Chapter 4: Network Access

* **OSI Model: OSI Physical Layer Provides means to transport the bits that make up a data link layer frame across the network media. This layer accepts complete frame from data link layer and encodes it as a series of signals that are transmitted onto the local media. The encoded bits that comprise a frame are received by an end device.**

Graphical user interface

Description automatically generated

**User data is segmented by transport layer, placed into packets by the network layer, and further encapsulated as frames by data link layer. Physical layer encodes the frames and creates electrical, optical, or radio wave signals that represent the bits in each frame. These signals are then sent on the media one at a time. Destination node physical layer retrieves these individual signals from the media, restores them into their bit representations, and passes the bits up to the data link layer as a complete frame.**

* **Physical layer media:** 1. Copper cable (signals are patterns of electrical pulses), 2. Fiber-optic cable (signals are patterns of light) 3. Wireless (signals are patterns of microwave transmissions).

Graphical user interface, text, application

Description automatically generated

* **Physical layer Standards: The TCP/IP standards are implemented in software and governed by the IETF. The physical layer standards are implemented in hardware and are governed by many organizations including ISO, EIA/TIA, ITU-T, ANSI, IEE**
* **Fundamentals of Physical Layer: 3 Function areas:**

1. **Physical components: Electronic hardware devices, media and other connectors that transmit and carry signals to represent bits. Hardware components like network adapters (NICs), interfaces and connectors, cable materials, and cable designs are all specified in standards associated with physical layer. [UTP, Coaxial, Connectors, NICs, Ports, Interfaces]**
2. **Encoding: Method of converting a stream of data bits into a predefined code. Codes are groupings of bits used to provide a predictable pattern that can be recognized both by sender and the received. In addition, encoding provides codes to control purposes such as identifying beginning and end of a frame. Common network encoding methods include 1) Manchester encoding (A 0 is represented by a high to low voltage transition, while 1 is represented as low to high voltage transition. 2) Non-Return to Zero (NRZ) (This is common means of encoding data that has two states termed “zero” and “one” and no neutral or rest position. A 0 may be represented by one voltage level on media and 1 representing different voltage on media**
3. **Signaling: Physical layer must generate the electrical, optical, or wireless signals that represent “0” and “1” on media. The method of representing the bits is called signaling method. Physical layer must define what type of signal represents “1” or “0”. Signals can be transmitted in two ways: 1) Asynchronous: Data signals are transmitted without an associated clock signal. Time spacing between data characters or blocks may be of arbitrary duration, meaning the spacing is not standardized. Frames require start and stop indicator flags 2) Synchronous: Data signals are sent along with a clock signal which occurs at evenly spaced time durations referred to as the bit time.**

**Modulation: process by which the characteristic of one wave modifies another wave. Following Modulation techniques are widely used. 1) Frequency Modulation (FM): Method of transmission in which carrier frequency varies in accordance with signal. 2) Amplitude modulation (AM): Amplitude of carrier varies in accordance with signal. 3) Pulse-coded modulation (PCM): technique in which an analog signal, is converted into digital signal by sampling the signal’s amplitude and expressing the different amplitudes as binary number. Sampling rate must be at least twice the highest frequency in the signal**

Graphical user interface, text

Description automatically generated

* **Bandwidth: Capacity of medium to carry data. Digital Bandwidth measures the amount of data that can flow from one place to another in a given amount of time. (Kilobits per second (kb/s) or megabits per second (mb/s)). Practical bandwidth is determined by combination of two factors: 1) Properties of Physical media 2) Technologies chosen for signaling and detect network signals**
* **Throughput: Measure of transfer of bits across the media over a given period. Factors influencing throughput: 1) Amount of Traffic 2) Type of traffic 3) latency created by the number of network devices encountered between source & destination**

**Latency refers to the amount of time, to include delays, for data to travel from one given point to another. Goodput is the measure of usable data transferred over a given period. It is throughput minus traffic overhead for establishing sessions, etc.**

* **Copper Cabling**
* **Characteristics of Copper Media: use of copper media because inexpensive, easy to install and has low resistance to electrical current. However, copper media is limited by distance and signal interference. Data transmitted on copper cables as electrical pulses. Signal Attenuation: The longer the signal travels, the more it deteriorates. The timing and voltage values of electrical pulses are susceptible to interference from two sources: 1) Electromagnetic Interference (EMI)/ Radio Frequency Interference (RFI)- EMI or RFI can distort, and corrupt data signals being carried by copper media. To counter this, copper cables are wrapped in metallic shielding and require proper grounding connections 2) Crosstalk- disturbance caused by the electric or magnetic fields of a signal on one wire to the signal in an adjacent wire. Example, cross talks in telephones. To counter this, some types of copper cables have opposing circuit wire pairs twisted together which effectively cancels the crosstalk**

**Susceptibility of copper cables to electronic noise can be limited by: Selecting cable type or category most suited to a given networking environment, designing a cable infrastructure to avoid known and potential sources of interference in building structure, using cable techniques that include the proper handling and termination of cables.**

* **Copper Media: 3 main types: Unshielded Twisted-Pair (UTP), Shielded Twisted-Pair (STP), Coaxial. These cables are used to interconnect nodes on a LAN and infrastructure devices.**

1. **Unshielded Twisted-Pair Cable- Most common networking media, UTP cabling, terminated with RJ-45 connectors, is used for interconnecting network hosts with intermediate networking devices, such as switches/routers. In LANs, UTP cable consist of four pairs of color-coded wires that have been twisted together and then encased in flexible sheath which protects from minor physical damage. Twisting of wires help protect against signal interference. Color codes identifies each individual pairs**
2. **Shielded Twisted-Pair Cable- provides better noise protection than UTP. STP is expensive and difficult to install. STP uses techniques of shielding to counter EMI and RFI and wire twisting to counter crosstalk. Two common variations of STP: 1) STP cable shields entire bundle of wires with foil eliminating virtually all interference 2) STP cable shields entire bundle of wires as well as the individual wire pairs with foil eliminating all interferences.**
3. **Coaxial Cable- Coaxial cable consist of copper conductor used to transmit the electronic signals, copper conductor is surrounded by a layer of flexible plastic insulation, the insulating material is surrounded in metallic foil, that acts as second wire in the circuit which also reduces the amount of outside electromagnetic interference, the entire cable is covered with a cable jacket to protect it from minor physical damage. Terminates with BNC, N type and F type connectors**

**The coaxial cable design has been adapted for us in 1) Wireless installations: Coaxial cables attach antennas to wireless devices. Coaxial cable carries radio frequency (RF) energy between the antennas and radio equipment. 2) Cable Internet installations: Cable service providers are currently converting their one-way systems to two-way systems to provide Internet connectivity to their customers. To provide these services, portions of coaxial cable and supporting amplification elements are replaced with fiber-optic cable. Combined use of fiber and coax is referred to as hybrid fiber coax (HFC)**

* **UTP Cabling- UTP cabling does not use shielding to counter the effects of RMI and RFI. To limit negative effect of crosstalk: 1) Cancellation: Designers now pair wires in circuit. Two wires in electrical circuit are placed together, their magnetic fields are exact opposite of each other (cancel each other) 2) Varying the number of twists per wire pair: Further enhance the cancellation effect of paired circuit. UTP cable must follow precise specifications governing how many twists are permitted per meter.**

**Types of UTP cabling: Ethernet Straight-through**: common type of networking cable. It is commonly used to interconnect a host to a switch and a switch to a router, **Ethernet Crossover**: An uncommon cable used to interconnect similar devices together. **Rollover:** A Cisco proprietary cable used to connect to a router or switch console port.

A picture containing diagram

Description automatically generated

**Fiber Optic Cabling:** Optical fiber is a flexible but extremely thin transparent strand of very pure glass. It permits the transmission of data over longer distances and at higher bandwidths. “light pipe,” to transmit light between the two ends with minimal loss of signal. Fiber-optic cabling is now being used in four types of industry, **Enterprise Networks (**used for backbone cabling applications and interconnecting infrastructure devices)**, FTTH and Access Networks** (provide always-on broadband services to homes)**, Long-Haul Networks** (Use long-haul terrestrial optical fiber network to connect countries and cities)**, Submarine Networks** (Special fiber cables used to provide reliable high-speed, high-capacity solutions capable of surviving harsh undersea environments up to transoceanic distances**.**

Fiber media cable design: **Core** (Consist of pure glass and part of fiber where light is carried), **Cladding (**Glass that surrounds core and act as mirror, the light pulses propagate down the core while cladding reflects light pulses), **Jacket (**Protect glass)

Light Pulses Representing transmitted data as bits on media generated by: **Lasers, Light emitting Diodes (LEDs)**

**Photodiodes** detects the light pulses and convert them to voltages that is reconstructed into data frames.

**Fiber-Optic cables can be classified as: Single-mode fiber (SMF):** Consist of very small core and uses expensive laser technology to send ray of light, **Multimode Fiber (MMF):** Consist of a larger core and uses LED emitters to send light pulses.

**Optical fiber connector** terminates the end of an optical fiber. Three most popular fiber-optic connectors: **Straight-Tip (ST):** older bayonet style connector used in multimode fiber, **Subscriber Connector (SC):** Square connector/Standard connector. It is widely adopted LAN and WAN connector, uses a push and pull mechanism, connector type used with multimode, single-mode fiber, **Lucent Connector (LC):** little/local connector, popularity due to its small size, used with single-mode fiber and supports multimode fiber.

**Three Common types of fiber-optic termination and splicing errors: Misalignment (**Fiber-optic media are not precisely aligned to one another when joined), **End Gap (**The media does not completely touch at the splice or connection), **End Finish (**The media ends are not well polished, or dirt is present at the termination. Optical Time Domain Reflectometer (OTDR) test fiber-optic cable

**Fiber-optic advantage over copper:** they are not electrical conductors; media is immune to electromagnetic interference. Optical fibers are thin and have relatively low signal loss, they can be operated at greater lengths than copper media.

**Fiber-optic disadvantage over copper:** More expensive than copper over same distance, Different skills and equipment required to terminate and splice cable infrastructure, More careful handling than copper media

* **Wireless Media**

Wireless disadvantage: **Coverage Area (**Wireless data communication technologies work well in open environments, however, certain construction materials used in buildings limit effective coverage), **Interference** (Wireless susceptible to interference and can be disrupted by such common devices as household cordless phones etc), **Security (**Devices and users who are not authorized for access to the network can gain access to the transmission. Network security is major concern.

**Standard IEEE 802.11 –** Wireless LAN (WLAN) technology

**Standard IEEE 802.15-** Wireless Personal Area Network (WPAN)

**Standard IEEE 802.16-** Worldwide Interoperability for microwave access (WiMAX)

**Wireless LAN-** A wireless LAN requires the following network devices: **Wireless Access Point (AP):** concentrates wireless signals from users and connects, usually through a copper cable, such as Ethernet, **Wireless NIC adapters:** Provides wireless communication capability to each network host.

**Benefits-** Saving on costly premises, convenience of host mobility. Disadvantage, network security concern.

* **The Data Link Layer:** the data link layer is responsible for the exchange of frames between nodes over a physical network media. It allows the upper layers to access the media and controls how data is placed and received on the media.
* The TCP/IP network access layer is the equivalent of the OSI: Data link (Layer 2), Physical (Layer 1)
* The Layer 2 notation for network devices connected to a common medium is called a node.
* Specifically, the data link layer performs these two basic services: It accepts Layer 3 packets and packages them into data units called frames, it controls media access control and performs error detection.
* The data link layer effectively separates the media transitions that occur as the packet is forwarded from the communication processes of the higher layers. The data link layer receives packets from and directs packets to an upper layer protocol, in this case IPv4 or IPv6. This upper layer protocol does not need to be aware of which media the communication will use.
* **Data Link Sublayers**

The data link layer is divided into two sublayers:

* **Logical Link Control (LLC)**: This upper sublayer defines the software processes that provide services to the network layer protocols. It places information in the frame that identifies which network layer protocol is being used for the frame. This information allows multiple Layer 3 protocols, such as IPv4 and IPv6, to utilize the same network interface and media.
* **Media Access Control (MAC)**: This lower sublayer defines the media access processes performed by the hardware. It provides data link layer addressing and delimiting of data according to the physical signaling requirements of the medium and the type of data link layer protocol in use.

Separating the data link layer into sublayers allows for one type of frame defined by the upper layer to access different types of media defined by the lower layer. Such is the case in many LAN technologies, including Ethernet.

* **Purpose of Data Link Layer:**

Layer 2 protocols specify the encapsulation of a packet into a frame and the techniques for getting the encapsulated packet on and off each medium. The technique used for getting the frame on and off media is called the **media access control** method.

The packets do not have a way to directly access these different media. It is the role of the OSI data link layer to prepare network layer packets for transmission and to control access to the physical media. The media access control methods described by the data link layer protocols define the processes by which network devices can access the network media and transmit frames in diverse network environments

Without the data link layer, network layer protocols such as IP, would have to make provisions for connecting to every type of media that could exist along a delivery path. Moreover, IP would have to adapt every time a new network technology or medium was developed. This is a key reason for using a layered approach to networking.

Different media access control methods may be required during a single communication. Each network environment that packets encounter as they travel from a local host to a remote host can have different characteristics.

Router interfaces encapsulate the packet into the appropriate frame, and a suitable media access control method is used to access each link.

At each hop along the path, a router:

* Accepts a frame from a medium
* De-encapsulates the frame
* Re-encapsulates the packet into a new frame
* Forwards the new frame appropriate to the medium of that segment of the physical network

**Layer 2 Frame Structure:** The data link layer prepares a packet for transport across the local media by encapsulating it with a header and a trailer to create a frame. Data link layer protocols require control information to enable the protocols to function.

the data link layer frame includes:

* **Header**: Contains control information, such as addressing, and is located at the beginning of the PDU.
* **Data**: Contains the IP header, transport layer header, and application data.
* **Trailer**: Contains control information for error detection added to the end of the PDU.
* Chart, funnel chart

  Description automatically generated

Framing breaks the stream into decipherable groupings, with control information inserted in the header and trailer as values in different fields. This format gives the physical signals a structure that can be received by nodes and decoded into packets at the destination.

**Generic frame field types include:**

* **Frame start and stop indicator flags**: Used by the MAC sublayer to identify the beginning and end limits of the frame.
* **Addressing**: Used by the MAC sublayer to identify the source and destination nodes.
* **Type**: Used by the LLC to identify the Layer 3 protocol.
* **Control**: Identifies special flow control services.
* **Data**: Contains the frame payload (i.e., packet header, segment header, and the data).
* **Error Detection**: Included after the data to form the trailer, these frame fields are used for error detection

The functional protocols and services at the data link layer are described by:

* Engineering organizations which set public and open standards and protocols.
* Communications companies which set and use proprietary protocols to take advantage of new advances in technology or market opportunities.

**Media Access Control**

Media access control is the equivalent of traffic rules that regulate the entrance of motor vehicles onto a roadway. There are different ways to regulate placing frames onto the media. The protocols at the data link layer define the rules for access to different media. Some media access control methods use highly controlled processes to ensure that frames are safely placed on the media. These methods are defined by sophisticated protocols, which require mechanisms that introduce overhead onto the network.

The actual media access control method used depends on:

* **Topology**: How the connection between the nodes appears to the data link layer.
* **Media sharing**: How the nodes share the media. The media sharing can be point-to-point such as in WAN connections or shared such as in LAN networks.

LAN and WAN topologies can be viewed in two ways:

**Physical topology**: Refers to the physical connections and identifies how end devices and infrastructure devices such as routers, switches, and wireless access points are interconnected.

**Logical topology**: Refers to the way a network transfers frames from one node to the next. This arrangement consists of virtual connections between the nodes of a network. These logical signal paths are defined by data link layer protocols.

It is the logical topology that influences the type of network framing and media access control used.

WANs are commonly interconnected using the following physical topologies:

* **Point-to-Point**: This is the simplest topology which consists of a permanent link between two endpoints. For this reason, this is a very popular WAN topology. In this arrangement, two nodes do not have to share the media with other hosts. Additionally, a node does not have to make any determination about whether an incoming frame is destined for it or another node. Therefore, the logical data link protocols can be very simple as all frames on the media can only travel to or from the two nodes.
* **Hub and Spoke**: A WAN version of the star topology in which a central site interconnects branch sites using point-to-point links.
* **Mesh**: This topology provides high availability but requires that every end system be interconnected to every other system. Therefore, the administrative and physical costs can be significant. Each link is essentially a point-to-point link to the other node. Variations of this topology include a partial mesh where some but not all of end devices are interconnected.

**Logical point-to-point**

The logical connection between nodes forms what is called a **virtual circuit.** The two nodes on either end of the virtual circuit exchange the frames with each other. This occurs even if the frames are directed through intermediary devices. The media access method used by the data link protocol is determined by the logical point-to-point topology, not the physical topology.

**Half-duplex communication**: Both devices can both transmit and receive on the media but cannot do so simultaneously.

**Full-duplex communication**: Both devices can transmit and receive on the media at the same time. The data link layer assumes that the media is available for transmission for both nodes at any time.

**LAN topologies:** End devices can be interconnected using the following physical topologies:

* **Star**: End devices are connected to a central intermediate device. Early star topologies interconnected end devices using hubs. However, star topologies now use switches. easy to install, very scalable and easy to troubleshoot.
* **Extended star or hybrid**: In an extended star topology, central intermediate devices interconnect other star topologies. In a hybrid topology, the star networks may interconnect using a bus topology.
* **Bus**: All end systems are chained to each other and terminated in some form on each end. Infrastructure devices such as switches are not required to interconnect the end devices. Inexpensive to use and easy to set up.
* **Ring**: End systems are connected to their respective neighbor forming a ring. Unlike the bus topology, the ring does not need to be terminated. Ring topologies were used in legacy Fiber Distributed Data Interface (FDDI) networks.

There are two basic media access control methods for shared media: Contention-based access, Controlled access

* **Contention-based access**: All nodes compete for the use of the medium but have a plan if there are collisions. These methods use a Carrier Sense Multiple Access (CSMA) process to first detect if the media is carrying a signal. If a carrier signal on the media from another node is detected, it means that another device is transmitting. When the device attempting to transmit sees that the media is busy, it will wait and try again after a short time period. If no carrier signal is detected, the device transmits its data. It is possible that the CSMA process will fail, and two devices will transmit at the same time creating a data collision. If this occurs, the data sent by both devices will be corrupted and will need to be resent.
  + **Carrier sense multiple access with collision detection (CSMA/CD)**: The end device monitors the media for the presence of a data signal. If a data signal is absent and therefore the media is free, the device transmits the data.
  + **Carrier sense multiple access with collision avoidance (CSMA/CA)**: The end device examines the media for the presence of a data signal. If the media is free, the device sends a notification across the media of its intent to use it. Once it receives a clearance to transmit, the device then sends the data.

Diagram, timeline

Description automatically generated

* **Controlled access**: Each node has its own time to use the medium. Figure 2 shows controlled access. This method is also known as scheduled access or deterministic. Usage of token passing method. Although controlled access is well-ordered and provides predictable throughput, deterministic methods can be inefficient because a device must wait for its turn before it can use the medium.
* Timeline

  Description automatically generated
* **Multi**-**Access Topology:** A logical multi-access topology enables several nodes to communicate by using the same shared media. Data from only one node can be placed on the medium at any one time. Every node sees all the frames that are on the medium, but only the node to which the frame is addressed processes the contents of the frame.
* **Ring Topology:** In a logical ring topology, each node in turn receives a frame. If the frame is not addressed to the node, the node passes the frame to the next node. This allows a ring to use a controlled media access control technique called token passing.

**Data Link Frame**

Each frame type has three basic parts:

* Header- The frame header contains the control information specified by the data link layer protocol for the specific logical topology and media used. (Header fields- Start frame, source/destination address fields, Type Field)
* Data-
* Trailer- The trailer is used to determine if the frame arrived without error. This process is called error detection and is accomplished by placing a logical or mathematical summary of the bits that comprise the frame in the trailer. A transmitting node creates a logical summary of the contents of the frame. This is known as the cyclic redundancy check (CRC) value. This value is placed in the Frame Check Sequence (FCS) field of the frame to represent the contents of the frame. When the frame arrives at the destination node, the receiving node calculates its own logical summary, or CRC, of the frame. The receiving node compares the two CRC values. If the two values are the same, the frame is considered to have arrived as transmitted. If the CRC value in the FCS differs from the CRC calculated at the receiving node, the frame is discarded.

All data link layer protocols encapsulate the Layer 3 PDU within the data field of the frame. However, the structure of the frame and the fields contained in the header and trailer vary according to the protocol.

A fragile environment requires more control. However, a protected environment requires fewer controls.

Header: For example, other Layer 2 protocol header frame fields could include:

* **Priority/Quality of Service field**: Indicates a particular type of communication service for processing.
* **Logical connection control field**: Used to establish a logical connection between nodes.
* **Physical link control field**: Used to establish the media link.
* **Flow control field**: Used to start and stop traffic over the media.
* **Congestion control field**: Indicates congestion in the media.

**LAN and WAN frames:** Common data link layer protocols include:

* Ethernet
* Point-to-Point Protocol (PPP)
* 802.11 Wireless

Table

Description automatically generatedTable, timeline

Description automatically generated

Table

Description automatically generated

Table

Description automatically generated