Chapter 3:

Data Link Layer Design Issues: Services Provided to the Network Layer, Framing, Error Control, Flow Control

Functions of the Data Link Layer: Provide service interface to the network layer, Dealing with transmission errors, Regulating data flow, Slow receivers not swamped by fast senders

- To accomplish these goals, the data link layer takes the packets from the, network layer and encapsulates them into frames for transmission

Services Provided to Network Layer: The principle service is to Transfer data from the network layer on source machine to the network

Services Provided to Network Layer Three typical services, Unacknowledged connectionless service.Acknowledged (Ack.) connectionless service.Acknowledged connection-oriented service.

Unacknowledged connectionless service.The source sends independent frames to the destination without Ack.No logic connection is established beforehand or released afterward.If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover it in the data link layer. This class of service is appropriate when the error rate is very low and the recovery is left to the higher layers.Most LANs use this servi layer on the destination machine.

Acknowledged connectionless service: No logic connection, but each frame is acknowledged.Useful for unreliable channels, such as wireless systems.Tradeoff between Ack. in data link layer and network layer.Frame has a max. length imposed by the hardware. E.g., a large message (in the network layer) is broken up into 10 frames. Ack in the data link layer is more efficient, if 2 frames are lost.

Acknowledged connection-oriented service: A connection is established before data transmission. The data link layer guarantees that each frame is received each frame is received exactly once and all frames are received in the right order. With connectionless (+ Ack) service, A lost Ack can cause a packet to be sent several times.

- An example - A WAN subnet consisting of routers. When a frame arrives at a router, the hardware checks it for errors (using error detection and correction codes), Then passes the frame to the data link layer software which might be embedded in a chip on the network interface board. The data link layer software checks to see if this is the frame expected, and if so, forwards the payload field (packet) to the routing software (network layer). the routing software then chooses the outgoing line and passes the packet back down to the data link layer software, which then transmit it. One copy of the data link layer software handles all the transmission lines.

Faming: The physical layer accepts raw bit streams (0/1).The data link layer needs to detect possible transmission errors. The usual approach is to break the bit streams into frames and compute checksum for each frame.When a frame arrives at the receiver, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows there are errors and can deal with it discarding the bad frame; reporting errors and asking for re-sending. Breaking bit streams into frames is more difficult than it seems.How to do framing?

Breaking bit streams into frames: inserting time gaps between frames, However, timing is hard to be guaranteed in networks. Gaps may be squeezed out and other gaps may be inserted during transmission.

Three methods: Character count Flag bytes with byte stuffing Starting and ending flags, with bit stuffing.

Character count : Using a field in the header to specify the number of characters (bytes) in the frame. Problem – the counter can be garbled by a transmission error.Hard to resynchronize. Rarely used anymore.

Flag bytes with byte stuffing: Each frame starts and ends with special bytes.The start byte and the end byte can be different. Most protocols use the same start and end bytes – flag byte.if the receiver loses synchronization, it can just search for the flag byte. The flag byte pattern may occur in the data. Byte (character) stuffing – the sender's data link layer inserts a special escape byte (ESC) before each "accidental" flag byte in the data. What if the ESC byte occurs in the data? stuffing with a ESC byte. A major disadvantage of byte stuffing - it is closely tied to the use of 8-bit characters.Starting and ending flags, with bit Stuffing For arbitrary sized characters - Bit stuffing.

Bit stuffing: Each frame begins and ends with a special bit pattern, 01111110 (in fact, a flag byte). Whenever the sender's data link layer encounters five consecutive 1s (11111) in the data, it automatically stuffs a 0 bit into the outgoing bit stream. When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit.

Error Detection and Correction: Two strategies for dealing with transmission errors. Including enough redundant information with each packet – to enable the receiver to correct errors. Including only enough redundancy to allow the receiver to detect errors. Error-Correcting Codes. Error-Detecting Codes Which strategy should be used? depending on the channel reliability.

m data bits + r check bits = n bits –codeword. The number of different corresponding bits between two codeword is called the **Hamming distance** E.g., 10001001 and 10110001. The Hamming distance is 3.

A simple Error-Detecting Code - Parity bit: The parity bit is chosen so that the number of 1 bits in the codeword is even. E.g., 1011010+0; 1001010+1; **An Error-Correcting Code – A Hamming code** The bits that are power of 2 (1, 2, 4, 8, etc) are check bits. The rest bits (3, 5, 6, 7, 9, etc) are data bits. Each check bit forces the parity of some collection of bits, including itself, to be even. A data bit may be included in several parity computations. For a data bit k, rewrite k as a sum of powers of 2, E.g., 11 = 1+2+8. 11 contributes to check bits 1, 2, and 8. The Hamming code can correct 1-bit transmission error. When a codeword is received, the receiver initializes a counter to zero. The receiver then examines each check bit k (k = 1, 2, 4, 8, If the check bit does not have the correct parity, k is added to the counter. If the counter is zero after all the check bits have been examined, the codeword is accepted as valid. If the counter is non-zero, it contains the location of the incorrect bit. E.g., if check bit 1, 2 and 8 are in error, then the error data bit Is 11. The Hamming code can be used to correct a single burst error –several consecutive bit errors in one transmission. A sequence of k consecutive codewords are arranged as a matrix. The data is transmitted one column at a time. When the frame arrives at the receiver, the matrix is re-constructed. This approach can correct a single burst error of length k or less.

PPP(point to point protocol): is a TCP/IP protocol that is used to connect one computer system to another. Computers use PPP to communicate over the telephone network or the Internet. ... It also allows multiple network communication protocols to use the same physical communication line.

Chapter 4:

The Channel Allocation Problem: The Channel Allocation Problem - In broadcast networks, one key issue is to determine who gets to use the channel, when there is competition for it. A sublayer of the data link layer – Medium Access Control (MAC) sublayer. Static Channel Allocation in LANs and MANs Dynamic Channel Allocation in LANs and MANs

Static Channel Allocation in LANs and MANs: FDM->What's the problem of using FDM? When the number of sender is large and continuously varying or the traffic is bursty, FDM is not efficient. TDM, CDMA

Dynamic Channel Allocation in LANs and MANs: Five key assumptions for Dynamic Channel Allocation: 1. Station Model. N independent stations (computers, telephones, etc.) – terminals. Each station generates a frame with probability for transmission. Once a frame is generated, the station is blocked until the frame has been successfully transmitted. 2. Single Channel Assumption A single channel is available for all communication. All stations can transmit on it and receive from it. 3. Collision Assumption. If two frames are transmitted simultaneously, they overlap in time and the resulting signal is garbled – collision. 4. (a) Continuous Time - Frame transmissions can begin at any time instant. (b) Slotted Time – Time is divided into discrete slots. Frame transmissions always begin at the start of a slot. 5.(a) Carrier Sense – Stations can tell if the channel is in use before trying to use it. (b) No Carrier Sense.

Multiple Access Protocols: ALOHA, Carrier Sense Multiple Access Protocols, Collision-Free Protocols, Limited-Contention Protocols, Wavelength Division Multiple Access Protocols, Wireless LAN Protocols

ALOHA: In the 1970's, Norman Abramson at Univ. of Hawaii devised ALOHA to solve the channel allocation problem in ground-based radio broadcasting system.The basic idea of ALOHA applies to all broadcast system. Pure ALOHA and slotted ALOHA. Pure ALOHA Let users transmit whenever they have data to be sent. Due to the feedback property of broadcasting, a sender can always find out if its frame was destroyed by listening to the channel. If listening while transmitting is not possible, Ack is needed. The throughput is max. by using a uniform frame size. If the 1st bit of a new frame overlaps with just the last bit of a frame, both frames will be totally destroyed, since the checksum can not distinguish between a total or partial loss.

Slotted ALOHA: S= G*exp(-G) max at G = 1 **Pure ALOHA: S = G*exp(-2G) max at G=0.5** **G= attempts per packet time, S = Throughput per frame time**

Carrier Sense Multiple Access Protocols: In LANs, stations can detect what other stations are doing. Carrier sense protocols – Protocols in which stations listen for a carrier and act accordingly. Persistent and Non-persistent CSMA (Carrier Sense Multiple Access) **1-persistent CSMA protocol**• When a station has data to send, it first listen to the channel to see if anyone else is transmitting. When the channel is idle, the station transmits a frame with prob. 1. If a collision occurs, the station waits for a random time and resend. The propagation delay affects the performance of the protocol. **(Q) Non-persistent CSMA protocol** A station senses the channel before transmission. If the channel is busy, it does not continuously sense it. It waits for a random time them starts sensing the channel. Better channel utilization but longer delays than 1-persistent CSMA. **Persistent and Non-persistent CSMA (Carrier Sense Multiple Access)** p-persistent CSMA protocol. It applies to slotted channels. When a station has data to send, it first senses the channel. When the channel is idle, the station transmits a frame with prob. P. With prob. 1-p, it defers to the next slot (and runs the same algorithm).

CSMA with Collision Detection (CD): Persistent and Non-persistent CSMA protocols are better than ALOHA because they ensure that no station begins to transmit when it senses the channel busy. Another improvement - Stations abort their transmission as soon as they detect a collision.If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately. They should abort the transmission as soon as the collision is detected. The protocol – CSMA/CD is widely used on LANs. E.g., Ethernet LANs. At time t0, a station has finished transmitting its frame. During contention period, each possible sender transmits a short packet. Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.If what it reads back is different from what it is putting out, a station knows that a collision is occurring (with certain signal encoding). CSMA/CD can be in one of three states: contention, transmission, or idle.

Collision-Free Protocols: For CSMA/CD, collision can still happen during contention period. The bit-map protocol Assume N stations, each contention period consists of N slots. If station 0 has a frame to transmit , it transmits a 1 bit during slot 0. After N slots, each station has complete knowledge of which stations wish to transmit. Then they begin transmitting in numerical order.After the last station has transmitted its frame, another N-bit contention slot begins. Binary station addresses are used. Each possible sender broadcasts its address, starting with the highest bit. The bits in each address are BOOLEAN ORed together – Binary countdown. As soon as a station sees that a high-order bit position of 0 has been overwritten with a 1, it gives up.

Wavelength Division Multiple Access Protocols: A channel is divided into multiple sub-channels using FDM, TDM, and dynamically allocate them as needed. Each station has two channels, two transmitters and two. Receivers. A narrow channel is provided as a control channel to signal the station. A wide channel is provided to transmit data frames.

Wireless LAN Protocols: Hidden station problem A->B. C can not hear the transmission of A. When C->B, collision happens at B.

Uses of Computer Networks: Why people are interested in Computer Networks? Sharing Resource – programs, equipment, data, etc. E.g., sharing a printer. Sharing Information – bank, company, etc. A powerful communication medium among people. Email, Messenger, Video Conference, Voice over IP, etc. E-business & E-commerce – doing business with consumers over the Internet. Online stores - books, computers , airline tickets, cars, etc. Online banking. Online auction – eBay, etc. What they can be used for? Business Applications ,Home Applications, Mobile Users

The 802.11 MAC Sublayer Protocol: Most radios are half duplex – they can not transmit and listen for noise bursts at the same time on a single freq. 802.11 does not use CSMA/CD. 802.11 supports DCF (Distributed Coordination Function) – no central control. PCF (Point Coordination Function) – uses base stations to control all activity. The hiddens station problem and exposed station problem arise. 802.11 DCF Uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) Both physical channel sensing and virtual channel sensing. C -- A->B -- D Node C and D insert NAV (Network Allocation Vector) indicating virtual channel busy. not really signal. To deal with noise, frames are fragmented into smaller pieces. The fragments are numbered and Ack. Using a stop-and-wait protocol.

After a frame has been sent, a certain amount of idle time is needed before any station may send a (control or data) frame. SIFS – Short InterFrame Spacing; PIFS – PCF InterFrame Spacing; DIFS - DCF InterFrame Spacing; EIFS - Extended InterFrame Spacing.

The 802.11 Frame Structure: Frame control (11 subfields): Protocol version; Type (data or control); Subtype (RTS/CTS); To DS and From DS (frame intercell distribution system); MF (more fragments); Retry (retransmission); Power mgmt (sleep state); More (additional frames); W (frame is encrypted using WEP (Wired Equivalent Privacy); O (frames must be processed strictly in order).Duration – how long the frame and its Ack. will occupy the channel. 4 addresses – source, destination, and source & destination base stations. Sequence - fragment #

The 802.16 MAC Sublayer Protocol: Service Classes->Constant bit rate service, Real-time variable bit rate service, Non-real-time variable bit rate service, Best efforts service

Data Link Layer Switching: Bridges from 802.x to 802.y: Different LANs can be connected by bridges. Bridges operate in the data link layer and use data link layer address to do routing. Since bridges do not examine the payload field, they can transport IPv4, IPv6, ATM, OSI, or any other kinds of packets. Routers examine the payload field (IP address in the network layer). Local Internetworking Spanning Tree Bridges Remote Bridges Repeaters, Hubs, Bridges, Switches, Routers, Gateways Virtual LANs

Application layer-> Application gateway, Transport layer->Transport gateway, Network layer-> router, Data link layer-> Bridge, Switch, Physical Layer-> repeater, hub

Chapter 1:

Network Hardware: Taxonomy of Computer Networks: Transmission Technology: Broadcast links, Point-to-point links.**Network Scale:** Home Networks, Local Area Networks,Metropolitan Area Networks Wide Area Networks, Wireless Networks, Internetworks

Broadcast Networks: Types of transmission technology: **Broadcast links**: A single communication channel is shared by all, computers in the network., Packets sent by any machine are received by all the others. An address field within the packet specifies the receiver. Broadcasting – transmission to all machines. Multicasting – transmission to a subset of all machines. **Point-to-point links:** Point-to-point networks consist of many connections between individual pairs of machines, e.g., Internet. Selecting the route (path) is an issue – routing. Unicasting – Point-to-point transmission with one sender and one receiver.

Local Area Networks (LANs): LANs are privately-owned networks Within a single building or campus. Up to a few miles in size. LANs are distinguished from other kinds of networks **by three characteristics: Size:** LANs are restricted in size. The worst-case transmission time is bounded and known in advance. **Transmission technology:** Cable – 10 Mbps to 100 Mbps (1 Mbps = 1,000,000 bits/sec). Low delay (microseconds or nanoseconds). Few errors from transmission. New LANs operate at up to 10 Gbps (1 Gbps = 1,000,000,000 bits/sec). **Topology:** Bus, Ring **Bus:** At any instant at most one machine is the master and is allowed to transmit. An arbitration mechanism is needed to resolve the conflicts when two or more machines want to transmit at the same time. centralized or distributed. The IEEE 802.3 - Ethernet is a bus-based broadcast network with distributed control. 10 Mbps to 10 Gbps. (b) **Ring:** Each bit circumnavigates the entire ring without waiting for the rest of the packet. An arbitration mechanism is needed to resolve the concurrent transmission issue. E.g., round robin – each computer takes turn. IEEE 802.5 – the IBM token ring network.

Wireless Networks: Categories of wireless networks: **Cellular Networks** Providing cell phone service. **WLANs** (Wireless Local Area Networks) IEEE 802.11; etc. **WPANs** (Wireless Personal Area Networks) IEEE 802.15.1 (Bluetooth); 802.15.3; 802.15.4. **WMANs** (Wireless Metropolitan Area Networks) IEEE 802.16; etc. **Wireless MANETs** (Mobile Ad Hoc Networks), **Wireless Sensor Networks**

Protocol Hierarchies: Today's network software is highly structured. To reduce the design complexity, most networks are organized as a stack of layers (levels). One layer build upon another. The number of layers, the name, content and function of each layer - differ from network to network. Each layer offers certain services to the higher layers Shielding those layers from the details of the implementation of the Services. The concept of layering is similar to information hiding, abstract data type, etc. **A protocol** is an agreement between the (two or more) communicating parties on how communication is to proceed. Behavior protocol – e.g., introducing a woman to a man. The entities comprising the corresponding layers on different machines are called **peers** Processes, hardware devices, or even human beings.Peers communicate by using the protocol. An interface defines the primitive operations and services to the upper layer. A set of layers and protocols is called a **network architecture.**

The OSI Reference Model: The OSI (Open System Interconnection): Reference Model is based on a proposal developed by the ISO (International Standards Organization). Seven Layers **The Physical Layer:** Transmission of raw bits (1 or 0) over a communication channel. Design Issues How many volts should be used to represent a 1 (and 0)? Transmission proceed simultaneously in both direction? **The Data Link Laye**r: Providing services to the Physical and Network Layers To transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer Having the sender break up the input data into data frames A typical data frames ranges from a few hundred to thousand bytes. If the service is reliable, the receiver sends back ACK frame. Error Control Detecting and correcting transmission errors. Flow Control How to keep a fast transmitter from drowning a slow receiver? Medium Access Control For broadcast networks. **The Network Layer:** The Network Layer controls the operation of the subnet. The inter-connection of heterogeneous networks (subnets). The addressing, the lower layer protocols may differ.Routing How packets are routed from source to destination? Routes can be based on static tables, or determined dynamically. Congestion Control. Congestion happens when too many packets are present in a subnet at the same time. Quality of Service Delay, bandwidth, jitter, etc. **The Transport Layer:** (sender) accepts data from above, and splits it into smaller units if needed, then passes them to the network layer, (receiver) ensures the pieces all arrive correctly at the other end. is a true end-to-end layer – between source and destination. In the lower layers, the protocols are between neighbor machines. **The Session Layer**: Allows users on different machines to establish sessions Session services•Dialog control – keeping track of whose turn it is to transmit. Token management – preventing two parties from attempting the same critical operation at the same time. •Synchronization – Checkpointing long transmissions to allow them to continue from where they were after a crash. The Presentation Layer is concerned with the syntax and semantics of the information transmitted. manages abstract data structures. To make it possible for computers with different data representations to communicate. allows higher-level data structures (e.g. banking records) to be defined and exchanged **The Application Layer:** contains a variety of commonly-used protocols, such as HTTP (HyperText Transfer Protocol) - WWW, FTP – file transfer. SMTP - email.

The TCP/IP Reference Model: ARPANET A research network sponsored by the DoD. Connected hundreds of univ. and government networks using leased telephone lines. A new architecture was needed – TCP/IP Reference Model, when satellite and radio networks were added.One major design goal was that Connections remain intact as long as the source and destination machines were functioning even if some machines or transmission lines in between were down. **The Host-to-Network Layer**: The TCP/IP model does not specify this layer. **The Internet Laye:r** A packet-switching network based on a connectionless layer. defines an official packet format and protocol – IP (Internet Protocol). delivers IP packets. is similar in functionality to the OSI network layer.**The Transport Layer** :TCP (Transmission Control Protocol). A reliable connection-oriented protocol. It fragments the incoming byte stream into fixed-size packets and passes them to the internet layer. TCP also handles flow control and congestion control. UDP (User Datagram Protocol). An unreliable, connectionless protocol. UDP is widely used for applications in which prompt delivery is more important than accurate delivery, e.g., speech and video.

The Application Layer: contains a variety of higher-layer protocols, such as TELNET – remote login, virtual terminal. DNS (Domain Name System) – mapping host names onto IP addresses.

Hybrid Model: Application layer->Transport layer->Network layer->Data link layer->Physical Layer

Chapter 2:

The Theoretical Basis for Data Communication: Maximum Data Rate of a Channel: Nyquist's Theorem: Maximum data rate = 2Hlog_2V bits/sec H – bandwidth of the filter (channel). V – number of discrete levels (e.g., binary – 2). **Shannon's result for a noise channel: Maximum data rate = Hlog_2(1+S/N) bits/sec,** S/N – the ratio of signal power to noise power

Twisted Pair: A twisted pair consists of two insulated copper wires 1mm thick. When two wires are twisted, the waves cancel out, so the wire radiates less effectively – less interference. Twisted pairs are commonly used in telephone system. from telephones to the switching office. Twisted pairs can be used to transmit both analog and digital signals. The bandwidth depends on the thickness of the wire and the distance. Several megabits/sec. for a few kilometers. Two typical twisted pairs. **Category 3 UTP** (Unshielded Twisted Pair) Shielded Twisted Pair: The expensive shielded twisted pair Cables by IBM in 1980s. **Category 5 UTP** More twists per centimeter Less crosstalk and better-quality signal over longer distance

Coaxial Cable: Coaxial Cable has better shielding than twisted pairs so it can span longer distances at higher speeds. Two kinds of coaxial cables are widely used 50-ohm cable – digital signal. 75- ohm cable – analog transmission, cable TV, and Internet over cable.

The Electromagnetic Spectrum: Frequency,f, - the number of oscillations per second of a wave. Wavelength – the distance between two consecutive maxima of a wave. The speed of light c in vacuum is 300,000,000 meter/sec. **fλ=x.**

Radio Transmission: In the **VLF, LF, and MF** bands, radio waves follow the curvature of the earth. Less than 1,000 km. (AM radio use MF band) In the **HF and VHF** bands, the ground waves tend to be absorbed. They bounce off the ionosphere (a layer of charged particles at the height of 100~500km). The signals can bounce several times. (Amateur radio uses these bands

Communication Satellites: Geostationary –Earth Orbit (GEO) Satellites Stationary to the Earth. **Medium-Earth Orbit (MEO)** Satellites E.g., GPS satellites orbiting at 18,000 km. **Low-Earth Orbit (LEO**) Satellites Closer to the earth The ground stations do not need much power. The round-trip delay is small. Need a large number of satellites to cover the earth.**VSATs (Very Small Aperture Terminals)** Low-cost microstation with small antennas – 1 m (vs 10 m for standard GEO station antenna). A hub (with large antenna) is used to relay traffic between VSATs.

Multiplexing Techniques: Frequency Division Multiplexing (FDM), Wavelength Division Multiplexing (WDM), Time Division Multiplexing (TDM), Code Division Multiplexing (CDM)

TDM: TDM can be handled entirely by digital electronics. Codec (coder-decoder) is a device that convert analog signals to digital signals (digitize). For voice traffic, a codec makes 8000 samples per second (125 sec/sample) T1 is a typical frame for voice traffic – 193 bit / 125 μsec = 1.544 Mbps.

The Mobile Telephone System: First-Generation Mobile Phones: Analog Voice Using analog modulation - The traditional method of modulating radio signals so that they can carry information. E.g., AM (amplitude modulation) and FM (frequency modulation). **Second-Generation (2G) Mobile Phones: Digital Voice** Using digital modulation - reduces voice to binary code - the zeros and ones. At the receiving end , the information is reconverted. Digital transmission offers stronger reception, less static, greater call handling capacity, fewer dropped calls, and improved call privacy. T**hird-Generation (3G) Mobile Phones: Digital Voice and Data.** E.g., Sprint and Verizon offer EVDO (Evolution-Data Optimized) 3G data service for cell phones.

Advanced Mobile Phone System: In AMPS, a cell is about 10 to 20 km across. Each cell uses some set of frequencies not used by its neighbors. Frequency reuse. Handoff –

When a cell phone travels across cells, a new channel is used. Totally 832 full-duplex channels in AMPS, each simplex channel is 30 kHz.

AMPS Channel Categories: The 832 channels of AMPS are divided into four categories: Control (base to mobile) to manage the system,**Paging (base to mobile)** to alert users to calls for them, **Access (bidirectional)** for call setup and channel assignment**, Data (bidirectional)** for voice, fax, or data**, Digital Voice : D-AMPS** (Digital Advanced Mobile Phone System)Four systems in use now: D-AMPS, GSM, CDMA, and PDC (Personal Digital Cellular).