cyclic Redundancy Check, a fixed, fast number of check bits (usually called checksums) are added to the message that must be transmitted. The information receiver receives the information and checks whether there is an error in the parity bit. Mathematically, the data receiver evaluates the additional verification value by finding the remainder of the polynomial division of the transmitted content. If an error appears to have occurred, a negative acknowledgment is sent for data retransmission. The cyclic redundancy check also applies to storage devices such as hard drives. In this case, the parity bit is assigned to each block on the hard disk. When the PC reads a corrupted or incomplete file, it will trigger a cyclic redundancy error. The CRC can come from another storage device or CD / DVD. Common causes of errors include system crashes, incomplete or corrupted files, or files with many mistakes. The design of the CRC polynomial depends on the length of the supposedly protected block. The error protection function can also determine the CRC layout. The resources available for CRC implementation can have an impact on performance.

CRC can be a specific type of checksum and is also very useful. As mentioned earlier, a data set of any size is mapped to a fixed-size string during this period, which engineers can call a hash function.

Framing

Overview

Framing is a technique performed by the information link layer. The frame can be a point-to-point connection between two computers or devices, consisting of a cable, during which data is transmitted in the form of a bitstream. However, these bits must be framed indiscernible data blocks. Framing provides how the sender sends a set of bits that is meaningful to the receiver. Ethernet, Token Ring, Frame Relay, and other link-layer technologies have their frame structure. The frame header contains information such as a bug check code. The frame can be a point-to-point connection between two computers or devices, consisting of a cable, during which data is transmitted in the form of a bitstream. However, these bits must be framed indiscernible data blocks. Framing can be a function of the information link layer. Provides how the sender transmits a set of bits that is meaningful to the receiver. Ethernet, Token Ring, Frame Relay, and other link-layer technologies have their frame structure. The link-layer extracts the message from the sender and provides it to the receiver by giving the sender and receiver addresses. The advantage of using frames is that the data is intermittently divided into recoverable blocks, which can easily be checked for corruption.

Character Count

This method uses fields in the header to specify the number of characters in the frame. When the target's information link layer sees the number of characters, it knows what percentage of the characters are behind, knowing where the top of the frame is. The disadvantage is that if the count becomes distorted due to transmission errors, the destination will lose synchronization and not locate the beginning of subsequent frames. This method has never been used, and it is usually necessary to count the total number of characters in the frame. This is generally done using a field in the title. The character counting method ensures that there are a few real characters behind the link layer of the receiver or destination and the position of the end of the frame.

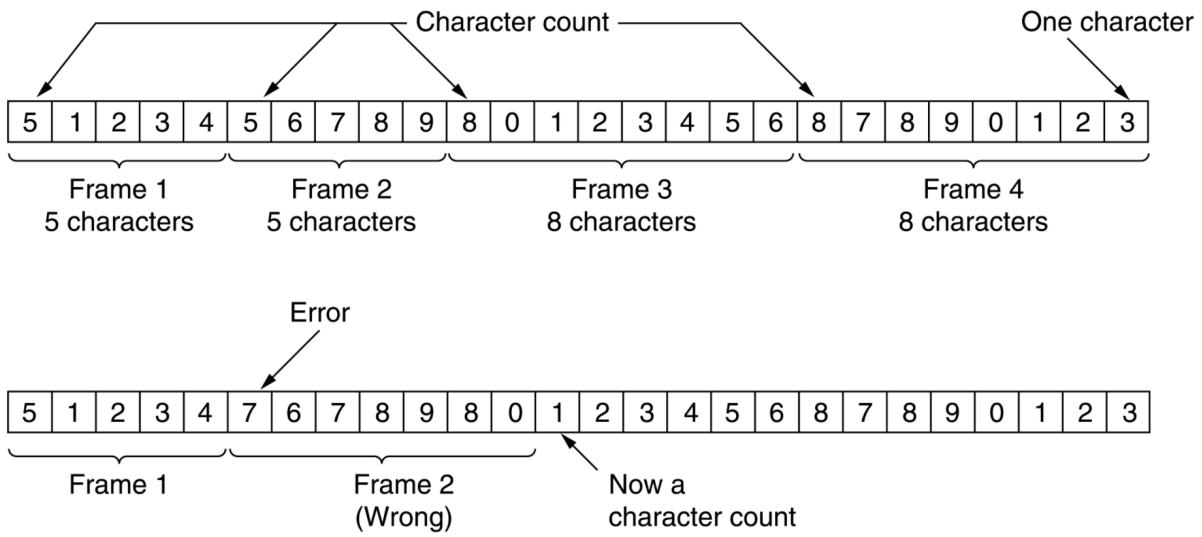

Figure 1: Character Count

Character Stuffing

Each frame begins with the ASCII character sequence DLE STX and ends with the DLE sequence ETX. (DLE is link escape, STX is the beginning of TeXt, and ETX is the end of TeXt.) This method overcomes the shortcomings of the character count method. If the destination is out of sync, look for the DLE STX and DLE ETX characters. However, if binary data is being transmitted, the characters DLE STX and DLE ETX may appear in the data. Since this interferes with the frame, a form called character padding is used. The sender link-layer inserts an ASCII DLE character into the data before the DLE character. Before this data is transmitted to the network layer, the receiver link layer deletes this DLE. However, character padding is closely related to 8-bit characters, which is usually a severe obstacle to transmitting characters of any size.

In byte padding (or character padding), when a personality has an identical pattern to the flag, a specific byte is added to the frame information part. The info part is filled with an extra byte. This byte is usually called the escape character (ESC), and it has a predefined bit pattern. Whenever the receiver finds an ESC character, it deletes it from the message part and treats subsequent characters as data, not boundary markers. Character padding is also called byte padding or character-oriented framing, which is the same as bit padding. Still, byte padding operates in bytes, while bit padding operates in bits. In byte padding, when there is a message or character with an identical pattern, a particular byte with a predefined pattern (basically called ESC (the escape character)) is added to the information part of the information stream or frame byte.

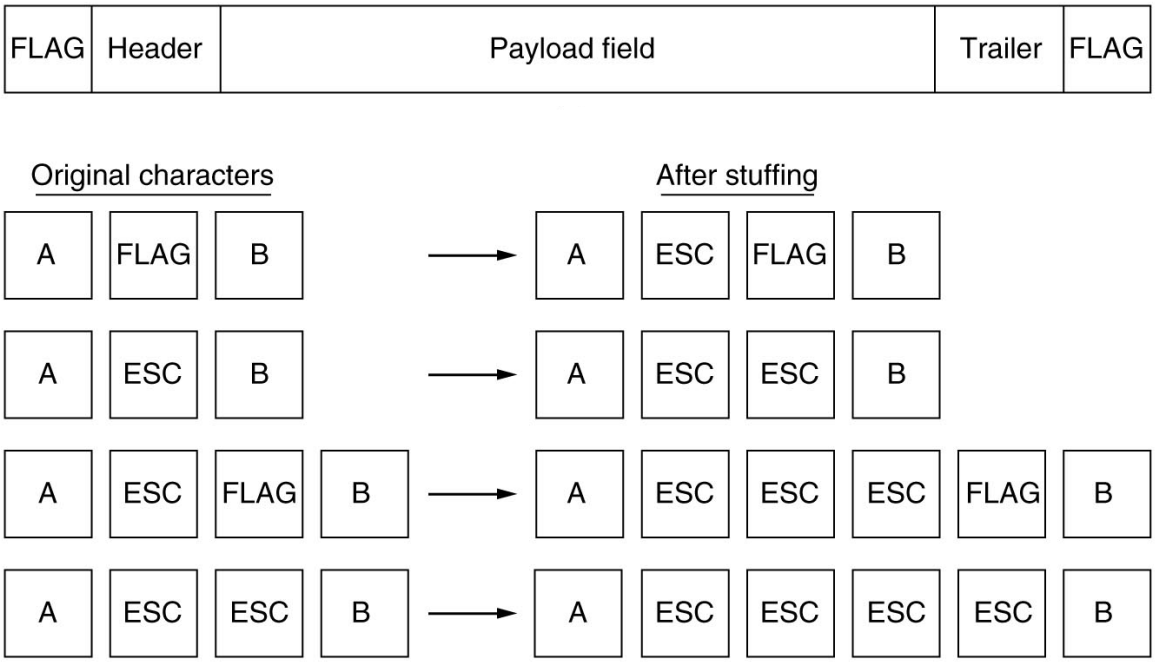

Figure 2: Character Stuffing

Bit Stuffing

It refers to the insertion of one or more bits into the knowledge transmission to provide signaling information to the receiver. The receiver knows how to detect, remove, or ignore padding bits. In the link layer of the open systems interconnection model, the bitstream is divided into units or frames that are easier to manage. Each frame contains sending and receiving information to facilitate transmission. An 8-bit flag byte is injected at the beginning and end of the sequence to separate the frames. This prevents the receiver from interpreting the flag as part of the transmitted information. Bit padding can also be used for other purposes. For example, you can increase a bitstream without an equivalent bitrate to a comparable rate to fill a buffer or fill a frame.

Regardless of the intended purpose, the state of the stuffing bits is transmitted to the receiving end of the information transmission, where the additional bits are extracted and sent back to their original shape or bit rate. In this way, bit stuffing allows multiple channels to be synchronized, maximizing available bandwidth.

Alternatively, bit stuffing is usually used for limited run-length encoding, limiting the number of bits that can be passed without conversion. This reduces the number of consecutive bits with equivalent values during the data stream to ensure reliable transmission and reception. However, bit stuffing alone does not guarantee that the

payload is free of transmission errors. Instead, it just ensures that the information starts and ends at the correct location. For this reason, unplanned error detection techniques should look for problems at the top of the frame, and if there are errors, resend the frame. Some consider bit stuffing to include bit stuffing, adding bits to the stream to form a streaming unit that fits a typical size. It is different from bit capture, a kind of in-band signaling.

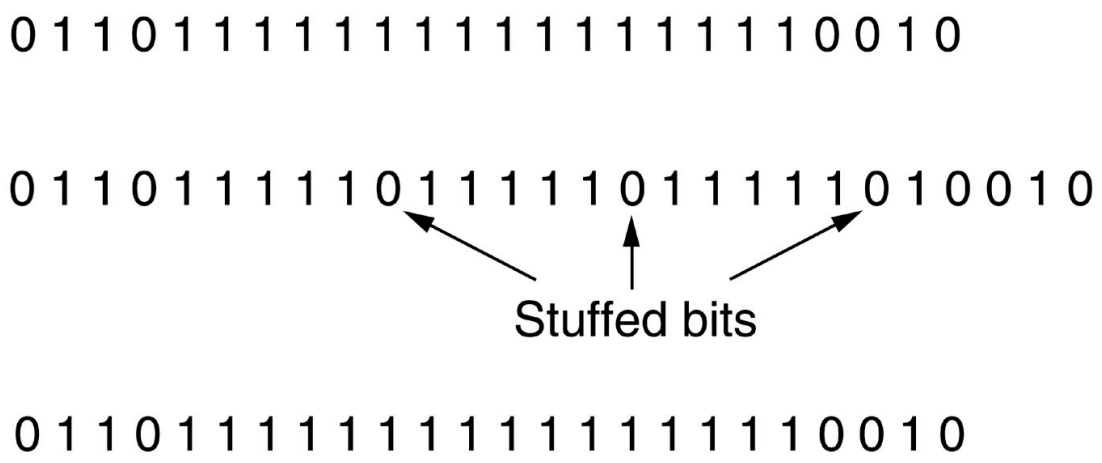

Figure 3: Bit Stuffing

Interview Questions

Data Link Layer

Q1. What Is a MAC Address? **(Cisco)**

Answer: The MAC (Media Access Control) address is a globally unique address written into the hardware during manufacturing. The MAC address can be a unique value associated with the network adapter. MAC address is also called hardware address or physical address. They uniquely identify the adapter on the LAN. The MAC address is a 12-digit hexadecimal number (48 digits in length).

Q2. What are the 2 sub-layers of the ink layer? **(Dell)**

Answer: The information link layer (Layer 2) of the OSI model actually consists of two sub-layers: the Media Access Control (MAC) sub-layer and the Logical Link Control (LLC) sub-layer. The MAC sublayer controls device interaction. The LLC sublayer handles addressing and multiplexing. The physical addressing of the network connection exists at the information link layer. The information link layer combines bits of data into entities called frames. There are network topologies like Ethernet at the information link layer. Network switches are the most common network equipment at the information link layer.

Q3. What is the function of LLC? **(Cisco)**

Answer: Use the L3 protocol to multiplex/demultiplex to the interface of the above (Layer3) network. When receiving a frame from the lower physical layer, LLC is responsible for observing the L3 protocol type and transmitting the datagram to the correct L3 protocol (demultiplexing) of the upper network layer. LLC can optionally provide reliable frame transmission by the sending node. The sending node numbers each transmitted frame (sequence number), and the receiving node recognizes each received frame (acknowledgment number). Therefore, the sending node retransmits the lost frame. frame.

Q4. What are the MAC modes of shared transmission media? **(Arista)**

Answer: Round Robin, Reservation, and Contention are three ways to share the access medium used by the MAC protocol. In the MAC reservation mode, each station in the network must reserve a time slot for its limited or unlimited time to access the shared medium. In the MAC implementation competition mode, each station in the network can transmit data at the same time regardless of whether there is a conflict.

Pure Aloha

ALOHA can be a system to coordinate and arbitrate access to shared communication network channels. Norman Abramson of the University of Hawaii and his colleagues developed it in the 1970s, the first system for terrestrial broadcasting. Still, the system has been implemented in a satellite communication system. Shared communication systems like ALOHA need a way to deal with conflicts that occur when two or more methods are scheduled to transmit on the channel simultaneously. In the ALOHA system, the node will send it as long as there is data to be sent. If another node transmits simultaneously, a collision will occur, so the transmitted frame will be lost. However, the node can listen to intermediate transmissions, including its communications, and determine whether a structure has been sent. In pure ALOHA, the transmission time is continuous. Whenever a station has a frame available, it will send the frame. If a collision occurs and the frame is destroyed; as a result, the sender will randomly wait for a while before retransmitting.
ALOHA can be a media access control (MAC) protocol to transfer knowledge over shared network channels. With this protocol, multiple data from multiple nodes circulates in various channels for transmission. In pure ALOHA, the transmission time is continuous. As long as a station has a frame available, it will ship the frame. If a collision occurs and the frame becomes corrupted; as a result, the sender waits its random time before retransmitting.

- When the network station needs to send a frame, it will send it immediately and wait for confirmation.
- If the sender receives an acknowledgment, the sender can send subsequent frames.
- If there is no confirmation, the sender thinks the frame has been distorted and retransmits the equivalent frame after a random time to avoid a collision.

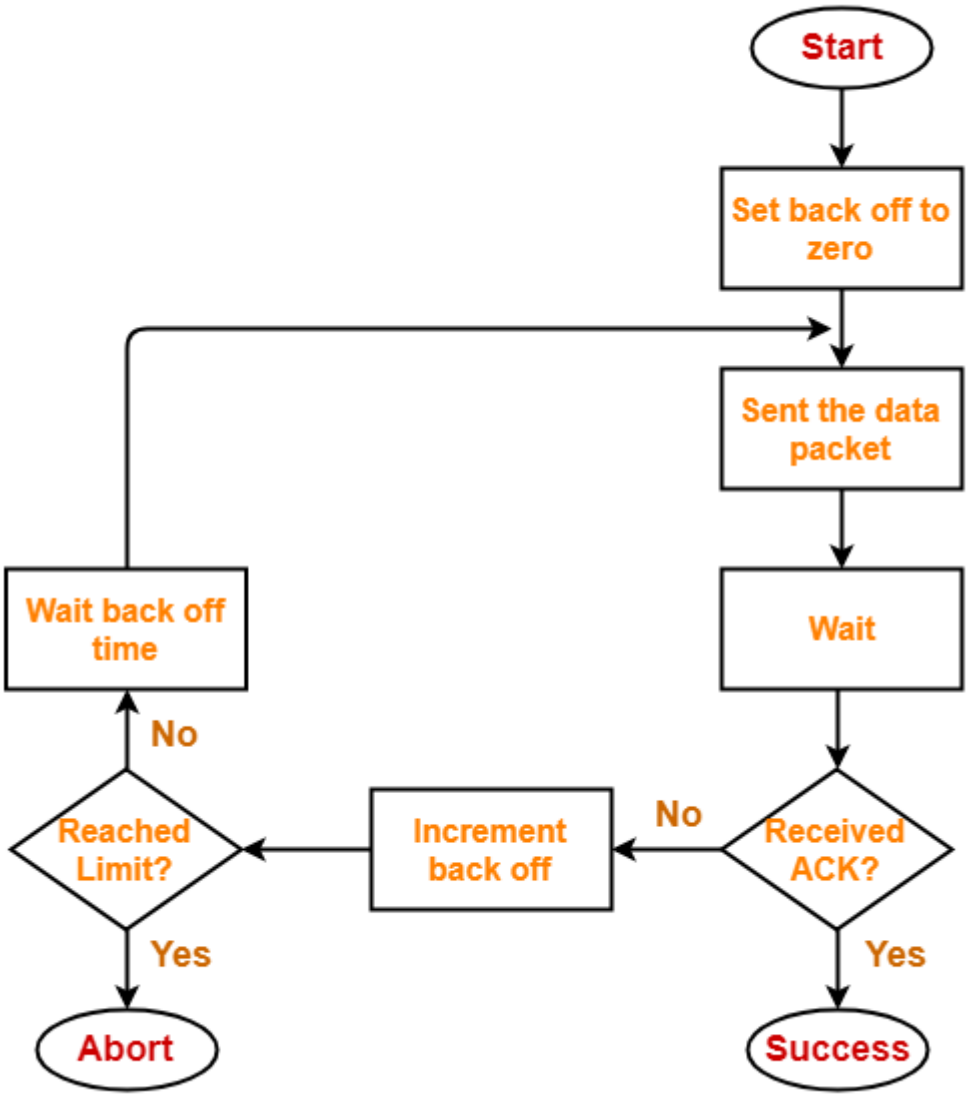

Figure 1: Flow Chart Pure Aloha

Pure ALOHA protocol frames are often sent at any time, so the probability of collision will be very high. Therefore, to avoid frame collisions, no other structures should be sent within your TRM. We will explain this with the help of the brittle period concept, as shown in the figure. Let a frame be transmitted at time t0 and t is the time necessary for its transmission. If another station sends a frame between t0 and t0 + t, then the top of the structure will reach the frame forwarded earlier.

In the same way, if another station resends a frame between the interval t0 + t and t0 + 2t, it will end as a garbage frame due to a collision with the coordinate system. Therefore, 2t is the vulnerable interval of the frame. In case the frame encounters a

crash, the frame will be retransmitted after a random delay. Therefore, for the probability of successful transmission, no additional frames should be transmitted within the vulnerable interval of 2t.

Slotted Aloha

ALOHA can be a multiple access protocol used to transfer knowledge over shared network channels. It operates within the media access control sublayer (MAC sublayer) of the Open Systems Interconnection (OSI) model. With this protocol, multiple data from multiple nodes circulates in various channels for transmission. Each node or station sends a frame without trying to detect whether the channel is idle or busy. On an empty channel, the structure will be transmitted successfully. If two frame plans occupy the track simultaneously, frame collisions will occur so that these frames will be discarded. These stations may prefer to retransmit the damaged frame until the transmission is successful repeatedly.

In the ALOHA system, the node will send it as long as there is data to send. If transmission by another node takes place at the same time, a collision will occur, and the transmitted frame will be lost. However, the node can listen to the intermediate transmission, including its communication, and determine if the fabric has been sent. In pure ALOHA, TRM is continuous. As long as the site has a frame available, it will ship the frame. If there is a collision, the structure is destroyed; as a result, the sender will randomly wait for a while before retransmitting. The slot ALOHA reduces the number of crashes and doubles the capacity of pure ALOHA. The shared channel is divided into various discrete time slots called time slots. A station can only transmit at the beginning of each time slot. However, there may still be conflicts if a station tries to convey at the beginning of the equivalent time slot.

- Slotted Aloha divides the shared channel time into discrete time slots.
- Any station can transmit its data in any time slot.
- The only condition is that the station must start its transmission from the beginning of the time slot.
- If the beginning of the time slot is lost, the station must wait until the beginning of the next time slot.
- A collision will occur if two or more stations try to transmit data at the beginning of the equivalent time slot.

Pure Aloha	Slotted Aloha
In Pure Aloha, any station can transmit data at any time.	In Slotted Aloha, any station can only transmit data at the beginning of any time slot.
In Pure Aloha, time is continuous, not globally synchronized.	In Slotted Aloha, time is discrete and globally synchronized.
Time vulnerable = 2 x Tt.	Time vulnerable = Tt.
Probability of successful transmission of the knowledge package = G x e2G	Probability of successful transmission of the knowledge package = G x eG
Maximum efficiency = 18.4%.	Maximum yield = 36.8%.
Reduce the number of collisions.	Slotted Aloha cuts the number of collisions in half, doubling the efficiency.

Table 1: Pure VS Slotted Aloha

CSMA/CD

Overview

Carrier-sense multiple access with collision detection (CSMA/CD) is a media access control (MAC) method used most notably in early Ethernet technology for local area networking. The concept of Ethernet is that all networked devices should be able to transmit on the network at any time. This school of thought directly opposes technologies such as the token ring, which boasts a deterministic approach to media access. Specifically, token ring networks pass tokens around the web round-robin fashion, from one networked device to the next. Only a network device with the ticket is eligible to broadcast on the network.

In the topology shown in the figure below, all devices are directly connected to the network and can transmit freely at any time if they need a reason to believe that there is no other transmission on the cable currently. Ethernet only allows one frame to enter a network segment at any time. Therefore, before a tool on this network transmits, it will listen to the line to determine if traffic is currently sharing. If no traffic is detected, it sends data. But what if two devices have data to transmit at the same time? If they listen to the line simultaneously, they may mistakenly conclude that it is safe to send data at the same time. However, when two devices send their data at the same time, conflicts occur. As shown in Figure 1, disputes can cause data corruption.

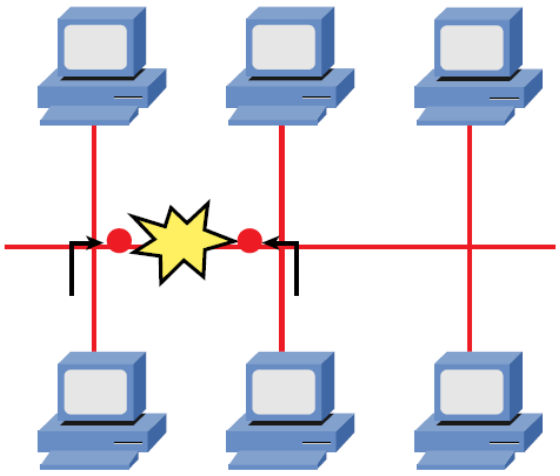

Figure 1: Collision

Collision

A network conflict occurs when something happens to the information sent from the physical network medium to prevent it from reaching its destination. It encounters another signal from one of the other hosts on the network. When these signals are combined, it will generate a useless signal on the network. A conflict occurs when the sending device does not receive a copy of the transparent response within the allotted time. This caused problems for both network devices, as they both had to wait longer and longer until they were ready to transmit information. If the network is busy enough, the network equipment may spend too much time relaying data.

Conflicts can only occur at the physical layer within the OSI model. When multiple devices share traditional media at the physical layer, this happens once you connect various devices to the hub, and you may conflict. The areas in the network where conflicts may occur are called conflict domains. So, what are the benefits of the change? The switch acts as a kind of multi-port bridge, and yes, it joins two conflict domains. What about the introduction of the bridge? The bridge divides the network into two or more parts, and each bit is a separate collision domain. Fewer network devices in the collision domain will reduce the chance of a collision, a bit like fewer cars on the road will reduce the likelihood of an accident.

Process

The CSMA / CD process is divided into several steps. The procedure is based on traditional group dialogue: permanent communication. Not all participants must speak directly, which can generate confusion. Instead, they should speak one after the other so that each participant can fully understand the contribution of the others to the discussion. Without realizing this, our conversation behavior is like this: when others speak, we step back and listen. After the other participants have completed their contributions, for the moment, we wait a short period and only start the conversation when the equivalent participant or other participants in the discussion have not begun to mention anything. If we start lecturing others simultaneously, we will stop our attempts, wait a while, and try again.

The CSMA / CD process is very similar. First, the station monitors the transmission medium. As long as you are frequently busy, the tracking will continue. The station will send the knowledge packet only when the media is free and at a particular time (at intervals between frames). At the same time, the transmitter continues to observe the transmission medium to determine if it detects any data conflicts. If no other participants try to send their data through the medium at the top of the flow and no matches occur, the flow is successful.

Collision Avoidance

Some of the most commonly used methods of collision avoidance:

- Carrier detection schemes
- Pre-programmed Time Slot
- Random Access Time
- Exponential Fallback After Collision Detection

Collision Avoidance in the Network It mainly occurs in networks with multiple access carriers Detection in the network (CSMA). The following principle usually supports this: A node willing to transmit data needs to monitor the channel for a while to determine whether other nodes are also sending on the wireless channel. The node can initiate the transmission; otherwise, the information will be postponed. Collision avoidance improves CSMA performance by preventing multiple nodes from transmitting at the same time. Reduce the probability of collisions by using randomly truncated binary exponential fallback times. Conflict avoidance splits the wireless channel equally among the transmitting nodes in the conflict domain. It is complemented by the exchange of requests to send data packets. The sender and receiver nodes will be warned not to transmit during the mainstream.

A popular circumvention scheme is characterized by a four-way handshake initiated by the sender. The transmission of the knowledge packet and the reception confirmation are sent before the invitation and authorization. Nodes listening to these packets postpone access to the channel to avoid collisions.

Interview Questions

MAC Sublayer

Q1. What happens in Pure Aloha if Collison occurs? **(Tech Mahindra)**
Answer: In pure ALOHA, the TRM is continuous. As long as a station features a frame available, it'll ship the frame. If a collision occurs and therefore the frame becomes corrupted; as a result, the sender waits its random time before retransmitting.

Q2. Which has the most negligible amount probability for collisions Pure aloha or slotted? **(Redington India)**
Answer: Pure aloha can reduce collisions by waiting random time before retransmitting; this indeed refuses collisions. On the other hand, Slotted Aloha cuts the number of collisions in half, doubling efficiency using discrete time slots.

Q3. What's a collision domain? **(Mindtree)**
Answer: The collision domain is the part of the network where packet collisions may occur. When two devices send data packets on the shared network segment at the same time, conflicts arise. Data packet conflicts, both devices must send data packets again, thereby reducing network efficiency. Conflicts often occur in a hub environment because every port on the hub is in the same collision domain. However, each port is located on a bridge, switch, or router in a separate conflict domain.

Q4. When do collisions happen on a network? **(L&T Infotech)**
Answer: A network collision occurs when two or more devices plan to transmit data over a network at an equivalent time. For instance, if two computers on an Ethernet network send data at an identical moment, the info will "collide" and not finish transmitting. This is often why most networking protocols confirm that packets are received before sending additional data.

Q5. The way to avoid collisions during a network? **(Infosys)**

Answer: A collision can only occur at the physical layer within the OSI model. When multiple devices share traditional media at the physical layer, which happens once you have multiple devices connected with a hub, there's an opportunity that you will have a collision. The switch acts sort of a multiport bridge that, yes, bridges two collision domains. What happens with the introduction of the bridge? The bridge breaks the network into two or more pieces, with each bit being a separate collision domain. Fewer network devices during a collision reduce the prospect of a collision, a bit like fewer cars on the street minimize the possibility of an accident.

Network Layer Protocols

Overview

Internet Control Message Protocol can be a network layer protocol used by network devices to diagnose network communication problems. ICMP is used primarily to determine whether data arrives at its intended destination in time. The ICMP protocol is generally used in network devices such as routers. ICMP is essential for error testing and reporting, but it can also be used for distributed denial of service (DDoS) attacks. It is a protocol by which devices in the network often communicate with data transmission problems. In this definition of ICMP, the first method used by ICMP is to determine whether the data arrives at the destination at the correct time. This makes ICMP an essential aspect of the error reporting process and testing to assess data transmission status over the network. However, it can also run distributed denial of service (DDoS) attacks. The way ICMP works in network communication is similar to communication between a carpenter who builds a house and a home improvement store. Assuming that all the components arrive in the correct order, the store will deliver utility poles, floors, roofing materials, insulation materials, etc.

ARP

Address Resolution Protocol (ARP) can be a protocol or program that connects changing Internet Protocol (IP) addresses to hard and fast physical machine addresses, also known as media access control addresses (MAC). The IP and MAC addresses have different lengths and need to be converted so that the system can recognize each other. The most widely used IP today is IP version 4 (IPv4). The length of the IP address is 32 bits. However, the size of the MAC address is 48 bits. ARP converts the address from 32 bits to 48 bits and vice versa. There is a network model called the Open Systems Interconnection (OSI) model. The OSI model was first developed in the late 1970s, and the usage layer provides the IT team with a visualization of what is happening in a particular network system. This will help determine which layer affects the applications, devices, or software installed on the network and which IT or engineering professional is responsible for managing that layer. The MAC address is also called the information link layer, which establishes and terminates a connection between two physically

connected devices for data transmission. The IP address is further mentioned because the network layer is responsible for forwarding knowledge packets through different routers. ARP works between these layers. Devices that are in a local area network (LAN) are programmed to communicate using link-layer addresses. The switch is not configured for a specific IP, allowing the destination to decide to match the IP within the equivalent broadcast domain. Tools that are not connected to the network will not have an IP address. In this case, the network must resort to the use of MAC addresses for communication. If a tool wants to talk to another device on the same LAN, it must know the MAC address of the other device's NIC. This allows communication between 2 end devices to be unicast.

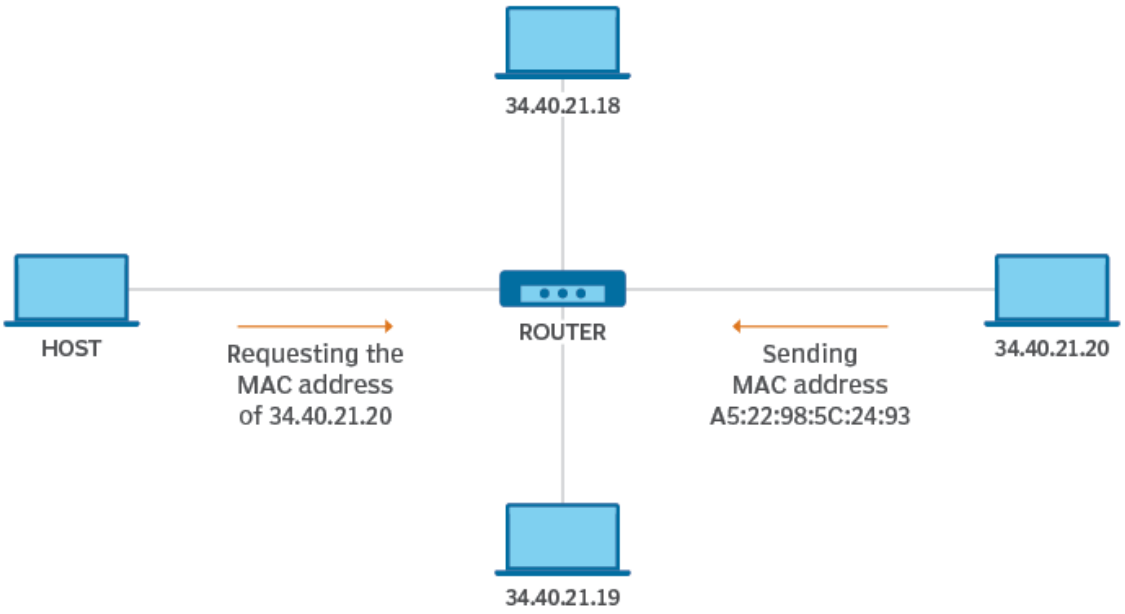

Figure 1: ARP

RARP

RARP is used on older diskless workstations. These old hosts do not have disks and, therefore, cannot store IP addresses. They have a hard-coded MAC address. When the workstation starts, it transmits RARP requests using its MAC address. In the host equivalent network, we have a RARP server that logs RARP requests. The server has a table that contains a combination of MAC and IP addresses. When it receives a RARP request, it checks its table to find the IP address that matches the MAC address in the RARP request packet. Then, the RARP server responds to the host with a RARP reply. When the host receives the RARP response, it knows its IP address.

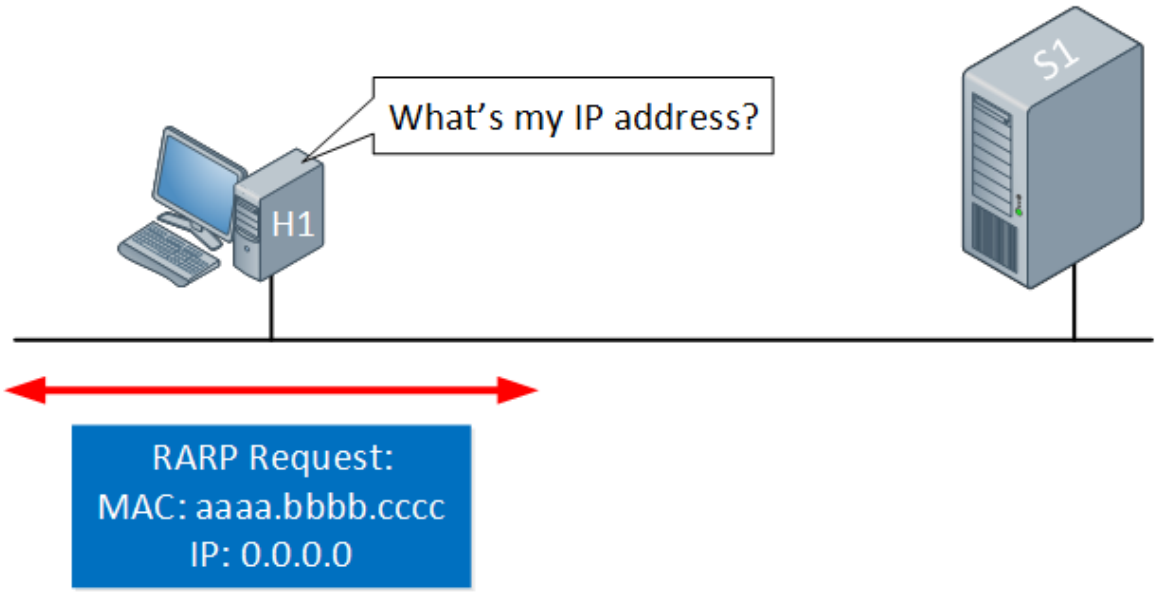

Figure 2: RARP

BOOTP

Bootstrap Protocol (BOOTP) provides a dynamic method of associating workstations with servers. It also provides a process for assigning workstation Internet Protocol (IP) addresses and initial program load (IPL) sources. BOOTP can be TCP/IP protocol. It allows the client to look up its IP address and thus the uploaded file's name from the webserver. The customer uses BOOTP to find this information without the customer's user intervention. The BOOTP server listens on the well-known port 67 of the BOOTP server, also used by the Dynamic Host Configuration Protocol (DHCP). Therefore, BOOTP and DHCP cannot run simultaneously on equivalent systems. (DHCP is the preferred method to support BOOTP clients.) When the server receives a request from the client, it sets an IP address for the client and returns a response to it. This response contains the IP address of the client and thus the name of the uploaded file. The client then initiates a Trivial File Transfer Protocol (TFTP) request to the server to get the uploaded file. The

The bootstrap protocol is used during the startup process to determine the network connection during the initial startup of the computer. Initially, the protocol used a floppy disk, but it was quickly integrated into the motherboard's hardware and network adapter, so no drivers were required.

BOOTP can be a broadcast protocol because it must send dubbing messages to all available hosts on the network to request responses or resources. BOOTP is used during the boot process when the PC is initially started, hence the name. BOOTP initially

required the use of a floppy disk to determine the initial network connection. Still, this method was quickly integrated into the BIOS of the network interface card and motherboard to allow direct network boot.

BOOTP is designed for diskless systems because they need a protocol to communicate with the server to obtain the network address and information about which operating system to use. The computer then downloads the operating system through a standard file transfer protocol.

DHCP

Dynamic Host Configuration Protocol (DHCP) can be a network management protocol that does not automatically configure devices on the IP network, allowing them to use network services such as DNS, NTP, and any communication protocol that support UDP or TCP. The DHCP server dynamically assigns IP addresses and other network configuration parameters to each device on the network to communicate with other networks. DHCP is an improvement on the old protocol called BOOTP. The first reason for the need for DHCP is to simplify the management of IP addresses on the network. No two hosts can have the same IP address. If you configure them manually, errors are likely to occur. Manual IP address assignment is often confusing in small networks, especially for mobile devices that do not permanently require IP addresses. In addition, most users are not technically capable of locating and assigning IP address information on the computer. Automating this process makes the lives of users and network administrators easier. The following are the components of DHCP:

- **DHCP Server** A network device runs the DCHP service, containing the IP address and related configuration information. This is usually the most typical server or router, but it could also be anything that acts like a number, such as an SDWAN device.
- **DHCP Client** - An endpoint that receives configuration information from a DHCP server. This will be a computer, mobile device, IoT endpoint, or any device that needs to be connected to the network. Most configurations receive DHCP information by default.
- **IP Address Pool** - The range of addresses available to DHCP clients. The addresses are generally distributed from smallest to largest.
- **Subnet:** An IP network is generally divided into segments called subnets. Subnets help maintain the manageability of the network.
- **Lease:** The length of time that the DHCP client retains the IP address information. When the lease expires, the customer must renew it.

- **DHCP Relay:** The router or host listens for messages from the client broadcast on its network and then forwards them to the configured server. The server then sends the responses to the relay agent, passing them on to the client. This will not centralize the DHCP servers instead of having one server on each subnet.

Routing Algorithms

Overview

The routing algorithm can establish a route or path to transmit data packets from source to destination. They help to direct Internet traffic effectively. Once the knowledge pack leaves its source, you can choose between different routes to succeed at its destination. The routing algorithm calculates the simplest route mathematically, the "lowest cost route" that data packets often pass through.

- To transmit data from source to destination, the network layer must determine the simplest route through which data packets are often transmitted.
- Regardless of whether the network layer provides datagram services or virtual circuit services, most of the work of the network layer is to provide the simplest route. The routing protocol provides this job.
- The routing protocol can be a routing algorithm that provides the simplest route from source to destination. The simplest route is the "lowest cost route" from the start point to the endpoint.
- Routing is the process of forwarding data packets from source to destination, but the routing algorithm determines the simplest route for sending data packets.

These routing algorithms are designed for SAF networks that use central queues. Avoid deadlocks by dividing the buffer into multiple classes and restricting the movement of packets from one buffer to another so that the buffer classes do not decrease. These algorithms are called jump algorithms. The single-hop algorithm first injects the data packet into the current node's zero complexity buffer. Whenever a data packet is stored in a complexity buffer, I reach a different node through a hop; it will be moved to a complexity buffer I + 1. This routing algorithm is understood as a positive hop algorithm. Every time a data packet requests a replacement buffer, deadlock can be avoided by using the best buffer.

Flooding

Flooding can be a non-adaptive routing technology that follows this simple method. When a knowledge packet arrives at the router, it is sent to all outgoing links except the one it reaches. When source data packets (without routing data) are transmitted to any

connected network nodes, flooding similar to broadcast occurs. Since flood uses all routers in the network, it also uses the shortest route. The flooding algorithm is easy to implement. The network routing data is not initially included in the data packet. The hop count algorithm is used to track the visited network route or topology. The data packet tries to access all available network paths and finally reaches its destination, but there is always the possibility of the data packet being copied. Hop count and some selective flooding techniques are used to avoid communication delay and duplication. Flood is further used as a denial of service attack, interrupting network services by flooding network traffic. The service is flooded with many incomplete server connection requests. Due to the flood of requests, the server or host is not ready to handle real requests simultaneously. The flood attack fills up the memory buffer on the server or host; once it is full, no more connections can be established, resulting in a denial of service. The different types of floods are:

- In controlled floods, two algorithms are used to ensure that floods are frequently controlled. These algorithms are reverse path forwarding and sequence number control flooding.
- There is no conditional logic to regulate how a node distributes information packets to its counterparts in an uncontrolled flood. Without these restrictions, equivalent packages may be distributed repeatedly. These are called broadcast storms or ping storms.
- In selective flooding, a node is configured only to send incoming packets to routers in one direction. This will help prevent many accidents from uncontrolled floods, but it is not as complicated as controlled floods.

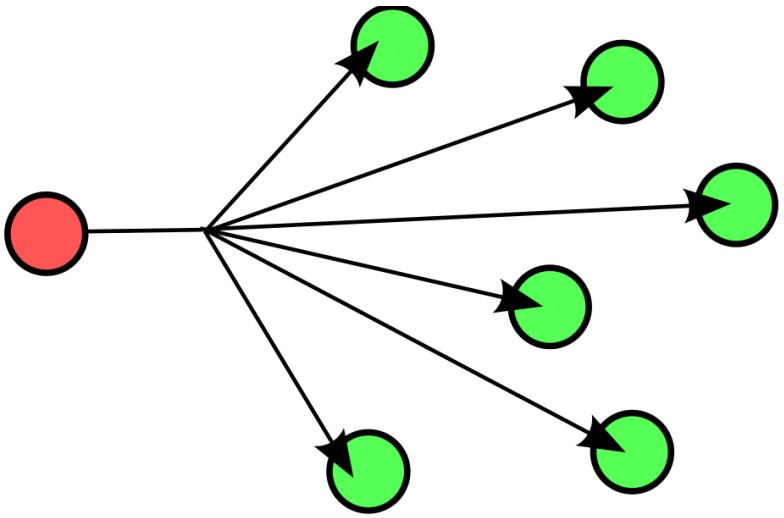

Figure 1: Flooding

Distance Vector

Distance vector routing protocols fall into two categories: distance vector or link state. Here, we examine the distance vector routing protocol; the next section introduces the link-state routing protocol. The distance vector algorithm was developed by R. E. Bellman, L. R. Ford, and D. R. Fulkerson are sometimes referred to as the BellmanFord or FordFulkerson algorithms. The name distance vector is derived from the fact that the route is advertised as a vector of (distance, direction), where the metric defines the distance, and the next-hop router defines the direction. For example, "Destination A can be within five hops, within the address of router X in the next-hop." As the statement implies, each router learns routes from the perspective of its neighbors and then advertises routes from its perspective. Because each router relies on its neighbors to obtain information, and this information may be learned from neighbors, etc., distance vector routing is often jokingly called "rumor routing." Distance vector routing protocols include:

- IP Routing Information Protocol (RIP)
- XNS RIP of Xerox Network System
- Novell IPX RIP
- Cisco Internet Gateway Routing Protocol (IGRP)
- DEC DNA Phase IV
- Routing Table Maintenance Protocol (RTMP)

The routing protocol is an efficient distributed database system. They spread information about the network topology between the routers on the network. Each router on the web uses this distributed database to formulate the most straightforward acyclic route through the network to succeed at any given destination. There are two basic methods for disseminating information over the web:

- By distributing the vector, each router on the network advertises the destinations it can reach, and specific information is used to determine the easiest route to each accessible destination. The router can determine the simplest vector (path) by checking the goals that can be reached through each neighboring or neighboring router and combining some additional information (as a measure of the convenience of the route). There are two vector-based protocols: distance vector and path vector.
- Distributes the connected link status to routers; each router floods (or to everyone in the network or any other router, whether directly adjacent or not) the quality of each link it connects. This information is used independently by each router in the routing domain to create a tree representing the network

topology (called the shortest-path tree). The routing protocol that distributes the link state of the connection is called the link-state algorithm.

Link State

The link-state router is updated from all routers in the entire network, passing information to the nearest router. The link-state protocol router does not continuously broadcast its routing table like the distance vector protocol but only informs neighboring routers when a change is detected. Distance vector routing protocols are considered easy to learn, while link-state routing protocols are known for being very complex and even daunting. However, link-state routing protocols and ideas are not difficult to learn. In some respects, the link-state process is easier to understand than the distance vector concept. Updating the processing system seems to be the key to the robustness of the link-state protocol. Although there are some differences between these two protocols, in general, the link-state protocol differs from the distance vector protocol in the following ways:

- Infrequent routing updates.
- High scalability supports more extensive networks.
- Divides the entire network into smaller segments to limit the scope of routing changes.
- Only updates about link status and topology changes are sent.
- The triggered update can immediately notify the system of differences, reducing convergence time.
- The network design may reduce the size of the link-state database. When the network ID is set by doubling the support path summary, the reduction in the number of paths will reduce the dimensionality of the link-state database.
- The knowledge age is limited because LSA aging always keeps the information up to date.
- The routing loop is almost eliminated because the router knows what the entire topology is like.
- Must support the routing table, the link-state database, and the adjacency database (which can be a table that lists adjacent devices), which requires a lot of memory.
- Running Dijkstra's algorithm (the mathematical formula usually calculates the shortest path) requires CPU cycles on the router. For more extensive networks, this requirement means more CPU time is spent on calculations.
- In large network deployments, the link-state protocol may require extensive adjustments to function correctly. This demand will pose a significant challenge for network administrators.

Path Vector

The Route Vector Protocol does not believe in the value of reaching a particular destination to calculate whether each available route is acyclic. In contrast, the path-vector protocol believes that path analysis will succeed at the goal of determining if it is acyclic. This protocol is a distance-vector protocol; it does not believe in space to ensure an acyclic path but is based on the analysis of the course itself. It is typically implemented in environments where it is difficult to guarantee a uniform metric (distance) between routing domains. The route is accumulated on each router and included in each advertisement so that any router that receives it can verify the acyclic course before spreading the knowledge. BGP4 is the best example of PR using this technology. The most significant disadvantage is the size of the ad, which grows with the number of jumps. As far as IPv6 is concerned, BGP4 enhanced through multi-protocol extension is still the preferred routing vector RP for exchanging IPv6 routes between autonomous systems.

Path Vector (PV) protocols, such as BGP, are used in all domains called autonomous systems. During the path vector protocol, routers not only receive space vectors for specific destinations from their neighbors; on the contrary, nodes also receive space as routing information (also known as BGP routing attributes), which can be calculated by nodes (through the BGP routing process) How the traffic is routed to the destination.

Interview Questions

Network Layer

Q1. How is RARP different from ARP protocol? **(Larsen & Toubro Infotech)**
Answer: ARP identifies the physical address associated with a given network address. Generally, ARP is a mapping process from the network layer to the data link layer to determine the MAC address of a specific Internet protocol address. In RARP, reverse ARP is the network protocol address used by the client computer on the LAN to request the Internet protocol. (IPv4) ARP table from the gateway router. The network router creates a table in the gateway router and assigns the MAC address to the corresponding IP address through the table.

Q2. What is the difference between Bootp and DHCP? **(Mphasis Ltd)**
Answer: BOOTP and DHCP protocols are used to obtain the host's IP address and boot program information. The two protocols work differently in some ways. The DHCP protocol is an extended version of the BOOTP protocol. The main difference between BOOTP and DHCP is that BOOTP supports static configuration of IP addresses, while DHCP supports dynamic configuration. This means that DHCP will automatically assign and obtain IP addresses from computers connected to the Internet and provide some additional functions.

Q3. What is Flooding? **(Hexaware Technologies)**
Answer: When a router uses a non-adaptive routing algorithm to send an incoming data packet to any outgoing link except the node where the data packet arrives, flooding occurs in the computer network. Flooding is a method of quickly distributing routing protocol updates to every node on a large network. Examples of these protocols include open shortest path first and distance vector multicast routing protocols.

Q4. Categorize distance vector routing protocols? **(Wipro)**

Answer: Distance vector routing protocols fall into two categories: distance vector or link state. In the distance vector, each router on the network advertises the destinations it can reach, and specific information is used to determine the easiest route to each accessible destination. In link-state router is updated from all routers in the entire network, passing information to the nearest router.

Q5. How link state is different from distance vector protocol? **(Mphais)**

Answer:

- Infrequent routing updates.
- High scalability supports more extensive networks.
- Divides the entire network into smaller segments to limit the scope of routing changes.
- Only updates about link status and topology changes are sent.
- The triggered update can immediately notify the system of differences, reducing convergence time.
- The network design may reduce the size of the link-state database. When the network ID is set by doubling the support path summary, the reduction in the number of paths will reduce the dimensionality of the link-state database.

IP Header

A router or computer cannot determine the size of a packet without additional information. Individuals can tick a letter or box and tell how big it is, but the router cannot. Therefore, the IP layer needs other information in addition to the source and destination IP addresses. It is a logical representation of knowledge that is used at the IP layer to achieve the delivery of data. This information is a header and is similar to the addressing information on the envelope. The title contains the knowledge required to route data on the web and has an equivalent format regardless of the type of knowledge sent. This is usually the same as an envelope, and the address format is the same irrespective of the letter. The IPV4 header format is 20 to 60 bytes long. It contains the information necessary for routing and delivery. The IP header can be the prefix of an IP packet that includes information on the IP version, packet length, source and destination IP addresses, etc. It consists of the following fields:

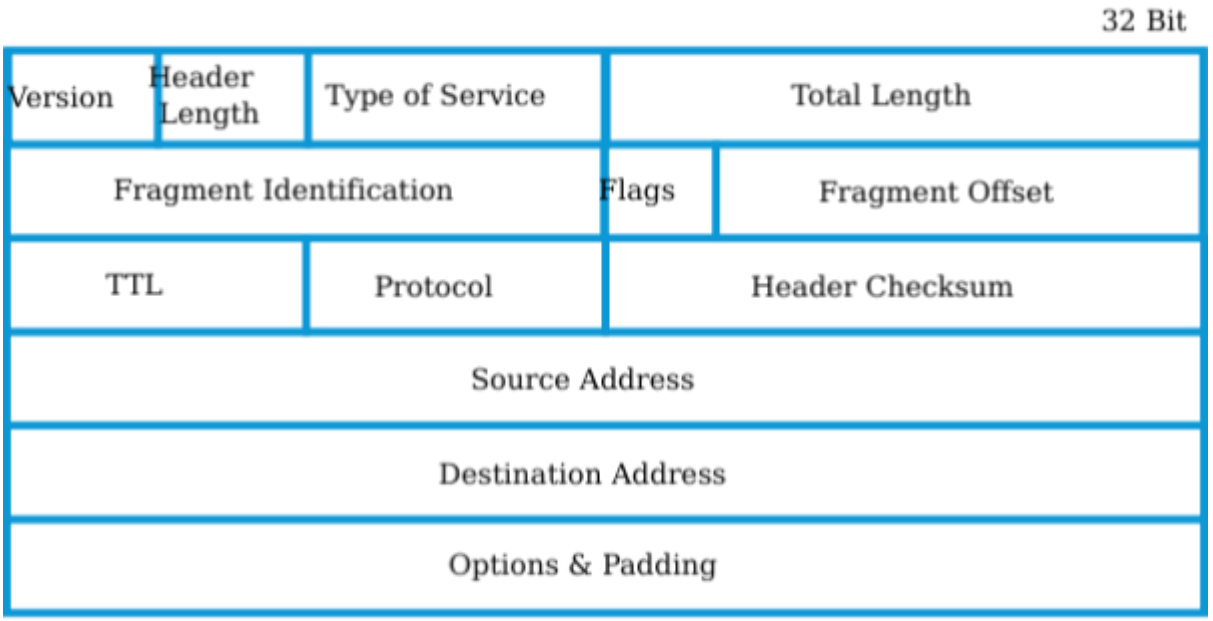

Figure 1: IPv4 Header

- **Version**: The primary field tells us which IP version we are using; only IPv4 uses this header, so you will always find the decimal value 4.
- **Header Length:** These 4th Fields tell us the length of the IP header in 32-bit steps. The size of an IP header is twenty bytes, so in 32-bit steps, you will see the value 5. The maximum value that we create with 4 bits is 15, so with 32-bit increments, this can result in a header- Length of 60 bytes. This field is also known as the length of the web header (IHL).
- **Service Type:** This is typically used for Quality of Service (QoS). We use 8 bits to mark the packet, and we use these bits to provide specific processing for the packet. You will read more about this field in my IP Precedence and DSCP course.
- **Total Length:** This 16-bit field indicates the full size (in bytes) of the IP packet (header and data). The minimum size is twenty bytes (if you have no data), so the maximum length is 65,535 bytes which is the best value you can get with 16 bits.
- **Fragment Identification:** If the IP data packet is segmented, each segmented data packet uses the corresponding 16-bit number to identify which IP data packet in which it belongs to.
- **IP Flags:** These three bits are used for fragmentation:
    - The first bit is usually set to 0.
    - The second bit is called the DF (Don't Fragment) bit, which means the packet should not be fragmented.
    - The third bit is called the MF bit (More Fragment) and is found on roughly all fragmented packets except the last one.
- **Fragment Offset:** These 13 fields indicate the position of the fragment in the original fragmented IP packet.
- **Time to live:** Every time an IP packet passes the router, the measurement time field is reduced by 1. As soon as it reaches 0, the router discards the packet and sends an ICMP timeout message to the sender. The timing field is 8 bits and is used to prevent the box from looping forever (if you have a routing loop).
- **Protocol:** These eight fields tell us which protocol is encapsulated in the IP packet. For example, the value of TCP is 6, and the importance of UDP is 17.
- **Header Checksum:** The checksum of the header is stored in these 16 fields. The recipient can use the checksum to see if the title contains any errors.
- **Source Address:** Here, you will find the 32-bit source IP address.
- **Destination address:** here is the 32-bit destination IP address.
- **Options & Padding:** This field is not commonly used, is optional, and has a variable length to support the options used. Once this field is used, the value in the header length field will increase. A possible option is "source routing," where the sender requests a specific routing path.

IPv6

Overview

IPv6 is the internet protocol (IP) standard of the next generation intended to replace the IPv4, which many internet services are still used today. Every computer, mobile, and other device connected to the Web needs a numeric IP address to talk to other devices. The first IP address scheme, called IPv4, is short of direction. IPv6 is the latest version of the Web protocol, which identifies devices on the WebWeb so that they are often. Each device that uses the Web is placed through your IP address so that the Internet communication is the figure. In a sense, it's a bit like road directions and postcodes you would like to understand to send a letter by post. The previous version, IPv4, uses a 32-bit addressing scheme to admit 4.3 billion devices, which was thought to be enough. However, the expansion of the Web, personal computers, smartphones, and the network of devices of things shows that the planet needed more addresses.

Fortunately, the Web Engineering Working Group (IETF) was recognized 20 years ago. In 1998, created IPv6, which instead uses the 128-bit address to admit about 340 billion (or 2 to power 128, if desired). Instead of the IPv4 address method of 4 sets of Threedigit numbers, IPv6 uses eight groups of 4 hexadecimal, separated by settlers. IPv4 is based on the 32-bit address, limiting it to a complete of 4,300 million directions. IPv6 is based on the 128-bit address and can support the 340 inversions, which are the 340 trillion addresses3. Having more addresses has grown in importance with the expansion of intelligent devices and connectivity. IPv6 provides enough unique IP addresses worldwide for each network currently on Earth, which helps ensure that suppliers can keep up with the expected proliferation of IP-based devices. Furthermore, the approach, the advantages of IPv6 include:

- **More Effective Routing** – IPv6 reduces the dimensions of steering tables and makes the address better and progressive. In IPv6 organizations, a fracture is served by the origin gadget against a switch, which uses a convention to detect the largest transmission unit of the way it is revealed.
- **Additional understanding of the competent packages**: contrasts and, therefore, IPv4 and IPv6 do not contain any reliable control. Accordingly, the control sum must not be recalculated to each rebound of the switch.

- **Corrientes coordinated information**: IPv6 defends multicast against communication. The multicast allows data transfer capacity; package flows increased to different time objections, saving the organization's transmission capacity.
- **Worked at the network layout:** IPv6 gadgets can be obtained freely when referring to other IPv6 devices. Therefore, the installation companies that will be performed incorporate the task of the IP address and the numbering of the gadget.
- **Security**: IPsec security, which provides secret, validation, and honesty of knowledge, is registered in IPv6.

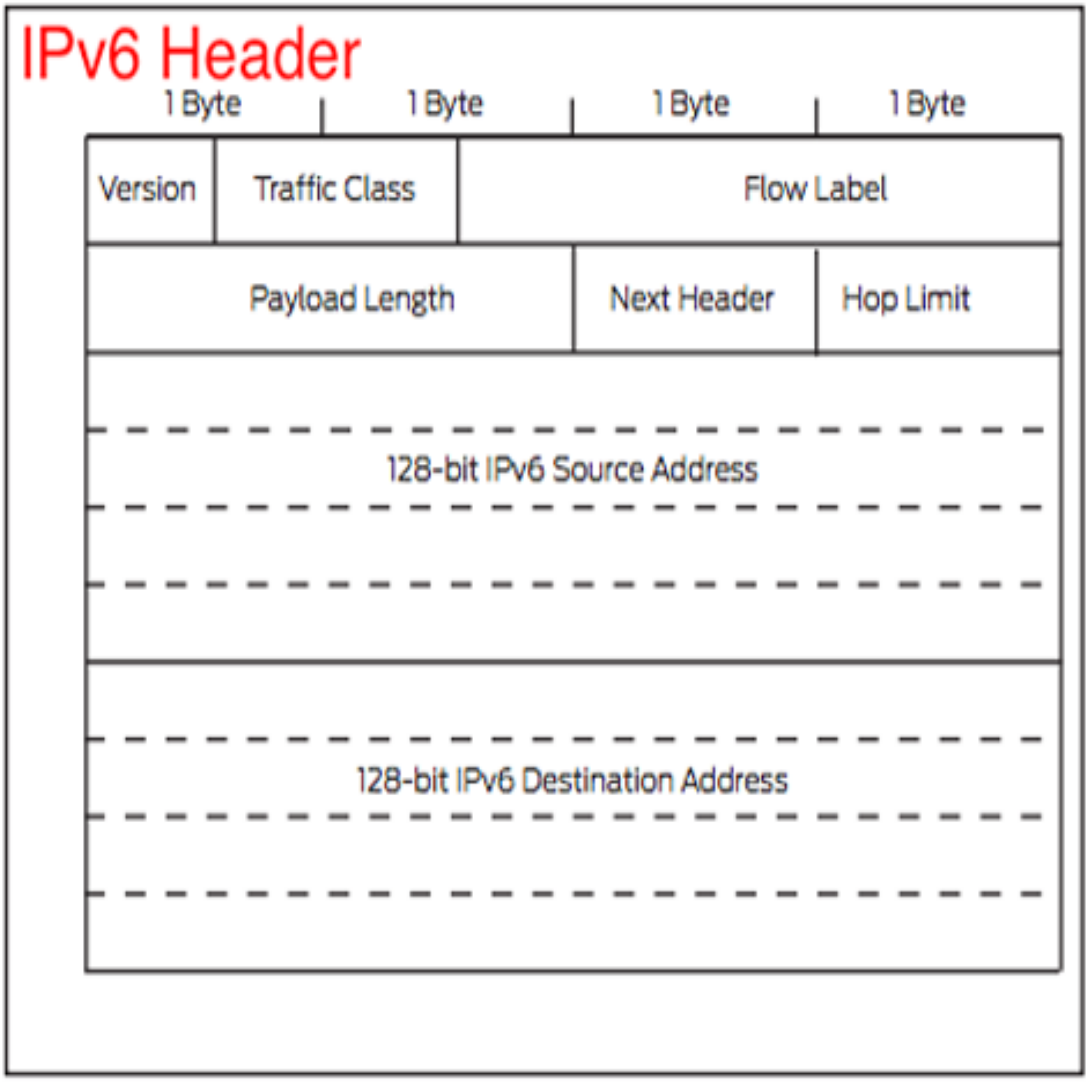

Figure 1: IPv6 Header

IPv6 address formats

The format of the IPv6 address expands the addressing capacity. The IPv6 address size is 128 bits. Even the representation of the IPv6 address is x: x: x: x: x: x: x: x, where each x is that the hexadecimal values of the eight pieces of 16 bits of the address. IPv6 addresses range from 0000:0000:0000:0000:0000:0000:0000:0000 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Furthermore, in this preferred format, IPv6 addresses could be established in two other abbreviated forms:

- **Skip Zeros**

  Specify IPv6 addresses when the initial zeros is omitted. For example, IPv6 1050 address: 0000: 0000: 0000: 005: 0611: 323c: 326b are often written as 1050: 0: 0: 0: 5: 611: 323c: 326b.

- **Double colon**

  Specify the IPv6 addresses using double Pons (: :) in situ of a series of zeros. For example, IPv6 address FF06: 0: 0: 0: 0: 0: 0: C3 are often written as FF06 :: C3. The two colors are often used only on one occasion in an IP address.

Devices

Hub

Network hubs are a Layer 1 device consistent with the Open Systems Interconnection (OSI) reference model. They operate at the physical layer as against a software application. These hubs use by forwarding packets of data to all or any other computers connected to the device. When a packet arrives at one among the ethernet ports, it's then copied to the opposite ports so that all segments of the connection can access the knowledge stored within the packet. These are common connection points for network devices, which connect segments of a LAN (local area network) and should contain multiple ports – an interface for connecting network devices like printers, storage devices, workstations, and servers. A knowledge packet arriving at one Hub's port could also be copied to other ports, allowing all network segments to possess access to the info packet. It Hub may be a networking device that permits you to attach multiple PCs to one network. It's wont to connect segments of a LAN. A hub stores various ports, so it's copied to multiple other ports when a packet arrives at one port. A hub has the following features:

- It works with broadcasting and shared bandwidth.
- It has one broadcast domain and one collision domain
- Works at the physical layer
- A virtual LAN can't be created employing a hub
- Provides support for half-duplex transmission mode
- A hub has just one broadcast domain
- It does not support spanning tree protocol
- Packet collisions occur mainly inside a hub

Figure 1: HUB

Repeaters

The repeater may be a network hardware device that's worked at the physical layer, and it helps to amplify or regenerate the signals before retransmitting them. The repeater is additionally referred to as "Signal Boosters." A repeater can increase the info signal from one network segment then pass it to a different network segment, thus scaling the dimensions of the network. The repeater allows the transfer of the info through an outsized area distance. It can ensure security and quality of knowledge and retransmitting the information with securely preserving the signals. This device has limited use in specific situations. They do not read the info frames in the least. It makes sure that data is repeated out on each port. These are analog devices that employment with signals to which they're connected. A sign appearing on one port is regenerated and placed on another port; this extends the LAN strength. It doesn't understand packets or frames. It only understands the symbol, which converts bits as volts.

- **Restriction for Number of Repeaters:** you've got the only limitation within the number of repeaters used on the distinct network. If you are trying to attach more repeaters to the web, it'll generate the noise on the wire and enhance the probabilities for packet collision.
- **Less Segmentation:** A repeater isn't the ability to segment the network. For example: if you employ two different types of cables, each with segments. So, it's unable to generate separate traffic from one thread to another.
- **Collision Domain:** When all information is moved to varied domains, repeaters aren't ready to separate the connected network devices. Moreover, the repeater cannot spot if it's an associated unit of the same collision domain.
- **Bandwidth Usage:** A wireless repeater can transmit the signals in both directions in between the router and computer. When the computer attaches to the wireless repeater, then bandwidth is effectively halved.
- **Network Architecture:** A repeater cannot attach networks alongside different network architectures. So, to satisfy this purpose, you'll use the gateway or router.

Figure 2: Repeater

Switch

Switches are essential building blocks for any network. They connect multiple devices, like computers, wireless access points, printers, and servers, on an equivalent network within a building. A switch hence, enables connected devices to share information and ask one another. A network switch may be a device that operates at the info Link layer of the OSI model—Layer 2. It takes packets being sent by devices connected to its physical ports and sends them out again, but only through the ports that cause the devices the packets are intended to succeed in . they will also operate at the network layer--Layer 3, where routing occurs. Switches are a standard component of networks supported by ethernet, Fibre Channel, Asynchronous Transfer Mode (ATM), and InfiniBand. Generally, though, most switches today use ethernet. Once a tool is connected to a switch, the switch notes its media access control (MAC) address, a code baked into the device's network interface card (NIC) that attaches to a coaxial cable that connects to the switch. The switch uses the MAC address to spot which secured outgoing device packets are sent and where to deliver receiving packets.

The MAC address identifies the physical device against the network layer (Layer 3) IP address, which may be assigned dynamically and change over time. When it sends a packet to a different device, it enters the switch, and therefore the switch reads its header to work out what to do with it. It matches the destination address and sends the packet out through the acceptable ports in the destination devices. To scale back the

prospect for collisions between network traffic getting to and from a switch and a connected device at an equivalent time, most switches offer full-duplex functionality during which packets coming from and getting to a tool have access to the complete bandwidth of the switch connection.

Figure 3: Switch

Switch Features

- **Connect multiple hosts**: Normally, a switch provides excessive ports for cable connections, allowing star routing. It's usually wont to connect multiple PCs to the network.
- **Forwards a message to a selected host**: a bridge, a switch uses an equivalent forwarding or filtering logic on each port. When any host on the network or switch sends a message to a different host on an equivalent network or an equivalent switch, the switch receives and decodes the frames to read the message's physical (MAC) address portion.
- **Manage traffic**: A network switch can manage traffic either coming into or exiting the network and may connect devices like computers and access points with ease.
- **Keep electrical signal undistorted**: When a switch forwards a frame, it regenerates an undistorted square electrical signal.
- **Increase LAN bandwidth**: A switch divides a LAN into multiple collision domains with independent broadband, thus significantly increasing the bandwidth of the LAN.

Router

A router may be a device that connects two or more networks or subnetworks. It does two primary functions: It manages traffic between these networks by forwarding data

packets to their intended IP addresses and allowing multiple devices to use an equivalent Internet connection. There are several routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN may be a group of connected devices restricted to a selected geographical area. A LAN usually requires one router. A WAN, against this, may be an extensive network opened up over a vast geographical area. Large organizations and corporations that operate in multiple locations across the country, as an example, will need separate LANs for every site, which then hooks up with the opposite LANs to make a WAN.

Routers guide and direct network data, using packets that contain various sorts of data—such as files, communications, and straightforward transmissions like web interactions. The info packets have several layers or sections, one among which carries identifying information like sender, data type, size, and most significantly, the destination IP (Internet protocol) address. The router reads this layer, prioritizes the info, and chooses the most straightforward route for every transmission.

- Routers are multi-port devices with high–speed backbones
- It also supports filtering and encapsulation like bridges
- Like bridges, routers also are self-learning, as they will communicate their existence. To other devices and may learn of the presence of the latest routers, nodes, and new LAN endpoints.
- They route the traffic by considering the network as an entire. This characteristic makes them superior to hubs and bridges because they view the network on a link-by-link basis.
- The packet handled by the router may include:
    - A destination address.
    - The priority level of the packet.
    - The least-cost route for the packet.
    - Minimum route delay.
    - Minimum route distance.
    - Route congestion level of the packet.
- Routers constantly monitor the conditions of the whole network as an entire to dynamically adapt to changes within the state of the network.
- They typically provide some level of redundancy so that they're less vulnerable to catastrophic failure.

Figure 4: Router

Gateway

A gateway may be a network node that forms a passage between two networks operating with different transmission protocols. The network gateway's foremost common sort of gateways operates at layer 3. A gateway can work at any of the seven layers of the OSI model. It acts because the entry-exit point for a network since all traffic that flows across the networks should undergo the gateway. Only the interior traffic between the nodes of a LAN doesn't experience the gateway.

- Gateway is found at the exit of a network and manages all data in and out from the network.
- It forms a route between two different networks that want to operate with one other using transmission protocols.
- A gateway also operates as a protocol converter, providing compatibility between the various protocols utilized in the two different networks.
- The feature that differentiates a gateway from other network devices is that it can operate at any OSI model layer.
- It also stores information about the routing paths of the communicating networks.
- A gateway node could also be supplemented as a proxy server or firewall when utilized in an enterprise scenario.
- A gateway is usually implemented as a node with multiple NICs (network interface cards) connected to different networks. However, it also can be configured using the software.
- It uses a packet switching technique to transmit data across the networks.

Figure 5: Gateway

Interview Questions

Network Layer

Q1. What's the maximum size of an IP Header? Also, what is the use of TTL? **(Birlasoft)**
Answer: The IPV4 header format is 20 to 60 bytes long. Time to live is a value for the amount of time a packet of data must be present on a computer or network before being dropped. The meaning of TTL or the duration of the packet depends on the context. It is a value in an IP packet that informs a network router when the packet has been on the network for too long and should be discarded. The time field is 8 bits long and is used to prevent the box from repeating forever (when you have a routing loop).

Q2. How many bits is IPv6? What is the primary advantage of IPv6? **(Adobe Systems)**
Answer: The IPv6 is 128Bits long, whereas IPV4 is 32bits long. IPv6 reduces the dimensions of steering tables and makes the address better and progressive. In IPv6 organizations, a fracture is served by the origin gadget against a switch, which uses a convention to detect the largest transmission unit of the way it is revealed.

Q3. What is the format of IPv6? Give an example? **(Microsoft Corporation)**
Answer: An IPv6 address is represented as eight groups of four hexadecimal digits, and each group represents 16 bits (two octets, a group sometimes called a hextet). An example of an IPv6 address is: 2001: 0db8: 85a3: 0000: 0000: 8a2e: 0370: 7334. The standards offer flexibility in the representation of IPv6 addresses.

Q4. What are Routers? How are they different from Hubs? **(Think Palm Technologies)**
Answer: A Router is a device on the network that is responsible for connecting two or more network segments. It is used to transfer information from source to destination. The routers send the information in the form of data packets. When these data packets

are forwarded from one router to another, it reads the network address on the packets and identifies the destination network. The hub and switch are network-connected devices. The hub works at the physical layer and is responsible for sending the signal to the port to respond to the call, while the switch allows the connection to be configured and terminated as needed.

Q5. Which layer does a Router work on? Define the role of a router in a network? **(Mphais)**

Answer: Routers operate at the third layer of the OSI model, the network control layer. Instead of forwarding packets based on Media Access Control (MAC) layer addresses (as bridges do), a router examines the data structure of the packet. It determines whether or not it should be forwarded. A router stores and forwards data packets, each containing a source and destination network address, from one LAN or WAN to another. Routers are "smarter" than bridges because they find the best path for whatever data is sent to them from the old Router or the end of the LAN.

TCP & UDP

TCP

Transmission Control Protocol (TCP) can be a transmission protocol used in addition to IP to ensure reliable data packets. TCP includes mechanisms that can solve many problems caused by packet-based messaging, such as lost packets, out-of-order packets, duplicate packets, and corrupted packets. Since TCP is the most commonly used protocol besides IP, the Web protocol stack is usually called TCP/IP. It is a typical method; it defines how to establish and maintain a network session, applications can exchange data through it. TCP is used with the Web Protocol (IP), which describes how computers send knowledge packets to each other. Together, TCP and IP are the basic rules that define the Web. TCP organizes data so that it is often transferred between the server and the client. It guarantees the integrity of the information transmitted over the network. Before sending data, TCP establishes a connection between the source and the target and keeps it until the communication starts. Then a large amount of knowledge is broken down into smaller packages while ensuring data integrity throughout the process.

Therefore, all high-level protocols that need to transmit data use the TCP protocol. Examples include peer-to-peer sharing methods such as File Transfer Protocol (FTP), Secure Shell (SSH), and Telnet. It is also common to send and receive e-mail using the Internet Message Access Protocol (IMAP), Post Office Protocol (POP), and Simple Mail Transfer Protocol (SMTP), as well as the Hypertext Transfer Protocol (HTTP) for Web access.

TCP connection

Establishing a connection requires that both the client and the server participate in the so-called three-way handshake. This method is usually weakened as follows:

- The client sends an SYN packet to the server- a connection request from its source port to its destination port.
- The server replies with an SYN/ACK packet to confirm receipt of the connection request.
- The client receives the SYN and ACK packet and replies with its ACK packet.

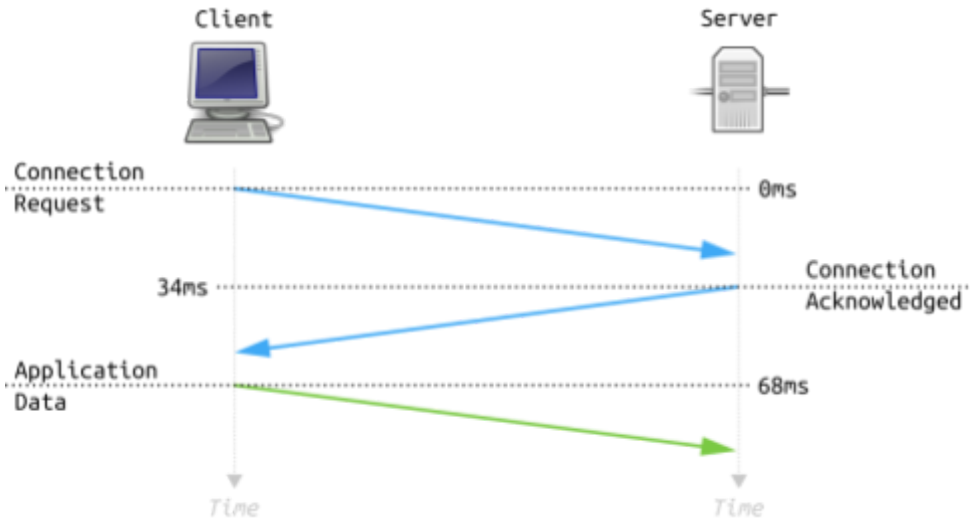

Figure 1: Three-Way Handshake

TCP Header

TCP surrounds each data packet with a header, which contains ten required fields for a total of 20 bytes (or octets). Each title includes information on the connection and the data currently being sent.

- **Source Port** -The port of the sending device.
- **Destination port** - The port of the receiving device.
- **Sequence Number** - The tool that initiates the TCP connection must choose a random initial sequence number, which is then incremented according to the number of bytes transmitted.
- **Confirmation Number** - The receiving device has a zero-based confirmation number. The number is incremented according to the number of bytes received.
- **TCP Data Offset** - This represents the size of the TCP header, expressed in 32-bit words. One word means four bytes.
- **Reserved data** - reserved fields are usually set to zero.
- **Control flags** - TCP uses nine control flags to manage the data flow in certain situations, such as B. When resetting is initiated.
- **TCP checksum window size** - The sender generates a checksum and transmits it in the header of each packet. The receiving device can use the checksum to detect errors in the received header and payload.
- **Urgent pointer** - When the URG control flag is an approximate value, this value indicates the offset of the sequence number indicating the last binding data byte.

- TCP optional data These are optional fields used to set the maximum segment size, selective acknowledgment, and activate window scaling for more efficient use of high-bandwidth networks.

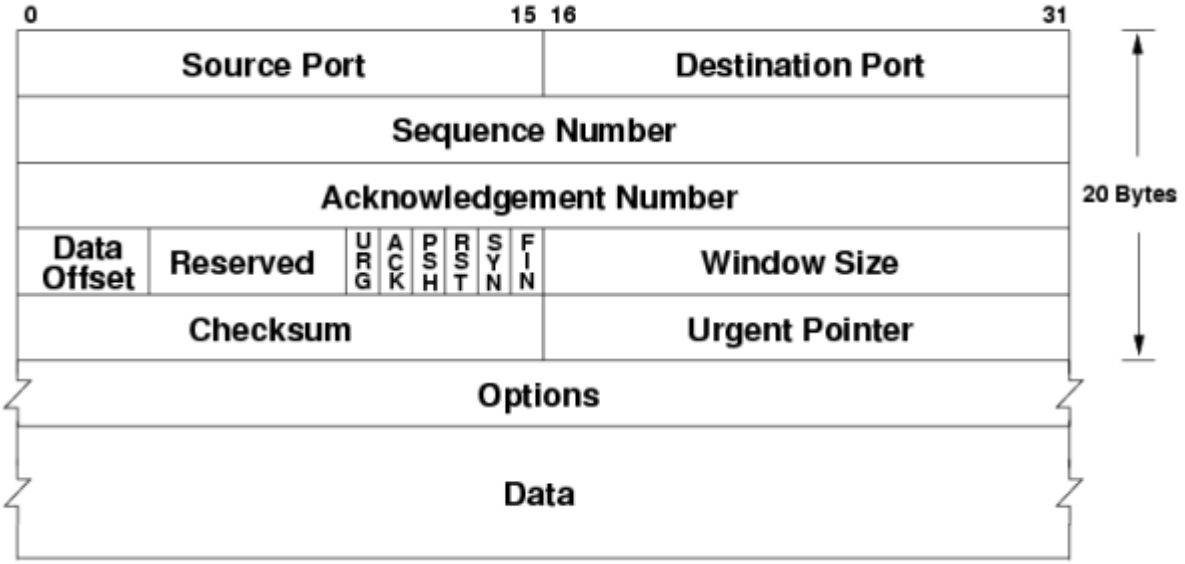

Figure 2: TCP Header

UDP

User Datagram Protocol (UDP) is mainly used to establish low-latency and fault-tolerant connections between applications on the Web. It speeds up the transfer by enabling knowledge transfer before the recipient reaches an agreement. Therefore, UDP is beneficial in time-sensitive communications, including Voice Internet Protocol (VoIP), naming systems DNS; to find and play video or audio. Like all network protocols, UDP can be a standardized method for transferring data between two computers on the network. Compared with other protocols, UDP accomplishes this process in a simple way: it sends data packets (knowledge transfer unit) to the target computer without first establishing a connection, specifying the order of the data packets or checking whether they arrive in this way (UDP packets are called "datagrams.")

UDP is faster than TCP, another popular transport protocol, but has lower reliability. The two computers begin to establish a connection during TCP communication using an automatic process called "handshake." When this handshake is completed, only once does one computer transmit the data packet to another computer.

UDP communication does not go through this process. Instead, one computer can start sending data to another computer:

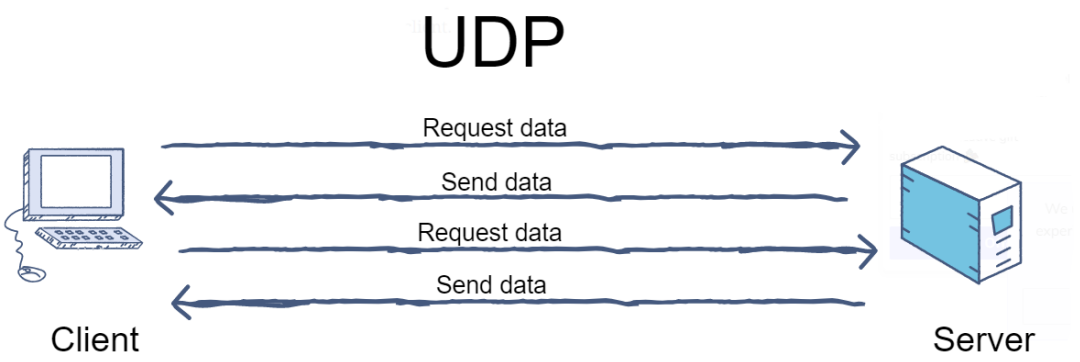

Figure 3: UDP Connection

UDP Header

- **Source port** - It is the port of the device sending the information. When the target computer does not need to reply to the sender, this field is usually set to zero.
- **Destination port** - It is the port of the device that is receiving the message. The UDP port number is usually between 0 and 65,535.
- **Length** - Represents the number of bytes, including the UDP header and UDP payload. The limit of the UDP length field is determined by the underlying IP protocol that does not transmit information.
- **Checksum** - The checksum enables the receiving device to check the integrity of the packet header and user data. It is optional in IPv4 but mandatory in IPv6.

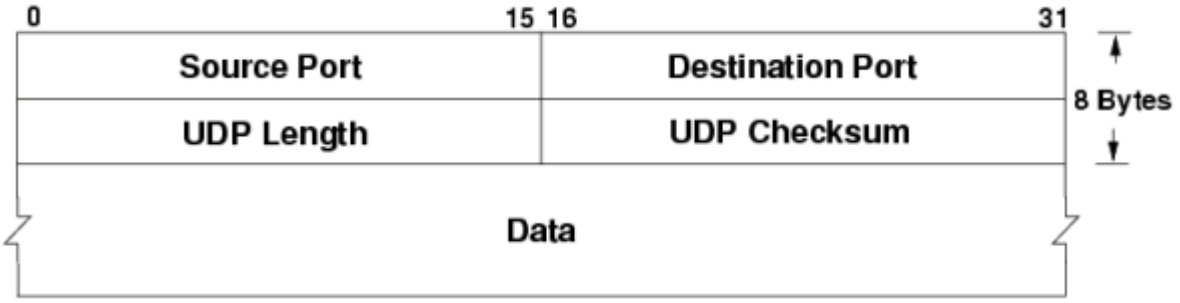

Figure 4: UDP Header

TCP Timers

Overview

The TCP keepalive timeout defines the time interval for the TCP connection to check whether the FCIP connection is working correctly. This ensures that FCIP connection failures are quickly detected, even if the connection is inactive. When the TCP connection is idle for the required time interval, a TCP keepalive packet is sent to verify if the link is active. The MDS switch uses the "TCP keepalive timeout" command to specify the number of keepalive timeout seconds (the range is between 1 and 7200 seconds, and the default value is 60). During the time interval when the connection is inactive within the configured time interval, eight keepalive probes are sent at an interval of 1 second. If no response to these eight probes is received and the connection remains idle, the FCIP connection will be automatically closed. TCP uses multiple timers to ensure that there is no excessive delay in communication. Some of these timers are elegant and can handle problems that were not obvious during the initial analysis. Every timer used by TCP helps to ensure that data is sent correctly from one connection to another.

Timer Types

The four central timers used by TCP implementation are

1. Timeout Timer
2. Time Waiting Timer
3. Keep Alive Timer
4. Persistent Timer

Time Out Timer

TCP uses an outgoing timer to retransmit lost segments.

- The sender starts the out-of-office timer after transmitting the TCP segment to the receiver.
- If the sender receives an acknowledgment before the timer appears, they will stop the timer.

- If the sender does not receive a declaration, the timer bursts, a TCP retransmission occurs.
- The sender resends the equivalent segment and resets the timer.
- The value of the timeout timer is dynamic and will change with the amount of traffic on the network. The timeout timer is also called the retransmission timer.

Time Wait Timer

TCP uses a time wait timer during connection termination.

- The sender starts the time waiting for the timer after sending the ACK of the second FIN segment.
- If the final confirmation is lost, retransmission is allowed.
- It can prevent the port that has just been closed from being opened again quickly by another application.
- It ensures that any segment that flows to the port that was just closed is discarded.
- The value of your time waiting for the timer is usually set to twice the lifetime of the TCP segment.

Keep-Alive-Timer

TCP uses Keep-Alive-Timer to stop TCP connections that have not been used for a long time.

- Each time the server receives a message from the client, it resets the keepalive timer to 2 hours.
- If the server does not receive any message from the client for two hours, it will send ten detection segments to the client.
- These probe segments are sent within 75 seconds.
- If the server does not receive a response after sending 10 test segments, the client has failed.
- The server then automatically terminates the connection.

Persistent Timer

- TCP uses a persistent timer to affect a deadlock of Zerowidowsize.
- Even if the peer closes its receiver window, it still keeps the flow of window size information.

Congestion Policies

Overview

Congestion control and quality of service are the two closely related topics. Improving one means improving.
And ignoring one usually means missing the other. Most technologies used to stop or clear congestion have also enhanced the service standards of the entire network. In these applications, a large amount of knowledge needs to be quickly exchanged over a network of several gigabits per second. For this reason, various types of congestion control used in such broadband networks have been proposed. In this type of congestion control, the idle bandwidth of the network is usually used quickly by increasing the communication speed during communication.
On the other hand, complex types of traffic congestion will occur on the web. Therefore, when these types of congestion control and existing TCP communications coexist, the leading TCP communications will be highly compressed. An essential problem in packet-switched networks is congestion. When the network load-the number of packets sent to the network is greater than the network capacity and the number of packages that the network can handle, network congestion may occur. Congestion control refers to mechanisms and techniques used to regulate congestion and keep the load below capacity. We may wonder why the network is congested. Any system that involves waiting time will have traffic jams. For example, traffic jams occur on highways because any abnormal conditions in the river (such as hourly accidents) will cause blockage. Congestion occurs during the network or internetwork because routers and switches have queue buffers for storing data packets before and after processing. For example, a router has an inbound queue and an outbound queue for each interface.

Congestion factor

- The arrival rate of packets exceeds the capacity of the outbound link.
- There is not enough memory to store the incoming data packet.
- Traffic is heavy.
- The processor is slow.

Slow start Phase

TCP slow start is one of the main steps in the congestion control process. It compares the amount of knowledge that the sender can transmit (the congestion window is known) with the amount of knowledge that the receiver can accept (the receiver's window is known). The lower of the two values is the maximum amount of knowledge that the sender can transmit before receiving an acknowledgment from the receiver.

- The sender tried to talk to the recipient. The sender's initial data packet contains a small congestion window, determining the maximum window to support the sender.
- The recipient confirms the package and responds with his window size. If the receiver does not answer, the sender knows that it can no longer send data.
- After receiving the confirmation, the sender increases the window size of subsequent data packets. The window size gradually increases until the receiver cannot confirm each packet or reaches the sender or receiver window limit.
- After the limit is determined, the slow start task is completed. Other congestion control algorithms will take over the speed of the link.

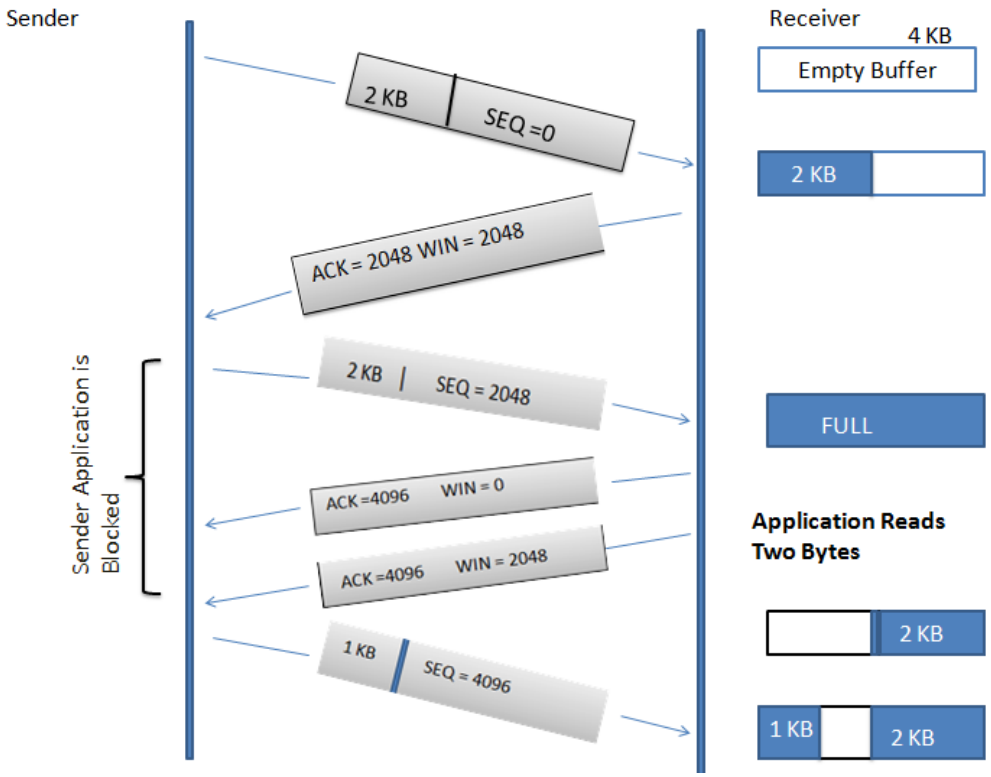

Figure 1: Slow start

Congestion Avoidance Phase

Traditional congestion control schemes help improve performance after congestion occurs. When the load is light, the throughput usually keeps pace with the load. As the load increases, the throughput increases. After the load reaches the network capacity, the throughput will no longer increase. As the load continues to grow, the queue starts to increase, which may cause packets to be dropped. If the load increases more than now, the throughput may drop suddenly, so the network is called congestion. The reaction time initially increases slightly with the load. As the queue is established, the response time increases linearly until the final response time increases sharply because the line restarts due to overflow. The purpose of throughput close to zero is called congestion resolution. This is usually the purpose of the reaction time approaching infinity. The congestion control scheme aims to realize that the network has reached the goal of congestion collapse leading to packet loss and to reduce the load to restore the network to a non-congested state.

Congestion Detection Phase

The transmitter returns to the slow start stage or the traffic jam avoidance stage. When congestion occurs, the size of the congestion window will decrease. The only way the sender can guess that congestion is happening is to retransmit a segment. Retransmission is required to recreate lost packets that are considered discarded by the router due to congestion. Retransmission may occur in two situations: when the RTO timer expires or when three repeated ACKs are received. Before the network can report back information, it must determine its status or load level. In general, the network may also be in one of n possible states. The traffic jam detection function helps assign these states to one of 2 possible load levels: overload or underload (above or below the knee). The Kary version of this function will end with a k-level load indication. For example, the overload detection function can support processor utilization, connection utilization, or queue length.

Application Layer protocols

Overview

The application layer is used by software such as web browsers and email clients. It provides protocols that allow the software to send and receive information and present it in meaningful data to all the users. Examples of application layer protocols are Hypertext Transfer Protocol, File Transfer Protocol, Post Office Protocol, Simple Mail Transfer Protocol, and Domain Naming system. An application layer protocol defines how application processes (clients and servers) running on different end systems transmit messages. In particular, an application layer protocol defines:

- Message types, e.g., ex. B. Request messages and reply to messages.
- The syntax of the different types of messages, i. H. the fields within the message and the kind of delimitation of the areas.
- The semantics of fields, i. H. the importance of the knowledge that the sector must contain;
- The Rules for determining when and how a process sends messages and responds to messages.

HTTP

It is an application protocol for collaborative, distributed hypermedia information systems that enable users to talk about data across the globe. HTTP was invented along with HTML to make the leading interactive text-based web browser - the first World Wide Web. Today, the protocol is one of the first means of using the web. HTTP allows users to interact with web resources, such as HTML files, passing hypertext messages between clients and servers, as a request-response protocol. HTTP clients generally use Transmission Control Protocol (TCP) connections to communicate with servers.

HTTP can be a TCP / IP-based communication protocol that delivers data (HTML files, image files, query results, etc.) over the Planet Wide Web. The standard port is TCP 80, but other ports are often used. It provides computers with a uniform way to communicate with each other. The HTTP specification defines how clients request data and send it to the server and respond to these requests.

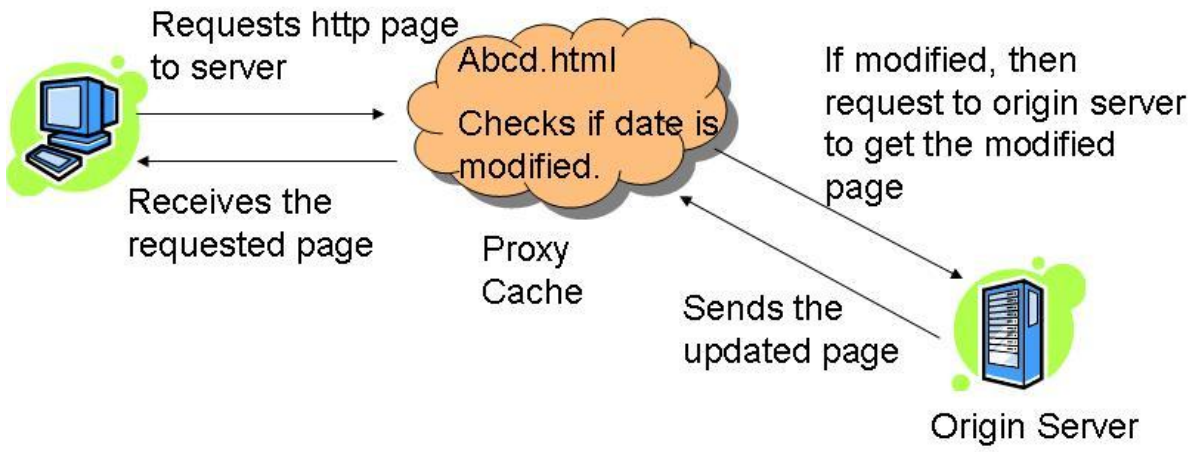

Figure 1: HTTP Request

FTP

File Transfer Protocol (FTP) can be a network protocol used to transfer files between computers using TTCP / IP connections. Within the TCP / IP suite, FTP is considered the application layer protocol. In an FTP transaction, the top user's computer is generally referred to as the localhost. The second computer involved in FTP can be a remote host, which is usually a server. Both computers must be connected to a network and properly configured to transfer files via FTP. Servers must be found to run FTP services, and therefore FTP software must be installed on the client to access these services. Although many file transfers are often done using the Hypertext Transfer Protocol (HTTP), another protocol within the TCP / IP suite, FTP, is still used to transfer files in the background for other applications such as banking services. Sometimes it is also common to download new applications through web browsers.

It is a protocol that usually sends files from computer to computer, and one of them acts as a server as long as the two are connected online. FTP is a network protocol between the client and the server and allows users to download websites, files, and programs from other services. When the user wants to download the knowledge to his computer, he uses FTP. It does not use encryption. It relies on apparent text usernames and passwords for authentication, making data transmissions sent via FTP vulnerable to eavesdropping, spoofing, and other common attacks.

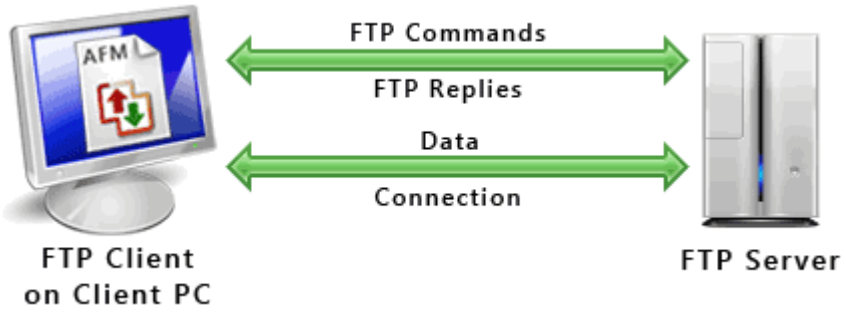

Figure 2: FTP Request

SMTP

It is used to send and receive emails. It is sometimes paired with IMAP or POP3 (for example, via a user-level application) that performs message retrieval, while SMTP primarily sends messages to be forwarded to a server. SMTP can send and receive email, but it is terrible at queuing incoming messages, hence the usual delegation to other protocols. Proprietary systems like Gmail have their email transfer protocols when using their servers, but they still use old SMTP to send emails on top of that. SMTP is an asymmetric protocol, which means that many clients interact with a server, using a base model popular in the 1980s that essentially no longer exists outside of email protocols today. SMTP runs on TCP / IP and listens on port 25. The actual transmission of mail is done through Message Transfer Agents (MTAs). Therefore, the system must have the MTA client send the mail, and the system must have an MTA server to receive the mail.
In principle, the respective mail transmission is done through message transfer agents (MTAs). To send the mail, the system must have the MTA client, and to receive the mail; the system must have an MTA server. To define the MTA client and server on the web, there is a convenient way called Simple Mail Transfer Protocol (SMTP).

- SMTP also uses TCP / IP to send and receive emails.
- SMTP is based on the client/server model.
- The original standard port for SMTP is port 25.
- With this protocol, the client that wants to send the email first opens a TCP connection to the SMTP server and then sends the email through the TCP connection. It is important to note that the SMTP server is usually in listening mode. As soon as it listens for a client's TCP connection, the connection starts on port 25, and after a successful relationship, the client immediately sends the email/message.

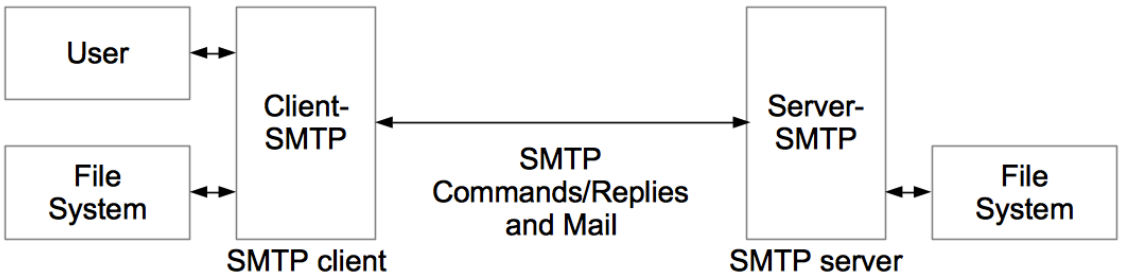

Figure 3: SMTP Request

DNS

The DNS is that the phone book of the web. People access information online using domain names such as nytimes.com or espn.com. Web browsers interact using Internet Protocol (IP) addresses. DNS translates domain names into IP addresses so that browsers can load Internet resources. Each device connected to the Internet has a unique IP address that other devices use to find the device. DNS servers make it unnecessary to remember IP addresses like 192.168.1.1 (on IPv4) or newer, more complex alphanumeric IP addresses like 2400: cb00: 2048: 1:: c629: d7a2 (on IPv6). The DNS resolution method involves converting a hostname (such as www.example.com) to an IP address supported by the computer (192.168.1.1). Every device on the web is assigned an IP address, which is important in finding an acceptable internet device. An address is used to find a specific house. When a user wants to load a web page, a translation must be between what the user typed in their browser (example.com) and the machine-friendly address needed to find the instance's .com web page.

To know the method behind DNS resolution, it is essential to know which hardware components a DNS request must pass. For the online browser, the DNS lookup is done "behind the scenes" and does not require interaction from the user's computer other than the initial query. The DNS process works as follows:

1. A browser, application, or device called a DNS client issues a DNS query or DNS address lookup and returns a hostname such as "example.com."
2. The request is received by a DNS resolver, which is responsible for finding the correct IP address for this hostname. The DNS resolver looks for a DNS name server containing the hostname's IP address in the DNS request.

3. The resolver starts with the Internet root DNS server. It works its way down the hierarchy to the top-level domain (TLD) DNS servers (here, ".com") to the name server that is responsible for the exact environment "Example. com ".
4. When the resolver reaches the authoritative DNS name server for "example.com," it receives the IP address and other relevant details and sends them back to the DNS client. The DNS request is now resolved.
5. The DNS client device can connect directly to the server with the correct IP address.

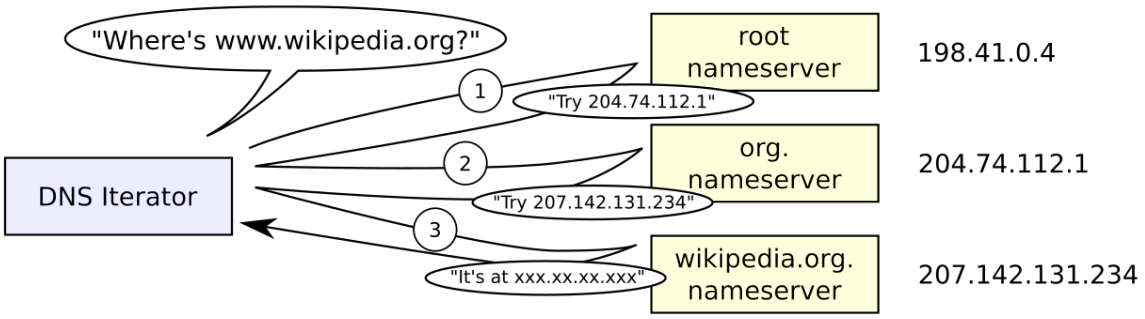

Figure 4: DNS Request

Interview Questions

Transport Layer

Q1. What is a TCP transmission control protocol? **(Oracle Corporation)**
Answer: TCP is one of the fundamental standards that define Internet rules and is included in the Internet Engineering Task Force (IETF) standards. In digital network communication, and guarantees the transmission of data from one end to the other. TCP is also responsible for organizing data to be transferred between a server and a client. It guarantees the integrity of the data transmitted over a network. Before sending data, TCP establishes a connection between a source and its destination, which it maintains until communication begins. Large amounts of data are then divided into smaller packets while maintaining data integrity throughout the process.

Q2. What are the TCP sequence number and the data offset in the TCP header? **(Larsen & Toubro Infotech)**
Answer: The sequence number that initiates the TCP connection must choose a random initial number that is then incremented according to the number of bytes transferred. The data offset in the TCP header indicates the size of the TCP header. They are expressed in 32-bit words. One word represents four bytes.

Q3. Differentiate between UDP and TCP. **(Mphasis)**
Answer: Transmission Control Protocol (TCP) is connection-oriented, i. H. Once a connection is established, then data can be transmitted in two directions. TCP has built-in systems to check for errors and ensure data is delivered in the order it was sent, making it the perfect protocol for transferring information such as still images, data files, and web pages. Transmission Control Protocol (TCP) is connection-oriented, i. H. After the connection is made, the data can be transmitted in two directions. TCP has built-in systems to check for errors and ensure that data is delivered in the order it was sent, making it the perfect protocol for transferring information such as still images, data files, and web pages.

Q4. What are TCP timers? What are the different timers? **(Xansa)**

Answer: TCP keepalive timeout defines the time interval for the TCP connection to verify if the FCIP connection is working correctly. This ensures that FCIP connection errors are caught quickly, even when the connection is idle. The four types of TCP timers are:

- Timeout timer
- Timeout timer
- Keep Alive Timer
- Persistent timer

Q5. What is DNS? What role does DNS play in a network? **(Xansa)**

Answer: All computers on the Internet, from your smartphone or laptop to the servers that serve content for large retail websites, find and communicate with each other using numbers. When anyone opens a web browser and goes to a website, they don't have to memorize and enter a long number. Instead, they can enter a domain name like example.com and end up in the right place anyway. Each domain can correspond to more than a single IP address. Some sites have even had hundreds or more IP addresses that correspond to a single domain name. For example, the IP that your computer accesses for www.google.com is likely to be different from the IP that someone in another country could access by typing the same site name into their browser.

Symmetric Key

Overview

In cryptography, an asymmetric key is a key that is used to encrypt and decrypt information. This means that decrypting information requires the same key that was used to encrypt it. In practice, keys represent a secret shared between two or more parties that can be used to maintain a private information connection. This requires that both parties have access to the secret key is one of the main disadvantages of symmetric key encryption compared to public-key encryption. By using symmetric encryption algorithms, the data is converted into a form that cannot be understood by anyone who doesn't have the secret key to decrypt it. Once the intended recipient, who has the key, has the message, the algorithm reverses its action to return the message to its original, understandable form. The secret key used by both sender and recipient can be a specific password/code or a random sequence of letters or numbers generated by a secure random number generator (RNG).

Following are types of symmetric encryption algorithms:

- **Block algorithms**. Fixed bit lengths are encrypted in electronic data blocks using a specific secret key. Since the data is encrypted, the system keeps it in its memory while waiting for entire blocks.
- **Flow algorithms**. Data is encrypted during transmission rather than stored in system memory.

The success depends on the strength of the random number generator used to generate the secret key. It is widely used today and mainly consists of two types of algorithms, block, and stream. Some common encryption algorithms include Advanced Encryption Standard and Data Encryption Standard. This type of encryption is generally much faster than asymmetric but requires that both the sender and the data recipient have the secret key. DES, one of the standard symmetric essential encryption methods, modifies the best symmetric essential methods by the National Institute of Standards and Technology. Your symmetric key is 56 bits long. When text is encrypted, it is divided into 64-bit components. Each component is encrypted with the symmetric key, after which all the ciphertext is sent to its destination over the Internet. At the goal, the

ciphertext is decrypted with the same key to generate the original text. Some examples of symmetric encryption algorithms are:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

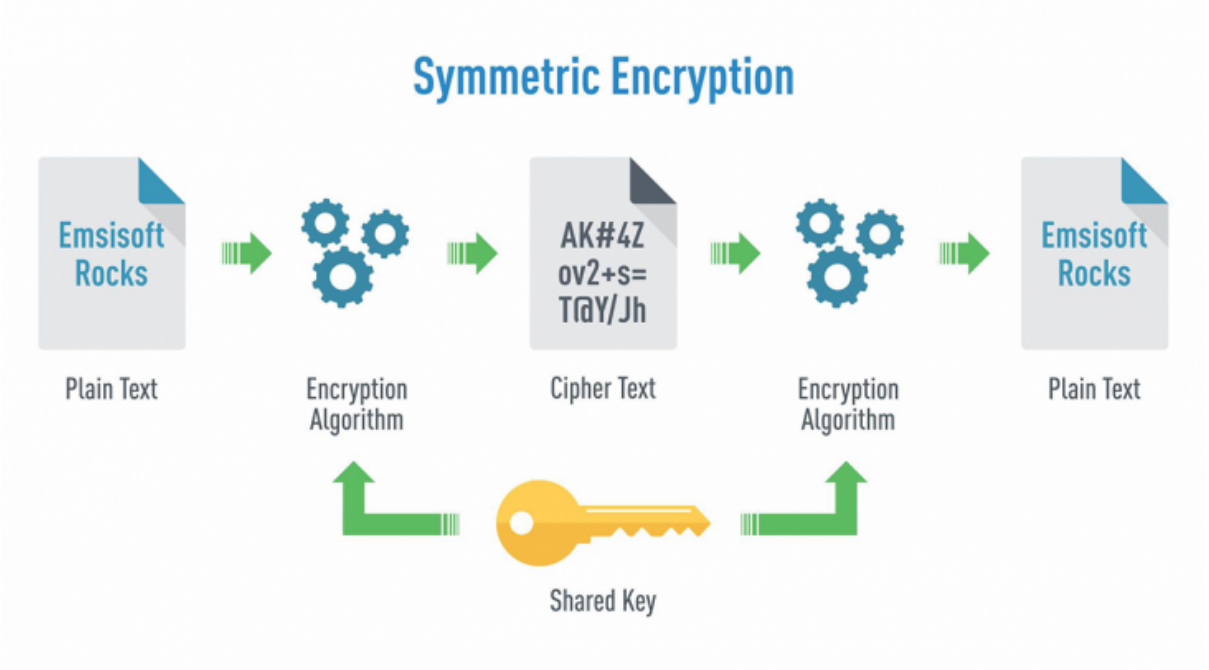

Figure 1: Symmetric Encryption

Asymmetric Key

Overview

Asymmetric cryptography is a technique that uses a related key pair, a public key and a personal key, to encrypt and decrypt a message and reserve it to guard against unauthorized access or unauthorized use. A public key's a cryptographic key that anyone can use to encrypt a message so that only the intended recipient can decrypt using their private key. A personal key also referred to as a secret key, is merely shared with the initiator of the key. When someone sends an encrypted message, they will extract the recipient's public key from a public directory and then use it to encrypt the message before sending it. The recipient of the message can decrypt the message with its associated private key. If the sender encrypts the message together with his private key, the message can only be decrypted; thereupon, the sender's public key authenticates. These encryption and decryption processes are administered automatically; Users don't get to lock and unlock the message physically. Many protocols are supported asymmetric cryptography, including the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols, which enable HTTPS.
The encryption process is additionally employed by software programs that require determining a secure connection over an insecure network, like a network. B. Internet browsers or that require to validate of a digital signature. Higher data security is that the main advantage of asymmetric cryptography. It's the original secure encryption method because users never need to reveal or divulge their private keys, reducing the prospect that a cybercriminal will discover a user's private key in transit. Asymmetric cryptography also can be applied to systems where many users may have to encrypt and decrypt messages, including:

- **Encrypted email.** A public key is often wont to encrypt a message, and a personal legend is often wont to decrypt it.
- **SSL / TLS.** Asymmetric encryption is additionally used when establishing encrypted connections between websites and browsers.
- **Cryptocurrencies.** Bitcoin and other cryptocurrencies are supported asymmetric cryptography. Users have public keys that anyone can see and

personal keys that are kept secret. Bitcoin uses a cryptographic algorithm to make sure that only the rightful owners can spend it.

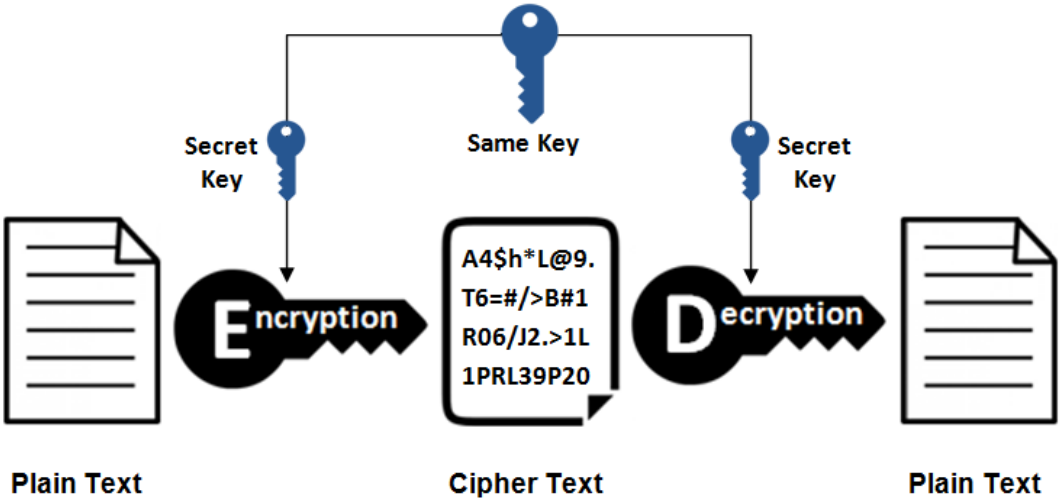

Figure 1: Asymmetric Encryption

Diffie Hellman

Overview

This key exchange was one of the significant advancements in public-key cryptography and is still widely implemented in several different security protocols. It allows two parties who have not yet met to create a vital key that they can use to protect their communication. This article explains what it is used for, how it works step by step, its different variations, and the security aspects that must be considered for secure implementation.

This key exchange also called an exponential key exchange, is a digital encryption method that uses numbers of certain powers to generate decryption keys based on components that are never transmitted directly, making the task of potential decryption of codes are mathematically overwhelming. It is a method for the secure exchange of cryptographic keys through a public communication channel. In reality, the keys are not exchanged but are derived together. It is named after its inventors Whitfield Diffie and Martin Hellman. It is a key exchange protocol that allows two parties to communicate through a public channel to create a shared secret without being transmitted over the Internet. DH allows both of you to use a public key to encrypt and decrypt your conversation or data using symmetric cryptography.

Working of Diffie-Hellman key exchange

It is complex and it can be challenging to become familiar with how it works. Let's first explain the Diffie-Hellman essential discussion with an analogy to make things a little more understandable. The best analogy is to imagine two people mixing colors. Let's use the crypto standard and say their names are Alice and Bob. They both initially agree on a random color. Let's say they message each other and choose yellow as their standard color.

They set their color. It does not tell the other party of its choice. Let's say Alice chooses red while Bob chooses a slightly greenish-blue. The next step is for Alice and Bob to mix their secret color (red for Alice, green-blue for Bob) with the mutually agreed yellow. Alice gets an orange blend, while Bob's result is a deeper blue, according to the diagram. Once they have finished shuffling, they send the result to the other party. Alice gets a deeper blue while Bob gets the color orange. After you get the mixed result from

your partner, add her secret color to it. Alice takes the deepest blue and adds her unique red color, while Bob adds her secret green-blue to the orange mix she just received. The result? They both come out the same color, which in this case is a disgusting brown. It may not be the type of color you want to paint your living room with, but it is a standard color nonetheless. This traditional color is known as the shared secret. The critical part of the Diffie-Hellman key exchange is that both parties achieve the same result without having to send the entire shared secret over the communication channel. Picking a standard color, your secret colors, swapping the mix, and then adding your color back gives both parties a chance to come up with the same shared secret without having to submit everything.

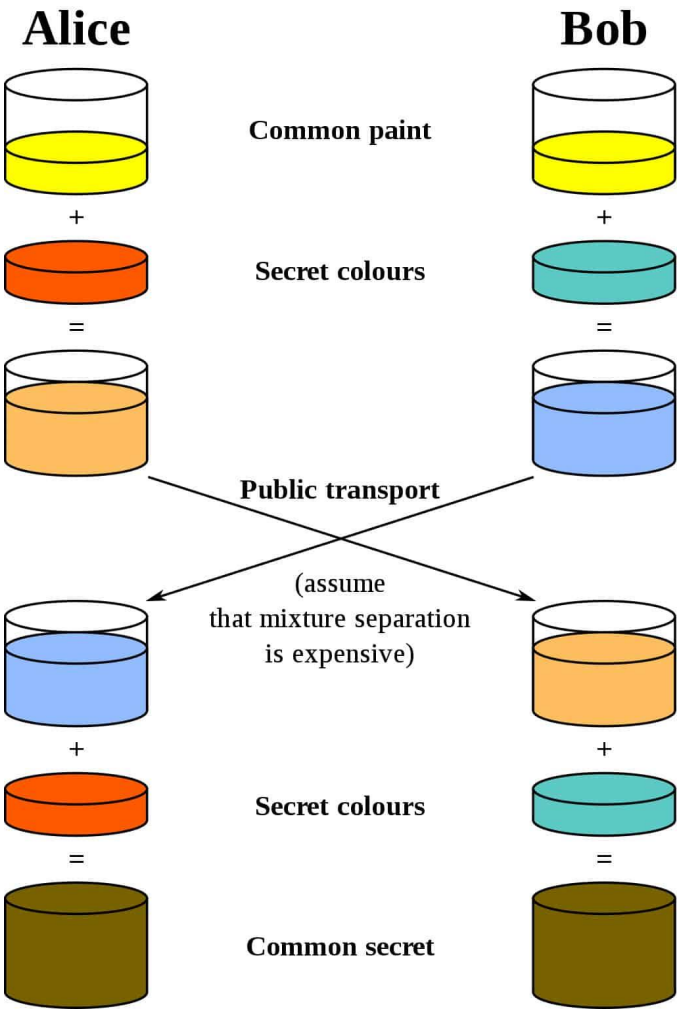

Figure 1: Diffie Hellman

RSA

Overview

The RSA is a series of cryptographic algorithms used for specific security purposes or services that enable public-key encryption and universally defend sensitive data, especially when dispatched to through an insecure network cognate as the Internet. Public critical cryptography, also known as asymmetric cryptography, uses two different but mathematically related keys, one public and one private. The public key can be participated by everyone, while the private key must be kept secret. With RSA cryptography, both the public and private keys can encode a communication; the antipodean key used to encode a communication is used to break it. This criterion is one of the reasons why RSA has to get the most universally used asymmetric algorithm; it provides how-to cinch confidentiality, integrity, authenticity, and non-repudiation of electronic communication and data depot.

The following figure shows how asymmetric cryptography works:

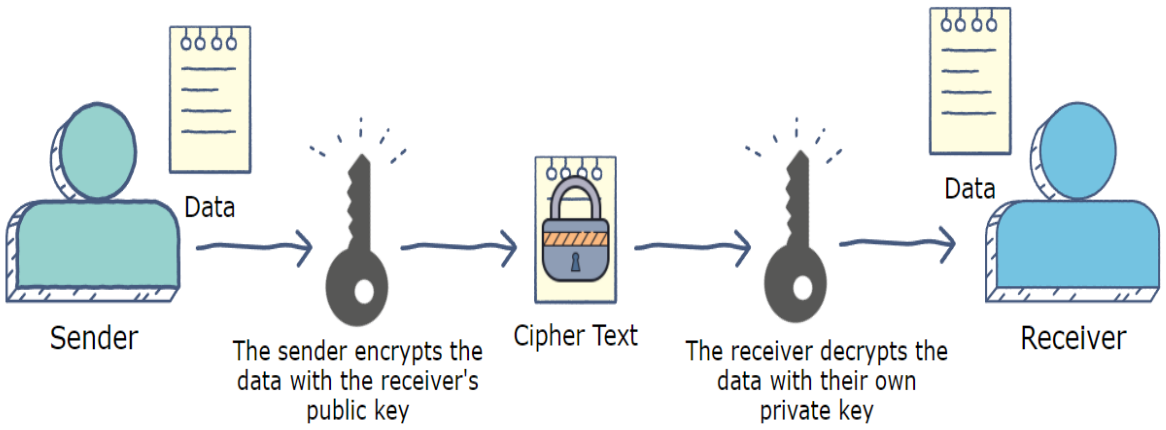

Figure 1: RSA

Working of RSA

The option to encode with the public or private key provides RSA dopeheads with a variety of services. However, the private key must be used to break the data, If the public key is used for encryption. This is ideal for dispatching hush-hush information over a network or Internet connection where the angel of the data sends the sender of the data their public key. The sender of the data either encrypts the hush-hush information with the public key and sends it to the angel. Since the public key encrypts the data, only the private key holder can break the sensitive data. This means that only the intended angel of the data can break it yea if the data was taken during transmission.

The other asymmetric encryption form with RSA is to encode communication with a private key. In this exemplar, the sender of the data encrypts the data with his private key and sends the encoded data and his public key to the angel of the data. The angel of the data can either break the data with the sender's public key and authenticate the sender's identity. With this form, data could be stolen and read in transport, but the real purpose of this type of encryption is to prove the original identity of the sender. However, the public key would not be competent to break the new communication. The angel would know that the data was modified in transport if stolen and modified in the vehicle.

The technical details of RSA are grounded on the idea that it's easy to bring about a number by multiplying two large enough calculus together, but factoring that number back into the original fluorescence is exceptionally hairy. The public and private keys are created with two calculus, which comprises two sizeable foremost calculus. They both use the same two foremost calculus to calculate their value. RSA keys usually are 1024 or 2048 bits long, making them extremely catchy to factor, although 1024- bit keys are believed to be fragile soon.

Digital Signature

Overview

An electronic signature uses a mathematical algorithm commonly used to verify a message's authenticity and integrity. Digital signatures always create a virtual fingerprint unique to identify users and protect the information in statements or digital documents. In emails, the content of the email becomes part of the digital signature. Digital signatures are much more secure than other forms of electronic signature.

The broad category of electronic signatures (eSignatures) includes many types of electronic signatures. The class of signatures includes digital signatures, which are a specific technology implementation of electronic signatures. Both digital signatures and other electronic signature solutions allow you to sign documents and authenticate the signer. However, there are differences in terms of purpose, technical implementation, geographical use, and legal and cultural acceptance of digital signatures compared to other types of electronic signatures.

The use of digital signature technology for electronic signatures differs significantly between countries that follow open and technology-neutral electronic signature laws, including the United States, Great Britain, Canada, and Australia and countries that follow signature models. Tiered electronics prefer locally defined standards based on digital signature technology, including many countries in the European Union, South America, and Asia. Additionally, some industries also support specific measures based on digital signature technology. The digital signature is a procedure that ensures that the content of a message has not been modified during transmission. When you digitally sign a document as a server, you add a one-way (encrypted) hash of the message content with your public and private key pair. Your client can still read it, but the process creates a "signature" that only the server's public key can decrypt. The client can then use the server's public key to verify the sender and the integrity of the message content. Whether it's an email, an online order, or a watermarked photo on eBay, if the transfer arrives but the digital signature doesn't match the public key on the digital certificate, the customer knows the message has been modified.

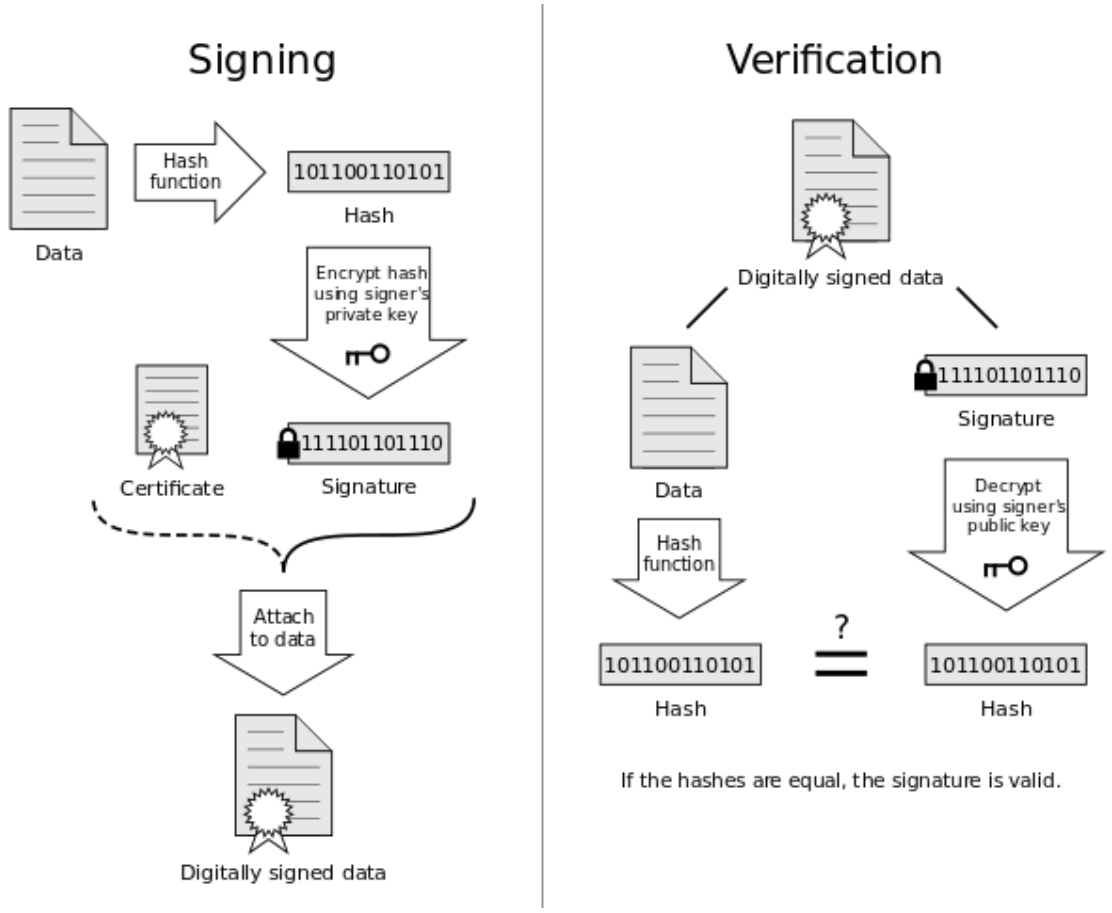

Figure 1: RSA

Working of RSA

Digital signatures are only based on public-key cryptography, also known as asymmetric cryptography. Two keys are generated using a public key algorithm like RSA (RivestShamirAdleman), creating a pair of mathematically linked keys, one private and one public. Digital signatures work through the two mutually authenticating cryptographic keys of public-key cryptography. The person creating the digital signature uses a private key to encrypt the signature-related data, while this can only be decrypted using the signer's public key. If the recipient cannot open the document with the signer's public key, this is an indication that there is some problem with the paper or signature. This is how digital signatures are authenticated. Digital signature technology requires all parties to trust that the person who created the signature kept the private key secret. If someone else has access to the signature's private key, that party could create fraudulent digital signatures on behalf of the personal key holder.

Benefits of Digital Signatures

Security is the main advantage of digital signatures. Security features built into digital signatures ensure that a document is not altered and legitimate signatures. The following security features and methods are used with digital signatures:

- **Legal documents and contracts:** Digital signatures are legally binding. This makes them ideal for any legal document that requires a signature authenticated by one or more parties and guarantees that the record has not been altered.
- **Sales contracts:** Digital signing of contracts and sales contracts authenticates the identity of the seller and the buyer, and both parties can be sure that the signatures are legally binding and that the terms of the agreement have not been changed.
- **Financial Documents:** Finance departments digitally sign invoices so customers can trust that the payment request is from the right seller, not from a bad actor trying to trick the buyer into sending payments to a fraudulent account.
- **Health Data** - In the healthcare industry, privacy is paramount for both patient records and research data. Digital signatures ensure that this confidential information was not modified when it was transmitted between the consenting parties.
- Federal, state, and local government agencies have stricter policies and regulations than many private sector companies. From approving permits to stamping them on a timesheet, digital signatures can optimize productivity by ensuring the right person is involved with the proper approvals.
- **Shipping Documents:** Helps manufacturers avoid costly shipping errors by ensuring cargo manifests or bills of lading are always correct. However, physical papers are cumbersome, not always easily accessible during transport, and can be lost. By digitally signing shipping documents, the sender and recipient can quickly access a file, check that the signature is up to date, and ensure that no tampering has occurred.

Interview Questions

Network Security

Q1. What is a symmetric key? **(Hicube Infosec Pvt. Ltd)**
Answer: Symmetric encryption is a type of encryption that uses only one key (a secret key) to encrypt and decrypt electronic information. Entities that communicate using symmetric encryption must exchange the key before it can be used in the decryption process. This encryption method differs from asymmetric encryption, in which a key pair, one public and one private, is used to encrypt and decrypt messages.

Q2. How is Asymmetric encryption different? **(K7 Computing Pvt. Ltd)**
Answer: Symmetric encryption consists of one key for encryption and decryption, while asymmetric encryption consists of two cryptographic keys known as a public key and a private key. Asymmetric cryptography is a technique that uses a related key pair, a public key and a personal key, to encrypt and decrypt a message and reserve it to guard against unauthorized access or unauthorized use. A public key's a cryptographic key that anyone can use to encrypt a message so that only the intended recipient can decrypt using their private key.

Q3. How does the Diffie Hellman exchange works? **(Wi-Jungle)**
Answer: DH is usually explained by two sample groups, Alice and Bob, who start a dialogue. Everyone has information they want to share while keeping it a secret. To do this, they agree to some benign public information that is mistaken for their privileged information by being transmitted through an insecure channel. Their secrets are mixed with the public information or public key, and while the secrets are being exchanged, the information they want to share is mixed with the shared secret. When they decipher the other's message, they can extract the public information and, knowing their own secret, infer the new information that they took with them. While this method may seem straightforward to describe, decryption by an outside party trying to spy using

long strings of numbers for public and private keys is mathematically impractical, even with significant resources.

Q4. What are RSA algorithms? **(eSec Forte Technologies)**

Answer: The RSA is a series of cryptographic algorithms used for specific security purposes or services that enable public-key encryption and universally defend sensitive data, especially when dispatched to through an insecure network cognate as the Internet. Public critical cryptography, also known as asymmetric cryptography, uses two different but mathematically related keys, one public and one private.

Q5. What are digital certificates? **(Quick Heal Technologies Ltd.)**

Answer: A digital certificate, also known as a public key certificate, is used to cryptographically link the ownership of a public key to the entity that owns it. Digital certificates are used to share public keys for encryption and authentication. Digital certificates include the public key to be certified, identifying information about the entity that owns the public key, metadata related to the digital certificate, and a digital signature of the public key created by the certifier.