Unit 3 : Network Protocols, Network Routing

LECTURER : NANDAN PANDYA

COURSE: BACHELOR OF COMPUTER APPLICATIONS (BCA)

SEMESTER: 4TH

SUBJECT: NETWORK TECHNOLOGY AND ADMINISTRATION

SUBJECT CODE: CS-21

COLLEGE: KAMANI SCIENCE COLLEGE, AMRELI

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Topics

- Packets & Protocols
- Connection Oriented Protocol :TCP& connection less protocols-UDP
- TCP/IP STACK or TCP/IP Model
- - HTTP
  - FTP
  - SMTP
  - POP3
  - SNMP
  - TELNET
- ARP and RARP
- IPX/SPX
- AppleTalk, NetBIOS Name protocol
- L2CAP, RFCOMM Protocol
- Routing, Requirements of routing , Types of Routing – static , dynamic and default
- Routing protocols
- Exterior Routing protocol: BGP
- Interior Routing protocol :
- (1)Distance vector routing - RIP ,IGRP , EIGRP
- (2)Link state routing : OSPF , IS IS

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Packets

- A packet is a small segment of a larger message. Data sent over computer networks, such as the Internet, is divided into packets. These packets are then recombined by the computer or device that receives them.

Protocol

- A protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless.

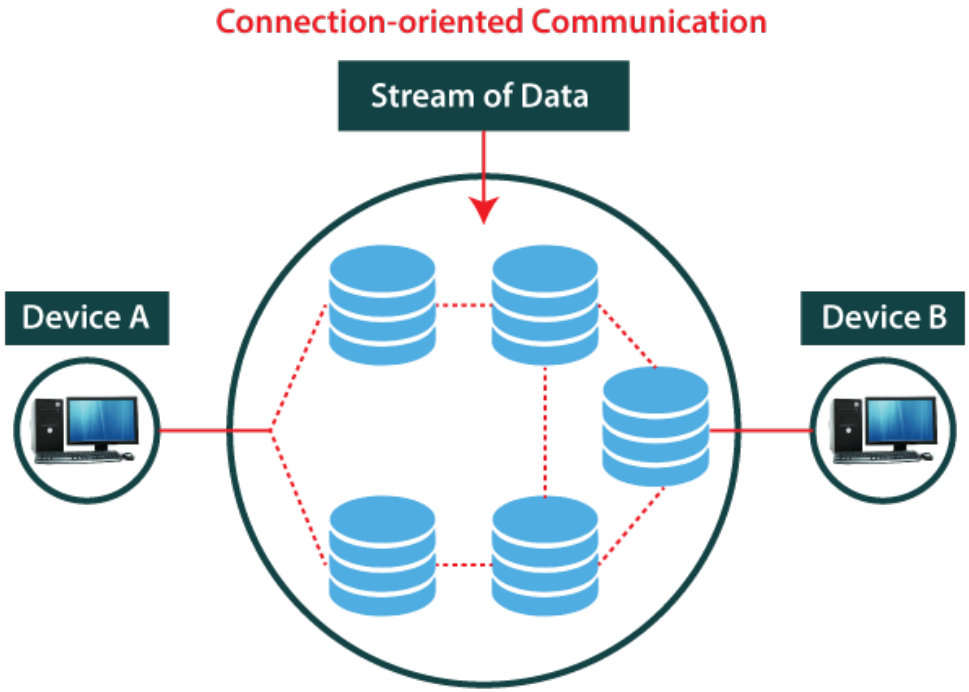
Connection Oriented Protocol: TCP

- A connection-oriented service is a network service that was designed and developed after the telephone system. A connection-oriented service is used to create an end to end connection between the sender and the receiver before transmitting the data over the same or different networks. In connection-oriented service, packets are transmitted to the receiver in the same order the sender has sent them. It uses a handshake method that creates a connection between the user and sender for transmitting the data over the network. Hence it is also known as a reliable network service.

Cont..

- Suppose, a sender wants to send data to the receiver. Then, first, the sender sends a request packet to a receiver in the form of an **SYN** packet. After that, the receiver responds to the sender's request with an (SYN-ACK) signal/packets. That represents the confirmation is received by the receiver to start the communication between the sender and the receiver. Now a sender can send the message or data to the receiver.
- Similarly, a receiver can respond or send the data to the sender in the form of packets. After successfully exchanging or transmitting data, a sender can terminate the connection by sending a signal to the receiver. In this way, we can say that it is a reliable network service.

Cont..


Connection-oriented Communication
Stream of Data
Device A
Device B

TCP

- TCP (Transmission Control Protocol) is a connection-oriented protocol that allows communication between two or more computer devices by establishing connections in the same or different networks. It is the most important protocol that uses internet protocol to transfer the data from one end to another. Hence, it is sometimes referred to as TCP/IP. It ensures that the connection is established and maintained until the data packet is transferring between the sender and receiver is complete.
- It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.
- The main functionality of the TCP is to take the data from the application layer. Then it divides the data into a several packets, provides numbering to these packets, and finally transmits these packets to the destination. The TCP, on the other side, will reassemble the packets and transmits them to the application layer. As we know that TCP is a connection-oriented protocol, so the connection will remain established until the communication is not completed between the sender and the receiver.

Need of TCP

- In the layered architecture of a network model, the whole task is divided into smaller tasks. Each task is assigned to a particular layer that processes the task. In the TCP/IP model, five layers are application layer, transport layer, network layer, data link layer, and physical layer. The transport layer has a critical role in providing end-to-end communication to the directly application processes. It creates 65,000 ports so that the multiple applications can be accessed at the same time. It takes the data from the upper layer, and it divides the data into smaller packets and then transmits them to the network layer.

Features of TCP protocol

- **Transport Layer Protocol**: TCP is a transport layer protocol as it is used in transmitting the data from the sender to the receiver.
- **Reliable** :TCP is a reliable protocol as it follows the flow and error control mechanism. It also supports the acknowledgment mechanism, which checks the state and sound arrival of the data. In the acknowledgment mechanism, the receiver sends either positive or negative acknowledgment to the sender so that the sender can get to know whether the data packet has been received or needs to resend.
- **Order of the data is maintained**: This protocol ensures that the data reaches the intended receiver in the same order in which it is sent. It orders and numbers each segment so that the TCP layer on the destination side can reassemble them based on their ordering.
- **Connection-oriented**: It is a connection-oriented service that means the data exchange occurs only after the connection establishment. When the data transfer is completed, then the connection will get terminated.
- **Full duplex**: It is a full-duplex means that the data can transfer in both directions at the same time.
- **Stream-oriented** :TCP is a stream-oriented protocol as it allows the sender to send the data in the form of a stream of bytes and also allows the receiver to accept the data in the form of a stream of bytes. TCP creates an environment in which both the sender and receiver are connected by an imaginary tube known as a virtual circuit. This virtual circuit carries the stream of bytes across the internet.

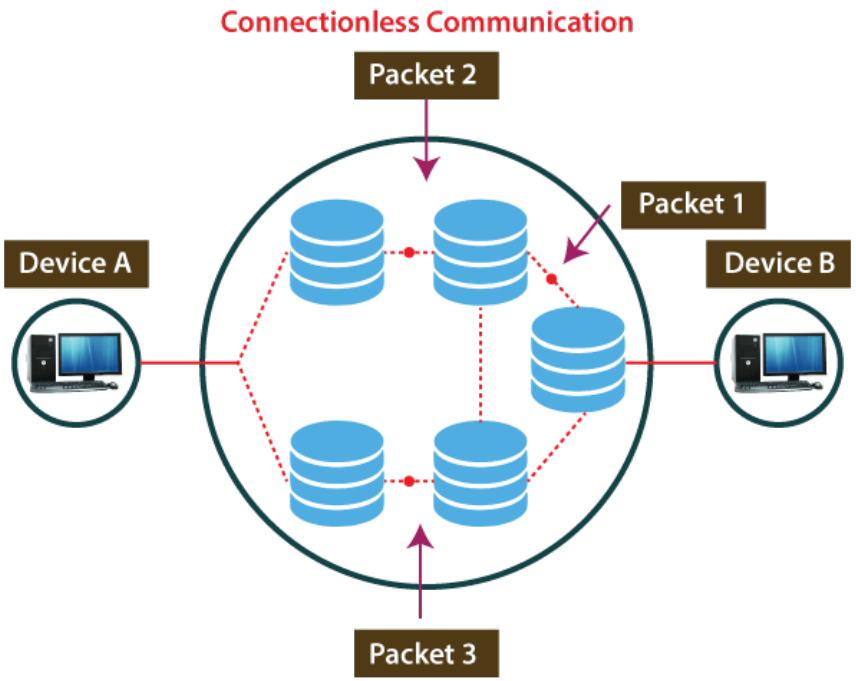
Connection Less Protocol: UDP

- A connection is similar to a postal system, in which each letter takes along different route paths from the source to the destination address. Connectionless service is used in the network system to transfer data from one end to another end without creating any connection. So it does not require establishing a connection before sending the data from the sender to the receiver. It is not a reliable network service because it does not guarantee the transfer of data packets to the receiver, and data packets can be received in any order to the receiver. Therefore we can say that the data packet does not follow a defined path. In connectionless service, the transmitted data packet is not received by the receiver due to network congestion, and the data may be lost.

Cont..

- **For example**, a sender can directly send any data to the receiver without establishing any connection because it is a connectionless service. Data sent by the sender will be in the packet or data streams containing the receiver's address. In connectionless service, the data can be travelled and received in any order. However, it does not guarantee to transfer of the packets to the right destination.

Cont..


Connectionless Communication
Packet 2
Packet 1
Device A
Device B
Packet 3

UDP

- The UDP (User Datagram Protocol) is a connectionless protocol that allows communication between two or more devices without establishing any connection. In this protocol, a sender sends the data packets to the receiver that holds the destination address. A UDP does not ensure to deliver the data packets to the correct destination, and it does not generate any acknowledgment about the sender's data. Similarly, it does not acknowledge the receiver about the data. Hence, it is an unreliable protocol.

Cont..

- The UDP protocol allows the computer applications to send the messages in the form of datagrams from one machine to another machine over the Internet Protocol (IP) network. The UDP is an alternative communication protocol to the TCP protocol (transmission control protocol). Like TCP, UDP provides a set of rules that governs how the data should be exchanged over the internet. The UDP works by encapsulating the data into the packet and providing its own header information to the packet. Then, this UDP packet is encapsulated to the IP packet and sent off to its destination. Both the TCP and UDP protocols send the data over the internet protocol network, so it is also known as TCP/IP and UDP/IP. There are many differences between these two protocols. UDP enables the process to process communication, whereas the TCP provides host to host communication. Since UDP sends the messages in the form of datagrams, it is considered the best-effort mode of communication. TCP sends the individual packets, so it is a reliable transport medium. Another difference is that the TCP is a connection-oriented protocol whereas, the UDP is a connectionless protocol as it does not require any virtual circuit to transfer the data.
- UDP also provides a different port number to distinguish different user requests and also provides the checksum capability to verify whether the complete data has arrived or not; the IP layer does not provide these two services.

Need of UDP

- The UDP is an unreliable protocol, but we still require a UDP protocol in some cases. The UDP is deployed where the packets require a large amount of bandwidth along with the actual data. For example, in video streaming, acknowledging thousands of packets is troublesome and wastes a lot of bandwidth. In the case of video streaming, the loss of some packets couldn't create a problem, and it can also be ignored.

Features of UDP protocol

- **Transport layer protocol**: UDP is the simplest transport layer communication protocol. It contains a minimum amount of communication mechanisms. It is considered an unreliable protocol, and it is based on best-effort delivery services. UDP provides no acknowledgment mechanism, which means that the receiver does not send the acknowledgment for the received packet, and the sender also does not wait for the acknowledgment for the packet that it has sent.
- **Connectionless**: The UDP is a connectionless protocol as it does not create a virtual path to transfer the data. It does not use the virtual path, so packets are sent in different paths between the sender and the receiver, which leads to the loss of packets or received out of order.
- **Ordered delivery of data is not guaranteed**: In the case of UDP, the datagrams are sent in some order will be received in the same order is not guaranteed as the datagrams are not numbered.
- **Ports**: The UDP protocol uses different port numbers so that the data can be sent to the correct destination. The port numbers are defined between 0 and 1023.
- **Faster transmission**: UDP enables faster transmission as it is a connectionless protocol, i.e., no virtual path is required to transfer the data. But there is a chance that the individual packet is lost, which affects the transmission quality. On the other hand, if the packet is lost in TCP connection, that packet will be resent, so it guarantees the delivery of the data packets.

Cont..

- **Acknowledgment mechanism**: The UDP does have any acknowledgment mechanism, i.e., there is no handshaking between the UDP sender and UDP receiver. If the message is sent in TCP, then the receiver acknowledges that I am ready, then the sender sends the data. In the case of TCP, the handshaking occurs between the sender and the receiver, whereas in UDP, there is no handshaking between the sender and the receiver.
- **Segments are handled independently**: Each UDP segment is handled individually of others as each segment takes different path to reach the destination. The UDP segments can be lost or delivered out of order to reach the destination as there is no connection setup between the sender and the receiver.
- **Stateless**: It is a stateless protocol that means that the sender does not get the acknowledgement for the packet which has been sent.

Connection Oriented v/s Connectionless Service/Protocol

Comparison Parameter	Connection-oriented Service	Connection Less Service
Related System	It is designed and developed based on the telephone system.	It is service based on the postal system.
Definition	It is used to create an end to end connection between the senders to the receiver before transmitting the data over the same or different network.	It is used to transfer the data packets between senders to the receiver without creating any connection.
Virtual path	It creates a virtual path between the sender and the receiver.	It does not create any virtual connection or path between the sender and the receiver.
Authentication	It requires authentication before transmitting the data packets to the receiver.	It does not require authentication before transferring data packets.
Data Packets Path	All data packets are received in the same order as those sent by the sender.	Not all data packets are received in the same order as those sent by the sender.

Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

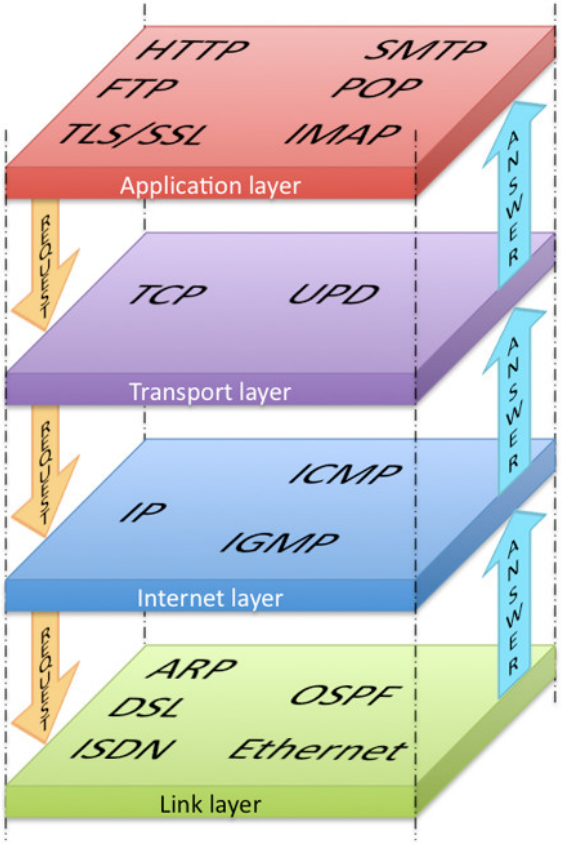
Cont..

Bandwidth Requirement	It requires a higher bandwidth to transfer the data packets.	It requires low bandwidth to transfer the data packets.
Data Reliability	It is a more reliable connection service because it guarantees data packets transfer from one end to the other end with a connection.	It is not a reliable connection service because it does not guarantee the transfer of data packets from one end to another for establishing a connection.
Congestion	There is no congestion as it provides an end-to-end connection between sender and receiver during transmission of data.	There may be congestion due to not providing an end-to-end connection between the source and receiver to transmit of data packets.
Examples	Transmission Control Protocol (TCP) is an example of a connection-oriented service.	User Datagram Protocol (UDP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP) are examples of connectionless service.

TCP/IP

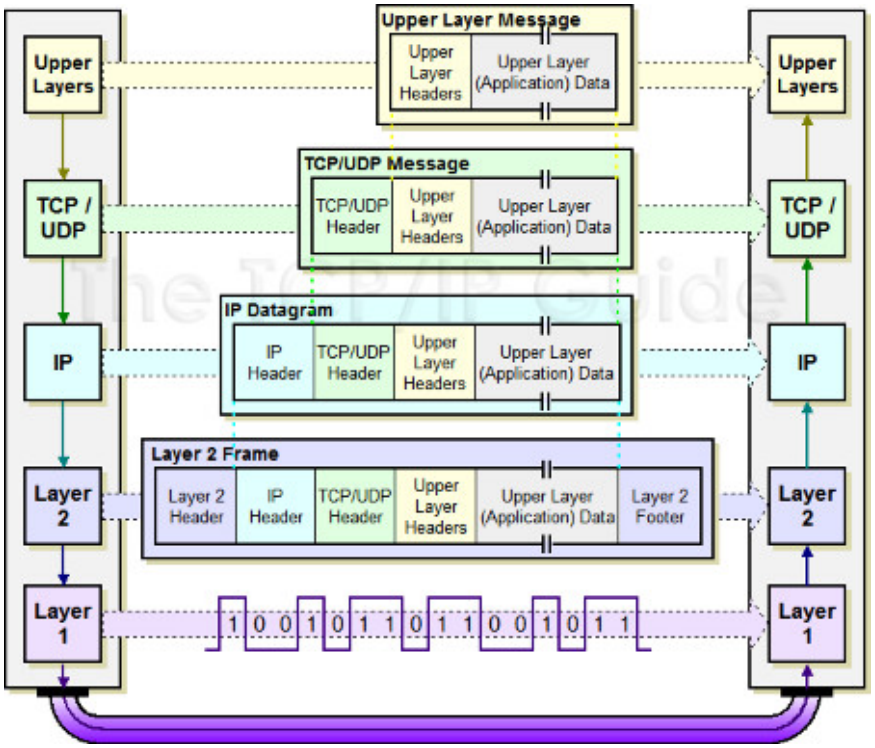
- The TCP/IP Stack, or the internet protocol suite, is a set of communication protocols used by the Internet or similar networks. Originally resulting from research at DARPA (Defense Advanced Research Projects Agency). The TCP/IP stack has gradually grown to include a suite of protocols
- The TCP/IP stack consists of a series of Protocols. Some you will be familiar with (HTTP, FTP, SMTP) and some may be more foreign to you (ISDN, IGMP, ARP).
- The TCP/IP Stack works just like the OSI model by establishing a set of rules and standards for communication in and between the different layers. These rules ensure that different products can communicate with each other because they are developed around the same guidelines.

TCP/IP Stack



Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Cont..



Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Protocols

- **HTTP**: The Hypertext Transfer Protocol is a foundation of the World Wide Web. It is used for transferring webpages and other such resources from the HTTP server or web server to the web client or the HTTP client. Whenever you use a web browser like Google Chrome or Firefox, you are using a web client. It helps HTTP to transfer web pages that you request from the remote servers.
- **SMTP**: SMTP stands for Simple mail transfer protocol. This protocol supports the e-mail is known as a simple mail transfer protocol. This protocol helps you to send the data to another e-mail address.
- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework which is used for managing the devices on the internet by using the TCP/IP protocol.

Cont..

- **DNS**: DNS stands for Domain Name System. An IP address that is used to identify the connection of a host to the internet uniquely. However, users prefer to use names instead of addresses for that DNS.
- **TELNET**: TELNET stands for Terminal Network. It establishes the connection between the local and remote computer. It established connection in such a manner that you can simulate your local system at the remote system.
- **FTP**: FTP stands for File Transfer Protocol. It is a mostly used standard protocol for transmitting the files from one machine to another.

Cont..

- **POP3**: POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.
- **IMAP:** IMAP (Internet Message Access Protocol) provides the user more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.
- **Note:** POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP), a protocol for transferring e-mail across the Internet. You send e-mail with SMTP and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP.

ARP

- Address Resolution Protocol is a communication protocol used for discovering physical address associated with given network address. Typically, ARP is a network layer to data link layer mapping process, which is used to discover MAC address for given Internet Protocol Address.
- In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine. ARP is used to get the physical address (MAC address) of destination machine.
- Before sending the IP packet, the MAC address of destination must be known. If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination. Since ARP-discovery is broadcast, every host inside that network will get this message but the packet will be discarded by everyone except that intended receiver host whose IP is associated. Now, this receiver will send a unicast packet with its MAC address (ARP-reply) to the sender of ARP-discovery packet. After the original sender receives the ARP-reply, it updates ARP-cache and start sending unicast message to the destination.

RARP

- Reverse ARP is a networking protocol used by a client machine in a local area network to request its Internet Protocol address (IPv4) from the gateway-router's ARP table. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.
- When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use. So the machine sends a RARP broadcast packet which contains its own MAC address in both sender and receiver hardware address field.
- A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets. Now the RARP server attempt to find out the entry in IP to MAC address mapping table. If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.
- LAN technologies like Ethernet, Ethernet II, Token Ring and Fiber Distributed Data Interface (FDDI) support the Address Resolution Protocol.
- RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP (Bootstrap Protocol) and DHCP(Dynamic Host Configuration Protocol).

IPX/SPX

- Internetwork Packet Exchange or Sequenced Packet Exchange is a primary protocol of the Novell NetWare. IPX/SPX server is used mainly on the networks that make use of the Novell NetWare network OS. The IPX/SPX protocols offer services that are similar to one offered by the IP & TCP. Just like IP, Internetwork Packet Exchange is the connectionless network protocol.
- And SPX runs over the IPX at a transport layer and, just like TCP, offer connection-oriented and guaranteed delivery. IPX and SPX offer many similar features like TCP/IP, it is the routable transport protocol, which allows the networks to get segmented. But, network segmentation with the IPX/SPX can be done with the network numbers & not with the subnet masks. Both the server protocols are quite similar and rely on the internal protocols for their network communication.

IPX

- IPX is known as the connectionless datagram transmission service. As it is connectionless, just like UDP, it doesn't need any kind of preliminary connection setting to send the data packets. One disadvantage to the connectionless communication is that its flow control & error correction aren't provided during the network communication. Additionally, packet delivery isn't guaranteed. IPX offers to route and addressing of the packets within or between the network segments.

SPX

- SPX has similar operations like TCP and it is connection-oriented transfer over IPX. Because of this, error correction and flow control are offered all along with the packet delivery acknowledgments. And SPX allows one single packet to stay unacknowledged at a time. Suppose the packet gets unacknowledged, then the packet gets retransmitted 8 times and supposes there is not any acknowledgment, then SPX considers its connection failed.

AppleTalk

- AppleTalk is a set of proprietary networking protocols developed by Apple for their computer systems. AppleTalk was included in the original Macintosh released in 1984. In 2009, it became unsupported with the release of Mac OS X v10.6 and was dropped in favor of TCP/IP networking, allowing Apple computers to use the same standard to communicate with other computers.
- The design of AppleTalk followed the OSI Model of protocol layering with two protocols aimed at making the system completely self-configuring.
- AppleTalk Address Resolution Protocol (AARP): Allowed hosts to automatically generate their own network addresses
- Name Binding Protocol (NBP): A dynamic system that maps network addresses to user-readable names.

NetBIOS

- NetBIOS stands for Network Basic Input/Output System, is a specification created by IBM and Microsoft that allows distributed applications to access each other's network services independent of the transport protocol used.
- NetBIOS provides network input/output services to support client/server applications on a network. From an architectural viewpoint, the NetBIOS specification defines two things:
- An inter process communication (IPC) mechanism or application programming interface (API) that allows applications that are NetBIOS-enabled to communicate remotely over a network and request services from lower levels of the protocol stack. This is the primary and original definition of NetBIOS.
- A protocol operating at the session and transport layers of the Open Systems Interconnection (OSI) reference model that enables functions such as session establishment and termination as well as name registration, renewal, and resolution.
- NetBIOS can take different forms depending on the network protocol on which it is running.

L2CAP

- Logical Link Control and Adaptation Protocol (L2CAP) is a protocol used in the Bluetooth standard that provides adaption between higher layers and the baseband layer of the Bluetooth stack. It operates just above the host-controller interface (HCI) passing data frames from the higher layers to either HCI or Link Manager.

Functions of L2CAP

- Adaptation between higher-layer frames and lower layer frames of the Bluetooth protocol stack.
- Support for both connection-oriented as well as connectionless services.
- Supporting two links for the Baseband layer
  - Synchronous Connection-Oriented (SCO) links for real-time voice traffic using reserved bandwidth.
  - Asynchronous Connection-Less (ACL) links for best-effort traffic.
- Multiplexing of higher layer protocols, which allows them to use the links provided by the lower layers.
- Segmentation and reassembly of data packets of the upper layer that are larger than the capacity of the radio layer underneath.
- Group management.
- Quality of Service (QoS) for upper-layer protocols.

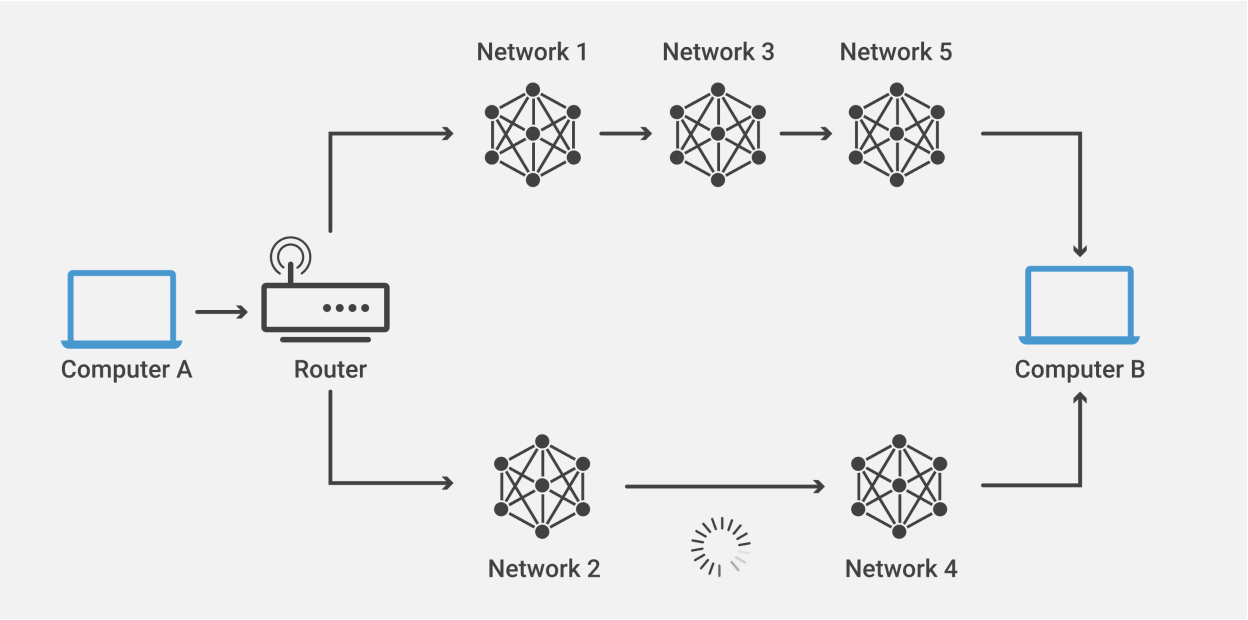
RF COMM

- RF Comm is is the transmission of information and control commands from one communication device to another communication device (such as from a computer to an accessory device) that is performed serially (one bit at a time). The Bluetooth system uses radio frequency communication (RF Comm) protocol to setup and coordinate the transfer of serial data.

Routing

- Network routing is the process of selecting a path across one or more networks. The principles of routing can apply to any type of network, from telephone networks to public transportation. In packet-switching networks, such as the Internet, routing selects the paths for Internet Protocol (IP) packets to travel from their origin to their destination. These Internet routing decisions are made by specialized pieces of network hardware called routers.
- Example: For a data packet to get from Computer A to Computer B, should it pass through networks 1, 3, and 5 or networks 2 and 4? The packet will take a shorter path through networks 2 and 4, but networks 1, 3, and 5 might be faster at forwarding packets than 2 and 4. These are the kinds of choices network routers constantly make.

Cont..



Prepared by: Prof. Nandan Pandya
Kamani Science College, Amreli

Features/Requirement of routing

- Learn routing information from neighboring routers
- Advertise local routing information to neighboring routers
- Calculate the best route for each subnet of the network
- Provide a virtual map of all routes of the network
- Calculate the cost of each route and help the router choose the best and fastest route
- Detect any change in the network and update all routers about that change

Static Routing

- Static routing protocols are used when an administrator manually assigns the path from source to the destination network. It offers more security to the network.
- **Advantages**
  - No overhead on router CPU.
  - No unused bandwidth between links.
  - Only the administrator is able to add routes
- **Disadvantages**
  - The administrator must know how each router is connected.
  - Not an ideal option for large networks as it is time intensive.
  - Whenever link fails all the network goes down which is not feasible in small networks.

Dynamic Routing

- It helps routers to add information to their routing tables from connected routers automatically. These types of protocols also send out topology updates whenever the network changes' topological structure.
- **Advantage**
  - Easier to configure even on larger networks.
  - It will be dynamically able to choose a different route in case if a link goes down.
  - It helps you to do load balancing between multiple links.
- **Disadvantage**
  - Updates are shared between routers, so it consumes bandwidth.
  - Routing protocols put an additional load on router CPU or RAM.

Default Routing

- Default routing can be considered a special type of static routing. The difference between a normal static route and a default route is that a default route is used to send packets destined to any unknown destination to a single next hop address.

Exterior Gateway protocol

- Exterior Gateway Protocol (EGP) is used to exchange net-reachability information between Internet gateways belonging to the same or different autonomous systems.
- EGP was developed by Bolt, Beranek and Newman in the early 1980s. It was first described in RFC 827 and formally specified in RFC 904 (1984).

Functions of EGP

- Establish a set of neighbors
- Check status of neighbors(if they are alive/reachable)
- Inform neighbors the networks that reachable within their AS's

BGP

- Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different AS.
- The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router. BGP's main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems' graph based on the information exchanged between BGP routers.

Interior Gateway Protocol

- An interior gateway protocol (IGP) is a type of protocol used for exchanging routing information between gateways (commonly routers) within an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to route network-layer protocols like IP.
- Interior gateway protocols can be divided into two categories: distance-vector routing protocols and link-state routing protocols. Specific examples of IGPs include Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Intermediate System to Intermediate System (IS-IS) and Enhanced Interior Gateway Routing Protocol (EIGRP).

Distance-vector routing protocols

- Routers running distance-vector routing protocols periodically broadcast routing and reachability information from all active interfaces. They also receive the same information from their neighbors on their active interfaces.
- Distance-vector protocols use timers to broadcast routing information. Once their periodic timer expires, they broadcast their routing information from all active interfaces, no matter whether the routing information has changed since the previous broadcast or not.

RIP

- RIP is used in both LAN and WAN Networks. It also runs on the Application layer of the OSI model. The full form of RIP is the Routing Information Protocol.
- The original version or RIPv1 helps you determine network paths based on the IP destination and the hop count journey. RIPv1 also interacts with the network by broadcasting its IP table to all routers connected with the network.
- RIPv2 is a little more sophisticated as it sends its routing table on to a multicast address.

IGRP

- Interior Gateway Routing Protocol is a distance vector routing protocol developed by Cisco systems for routing multiple protocols across small and medium sized Cisco networks.
- IGRP will route IP, IPX, Decent and AppleTalk which makes it very versatile for clients running many different protocols. It is somewhat more scalable than RIP since it supports a hop count of 100, only advertises every 90 seconds and uses a composite of five different metrics to select a best path destination.

EIGPR

- Enhanced Interior Gateway Routing Protocol is a hybrid routing protocol developed by Cisco systems for routing many protocols across an enterprise Cisco network.
- It has characteristics of both distance vector routing protocols and link state routing protocols. It is proprietary which requires that you use Cisco routers.
- There is the option to load balance traffic across equal or unequal metric cost paths.

Link-state routing protocols

- Unlike distance-vector routing protocols, the link-state routing protocols do not share routing and reachability information with anyone. Routers running link-state protocols share routing information only with neighbors. To discover neighbors, link-state protocols use a special protocol known as the hello protocol.
- After discovering all neighbors, the link-state protocols create three separate tables. One of these tables keeps track of directly attached neighbors, one determines the topology of the entire internetwork, and one is used as the routing table.
- From all available routes, to select the best route for each destination of the network, the link-state protocols use an algorithm called the Shortest Path First (SPF) algorithm.

OSPF

- Open Shortest Path First is a true link state protocol developed as an open standard for routing IP across large multi-vendor networks. A link state protocol will send link state advertisements to all connected neighbors of the same area to communicate route information. Each OSPF enabled router, when started, will send hello packets to all directly connected OSPF routers.
- The hello packets contain information such as router timers, router ID and subnet mask. If the routers agree on the information they become OSPF neighbors. Once routers become neighbors they establish adjacencies by exchanging link state databases.

IS IS

- IS-IS is a link-state routing protocol, which means that the routers exchange topology information with their nearest neighbors.
- The topology information is flooded throughout the Autonomous Systems(AS), so that every router within the AS has a complete picture of the topology of the AS.
- This picture is then used to calculate end-to-end paths through the AS
- In a link-state routing protocol, the next hop address to which data is forwarded is determined by choosing the best end-to-end path to the eventual destination.