Networking Protocols

Definition

A network protocol is a set of established rules that specify how to format, send and receive data so that computer network endpoints, including computers, servers, routers and virtual machines, can communicate despite differences in their underlying infrastructures, designs or standards.

To successfully send and receive information, devices on both sides of a communication exchange must accept and follow protocol conventions. In networking, support for protocols can be built into the software, hardware, or both.

Without network protocols, computers and other devices would not know how to engage with each other. As a result, except for specialty networks built around a specific architecture, few networks would be able to function, and the internet as we know it wouldn't exist. Virtually all network end users rely on network protocols for connectivity.

How do Network Protocols Work?

It is essential to understand how devices communicate over a network by recognizing network protocols. The Open Systems Interconnection (OSI), the most widely used model, illustrates how computer systems interact with one another over a network. The communication mechanism between two network devices is shown by seven different layers in the OSI model. Every layer in the OSI model works based on different network protocols. At every layer, one or more protocols are there for network communication. To enable network-to-network connections, the Internet Protocol (IP), for instance, routes data by controlling information like the source and destination addresses of data packets. It is known as a network layer protocol.

Types of Network Protocols

In most cases, communication across a network like the Internet uses the OSI model. The OSI model has a total of seven layers. Secured connections, network management, and network communication are the three main tasks that the network protocol performs. The purpose of protocols is to link different devices.

The protocols can be broadly classified into three major categories:

1. Network Communication
2. Network Management
3. Network Security

1. Network Communication

Communication protocols are important for the functioning of a network. They are so crucial that it is not possible to have computer networks without them. These protocols formally set out the rules and formats through which data is transferred. These protocols handle syntax, semantics, error detection, synchronization, and authentication. Below mentioned are some network communication protocol:

Hypertext Transfer Protocol(HTTP)

It is a layer 7 protocol that is designed for transferring a hypertext between two or more systems. HTTP works on a client-server model, most of the data sharing over the web is done through using HTTP.

Transmission Control Protocol(TCP)

TCP layouts a reliable stream delivery by using sequenced acknowledgment. It is a connection-oriented protocol i.e., it establishes a connection between applications before sending any data. It is used for communicating over a network. It has many applications such as emails, FTP, streaming media, etc.

User Datagram Protocol(UDP)

It is a connectionless protocol that lay-out a basic but unreliable message service. It adds no flow control, reliability, or error-recovery functions. UPD is functional in cases where reliability is not required. It is used when we want faster transmission, for multicasting and broadcasting connections, etc.

Border Gateway Protocol(BGP)

BGP is a routing protocol that controls how packets pass through the router in an independent system one or more networks run by a single organization and connect to different networks. It connects the endpoints of a LAN with other LANs and it also connects endpoints in different LANs to one another.

Address Resolution Protocol(ARP)

ARP is a protocol that helps in mapping logical addresses to the physical addresses acknowledged in a local network. For mapping and maintaining a correlation between these logical and physical addresses a table known as ARP cache is used.

Internet Protocol(IP)

It is a protocol through which data is sent from one host to another over the internet. It is used for addressing and routing data packets so that they can reach their destination.

Dynamic Host Configuration Protocol(DHCP)

it’s a protocol for network management and it’s used for the method of automating the process of configuring devices on IP networks. A DHCP server automatically assigns an IP address and various other configurational changes to devices on a network so they can communicate with other IP networks. it also allows devices to use various services such as NTP, DNS, or any other protocol based on TCP or UDP.

2. Network Management

These protocols assist in describing the procedures and policies that are used in monitoring, maintaining, and managing the computer network. These protocols also help in communicating these requirements across the network to ensure stable communication. Network management protocols can also be used for troubleshooting connections between a host and a client.

Internet Control Message Protocol(ICMP)

It is a layer 3 protocol that is used by network devices to forward operational information and error messages. ICMP is used for reporting congestions, network errors, diagnostic purposes, and timeouts.

Simple Network Management Protocol(SNMP)

It is a layer 7 protocol that is used for managing nodes on an IP network. There are three main components in the SNMP protocol i.e., SNMP agent, SNMP manager, and managed device. SNMP agent has the local knowledge of management details, it translates those details into a form that is compatible with the SNMP manager. The manager presents data acquired from SNMP agents, thus helping in monitoring network glitches, and network performance, and troubleshooting them.

Gopher

It is a type of file retrieval protocol that provides downloadable files with some description for easy management, retrieving, and searching of files. All the files are arranged on a remote computer in a stratified manner. Gopher is an old protocol and it is not much used nowadays.

File Transfer Protocol(FTP)

FTP is a Client/server protocol that is used for moving files to or from a host computer, it allows users to download files, programs, web pages, and other things that are available on other services.

Post Office Protocol(POP3)

It is a protocol that a local mail client uses to get email messages from a remote email server over a TCP/IP connection. Email servers hosted by ISPs also use the POP3 protocol to hold and receive emails intended for their users. Eventually, these users will use email client software to look at their mailbox on the remote server and to download their emails. After the email client downloads the emails, they are generally deleted from the servers.

Telnet

It is a protocol that allows the user to connect to a remote computer program and to use it i.e., it is designed for remote connectivity. Telnet creates a connection between a host machine and a remote endpoint to enable a remote session.

3. Network Security

These protocols secure the data in passage over a network. These protocols also determine how the network secures data from any unauthorized attempts to extract or review data. These protocols make sure that no unauthorized devices, users, or services can access the network data. Primarily, these protocols depend on encryption to secure data.

Secure Soket Layer(SSL)

It is a network security protocol mainly used for protecting sensitive data and securing internet connections. SSL allows both server-to-server and client-to-server communication. All the data transferred through SSL is encrypted thus stopping any unauthorized person from accessing it.

Hypertext Transfer Protocol(HTTPS)

It is the secured version of HTTP. this protocol ensures secure communication between two computers where one sends the request through the browser and the other fetches the data from the web server.

Transport Layer Security(TLS)

It is a security protocol designed for data security and privacy over the internet, its functionality is encryption, checking the integrity of data i.e., whether it has been tampered with or not, and authentication. It is generally used for encrypted communication between servers and web apps, like a web browser loading a website, it can also be used for encryption of messages, emails, and VoIP.