DATA COMMUNICATION AND COMPUTER NETWORKS

|  |
| --- |
| **Chapter 1:** |
| **Teaching Hours: 10** | **Marks Distribution** |
| **Remember =04 M** | **Understanding = 08M** | **Applying =04M** | **Total =16M** |

data communication is defined as exchange of data between two devices via some form of transmission media such as a cable, wire or it can be air or vacuum also. For occurrence of data communication, communicating devices must be a part of communication system made up of a combination of hardware or software devices and programs.

There are mainly five components of a data communication system:

**.** Message

**2.** Sender

**3.** Receiver

**4.** Transmission Medium

**5.** Set of rules (Protocol)

All above mentioned elements are described below:



**Figure –** Components of Data Communication System

1. **Message :**
This is most useful asset of a data communication system. The message simply refers to data or piece of information which is to be communicated. A message could be in any form, it may be in form of a text file, an audio file, a video file, etc.
2. **Sender :**
To transfer message from source to destination, someone must be there who will play role of a source. Sender plays part of a source in data communication system. It is simple a device that sends data message. The device could be in form of a computer, mobile, telephone, laptop, video camera, or a workstation, etc.
3. **Receiver :**
It is destination where finally message sent by source has arrived. It is a device that receives message. Same as sender, receiver can also be in form of a computer, telephone mobile, workstation, etc.
4. [Transmission Medium :](https://www.geeksforgeeks.org/types-transmission-media/)
In entire process of data communication, there must be something which could act as a bridge between sender and receiver, Transmission medium plays that part. It is physical path by which data or message travels from sender to receiver. Transmission medium could be guided (with wires) or unguided (without wires), for example, twisted pair cable, fiber optic cable, radio waves, microwaves, etc.
5. **Setofrules(Protocol) :**
To govern data communications, various sets of rules had been already designed by the designers of the communication systems, which represent a kind of agreement between communicating devices. These are defined as protocol. In simple terms, the protocol is a set of rules that govern data communication. If two different devices are connected but there is no protocol among them, there would not be any kind of communication between those two devices. Thus the protocol is necessary for data communication to take place.

Protocols and standards are important in computer networks. They are like the rules and guidelines that allow different devices and systems to communicate and work together smoothly. Protocols define how data is sent, received, and processed, while standards ensure that various technologies are compatible with each other. This coordination is critical for the Internet and other networks to function constantly and efficiently.

Network protocol ensures that different technologies and components of the network are compatible with one another, reliable, and able to function together. In this article, we are going to discuss every point about protocols and standards in computer networks.

**What is Protocol?**

A protocol is a set of rules that determines how data is sent and received over a network. The protocol is just like a language that computers use to talk to each other, ensuring they understand and can respond to each other’s messages correctly. Protocols help make sure that data moves smoothly and securely between devices on a network.

To make communication successful between devices, some rules and procedures should be agreed upon at the sending and receiving ends of the system. Such rules and procedures are called Protocols. Different types of protocols are used for different types of communication.



*Protocols*

In the above diagrams, Protocols are shown as a set of rules. Communication between the Sender and Receiver is not possible without Protocol**.**

**Key Elements of Protocol**

* **Syntax:** Syntax refers to the structure or the format of the data that gets exchanged between the devices. Syntax of the message includes the type of data, composition of the message, and sequencing of the message. The starting 8 bits of data are considered as the address of the sender. The next 8 bits are considered to be the address of the receiver. The remaining bits are considered as the message itself.
* **Semantics:** Semantics defines data transmitted between devices. It provides rules and norms for understanding message or data element values and actions.
* **Timing:** Timing refers to the synchronization and coordination between devices while transferring the data. Timing ensures at what time data should be sent and how fast data can be sent. For example, If a sender sends 100 Mbps but the receiver can only handle 1 Mbps, the receiver will overflow and lose data. Timing ensures preventing of data loss, collisions, and other timing-related issues.
* **Sequence Control:**Sequence control ensures the proper ordering of data packets. The main responsibility of sequence control is to acknowledge the data while it get received, and the retransmission of lost data. Through this mechanism, the data is delivered in correct order.
* **Flow Control:** [Flow control](https://www.geeksforgeeks.org/flow-control-in-data-link-layer/) regulates device data delivery. It limits the sender’s data or asks the receiver if it’s ready for more. Flow control prevents data congestion and loss.
* **Error Control:** [Error control](https://www.geeksforgeeks.org/error-control-in-data-link-layer/) mechanisms detect and fix data transmission faults. They include error detection codes, data resend, and error recovery. Error control detects and corrects noise, interference, and other problems to maintain [data integrity](https://www.geeksforgeeks.org/difference-between-data-security-and-data-integrity/).
* **Security** **:** Network security protects data confidentiality, integrity, and authenticity. which includes encryption, authentication, access control, and other security procedures. Network communication’s privacy and trustworthiness are protected by security standards.

**Types of Protocol**

* **Network Layer Protocols** **:**Network layer protocols operate in the network layer which is also known as the Layer 3 of the network  architecture. Network layer protocols are responsible for packet routing, forwarding, and addressing of data packets throughout the network. IP and [ICMP](https://www.geeksforgeeks.org/internet-control-message-protocol-icmp) are the network layer protocols.
* **Transport Layer Protocols**: Transport layer protocols work in the transport layer which provides end-to-end service ensuring data transfer across apps on different devices. [TCP](https://www.geeksforgeeks.org/what-is-transmission-control-protocol-tcp) and [UDP](https://www.geeksforgeeks.org/user-datagram-protocol-udp) are the most popular transport layer protocols.
* **Application Layer Protocol:**Application layer protocol working in the application layer of the network architecture provides communication between applications running on different devices. The application layer protocols enable cross-device communication. They format, exchange, and interpret application data. [HTTP](https://www.geeksforgeeks.org/http-full-form), [FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer), and [SMTP](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp)are examples.
* **Wireless Protocols:**Wireless protocols basically used in wireless communication which enables data transfer through wireless networks. [Bluetooth](https://www.geeksforgeeks.org/bluetooth), [Wi-Fi](https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity), and LTE protocols are examples.
* **Routing Protocols:**Routing protocol establishes the best/optimal network pathways throughout the network for fastest data transmission. Routers share information to develop and maintain routing tables. [RIP](https://www.geeksforgeeks.org/routing-information-protocol-rip), [OSPF](https://www.geeksforgeeks.org/open-shortest-path-first-ospf-protocol-states/), and [BGP](https://www.geeksforgeeks.org/border-gateway-protocol-bgp) are examples.
* **Security Protocols :**security protocol protects data confidentiality, integrity, and authenticity while transmission of data over the network. They include [SSL and TLS](https://www.geeksforgeeks.org/difference-between-secure-socket-layer-ssl-and-transport-layer-security-tls), encryption methods, and authentication protocols for providing data security.
* **Internet Protocols :**IP identifies devices uniquely. Internet protocol provides data communication through routing and  forwarding data packets from one device to another by unique addressing scheme.

**Important Protocols Used in Computer Network**

Here are some key protocols that are widely used in computer networks:

* **TCP (Transmission Control Protocol):**Ensures data is sent and received accurately by breaking it into packets, sending them, and reassembling them at the destination.
* **IP (Internet Protocol):**Addresses and routes the packets to make sure they reach the right destination.
* **HTTP/HTTPS (HyperText Transfer Protocol/Secure):** HTTP used for transferring web pages on the internet. When you browse a website, your browser uses HTTP to request and display web pages. And HTTPs is a secure version of HTTP that encrypts data to protect it from being intercepted.
* **FTP (File Transfer Protocol):** Used for transferring files between computers on a network. It allows users to upload and download files.**SMTP (Simple Mail Transfer Protocol):**Used for sending emails. It transfers emails from a client to a server or between servers.
* **DNS (Domain Name System):** It is used to translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network.
* **DHCP (Dynamic Host Configuration Protocol):** Automatically assigns IP addresses to devices on a network, ensuring each device has a unique address.
* **SSH (Secure Shell):** Provides a secure way to access and manage devices over a network. It encrypts the data, making it safe from eavesdropping.
* **SNMP (Simple Network Management Protocol):** Used for managing and monitoring network devices like routers, switches, and servers. It collects and organizes information about these devices

**How are Protocols Used in Cyber Attacks?**

Attackers can misuse the rules of how data is sent over the internet to cause problems for systems. One common way they do this is through distributed denial-of-service ([DDoS](https://www.geeksforgeeks.org/what-is-ddosdistributed-denial-of-service/)) attacks.

For example, in a SYN flood attack, attackers exploit the TCP protocol. Normally, a device sends a SYN packet to a server to start a connection, and the server responds, expecting a final response to complete the connection. Attackers send many SYN packets but never complete the connections. This overloads the server, preventing it from working properly for real users.

Cloudflare offers solutions to stop these kinds of attacks. One of their services, Cloudflare Magic Transit, protects against attacks targeting different levels of the network system. In the case of a SYN flood attack, [Cloudflare](https://www.geeksforgeeks.org/what-is-cloudflare/) manages the TCP connections for the server, so the server doesn’t get overwhelmed and can continue to serve real users.

**What is Standards?**

Standards are the set of rules for data communication that are needed for the exchange of information among devices. It is important to follow Standards which are created by various  Standard Organizations like IEEE, ISO, ANSI, etc.

**Types of Standards**

* **De Facto Standard:**The meaning of the word *” De Facto ”* is ” By Fact ”  or “By Convention”. These are the standards that have not been approved by any Organization but have been adopted as  Standards because of their widespread use. Also, sometimes these standards are often established by Manufacturers.
**For example** **:** Apple  and Google are two companies that established their own rules for their products which are different. Also, they use some same standard rules for manufacturing their products.
* **De Jure Standard:**The meaning of the word *“De Jure”* is  “By Law” or “By  Regulations”.Thus, these are the standards that have been approved by officially recognized bodies like [ANSI](https://www.geeksforgeeks.org/what-is-ansi/), [ISO](https://www.geeksforgeeks.org/iso-full-form/), [IEEE](https://www.geeksforgeeks.org/difference-between-ieee-802-3-802-4-and-802-5/), etc. These are the standards that are important to follow if it is required or needed.
**For example** **:** All the data communication standard  protocols like [SMTP](https://www.geeksforgeeks.org/simple-mail-transfer-protocol-smtp), TCP, IP, [UDP](https://www.geeksforgeeks.org/user-datagram-protocol-udp) etc. are important to follow the same when we need them.

**Protocol and Standard Compliance in Network Security**

* **Interoperability:** Protocols and standards allow devices and systems to communicate. These protocols ensure network components can function together, avoiding risks and security gaps produced by incompatible or unsupported systems.
* **Security Baseline :** Protocols and standards contain security principles and best practices that help secure network infrastructure. These protocols allow organizations to protect sensitive data via [encryption](https://www.geeksforgeeks.org/what-is-data-encryption/), [authentication](https://www.geeksforgeeks.org/difference-between-authentication-and-authorization/), and access controls.
* **Vulnerability Management :** Network security protocols and standards help organizations find and fix vulnerabilities. Many standards requires regular security assessments, vulnerability scanning, and penetration testing to discover network infrastructure flaws. Organizations can prevent [cyberattacks](https://www.geeksforgeeks.org/types-of-cyber-attacks/) and address vulnerabilities by following these compliance criteria.

**Best Practices for Ensuring Protocol and Standard Compliance**

* Use [cryptography](https://www.geeksforgeeks.org/cryptography-and-its-types) tools to secure personal data transported across your network, making sure that data encryption methods exceed industry requirements.
* Perform frequent security checks on all network devices to discover vulnerabilities and verify they fulfil compliance standards.
* Restrict user access to specified network zones to ensure secure data sharing and prevent unauthorized access.

In computer network bandwidth and data rate both are important concept to understand network performance. Although they are very closely related, but they have distinct differences. In this article we will see difference between bandwidth and datarate in detail.

**What is the Bandwidth?**

[Bandwidth](https://www.geeksforgeeks.org/what-is-bandwidth-definition-working-importance-uses/) is defined as the width of the spectrum. [Spectrum](https://www.geeksforgeeks.org/what-is-spread-spectrum/) is the range of frequencies contained in the signal. Since bandwidth is the width of the spectrum and spectrum is a range of frequencies, bandwidth is measured in Hertz or Mhz.

**Advantages of Bandwidth**

* It has a Higher Data Transfer Capacity which allows more data to be transferred simultaneously.
* It can be used to improve performance with more bandwidth.
* It helps to enhance the Quality of Service as it supports high-quality video streaming, online gaming, etc.

**Disadvantages of Bandwidth**

* The Higher bandwidth connections are typically more expensive.
* In some cases, the full potential of high bandwidth can’t be utilized.
* It needs more advanced infrastructure which can be expensive.

**What is the Data Rate?**

[Data Rate](https://www.geeksforgeeks.org/what-is-data-transfer-rate/) is defined as the amount of data transmitted during a specified period over a network. It is the speed at which data is transferred from one device to another or between a peripheral device and the computer. It is generally measured in [Megabits per second(Mbps)](https://www.geeksforgeeks.org/what-are-megabits-per-second-mbps/).

**Advantages of Data Rate**

* Data rate helps to show the actual speed of data transfer.
* The Data Rate can help in optimizing network resources and managing traffic.
* A high data rate ensures a better user experience with less buffering.

**Disadvantages of Data Rate**

* The Data Rate can go with Variable Speeds.
* The Data Rate Depends upon the Bandwidth.
* Many External Factors can influence the data rate.

**Difference between Bandwidth and Data Rate**

| **Bandwidth** | **Data Rate** |
| --- | --- |
| It is the potential of carrier channels that can carry data.  | It is the amount of data transmitted during a specified period over a network. |
| It is the difference between the range of frequencies.  | It is the speed of [Data Transmission](https://www.geeksforgeeks.org/transmission-modes-computer-networks/). |
| Normally it is measured in Hz or kHz or Mhz. | It is normally measured in Mbps or MBps. |
| It refers to the maximum data transmission capacity of the channel.  | It refers to the actual data transmission speed. |
| It is a physical layer property in the [OSI Model](https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/). | While it is common in all layers. |
| It shows the capacity of the channel. | It shows the present speed of data transmission. |
| It does not depend on the properties of the sender or receiver. | While it gets affected by the sender or receiver. |

Both Bit rate and Baud rate are generally used in data communication to measure the speed of data. **Bit rate** refers to the number of bits transmitted per second in a communication system, while **baud rate** refers to the number of signal units or symbols transmitted per second. In some cases, multiple bits can be encoded in a single symbol, making the bit rate higher than the baud rate.

**What is the Bit Rate?**

Bit rate refers to the number of bits transmitted per second and is, therefore, a measure of the rapidity at which data is being transmitted over a communication channel. It is normally expressed in Kbps, Mbps, or Gbps. It will, therefore, give the relative efficiency of computer processing or handling data.

Bit Rate = Baud Rate × No. of Bits per Baud

**What is the Baud Rate?**

It is defined to be the number of signal changes or symbols sent per second over a communication channel. This decides the extent to which a transmission medium, such as a wire or a wireless spectrum, is capable of changing its state in one second. Every such change can represent one or more bits of data.

Baud Rate = Bit Rate / No. of Bits per Baud

The baud rate is important in appreciating the amount of bandwidth required during any given transmission. A higher baud rate may signal a more frequent change in a given signal and thus change the clarity and speed of data transmission.

**Difference Between Bit Rate and Baud Rate**

| **Bit Rate** | **Baud Rate** |
| --- | --- |
| [Bit rate](https://www.geeksforgeeks.org/bit-rate/) is defined as the transmission of a number of bits per second. | [Baud rate](https://www.geeksforgeeks.org/baud-rate-and-its-importance/) is defined as the number of signal units per second. |
| Bit rate is also defined as per second travel number of bits. | Baud rate is also defined as per second number of changes in signal. |
| Bit rate emphasized computer efficiency. | While the baud rate emphasized data transmission. |
| The formula of Bit Rate is:=Baud Rate × Number of Bits per Baud | The formula of Baud Rate is:= Bit Rate / Number of Bits per Baud |
| Bit rate is not used to decide the requirement of bandwidth for transmission of the signal. | While baud rate is used to decide the requirement of bandwidth for transmission of the signal. |
| Bit Rate cannot determine the bandwidth. | Baud rate can determine the amount of bandwidth necessary to send the signal. |
| It counts the number of bits traveled per second such as Kbps, Mbps, Gbps, etc | It counts how many times the state of a signal is changing. |

A[computer network](https://www.geeksforgeeks.org/basics-computer-networking/) is a system that connects many independent computers to share information (data) and resources. The integration of computers and other different devices allows users to communicate more easily. A computer network is a collection of two or more computer systems that are linked together. A network connection can be established using either [cable](https://www.geeksforgeeks.org/what-is-coaxial-cable/) or [wireless media.](https://www.geeksforgeeks.org/wired-and-wireless-networking/) Hardware and software are used to connect computers and tools in any network.

**Local Area Network (LAN)**

LAN is the most frequently used network. A [LAN](https://www.geeksforgeeks.org/lan-full-form/)is a computer network that connects computers through a common communication path, contained within a limited area, that is, locally. A LAN encompasses two or more computers connected over a server. The two important technologies involved in this network are [Ethernet](https://www.geeksforgeeks.org/local-area-network-lan-technologies/)and [Wi-fi](https://www.geeksforgeeks.org/what-is-wi-fiwireless-fidelity/).  It ranges up to 2km & transmission speed is very high with easy maintenance and low cost. Examples of LAN are networking in a home, school, library, laboratory, college, office, etc.



*Local Area Network (LAN)*

**Advantages of a LAN**

* **Privacy:** LAN is a private network, thus no outside regulatory body controls it, giving it a privacy.
* **High Speed:** LAN offers a much higher speed(around 100 mbps) and data transfer rate comparatively to WAN.
* **Supports different transmission mediums:** LAN support a variety of communications transmission medium such as an Ethernet cable (thin cable, thick cable, and twisted pair), fiber and wireless transmission.
* **Inexpensive and Simple:** A LAN usually has low cost, installation, expansion and maintenance and LAN installation is relatively easy to use, good scalability.

**Disadvantages of LAN**

* The initial setup costs of installing Local Area Networks is high because there is special software required to make a server.
* Communication devices like an ethernet cable, switches, [hubs](https://www.geeksforgeeks.org/advantages-and-disadvantages-of-hub), routers, cables are costly.
* LAN administrator can see and check personal data files as well as[Internet](https://www.geeksforgeeks.org/internet-and-its-services) history of each and every LAN user. Hence, the privacy of the users are violated
* LANs are restricted in size and cover only a limited area
* Since all the data is stored in a single server computer, if it can be accessed by an unauthorized user, can cause a serious data [security threat](https://www.geeksforgeeks.org/computer-security-threats).

**Metropolitan Area Network (MAN)**

A [MAN](https://www.geeksforgeeks.org/man-full-form-in-computer-networking/) is larger than a LAN but smaller than a WAN. This is the type of computer network that connects computers over a geographical distance through a shared communication path over a city, town, or metropolitan area. This network mainly uses FDDI, CDDI, and ATM as the technology with a range from 5km to 50km. Its transmission speed is average. It is difficult to maintain and it comes with a high cost. Examples of MAN are networking in towns, cities, a single large city, a large area within multiple buildings, etc.



*Metropolitan Area Network (MAN)*

**Advantages of MAN**

* MAN offers high-speed connectivity in which the speed ranges from 10-100 Mbps.
* The security level in MAN is high and strict as compared to WAN.
* It support to transmit data in both directions concurrently because of dual bus architecture.
* MAN can serve multiple users at a time with the same high-speed internet to all the users.
* MAN allows for centralized management and control of the network, making it easier to monitor and manage network resources and security.

**Disadvantages of MAN**

* The architecture of MAN is quite complicated hence, it is hard to design and maintain.
* This network is highly expensive because it required the high cost to set up fiber optics.
* It provides less fault tolerance.
* The Data transfer rate in MAN is low when compare to LANs.

**5. Wide Area Network (WAN)**

WAN is a type of computer network that connects computers over a large geographical distance through a shared communication path. It is not restrained to a single location but extends over many locations. [WAN](https://www.geeksforgeeks.org/wan-full-form/) can also be defined as a group of local area networks that communicate with each other with a range above 50km. Here we use Leased-Line & Dial-up technology. Its transmission speed is very low and it comes with very high maintenance and very high cost. The most common example of WAN is the Internet.



*Wide Area Network (WAN)*

**Advantages of WAN**

* It covers large geographical area which enhances the reach of organisation to transmit data quickly and cheaply.
* The data can be stored in centralised manner because of remote access to data provided by WAN.
* The travel charges that are needed to cover the geographical area of work can be minimised.
* WAN enables a user or organisation to connect with the world very easily and allows to exchange data and do business at global level.

**Disadvantages of WAN**

* Traffic congestion in Wide Area Network is very high.
* The fault tolerance ability of WAN is very less.
* Noise and error are present in large amount due to multiple connection point.
* The data transfer rate is slow in comparison to LAN because of large distances and high number of connected system within the network.

Technology in imparting the communication systems has moved a long way from analog to digital technology. It is important for students, engineers and everybody interested in digital communications to know the differences between analog and digital communications. In this article, authors are going to explain what are primary differences between informative and persuasive communication.

**What is Analog Communication?**

In [Analog communication](https://www.geeksforgeeks.org/introduction-to-analog-communication/) the data is transferred with the help of analog signal in between transmitter and receiver. Any type of data is transferred in analog signal. Any data is converted into electric form first and after that it is passed through communication channel. Analog communication uses a continuous signal which varies in amplitude, phase, or some other property with time in proportion to that of a variable.

**Advantages of Analog Signals**

* It is Easier in processing.
* Analog Signals are best fitted to audio and video transmission.

**Disadvantages of Analog Signals**

* Analog tends to possess a lower quality signal than digital.
* The cables are sensitive to external influences.
* Analog wire is expensive and not easily portable.

**The below figure illustrates the Analog Communication System**



**What is Digital Communication?**

In [Digital communication](https://www.geeksforgeeks.org/introduction-to-digital-communication/) digital signal is used rather than analog signal for communication in between the source and destination. The digital signal consists of discrete values rather than continuous values. In digital communication physical transfer of data occurs in the form of digital bit stream i.e 0 or 1 over a point-to-point or point-to-multipoint transmission medium. In digital communication the digital transmission data can be broken into packets as discrete messages which is not allowed in analog communication.

**Advantages of Digital Communication**

* The speed of data transmission is quite high therefore, message transfer occurs almost instantly.
* The process of digital communication is quite efficient because speed and accuracy are always maintained in this system.
* The wireless nature of digital communication can be used to establish connections globally without major geographical constraints.

**Disadvantages of Digital Communication**

* Digital Communication lacks a personal touch due to a lack of proper interaction between users at both the ends of channel.
* With an increase in network coverage, the complexity of digital communication systems increases and therefore, implementation of such [circuits](https://www.geeksforgeeks.org/electric-circuit/) is difficult.

**The below figure illustrates the Digital Communication System**

