Chapter 3: Network Protocols and Communications

* **Communication: 3 things in communication: message source/sender, message destination/receiver, channel (provides pathway)**

**Sending of message must be sent from sender to receiver either face-to-face or over a network, governed by rules (protocols)**

* **Establishing rules: Requirements: identified sender and receiver, Common language and grammar, speed and time of delivery, confirmation, or acknowledgement requirements. Eg of computer protocols: message encoding/formatting/encapsulation etc.**
* **Message encoding: Encoding is the process of converting info into another, acceptable form of transmission. Decoding reverses this process to interpret the info. For encoding between hosts, converted into bits. Each bit is encoded pattern of sounds/light**
* **Message Formatting and Encapsulation: Correct format for each message sent. Eg: letters sent by humans. The process of placing one message format (the letter) inside another message format (envelope) is called encapsulation. De-encapsulation occurs when the receiver removes letter from the envelope. Frame: Each computer message is encapsulated in a specific format called the frame before it is sent over the network. Frame acts like an envelope.**

Table

Description automatically generated

* **Message size: Rule of Communication is Size. When people communicate with each other, the messages are broken down into smaller pieces/sentences to ensure each part of message is received and understood. Segmenting: In computers, the size restrictions of frames require source host to break a long message into individual pieces that meet both minimum and maximum requirements. Each segment is encapsulated in separate frames with address info. At receiving host, the messages are de-encapsulated and put back together to be processed and interpreted**
* **Message Timing: People use timing when to speak, how fast or slow to talk, and how long to wait for a response.**

**Access Method: Access Method determines when someone can send messages. If two people talk same time, collision occurs. Computers also define an access method, Hosts on a network need to know when to begin to send messages and how to respond if error occurs**

**Flow Control: How much info can be sent and speed that it can be delivered. If one person speaks too fast, it is difficult to understand. In network communication, sending host can transmit messages at a faster rate than the destination host can receive and process. Source and destination hosts use flow control to negotiate correct timing for successful communication.**

**Response Timeout: If there is no response after a person asks a question, person acts accordingly that no answer is coming. Hosts on the network also specify how long to wait for responses and what action to take if response timeout occurs**

* **Message Delivery Options: one-to-one delivery: 2 person (known as unicast), one-to-all/one-to-many: group of recipients (known as multicast), multicasting is delivery of same message to a group of host destinations. If all hosts need to receive the message at the same time, Broadcast is used (one-to-all).**
* **Protocols: Protocol suite: a group of inter-related protocols necessary to perform a communication function, these are implemented by hosts and networking devices in software, hardware, or both.**

Graphical user interface, text

Description automatically generated

**Content of Communication –** **Best way to visualize it is to view interaction as a stack. Bottom layer (Physical Layer) -we have two people with each who can speak out loud, second layer (Rules Layer) – agreement to speak the common language, top layer (Content Layer) – words that are spoken.**

* **Network Protocols- For devices to successfully interact, a network protocol suite must describe precise requirements and interactions. Common networking protocols are IP, HTTP, and DHCP.**

**Network protocols describe the following processes:**

* **How message is formatted or structured**
* **Process by which networking device share info about pathways with other networks.**
* **How and when error and system messages are passed between devices**
* **The setup and termination of data transfer sessions**
* **Interaction of Protocols: interaction between web servers and web client. This interaction uses several protocols/standards in process of exchanging info between them. Different protocols work together to ensure messages are received and understood.**

1. **Application Protocol- Hypertext Transfer Protocol (HTTP) is protocol that governs the way a web server and web client interact. It defines the content and formatting of requests and responses that are exchanged. Both client and server implement HTTP as part of their application. HTTP relies on other protocols to govern how the messages are transported between client and server**
2. **Transport Protocol- Transmission Control Protocol (TCP) is transport protocol, manages individual conversations between web servers and web clients. TCP divides HTTP messages into smaller pieces, called segments. Segments are then sent between web server and the client process. TCP also responsible for controlling size and rate at which messages are exchanged.**
3. **Internet Protocol- IP responsible for taking formatted segments from TCP, encapsulating them into packets, assigning them appropriate addresses, and delivering them across the best path to the destination host.**
4. **Network Access Protocol- Two primary functions: (Eg: Ethernet)**

* **Communication over a data link (Data link management protocols take the packets from IP and format them to be transmitted over the media)**
* **Physical transmission of data on the network media (The standards and protocols are for physical media govern how the signals are sent and how they are interpreted by receiving clients.**
* **Protocol suites and Industry Standards: The IP, HTTP, DHCP, are all part of the internet protocol suite known as Transmission Control Protocol/IP (TCP/IP). It is an open standard (freely available to the public).**

**A standards-based protocol is a process/protocol that has been endorsed by the networking industry and approved by std. org.**

**Use of standards in developing and implementing helps products from different manufacturers to interoperate successfully.**

**Proprietary protocols can be used by diff org. with permission from owner. Others can be implemented on equipment manufactured by proprietary vendor. Example: AppleTalk, Novell Netware. Several companies even come together to form proprietary software to meet the needs of its customers.**

* **Development of TCP/IP: IP suite is a suite of protocols required for transmitting and receiving info using the internet. It is commonly known as TCP/IP because first two networking protocols defined for this standard were TCP and IP**

**TCP/IP complete communication process using an example of web server transmitting data to client**

Graphical user interface

Description automatically generated with low confidence

1. **Web server’s HTML page is the data to be sent**
2. **Application protocol HTTP header is added to front of HTML data. Header contains various info, HTTP version, status code.**
3. **HTTP application layer protocol delivers HTML-formatted web page data to the transport layer. The TCP transport layer is used to manage individual conversation between web server and web client**
4. **IP info is added to the front of TCP info. IP assigns appropriate source and destination IP address (known as IP Packet)**
5. **Ethernet protocol adds info to both ends of IP packets, known as data link frame. This frame is delivered to nearest router along the path towards web client. This router removes ethernet info, analyze IP packet, determine best path for the packet, inserts packet into new frame, sends to neighboring router toward destination. Each router removes/adds data link each**
6. **This data is now transported through internetwork, consist of media and intermediary devices.**
7. **Client receives data link frames that contain data, each protocol header is processed and removed in opp order that it was added. Ethernet info is processed and removed, followed by IP protocol info, then TCP info, and finally HTTP info**
8. **Web page info is then passed on the client’s web browser software**

**Application Protocol- DNS, BOOTP, DHCP, SMTP, POP, IMAP, FTP, TFTP, HTTP**

**Transport Protocol-** UDP, TCP

**Internet Layer-** IP, NAT, ICMP, OSPF, BGRP

**Network Access Layer-** ARP, PPP, Ethernet, Interface drivers

* **Open standards: encourages competition and innovation. Also guarantee no single company monopolize the market (unfair)**

**Standard org are usually vendor-neutral, non-profit organizations establish to develop and promote concept of open standards**

**Standard org include:**

**The Internet society (ISOC)- responsible for promoting open development, evolution, and Internet use throughout the world.**

**The Internet Architecture Board (IAB)- responsible for overall management and development of internet standards**

**The Internet Engineering Task Force (IETF)- mission to develop, update and maintain internet and TCP/IP technologies (RFC docs)**

**The Internet Research Task Force (IRTF)- long-term research related to Internet and TCP/IP protocols, apps, technologies.**

**The Institute of Electrical and Electronics Engineers (IEEE)- creates and maintains std affecting wide range industries (power, energy)**

**The International Organization for Standardization (ISO)- world’s largest developer of international standards for variety of products**

* **Layered Model- visualize interaction between various protocols.**

**Benefits: Assists in protocol design (protocols operate at a specific layer have defined info), fosters competition, prevents technology or capability changes in one layer from affecting other layers, provides common lang to describe network functions/capabilities**

* **There are two basic types of networking models:**

1. **Protocol Model- matches structure of protocol suite. Hierarchical set of related protocols in suite typically represents all functionality required to interface human network with data network. The TCP/IP model is a protocol model**
2. **Reference Model-provides consistency within all types of network protocols and services by describing what must be done at a particular layer, but not prescribing how it should be accomplished. Primary purpose of reference model is to aid in clearer understanding of functions and processes involved.**

**OSI Model is most widely known as internetwork reference model. Used for data network design, operation specifications.**

* **OSI reference model- 1. Physical (describes mechanical, electrical means to activate, maintain and de-activate physical connections for bit transmission to and from network device, 2. Data link (describe methods for exchanging data frames between devices over common media), 3. Network (Network layer provides services to exchange individual pieces of data over network) 4. Transport (defines services to segment, transfer and reassemble data for individual comms between end devices. 5. Session (services to presentation layer to organize its dialogue and to manage exchange data). 6. Presentation (common representation of data transferred between application layer services). 7. Application (provides means for end-to-end connectivity)**
* **TCP/IP model – 1. Application- Represents data to the user, plus encoding and dialog entry. 2. Transport- Supports comm between diverse devices across diverse networks. 3. Internet- Determines the best path toward the network. 4. Network Access- Controls the hardware devices and media that make up the network.**
* **Data Encapsulation- Better to approach is to divide data into smaller, more manageable pieces to send over the network. The division of data stream into smaller pieces is called segmentation. Segmenting has two primary Benefits.**

1. **By sending smaller individual pieces from sources to destination. Multiplexing- the process is used to interleave the pieces of separate conversations together on the network.**
2. **Segmentation increases reliability of network communications. The separate pieces of each message need not travel the same pathway across the network. If a particular path fails, individual messages are then sent through alternatives.**

* **Downside of segmentation and multiplexing to transmit messages across a network is level of complexity added.**
* **Protocol Data Units (PDU) – the form that a piece of data takes at any layer. At each stage of process, PDU has diff names. PDUs are names acc to the TCP/IP suite: Data (general term for PDU at application layer, Segment (transport layer PDU), Packet (Network layer PDU), Frame (Data link layer PDU), Bits (a physical layer PDU used when physically transmitting data over medium**
* **Encapsulation: Data Encapsulation is process that adds additional protocol header info to the data before transmission. Original data is encapsulated or wrapped in several protocols before being transmitted. Application protocol, HTTP, begin process by delivering HTML formatted web page data to the transport layer. There the application data is broken into TCP segments. Each TCP segments is given a label (header), containing info about which process running on destination computer should receive the message. It also contains the info that enables destination process to reassemble the data back to its original format. The transport layer encapsulates web page HTML data within the segment and sends it to the internet layer, where IP protocol is implemented. Entire ECP segment is encapsulated within an IP packet, which adds another label (IP header), IP header contains source and destination host IP addresses, as well as info to deliver packet to corresponding destination process. Next, IP packet is sent to the network access layer where It is encapsulated within a frame header and trailer. Each frame header contains source and destination physical address. Physical address uniquely identifies devices. Trailer contains error checking info, finally bits are encoded onto the media by the server network interface Card (NIC).**
* **De-encapsulation: process is reversed at the receiving host. Process used by a receiving device to remove one or more of the protocol headers. The data is de-encapsulated as it moves up the stack toward the end-user application.**
* **Network address: logical address contains info required to deliver the IP packet from source device to destination device. A layer 3 IP address has 2 parts: network prefix (used by routers to forward the packet to proper network), host part (used by the last router in the path to deliver the packet to the destination device.**

**IP packet contains two IP addresses: Source IP address, Destination IP address**

* **Data Link Address: Data link, Layer 2 purpose is to deliver the data link frame from one network interface to another network interface over the same network. Before IP packet can be sent over wired/wireless network, it must be encapsulated in a data link frame so it can be transmitted over the physical medium, actual network. Ethernet LANs and wireless LANs are examples**

**Source data link address- Physical address of the device sending the packet. Initially it is NIC.**

**Destination Data link address- The physical address of the network interface of either the next hop router or the network interface of the destination device.**

**Ethernet MAC addresses- on an ethernet network, data link addresses are known as ethernet mac addresses**

**MAC addresses are 48-bit addresses that are physically embedded on the Ethernet NIC. Mac Address is also known as the physical address or burned-in address (BIA)**

**Address Resolution Protocol (ARP)- Sending host uses this protocol to discover MAC address of any host on the same network. The sending host sends an ARP request message to entire LAN. ARP request is broadcast message. Every device on LAN examines the to see if it contains its IP address. Only device with same IP Address responds with ARP reply. ARP reply contain MAC, IP**

* **Accessing Remote Resources**
* **Default Gateway- when a host needs to send a message to a remote network, it must use another router (default gateway). The default gateway is the IP address of an interface on a router on the same network as the sending host. Address of default gateway can be configured on local network. If wrongly configured, messages will not be delivered**
* **Moving data in the network: 1. Network Addresses 2. Data Link Addresses 3. Destination MAC address- when the receiving device is on diff network from sending device, this is ethernet MAC address of default gateway or router.**

**How does sending device determine the MAC address of the router: Each device knows IP address of the router through the default gateway configured in its TCP/IP settings. The default gateway address is the address of router interface connected to the same local network source device. All devices on the local network use the default gateway address to send messages to the router. After host knows default gateway IP Address, it can use ARP to determine the MAC address of that default gateway. Which is then placed in the frame.**