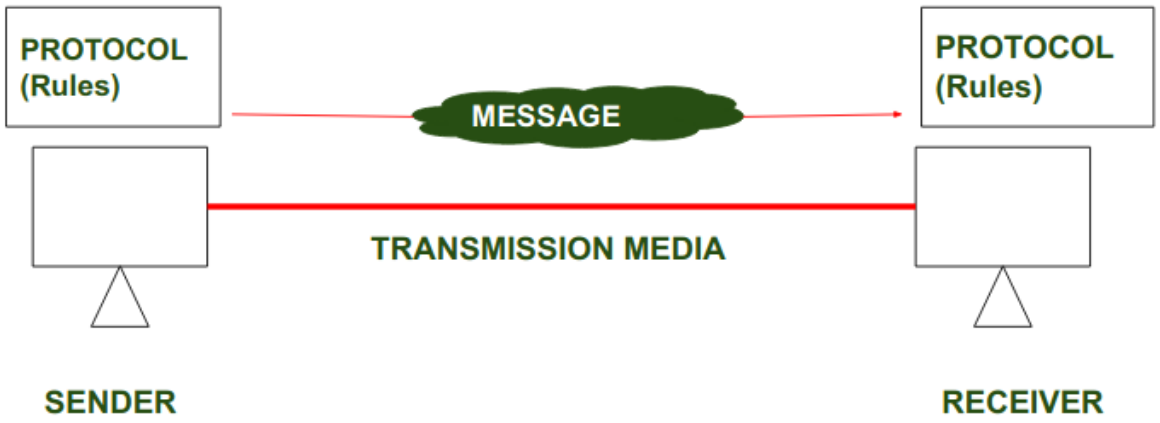
Protocol and Standard in Computer Networks

Computer networks are dependent on protocols and standards which plays a vital role, which enables communication between different devices and systems with one another and share data seamlessly. Network protocol ensures that different technologies and components of the network are compatible with one another, reliable, and able to function together.

Overview of Protocol

In Order 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 as Protocols. Different types of protocols are used for different types of communication.



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

Key Element of Protocol

- **Syntax:** syntax refers to the structure or the format of the data that gets exchanged between the devices. Syntax of message includes the type of data, composition of message and sequencing of message. The starting 8 bits of data is considered as the address of the sender. The next 8 bits is 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 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 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 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.
- **Security:** Network security safeguards 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.

Standards

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

Types of Standards

Standards are of two types :

- De Facto Standard.
- De Jure Standard.

De Facto Standard : The meaning of the work *" De Facto "* is " By Fact " or "By Convention".These are the standard s that have not been approved by any Organization , but have been adopted as Standards because of it's widespread use. Also , sometimes these standards are often established by Manufacturers.

For example : Apple and Google are two companies which established their own rules on their products which are different . Also they use some same standard rules for manufacturing for 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 body like ANSI , ISO , IEEE etc. These are the standard which are important to follow if it is required or needed.

For example : All the data communication standard protocols like SMTP , TCP , IP , UDP etc. are important to follow the same when we needed them.

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 are the network layer protocols.
- **Transport layer Protocols** : Transport layer protocols works in transport layer which provides end-to-end service ensuring data transfer across apps on different devices. TCP and 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, FTP, and SMTP are examples.
- **Wireless Protocols :** Wireless protocols basically used in wireless communication which enables data transfer through wireless networks. Bluetooth, Wi-Fi, 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, OSPF, and 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, 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.

Protocol and Standard Compliance in Network Security

Protocol and standard compliance protects data, resources, and networks. Protocol and standard compliance are crucial to network security for these reasons:

- **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, authentication, 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 and address vulnerabilities by following these compliance criteria.