**Network Standard Protocols Standards** are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed or performed.

**Common Standardization Organizations** (Huawei, 2020)

* **Institute of Electrical and Electronics Engineers (IEEE)** is an international society composed of engineering professionals. It aims to promote development and education in the electrical engineering and computer science fields.
  + IEEE is probably best known for the standardization of LAN technologies. IEEE’s Project 802 aided in

the standardization of Ethernet (802.3), token-ring (802.5), and Wireless LAN’s (802.11).

* **American National Standards Institute (ANSI)** is an organization composed of more than one thousand representatives from industry and government who together to determine standards for electronics, industry and other fields such as chemical and nuclear engineering, health and safety, and construction.
  + This organization is known for published standards such as American Standard for Code Information Interchange (ASCII) and Small Computer System Interface (SCSI).
* **Electronic Industries Alliance (EIA)** is a trade organization composed of representatives from electronics manufacturing firms across the United States. This organization writes ANSI standards and legislation favorable to the growth of computer and electronic industries.
* **Telecommunications Industry Association (TIA)** focuses on standards for information technology, wireless, satellite, fiber optics, and telephone equipment.
  + The best-known standards to come from the TIA/EIA alliance are its guidelines for how network cable should be installed in commercial buildings, known as the “TIA/EIA 568 – B Series”.
* **Internet Engineering Task Force (IETF)** is an organization that is responsible for the overall development of the Internet and the standardization of internetworking technologies. In short, the IETF sets standards for how systems communicate over the Internet.
  + **Internet Society (ISOC)** – This oversees the overall development on the Internet.
  + **Internet Engineering Steering Group (IESG)** – This oversees the activities of IETF and manages the process used to introduce or update Internet standards.
  + **Internet Architecture Board (IAB)** – This serves as the technology advisory group to the Internet Society and is responsible for the overall development of the protocols and architecture associated with the Internet.
  + **Internet Assigned Numbers Authority (IANA)** – This oversees Internet naming and addressing; they

are in charge of all “unique parameters” on the Internet including IP (Internet Protocol) addresses.

* **Organization for Standardization (ISO) -** The International Organization for Standardization (ISO) is an international standards organization responsible for a wide range of standards, including many that are relevant to networking.

**Application Layer Protocols** (Huawei, 2020)

The application layer provides interfaces for application software so that applications can use network services. The application layer protocol designates transport layer protocols and ports.

* ***Simple Mail Transfer Protocol (SMTP)*** refers to a TCP/IP protocol that specifies a reliable and efficient transfer of electronic mail service on the Internet.
* ***Post Office Protocol, version 3 (POP3)*** refers to a TCP/IP protocol that is designed to allow a workstation to retrieve mail that the server is holding for it.
* ***Trivial File Transfer Protocol (TFTP)*** is a small and simple alternative to FTP that uses UDP to transfer files between systems.
* ***File Transfer Protocol (FTP)*** refers to a TCP/IP protocol that enables the sharing of computer programs and/or data between hosts over a TCP/IP network. It uses TCP to create a virtual connection for control information and then creates a separate TCP connection for data transfer.
* ***Network File System (NFS)*** refers to a TCP/IP protocol that enables computers to mount drives on remote hosts and operate them as if they were local drives.
* ***Domain Name System (DNS)*** refers to a TCP/IP protocol that is used on the Internet for translating names of domains and their publicly advertised network nodes into IP addresses.
* ***Simple Network Management Protocol (SNMP)*** refers to a TCP/IP protocol that monitors and controls the exchange of management information between networks and network components; it enables network administrators to manage configurations, statistics collection, network performance, and security. SNMP model includes three (3) components:
  + ***Managed devices*** collect and store management information and make this information available to NMSs using SNMP.
  + *An* ***agent*** has local knowledge of management information and translates that information into a form compatible with SNMP.
  + ***NMS*** executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management.
* ***Terminal Emulation Protocol Network (Telnet)*** refers to a TCP/IP protocol that uses the TCP as the transport protocol to establish a connection between server and client.
  + It uses special software called a ***daemon***, which is referred to as a remote host. A connection using Telnet is called a ***Virtual Terminal (VTY) session, or connection***.
* ***Remote login application (rlogin)*** is a UNIX command that allows authorized users to log in to other UNIX machines (hosts) on a network and to interact as if the user were physically at the host computer. Once the user is logged into the host, the user can do anything that the host has permitted, such as read, edit, or delete files.
* ***Hypertext Transfer Protocol (HTTP)*** refers to an application-level protocol service and an Internet standard developed by the IETF that supports the exchange of information on the World Wide Web, as well as on internal networks.
* ***HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)*** is a secure message-oriented communications protocol designed for use in conjunction with HTTP.
  + ***Secure Sockets Layer (SSL)*** – is a security protocol that works at a socket level. This layer exists between the TCP layer and the application layer to encrypt/decode data and authenticate concerned entities.

**TCP and UDP Connections** (Karumachi, et. al., 2020)

Computers running on the Internet communicate to each other using either the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP).

* ***Transport Control Protocol (TCP)*** refers to a ***connection-oriented*** TCP/IP standard transport layer protocol that provides reliable data delivery, duplicate data suppression, congestion control, and flow control on which many application protocols depend.
  + Transport protocols are used to deliver information from one port to another and thereby enable communication between application programs.
  + The reliability of the communication between the source and destination programs is ensured through error-detection and error-correction mechanisms that are implemented within TCP.
* ***User Datagram Protocol (UDP)*** refers to a ***connectionless*** TCP/IP standard transport layer protocol that provides unreliable, best-effort service.
  + UDP is a protocol that sends independent packets of data, called **datagrams**, from one computer to another with no guarantees about arrival.
    - Sending datagrams is much like sending a letter through the postal service: The order of delivery is not important and is not guaranteed, and each message is independent of any other.

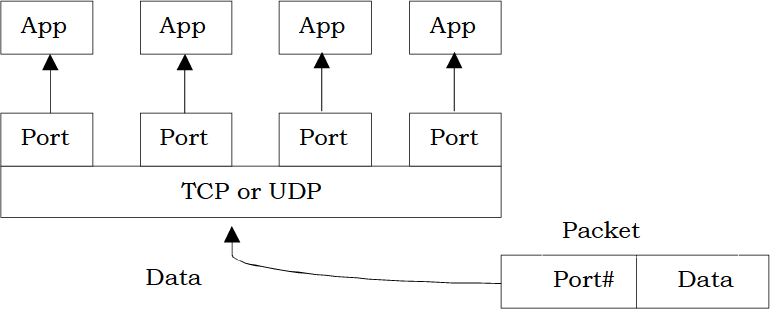
**Port Numbers** (Karumachi, et. al., 2020)

Data transmitted over the Internet is accompanied by addressing information that identifies the computer and the port for which it is destined.

* The computer is identified by its **32-bit IP address**, which it uses IP to deliver data to the **specific computer** on the network.
* **Ports** are identified by **a 16-bit number**, which TCP and UDP use to deliver the data to the **specific application**.

|  |  |
| --- | --- |
| **Port** | **Protocol** |
| **21** | File Transfer Protocol |
| **23** | Telnet Protocol |
| **25** | Simple Mail Transfer Protocol |
| **80** | Hypertext Transfer Protocol |

# TCP and UDP Formats TCP Header Fields



* Port numbers range from **0 to 65,535** because ports are represented by 16-bit numbers.
* The port numbers ranging from 0 - 1023 are restricted; they are reserved for use by well- known services such as HTTP and FTP and other system services called **well-known ports**.

(Karumachi, et. al., 2020)

* **Source Port** identifies the application that sends the segment. This field is 16 bits long.
* **Destination Port** identifies the application that receives the segment. This field is 16 bits long.
* **Sequence Number** refers to every byte of data sent over a TCP connection. The value of this field is equal to the sequence number of the first byte in a sent segment. This field is 32 bits long.
* **Acknowledgment Number** indicates the sequence number of the next segment's first byte that the receiver is expecting to receive. The value of this field is 1 plus the sequence number of the last byte in the previous segment that is successfully received. This field is 32 bits long.
* **Header Length** indicates the length of the TCP header. The unit is 32 bits (4 bytes). If there is no option content, the value of this field is 5, indicating that the header contains 20 bytes.
* **Reserved** - this field is always set to 0 as it is intended for future protocol changes. It is 6 bits long.
* **Control Bits** include FIN, ACK, and SYN flags which indicate the TCP data segments in different states.
* **Window** is used for TCP flow control. The value is the maximum number of bytes that are allowed by the receiver.
* **Checksum** is a mandatory field in which it is calculated and stored by the sender and verified by the receiver.

# UDP Header Fields

* **Source Port** identifies the application that sends the segment. This field is 16 bits long.
* **Destination Port** identifies the application that receives the segment. This field is 16 bits long.
* **Length** specifies the total length of the UDP header and data. The possible minimum length is 8 bytes because the UDP header already occupies 8 bytes.
* **Checksum** field refers to the checksum of the UDP header and UDP data. This field is 16 bits long.

**SYN-ACK Handshake** (Huawei, 2020)

|  |  |
| --- | --- |
| ***Three-way handshake*** is a method, in which the sender and the receiver inform their respective operating systems that a connection will be initiated before the actual data  communication begins.   * **SYN - Synchronize** * **ACK - Acknowledge** * **FIN - Finish** | Graphical user interface, text, application  Description automatically generated |

|  |  |
| --- | --- |
| **Sequence Number** and **Acknowledgment Number** fields to implement reliable and ordered data transmission. |  |
| **Window Sliding Mechanism**. requires the sender to receive an acknowledgment from the receiver after transmitting a certain amount of data. | Graphical user interface, application, email  Description automatically generated  TCP uses the sliding window mechanism to control the data transmission rate. |
| **TCP Shutdown (Four- Way Handshake)**  is engaged when the data transmission is complete in order to disconnect the TCP connection and release system resources. |  |

# References:

Comer, D. (2019). *The internet book: Everything you need to know about computer networking and how the internet works*. CRC Press.

Huawei. (2020). *HCIA-Datacom V1.0 Training Material*.

Karumanchi, N., Damodaram, A., & Rao, S. (2020). *Elements of computer networking: An integrated approach.* Career Monk.

Kurose, T & Ross, K. (2021). *Computer networking: A top-down approach.* Pearson. Robertazzi, T. (2017). *Introduction to computer networking.* Springer International.