Chapter 15

access point (AP): The role of AP is gluing two different environments together (one wired and one wireless)

wireless Characteristics:

- **Attenuation:** The strength of electromagnetic signals decreases rapidly because the signal disperses in all directions.
- **Interference:** A receiver may receive signals not only from the intended sender, but also from other senders if they are using the same frequency band.
- **Multipath Propagation:** A receiver may receive more than one signal from the same sender because electromagnetic waves can be reflected back from obstacles such as walls, the ground, or objects. The result is that the receiver receives some signals at different phases (because they travel different paths). This makes the signal less recognizable.
- **Error:** we think about the error level as the measurement of signal-to-noise ratio (SNR)
    - If SNR is high signal is stronger than the noise->able to convert signal to actual data.
    - If SNR is low signal is corrupted by the noise data cannot be recovered

CSMA/CD algorithm used in standard ethernet does not work in wireless LANs for three reasons- instead (CSMA/CA) is used for wireless LANs:

1. **Wireless hosts do not have enough power** to send and receive at the same time, in order to detect collision.
2. **The hidden station problem** prevents collision detection. station may not be aware of another station's transmission due to some obstacles or range problems, collision may occur but not be detected
3. **The distance between stations can be great.** Station at one end can't hear a collision at another end.

IEEE has defined the specifications for a wireless LAN, called **IEEE 802.11**, which covers the physical and data-link layers. It is sometimes called **wireless Ethernet.**

IEEE 802.11 standard defines two kinds of services:

- **The basic service set (BSS)**
    - BSS without an AP
    - A BSS with an AP
- **the extended service set (ESS):** is made up of two or more BSSs with APs

IEEE 802.11 also defines 3 types of stations based on their mobility in a wireless LAN:

1. **No-transition mobility:** is either stationary (not moving) or moving only inside a BSS:
2. **BSS-transition mobility:** can move from one BSS to another, but the movement is confined inside one ESS
3. **ESS-transition mobility:** can move from one ESS to another.

❖ **IEEE 802.11** does **not guarantee** that communication is **continuous during the move**

❖ **Figure 15.7: CSMA/CA and NAV** مهم جدا

IEEE 802.11 defines two MAC sublayers protocols:

❖ **Distributed coordination function (DCF)**

❖ **Point coordination function (PCF)**

What is the solution to the Hidden-Station Problem?

use the **handshake** frames à B sends RTS (the request to send) to A. B replies with CTS (clear to send) frame that contains the duration of data transmission from B to A, which will reach C.

What happens if there is a collision during Handshaking?

If there is a collision during Handshaking period -time when RTS or CTS control frames are in transition-, sender assumes there has been a collision if it has not received a CTS frame from receiver. The backoff strategy is employed, and the sender again.

A wireless LAN defined by IEEE 802.11 has three categories of frames:

❖ **Data Frames**

❖ **Management Frames**

❖ **Control Frames**

Values of subfields in control frames:

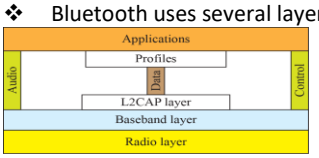
Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

The IEEE 802.11 addressing mechanism: (ايمن 23 سلايد)

Exposed station problem: 28 مهم سلايد

Describe Bluetooth with architecture.

- Bluetooth is a wireless LAN technology designed to connect devices of different functions when they are at a short distance from each other.
- A Bluetooth LAN is an ad hoc network. The devices, sometimes called gadgets, find each other and make a network called a piconet.
- Bluetooth uses several layers that do not exactly match those of the Internet model.



Bluetooth defines two types of networks:

- **Piconet:** can have up to eight stations, one called the primary; the rest are called secondaries. All the secondary stations synchronize their clocks and hopping sequence with the primary. piconet can have only one primary station. The communication between the primary and secondary stations can be one-to-one or one-to-many.
- **Scatternet:** A secondary station in one piconet can be the primary in another piconet. This station can receive messages from the primary in the first piconet and, acting as a primary, deliver them to secondary in the second piconet.

Bluetooth Layers:

- **The Logical Link Control and Adaptation Protocol (L2CAP):** is roughly equivalent to the LLC sublayer in LANs. It is used for data exchange on an ACL link;
- **The baseband layer** is roughly equivalent to the MAC sublayer in LANs. The access method is TDMA
- **Radio layer:** Equivalent to the physical layer of the Internet model

TDD-TDMA (time-division duplex TDMA): which is half-duplex -the sender and receiver send and receive data, but not at the same time-, the communication for each direction uses different hops, similar to walkie-talkies. We have 2 cases in TDMA

- **Single-Secondary Communication (42 الرسمة مهمه سلايد)**
- **Multiple-Secondary Communication**

Chapter 17

Write a short note about connecting devices

Hosts and networks do not normally operate in isolation. We use connecting devices to connect hosts together to make a network or to connect networks together to make an internet. Connecting devices can operate in different layers of the Internet model.

Three categories of connecting devices:

- **Hubs:** device operate in the physical layer. (Figure 17.2)
- **Link-layer switches:** operate in the physical and the data-link layers (Figure 17.3)
- **Routers:** operate in the first three layers.

Figure 17.5: Loop problem in a learning switch

Spanning Tree Algorithm Figure 17.6: Figure 17.7: Figure 17.8:

In the spanning tree system, there is only one path from any LAN to any other LAN (No loops)

three major differences between a router and a repeater or a switch:

1. A router has a physical and logical (IP) address for each of its interfaces.
2. A router acts only on those packets in which the link-layer destination address matches the address of the interface at which the packet arrives.
3. A router changes the source and distention link-layer addresses of the packet (source and destination MAC addresses) when it forwards the packet.

VIRTUAL LANS : A station is considered part of a LAN if it physically belongs to that LAN. The criterion of membership is geographic.

What characteristic can be used to group stations in a VLAN?

- **Interface Numbers**
- **MAC Addresses**
- **IP Addresses**
- **Multicast IP Addresses**
- **Combination**

How are the stations grouped into different VLANs? Stations are configured in one of three ways

- **Manual Configuration:** administrator types the port numbers, the IP addresses, or other characteristics.
- **Automatic Configuration:** the stations are automatically connected or disconnected from a VLAN using criteria defined by the administrator.

- **Semiautomatic Configuration:** A semiautomatic configuration is somewhere between a manual configuration and an automatic configuration. Usually, the initializing is done manually, with migrations done automatically.

Communication between Switches: Three methods have been devised for this purpose:

- **Table Maintenance**: when a station sends a broadcast frame to its group members, the switch creates an entry in a table and records station membership. The switches send their tables to one another periodically for updating.
- **Frame Tagging:** when a frame is traveling between switches, an extra header is added to the MAC frame to define the destination VLAN.
- **Time-Division Multiplexing (TDM)**: The connection (trunk) between switches is divided into time-shared channels. For example, if the total number of VLANs in a backbone is five, each trunk is divided into five channels. The traffic destined for VLAN 1 travels in channel 1, and so on.

Advantages of Switches over a hub: Collision Elimination, Connecting Heterogenous Devices

advantages to using VLANs:

- **Cost and Time Reduction**
- **Creating Virtual Work Groups**
- **Security**

Chapter 18

Packetizing: encapsulating the payload in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.

Routing: This means that there is more than one route from the source to the destination, the network layer is responsible for finding the best one. This is done by running some routing protocols to help the routers coordinate their knowledge about the neighborhood and to come up with consistent tables to be used when a packet arrives.

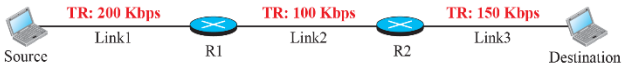
Forwarding: The action applied by each router when a packet arrives at one of its interfaces. A router normally use a decision-making table for applying this action. It is called (the forwarding table) or (the routing table). Figure 18.2

packet-switched approach:

- **Datagram Approach-Connectionless Service:** the packets in a message may or may not travel the same path to their destination, A packet belonging to a message may be followed by a packet belonging to the same message or to a different message. A packet may be followed by a packet coming from the same or from a different source.
  - The switches in this type of network are called routers.
  - The packet header has a source and destination addresses. The destination address defines where it should go and the router routes the packet based only on the destination address.
  - The source address defines where the packet comes from. It may be used to send an error message to the source if the packet is discarded.
  - **Figure 18.4: Forwarding process in a router when used in a connectionless network** (مهم جدا)
- **Virtual-Circuit Approach-Connection-Oriented Service**:
  - there is a relationship between all packets belonging to a message
  - Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams
  - After connection setup, the datagrams can all follow the same path.
  - In this type of service, not only must the packet contain the source and destination addresses, it must also contain a flow label, a virtual circuit identifier that defines the virtual path the packet should follow.
  - The forwarding decision is based on the value of the label.

NETWORK-LAYER PERFORMANCE:

- **Delay: The delays in a network can be divided into four types:**
  - Transmission delay.
  - Propagation delay.
  - Processing delay.
  - Queuing delay.



a. A path through three links

- **Throughput**: the number of bits passing through the point in a second, which is actually the transmission rate of data at that point. In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate. Throughput = minimum $\{TR_1, TR_2, \ldots TR_n\}$.
- **Packet Loss:** A router receives a packet while processing another one, store it in the input buffer waiting, but this buffer has a limited size, when it is full, the next packet is dropped.
  - The effect of packet loss on the Internet network layer is that the packet needs to be resent, which in turn may create overflow and cause more packet loss.
- **Congestion Control:** mechanisms are divided into 2 categories:

- open-loop congestion control (prevention) :List of policies are applied to prevent Congestion, handled by either the source or the destination, Retransmission Policy, Window Policy, Acknowledgment Policy, Discarding Policy and Admission Policy.
- closed-loop congestion control (removal): List of mechanisms are applied to try to alleviate congestion after it happens, Backpressure protocol, Choke Packet, Implicit Signaling and Explicit Signaling

A choke packet: is a packet sent by a node to the source to inform it of congestion.

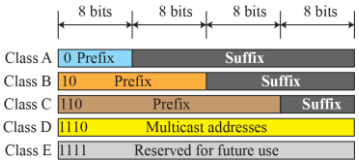
IPv4 ADDRESSES:

- An IPv4 address is a **32-bit** address that **uniquely** and **universally** defines the connection of a host or a router to the Internet.
- The IP address is the **address of the connection, not the host or the router**. It **changes** when moving to different network.
- The IP address unique, means defines only one connection to the internet
- The IP address universal, means that the addressing system must be accepted by any host that wants to be connected to the Internet.
- The address space is **2b** because each bit can have two different values (0 or 1).
- IPv4 uses 32-bit addresses, which means that the address space **is 232 or 4,294,967,296 (more than four billion).**

Hierarchy in Addressing:

1. The first part of the address called the prefix, defines the network
2. The second part of the address, called the suffix, defines the node

Classful Addressing:



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Subnetting: More levels of hierarchy can be created using subnetting. An organization (or an ISP) that is granted a range of addresses may divide the range into several subranges and assign each subrange to a subnetwork (or subnet).

Designing Subnets

1. The number of addresses in each subnetwork should be a power of 2.
2. The prefix length for each subnetwork should be found using the following formula:
   a. first address = (prefix in decimal) × 232 − n = (prefix in decimal) × N
3. The starting address in each subnetwork should be divisible by the number of addresses in that subnetwork. This can be achieved if we first assign addresses to larger subnetworks.

Address Aggregation: One of the advantages of the CIDR (classless interdomain routing) strategy is address aggregation (sometimes called address summarization or route summarization). When blocks of addresses are combined to create a larger block, routing can be done based on the prefix of the larger block.

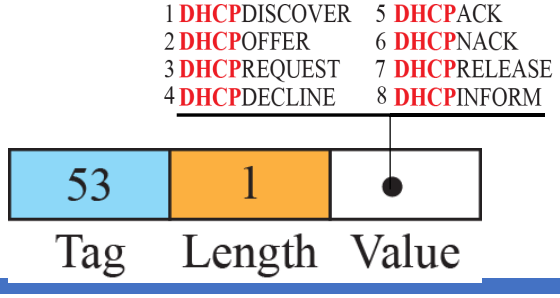
Figure 18.20: Slash notation (CIDR) -classless interdomain routing- (مهم جدا)

DHCP (Dynamic Host Configuration Protocol): After a block of addresses are assigned to an organization, the network administration can manually assign addresses to the individual hosts or routers. Or automatically using DHCP.

- DHCP is an application-layer program, using the client-server paradigm, that actually helps TCP/IP at the network layer.
- DHCP sometimes called plug - and - play protocol, A network manager can configure DHCP to assign permanent, temporary IP addresses to the host and routers.
- DHCP can be used to provide pieces of information to the host as: the computer address, the prefix, the address of a router, and the IP address of a name server.
- DHCP is a client-server protocol in which the client sends a request message and the server returns a response message.

Note that the client can use the IP address only when it is in the **BOUND, RENEWING, or REBINDING state.**

DHCP Option format: An option is composed of **three fields: a 1-byte tag field, a 1-byte length field, and a variable-length value field**. There are several tag fields that are mostly used by vendors. If the **tag field is 53, the** value field defines one of the **8 message types (مهم جدا)**



Network Address Translation (NAT): The technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world mapping between private and universal addresses, and support virtual private networks-. Using NAT-capable router that runs NAT software.
How the NAT-router knows the destination address for incoming packet?
can be done using a translation table or Using a Pool of IP Addresses, or Using Both IP Addresses and Port Addresses.
FORWARDING OF IP PACKETS: forwarding means to place the packet in its route to its destination. Means delivering packet to next hub.
MPLS routers, which can behave like a router and a switch.:

- **like a router:** it can forward the packet based on the destination address.
- **like a switch:** it can forward a packet based on the label.

Chapter 19

NETWORK-LAYER PROTOCOLS:

- **Internet Protocol version 4 (IPv4):** **Is responsible for packetizing, forwarding, and delivery of a packet**
- **ICMPv4 (Internet Control Message Protocol version 4):** helps IPv4 to handle some errors that may occur in delivery. ICMP messages are divided into two broad categories:
  - Error-reporting messages
  - Query messages
- **IGMP (Internet Group Management Protocol):** help IPv4 in multicasting.
- **ARP (Address Resolution Protocol):** used in address mapping (mapping network-layer addresses to link-layer addresses).

Datagram Format:

- Packets used by the IP are called datagrams.
- the IPv4 datagram format. A datagram is a variable - length packet consisting of two parts : header and payload (data)
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery
- It is customary in TCP/IP to show the header in 4 – byte
- Total Length: (header plus data) in bytes, helps receiving device to know when the packet has completely arrived Length of data = total length − (HLEN) × 4,

Fragmentation: A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled.

- When a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size of the frame payload. The value of the MTU differs from one physical network protocol to another.

Security issues of IP protocol:

- **packet sniffing**
- **packet modification**
- **IP spoofing**

IPSec: The IP packets today can be protected from the previously mentioned attacks using a protocol called IPSec (IP Security), where it creates a connection-oriented service between two entities to exchange IP packets.
Debugging Tools:

- **Ping:** use the ping program to find if a host is alive and responding. The source host sends ICMP echo-request messages.
- **Traceroute or Tracert**: The traceroute program in UNIX or tracert in Windows can be used to trace the path of a packet from a source to the destination. It can find the IP addresses of all the routers that are visited along the path.

MOBILE IP: the extension of IP protocol that allows mobile computers to be connected to the Internet at any location where the connection is possible.
Mobile IP has two addresses for a mobile host:

1. **home address:** permanent. it associates the host with its home network
2. **Care-of address:** Changes as the mobile host moves from one network to another. it is associated with the foreign network. When a mobile host visits a foreign network, it receives its care-of address during the agent discovery and registration phase

Agents: To make the change of address transparent to the rest of the Internet requires a:

- **The home agent:** is usually a router attached to the home network of the mobile host. When a remote host sends a packet to the mobile host. The home agent receives the packet and sends it to the foreign agent.
- **The foreign agent:** is usually a router attached to the foreign network. It receives packets sent by the home agent and deliver them to the mobile host.

Phases when communicate with a remote host:

1. **Agent discovery.**
2. **Registration.**
3. **Data transfer.**

Inefficiency in Mobile IP:

- **Double Crossing:** occurs when a remote host communicates with a mobile host that has moved to the same network (or site) as the remote host.
- **Triangle Routing:** Occurs when the remote host communicates with a mobile host that is not attached to the same network (or site) as the mobile host.
- **Solution** : remote host can **bind** care-of address to home address of a mobile host. E.g. home agent sends an **update binding packet** to remote host so that future packets to home host sent to care-of address. The remote host can keep this information in a cache.

Chapter 20

Least-Cost Routing: the source router chooses a route to the destination router in such a way that the total cost for the route is the least cost among all possible routes.

ROUTING ALGORITHMS:

- **Distance-Vector Routing:** The distance-vector (DV) routing uses the goal.
  - each node creates is its own least-cost tree with the rudimentary information it has about its immediate neighbors.
  - The incomplete trees are exchanged between immediate neighbors to make the trees more and more complete and to represent the whole internet.
  - We can say that in distance-vector routing, a router continuously tells all of its neighbors what it knows about the whole internet
  - **Use Routing Information Protocol (RIP)**
- **Link-State Routing:** A routing algorithm that directly follows our discussion for creating least-cost trees and forwarding tables is link-state (LS) routing.
  - This method uses the term link-state to define the characteristic of a link (an edge) that represents a network in the internet.
  - In this algorithm the cost associated with an edge defines the state of the link. Links with lower costs are preferred to links with higher costs;
  - if the cost of a link is infinity, it means that the link does not exist or has been broken.
- **Figure 20.16: Forwarding tables for figure 20.15** - example 20.1 (مهم جدا)
- **RIP Implementation:** RIP uses service of UDP on well-known port number 520.
  - **Use Open Shortest Path First (OSPF)**
- **Path-Vector Routing:** allow a sender to apply specific policies to the route a packet may take or wants to prevent its packets from going through.
- **Figure 20.19: Metric in OSPF (مهم جدا)**
  - **Use Border Gateway Protocol (BGP)**

Compare link-state routing with distance-vector routing:

- **In the distance-vector routing algorithm,** each router tells its neighbors what it knows about the whole internet;
- **in the link-state routing algorithm,** each router tells the whole internet what it knows about its neighbors

UNICAST ROUTING PROTOCOLS:

1. **Routing Information Protocol (RIP), based on the distance-vector algorithm.**
   - RIP is normally used in small Autonomous systems
2. **Open Shortest Path First (OSPF), based on the link-state algorithm.**
   - **OSPF is an open protocol, which means that the specification is a public document.**
3. **Border Gateway Protocol (BGP), based on the path-vector algorithm.**

❖ **Comparing** the forwarding tables for the **OSPF** and **RIP** in the **same** AS: The only **difference is the cost values.**

Chapter 23

TRANSPORT-LAYER: is located between the application layer and the network layer. It provides a process-to-process communication between two application layers, one at the local host and the other at the remote host. Communication is provided using a logical connection. **providing services to the application layer; it receives services from the network layer.**

For communication, we must define:

1. **The local host:** defined using IP addresses.
2. **Remote host:** defined using IP addresses.
3. **Local process:** Defined using port numbers.
4. **Remote process:** Defined using port numbers.

Port numbers

- **In TCP/IP:** The port numbers are integers between 0 and 65,535 (16 bits).
- **The client program** defines itself with a port number, called the ephemeral port number.
- **The server process:** TCP/IP has decided to use universal port numbers for servers; these are called well-known port numbers.

port numbers ranges:

- **Well-known ports:** The ports ranging from 0 to 1023 are assigned and controlled by ICANN.
- **Registered ports:** The ports ranging from 1024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.
- **Dynamic ports (or private):** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers.

Socket address: The combination of an IP address and a port number.

Encapsulation and Decapsulation:

- **Encapsulation At source,** transport layer receives data and adds its header. Then, encapsulates it in user datagrams, segments, or packets(general name), depending on protocol used.
- **Decapsulation at receiver,** message arrives at destination transport layer, decapsulates it the is drops header and delivers message to process running at application layer with sender socket address in case it needs to respond to message received.
- **Figure 23.8: (مهم جدا)**

Multiplexing and Demultiplexing:

- **Multiplexing** (many to one): an entity accepts items from more than one source, happens at source
- **Demultiplexing** (one to many): an entity delivers items to more than one source, happens at destination.

Flow Control: items produced faster than consumed, consumer overwhelmed and need to discard items. Items dilevered in 2 ways

- **Pushing:** sender delivers produced items without a request from consumer, need flow control to prevent discarding items
- **Pulling:** producer delivers items after consumer request, No flow control

Error Control (EC): Because network layer (IP) is unreliable, transport-layer has error control involves only sending and receiving transport-layers. EC is responsible for:

- 1. Detecting and discarding corrupted packets.
- 2. Keeping track of lost/discarded packets and resending them.
- 3. Recognizing duplicate packets and discarding them.
- 4. Buffering out-of-order packets until the missing packets arrive.

Connection transport-layer protocol, like a network-layer protocol, can provide two types of services:

- **connectionless:** independency between packets, (at network-layer mean different paths for different datagrams belonging to same message).
- **Connectionless Service:** no flow control, error control, congestion control implemented in a connectionless service. Source process divide message into chunks deliver them to transport layer one by one that treats each chunk as a single unit without any relation between chunks, which may arrive at destination lost or out of order.
- **connection-oriented:** means dependency involves only the 2 hosts, (at network-layer means a coordination between two end hosts and all routers in between).
- **Connection-Oriented Service:** flow control, error control, congestion control are used. client and server establish logical connection, then exchange data, finally connection needs to be torn down.
- **Figure 23.15: Connection-oriented service(مهم جدا)**

TRANSPORT-LAYER PROTOCOLS

Figure 23.18: FSMs for the simple protocol **مهم جدا**

- **Simple Protocol:** a simple connectionless protocol with neither flow nor error control. We assume that the receiver can immediately handle any packet it receives. In other words, the receiver can never be overwhelmed with incoming packets.
- **Stop-and-Wait Protocol:** a connection-oriented protocol called the Stop-and-Wait protocol, which uses both flow and error control. Both the sender and the receiver use a sliding window of size 23.
  - The sender sends one packet at a time and waits for an acknowledgment before sending the next one.
  - To detect corrupted packets, we need to add a checksum to each data packet. When a packet arrives at the receiver site, it is checked. If its checksum is incorrect, the packet is corrupted and silently discarded.
- **Go-Back-N Protocol (GBN):** several packets can be sent before receiving acknowledgments, but the receiver can only buffer one packet. We keep a copy of sent packets until acknowledgments arrive.
  - The Go-Back-N protocol simplifies the process at the receiver. The receiver keeps track of only one variable, and there is no need to buffer out-of-order packets; they are simply discarded
- **Selective-Repeat Protocol:** protocol resends only selective packets (lost one only).
- **Figure 23.33: Receive window for Selective-Repeat protocol مهم جدا**

❖ **Example 23.9 مهم جدا**

- The Go - Back - N protocol simplifies the process at the receiver. • The receiver keeps track of only one variable, and there is no need to buffer out - of order packets; they are simply discarded .
- this protocol is inefficient if the underlying network protocol loses a lot of packets.
- Each time a single packet is lost or corrupted, the sender resends all outstanding packets, even though some of these packets may have been received safe and sound but out of order

❖ **Bidirectional Protocols:** All 4 protocols discussed earlier are unidirectional: data packets flow in only one direction and acknowledgments travel in the other direction.

- In real life, data packets and acknowledgments are flow in both directions: from client to server and from server to client.
- A technique called piggybacking used to improve efficiency of bidirectional protocols, When a packet is carrying data from A to B, it can also carry acknowledgment feedback about arrived packets from B.

What is the improvement done in Go-Back-N ARQ protocol as compared to the Stop-and-Wait ARQ protocol?

Go back-N ARQ protocol is used to improve the efficiency of transmission of stop-and- wait ARQ protocol by sending multi frame while waiting for acknowledgement in order to utilize the bandwidth channel. The way Stop-and-Wait ARQ Protocol work is not fully utilize the bandwidth channel.

Chapter 24

- **User Datagram Protocol (UDP)** unreliable connectionless transport-layer protocol, used for its simplicity and efficiency in applications where error control can be provided by application-layer process.
  - **Transmission Control Protocol (TCP)** reliable connection-oriented protocol that can be used in any application where reliability is important. TCP uses a combination of GBN and SR protocols to provide reliability
    - TCP uses checksum (for error detection), retransmission of lost or corrupted packets, cumulative and selective acknowledgments, and timers.
  - **Stream Control Transmission Protocol (SCTP)** new transport-layer protocol that combines features of UDP and TCP. in an effort to create a protocol for multimedia communication.

If UDP is so powerless, why would a process want to use it?

With the disadvantages come some advantages. UDP is a very simple protocol using a minimum of overhead.

Segments: At transport-layer, TCP groups number of bytes into packet called a segment, then deliver it to network-layer that encapsulates it in IP datagram for transmission.

Numbering System: TCP has 2 fields in its segment header: sequence number and acknowledgment number.

These 2 fields refer to byte number and not a segment number, The bytes of data being transferred in each connection are numbered by TCP, numbering starts with an arbitrarily generated number.

Byte Number: When TCP receives bytes of data from a process, TCP stores them in the sending buffer and numbers them (chooses an arbitrary number between 0 and 232 − 1 for the number of the first byte).

Sequence Number: TCP assigns a sequence number to each segment that is being sent:

1. The sequence number of the first segment is the ISN (initial sequence number), which is a random number.
2. The sequence number of any other segment is the sequence number of the previous segment plus the number of bytes carried by the previous segment.

Acknowledgment Number: the acknowledgment number defines the number of the next byte that the party expects to receive.

The acknowledgment number is cumulative: which means that the party takes the number of the last byte that it has received, adds 1 to it, and announces this sum as the acknowledgment number. For example, if a party uses 5643 as an acknowledgment number, it has received all bytes from the beginning up to 5642.

how TCP, which uses the services of IP, a connectionless protocol, can be connection-oriented?

The point is that a TCP connection is logical, not physical. TCP operates at a higher level. TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted. IP is unaware of this retransmission. If a segment arrives out of order, TCP holds it until the missing segments arrive; IP is unaware of this reordering.

In TCP, connection-oriented transmission requires three phases:

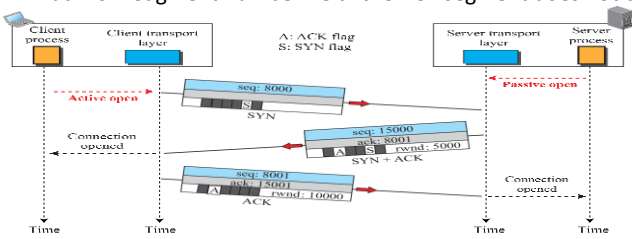
connection establishment, data transfer, and connection termination.

Connection establishment using three-way handshaking: TCP can now start the three-way handshaking process.

1. The client sends a control segment that carries no data called SYN segment for synchronization of sequence numbers→ only the SYN flag is set→ The client chooses a random number as the initial sequence number (ISN) and sends this number to the server.
2. The server sends SYN + ACK segment with two flag bits set as: SYN and ACK:
   a. →SYN to initialize a sequence number for numbering the bytes sent from the server to the client.

b. →ACK to acknowledges the receipt of the client SYN segment by displaying the next sequence number it expects to receive from the client.
c. →The segment also define the receive window size, rwnd (to be used by the client).
d. →the segment has a sequence number because it needs to be acknowledged.

3. The client sends an ACK segment to acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. the ACK segment does not consume any sequence numbers unless it data from the client.



Error control in TCP is achieved through the use of three simple tools:

1. **Checksum:** used to check for a corrupted segment.
2. **Acknowledgment:** to confirm the receipt of data segments. (cumulative & selective)
3. **Time-out.**

Four-way handshaking:

1. client sends 1st packet(contains INIT chunk.), verification tag (VT) of packet is 0 (not yet defined fro this direction (client to server)). initiation tag used for packets from other direction (server to client), initial TSN for this direction and advertises a value for rwnd. Note that no other chunks can be sent with the first packet.
2. server sends 2nd packet(contains an INIT ACK chunk), verification tag =value of initial tag in INIT chunk, This chunk initiate tag: used in other direction, defines the initial TSN, for data flow from server to client, and sets the server's rwnd, a cookie defines state of server at this moment.
3. client sends 3rd packet includes simple (COOKIE ECHO chunk), it echoes, without change, the cookie sent by server. SCTP allows inclusion of data chunks in this packet.
4. server sends 4th packet, contains (COOKIE ACK chunk), acknowledges receipt of COOKIE ECHO chunk. SCTP allows inclusion of data chunks with this packet.

Chapter 26

Hypertext Transfer Protocol (HTTP) is used to define how client-server programs can be written to retrieve web pages from Web. An HTTP client sends a request; an HTTP server returns a response. server uses port number 80; client uses a temporary port number. HTTP uses the services of TCP(connection-oriented and reliable protocol).

No persistent versus Persistent Connections

web page documents that uses hypertext may require several requests and responses, If they are located on different servers, so we need to create a new TCP connection for retrieving each object. But if the documents are on the same server, **methods** used are:

- **no persistent connection:** to retrieve each object using a new TCP connection, used by HTTP. Client request file, server sends respond and close connection
  - If there is N links to N files then connection opened and closed N+1 times, which impose overhead on server and N+1 buffers needed.
- **persistent connection:** to make a TCP connection and retrieve them all. Server leaves connection open for more requests, connection is closed if client request or after time-out.
  - Only one set of buffers and variables needs to be set for connection at each site

Uniform Resource Locator (URL): We need protocol type and 3 identifiers to define a web page: host, port, and path.

- **Protocol**: client-server application needed to access web page e.g. HTTP, FTP
- **Host**: can be IP address of server(e.g. 64.23.56.17)or unique name given to server(e.g. forouzan.com)
- **Port**: 16-bit integer, (e.g. HTTP = 80 port number)
- **Path**: identifies location and name of file in underlying operating system (lists directories from top to bottom, followed by file name)

Cookies: Needed by server to remember some information about the clients, note: a cookie made by the server and eaten by the server

Web Caching: Proxy Servers: A proxy server is a computer that keeps copies of responses to recent requests.

File Transfer Protocol (FTP) is the standard protocol provided by TCP/IP for copying a file from one host to another. FTP has solved some problems regarding file transfer, we can use HTTP, but FTP is a better choice to transfer large files or to transfer files using different formats.

FTP Connections:

- **The control connection** remains connected during entire FTP session. (**port 21)**
- **The data connection** is opened and closed for each file transfer activity. (**port 20)**

SSL-FTP: Secure Socket Layer between the FTP application layer and the TCP layer

Simple Mail Transfer Protocol (SMTP) a push protocol, MTA client and server in the Internet, SMTP simply defines how commands and responses must be sent between an MTA client and MTA server.

Post Office Protocol, version 3 (POP3): a pull protocol, Mail access starts with the client when the user needs to download its e-mail from the mailbox on the mail server. The client opens a connection to the server on TCP port 110. It then sends its user name and password to access the mailbox. The user can then list and retrieve the mail messages, one by one.
IMAP4 Internet Message Access Protocol: provide additional features(e.g. user can organize mail on server; hierarchy of mailboxes in a folder…etc).

Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client MTA to be sent through the Internet. The message at the receiving site is transformed back to the original data.

E-Mail Security protocols:
- **Pretty Good Privacy (PGP)**
- **Secure/Multipurpose Internet Mail Extensions (S/MIME)**

TELNET: generic client/server programs (called remote logging) that allow a user on the client site to log into the computer at the server site and use the services available there. Network administrators often use TELNET for diagnostic and debugging purposes.

SECURE SHELL (SSH): Although Secure Shell (SSH) is a secure application program that can be used today for several purposes such as remote logging and file transfer, it was originally designed to replace TELNET.

SSH is an application-layer protocol with three components:
- **(SSH-TRANS):** SSH Transport-Layer Protocol. SSH first uses this protocol to creates a secured channel on top of TCP
- **(SSH-AUTH):** SSH Authentication Protocol. after secure connection establishment, SSH call another procedure to authenticate client for server, Client sends a request message, server responds with success/fail message
- **(SSH-CONN):** SSH Connection Protocol. takes secure channel established by 2 previous protocols and lets client create multiple logical channels over it(provide multiplexing), Each channel can be used for a different purpose, such as remote logging, file transfer, and so on.

DOMAIN NAME SYSTEM (DNS): directory system that can map a name to an address, DNS is client-server application

A domain is a subtree of the domain name space. The name of the domain is the name of the node at top of subtree.

- **Recursive resolution:** DNS server, who received your query will do all the job of fetching the answer, and giving it back to you. During this process, the DNS server might also query other DNS server's in the internet on your behalf, for the answer.
- **iterative or Non-recursive query:** the name server, will not go and fetch the complete answer for your query, but will give back a referral to other DNS server's, which might have the answer. In our previous

Caching: Each time a server receives a query for a name that is not in its domain, it needs to search its database for a server IP address or request form another server, then it cache this address to cache memory, If the same or another client asks for same mapping, resolve problem but inform client that response is coming from cache memory and not from an authoritative source, the server marks the response as unauthoritative

Dynamic Domain Name System (DDNS): DNS master file updated dynamically. In DDNS, the binding information between name and address is sent by DHCP to a primary DNS server.
The primary server updates zone. The secondary servers are notified either actively(by sending message notify change) or passively(secondary check for any changes).

To protect DNS, IETF has devised a technology named DNS Security (DNSSEC) that provides message origin authentication and message integrity using a security service called digital signature

how DNS can be attacked?

1. The attacker may read the response of a DNS server to find the nature or names of sites the user mostly accesses. (find the user's profile).
2. The attacker may intercept the response of a DNS server and change it to a new response to direct the user to the site or domain the attacker wishes the user to access.
3. The attacker may flood the DNS server to overwhelm it or eventually crash it.

Describe the GIGABIT Ethernet.

The need for an even higher data rate resulted in the design of the Gigabit Ethernet Protocol (1000 Mbps). The IEEE committee calls it the Standard 802.3z. The goals of the Gigabit Ethernet were to upgrade the data rate to 1Gbps.
A main consideration in the evolution of Ethernet was to keep the MAC sublayer untouched. However, to achieve a data rate of 1Gbps, this was no longer possible. Gigabit Ethernet has two distinctive approaches for medium access: half-duplex and full-duplex. Almost all implementations of Gigabit Ethernet follow the full-duplex approach. The physical layer in Gigabit Ethernet is more complicated than that in Standard or Fast Ethernet.

Explain the use of cladding in fiber-optic?

Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.

Discuss about the Virtual LAN with the membership and configuration.

We can roughly define a virtual local area network (VLAN) as a local area network configured by software, not by physical wiring. A station is considered part of a LAN if it physically belongs to that LAN. Different characteristic can be used to group stations in a VLAN. Vendors use characteristics such as interface numbers, port numbers, MAC addresses, IP addresses, IP multicast addresses, or a combination of two or more of these.
The stations grouped into different VLANs and stations are configured in one of three ways: manually, semi-automatically, and automatically. In a multi-switched backbone, each switch must know not only which station belongs to which VLAN, but also the membership of stations connected to other switches. For example, switch A must know the membership status of stations connected to switch B, and switch B must know the same about switch A. Three methods have been devised for this purpose: table maintenance, frame tagging, and time-division multiplexing.

Differentiate the term Periodic and Nonperiodic signal.

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time. Both analog and digital signals.

Differentiate between FDMA and TDMA

FDMA: Bandwidth is divided and shared in frequency bands. Bandpass filter is used to confine the frequencies.
TDMA: Bandwidth is divided and shared in Time Slots. Each station transmits in allocated time slot.

تم بحمد الله

دعواتكم لكل من ساهم في اعداد هذا الملخص

بالتوفيق للجميع