Network protocols

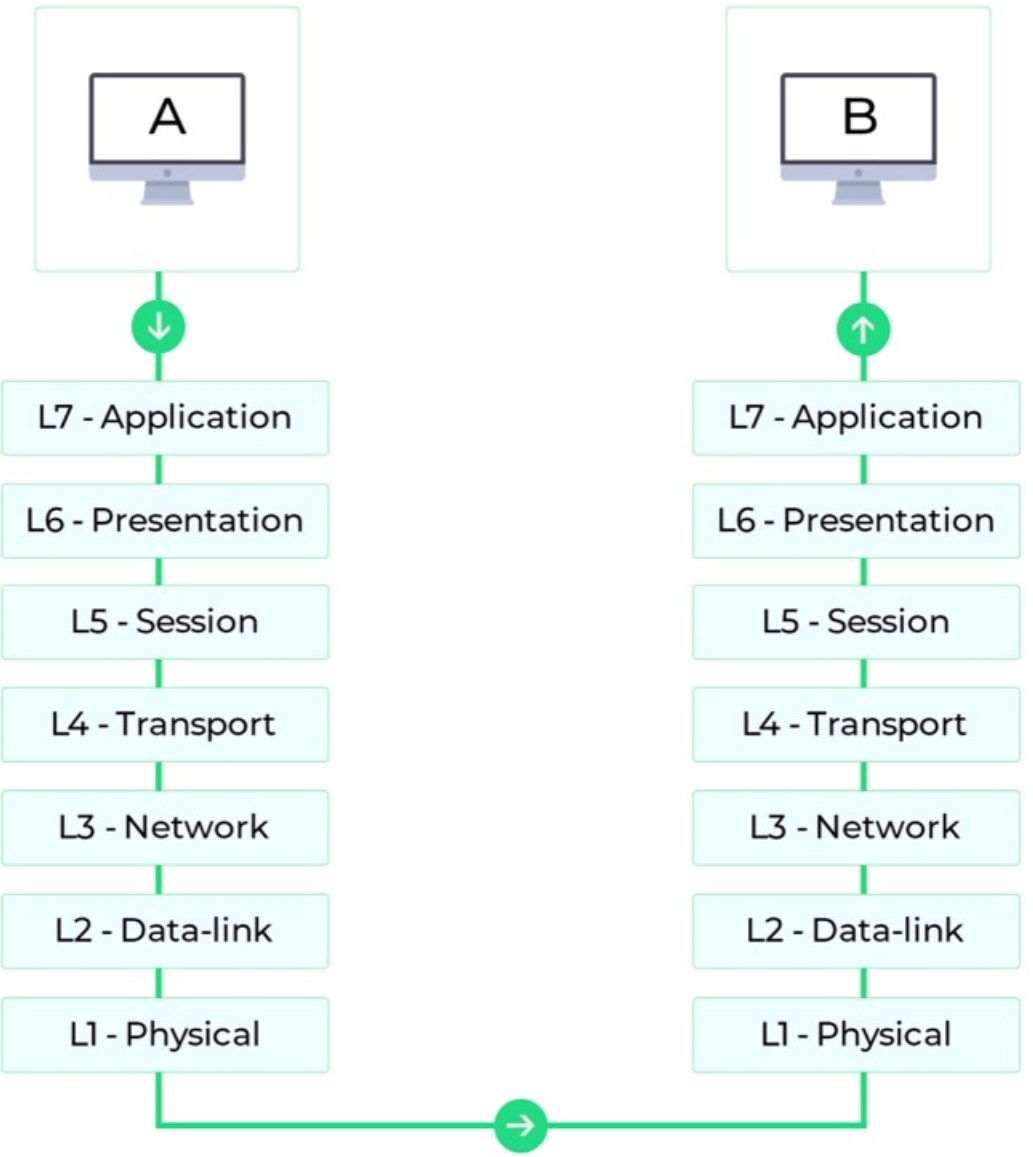
Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks. In other words, network protocols can be equated to languages that two devices must understand for seamless communication of information, regardless of their infrastructure and design disparities.

The OSI model: How network protocols work

To understand the nuances of network protocols , it's imperative to know about the Open Systems Interconnection (OSI) model first. Considered the primary architectural model for internet working communications, the majority of network protocols used today are structurally based on the OSI model.

The OSI model splits the communication process between two network devices into 7 layers. A task or group of tasks is assigned to each of these 7 layers. All the layers are self-contained, and the tasks assigned to them can be executed independently.

To put this into context, here is a representation of the communication process between two network devices following the OSI model:



The seven layers in the OSI model can be divided into two groups: upper layers, including layers 7, 6, and 5, and lower layers, including layers 4, 3, 2, and 1. The upper layers deal with application issues, and the lower layers deal with data transport issues.

Classification of network protocols

Now that you know how the OSI model works, you can dive straight into the classification of protocols. The following are some of the most prominent protocols used in network communication.

Application layer network protocols

1. DHCP: Dynamic Host Configuration Protocol

DHCP is a communication protocol that enables network administrators to automate the assignment of IP addresses in a network. In an IP network, every device connecting to the internet requires a unique IP. DHCP lets network admins distribute IP addresses from a central point and automatically send a new IP address when a device is plugged in from a different place in the network. DHCP works on a client-server model.

Advantages of using DHCP

- Centralized management of IP addresses.
- Seamless addition of new clients into a network.
- Reuse of IP addresses, reducing the total number of IP addresses required.

Network protocols divide the communication process into discrete tasks across every layer of the OSI model. One or more network protocols operate at each layer in the communication exchange.

Following are the detailed descriptions of the functioning of network protocols in each layer of the OSI model:

Though some say the OSI model is now redundant and less significant than the Transmission Control Protocol (TCP)/IP network model, there are still references to the OSI model even today as the model's structure helps to frame discussions of protocols and contrast various technologies.

Classification of network protocols

Now that you know how the OSI model works, you can dive straight into the classification of protocols. The following are some of the most prominent protocols used in network communication.

Disadvantages of using DHCP

- Tracking internet activity becomes tedious, as the same device can have multiple IP addresses over a period of time.
- Computers with DHCP cannot be used as servers, as their IPs change over time.

2. DNS: Domain Name System protocol

The DNS protocol helps in translating or mapping host names to IP addresses. DNS works on a client-server model, and uses a distributed database over a hierarchy of name servers.

Hosts are identified based on their IP addresses, but memorizing an IP address is difficult due to its complexity. IPs are also dynamic, making it all the more necessary to map domain names to IP addresses. DNS helps resolve this issue by converting the domain names of websites into numerical IP addresses.

Advantages

- DNS facilitates internet access.
- Eliminates the need to memorize IP addresses.

Disadvantages

- DNS queries don't carry information pertaining to the client who initiated it. This is because the DNS server only sees the IP from where the query came from, making the server susceptible to manipulation from hackers.
- DNS root servers, if compromised, could enable hackers to redirect to other pages for phishing data.

3. FTP: File Transfer Protocol

File Transfer Protocol enables file sharing between hosts, both local and remote, and runs on top of TCP. For file transfer, FTP creates two TCP connections: control and data connection. The control connection is used to transfer control information like passwords, commands to retrieve and store files, etc., and the data connection is used to transfer the actual file. Both of these connections run in parallel during the entire file transfer process.

Advantages

- Enables sharing large files and multiple directories at the same time.
- Lets you resume file sharing if it was interrupted.
- Lets you recover lost data, and schedule a file transfer.

Disadvantages

- FTP lacks security. Data, usernames, and passwords are transferred in plain text, making them vulnerable to malicious actors.
- FTP lacks encryption capabilities, making it non-compliant with industry standards.

4. HTTP: Hyper Text Transfer Protocol

HTTP is an application layer protocol used for distributed, collaborative, and hypermedia information systems. It works on a client-server model, where the web browser acts as the client. Data such as text, images, and other multimedia files are shared over the World Wide Web using HTTP. As a request and response type protocol, the client sends a request to the server, which is then processed by the server before sending a response back to the client.

HTTP is a stateless protocol, meaning the client and server are only aware of each other while the connection between them is intact. After that, both the client and server forget about each other's existence. Due to this phenomenon, the client and server can't both retain information between requests.

Advantages

- Memory usage and CPU usage are low because of lesser concurrent connections.
- Errors can be reported without closing connections.
- Owing to lesser TCP connections, network congestion is reduced.

Disadvantages

- HTTP lacks encryption capabilities, making it less secure.
- HTTP requires more power to establish communication and transfer data.

5. IMAP and IMAP4: Internet Message Access Protocol (version 4)

IMAP is an email protocol that lets end users access and manipulate messages stored on a mail server from their email client as if they were present locally on their remote device. IMAP follows a client-server model, and lets multiple clients access messages on a common mail server concurrently. IMAP includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and removing flags; and much more. The current version of IMAP is version 4 revision 1.

Advantages

- As the emails are stored on the mail server, local storage utilization is minimal.
- In case of accidental deletion of emails or data, it is always possible to retrieve them as they are stored on the mail server.

Disadvantages

- Emails won't work without an active internet connection.
- High utilization of emails by end users requires more mailbox storage, thereby augmenting costs.

6. POP and POP3: Post Office Protocol (version 3)

The Post Office Protocol is also an email protocol. Using this protocol, the end user can download emails from the mail server to their own email client. Once the emails are downloaded locally, they can be read without an internet connection. Also, once the emails are moved locally, they get deleted from the mail server, freeing up space. POP3 is not designed to perform extensive manipulations with the messages on the mail server, unlike IMAP4. POP3 is the latest version of the Post Office Protocol.

Advantages

- Read emails on local devices without internet connection.
- The mail server need not have high storage capacity, as the emails get deleted when they're moved locally.

Disadvantages

- If the local device on which the emails were downloaded crashes or gets stolen, the emails are lost.

7. SMTP: Simple Mail Transfer Protocol

SMTP is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a push protocol and is used to send the email, whereas POP and IMAP are used to retrieve emails on the end user's side. SMTP transfers emails between systems, and notifies on incoming emails. Using SMTP, a client can transfer an email to another client on the same network or another network through a relay or gateway access available to both networks.

Advantages

- Ease of installation.
- Connects to any system without any restriction.
- It doesn't need any development from your side.

Disadvantages

- Back and forth conversations between servers can delay sending a message, and also increases the chance of the message not being delivered.
- Certain firewalls can block the ports used with SMTP.

8. Telnet: Terminal emulation protocol

Telnet is an application layer protocol that enables a user to communicate with a remote device. A Telnet client is installed on the user's machine, which accesses the command line interface of another remote machine that runs a Telnet server program.

Telnet is mostly used by network administrators to access and manage remote devices. To access a remote device, a network admin needs to enter the IP or host name of the remote device, after which they will be presented with a virtual terminal that can interact with the host.

Advantages

- Compatible with multiple operating systems.
- Saves a lot of time due to its swift connectivity with remote devices.

Disadvantages

- Telnet lacks encryption capabilities and sends across critical information in clear text, making it easier for malicious actors.
- Expensive due to slow typing speeds.

9. SNMP: Simple Network Management Protocol

SNMP is an application layer protocol used to manage nodes, like servers, workstations, routers, switches, etc., on an IP network. SNMP enables network admins to monitor network performance, identify network glitches, and troubleshoot them. SNMP protocol is comprised of three components: a managed device, an SNMP agent, and an SNMP manager.

The SNMP agent resides on the managed device. The agent is a software module that has local knowledge of management information, and translates that information into a form compatible with the SNMP manager. The SNMP manager presents the data obtained from the SNMP agent, helping network admins manage nodes effectively.

Currently, there are three versions of SNMP: SNMP v1, SNMP v2, and SNMP v3. Both versions 1 and 2 have many features in common, but SNMP v2 offers enhancements such as additional protocol operations. SNMP version 3 (SNMP v3) adds security and remote configuration capabilities to the previous versions.

Presentation layer network protocols

LPP: Lightweight Presentation Protocol

The Lightweight Presentation Protocol helps provide streamlined support for OSI application services in networks running on TCP/IP protocols for some constrained environments. LPP is designed for a particular class of OSI applications, namely those entities whose application context contains only an Association Control Service Element (ACSE) and a Remote Operations Service Element (ROSE). LPP is not applicable to entities whose application context is more extensive, i.e., contains a Reliable Transfer Service Element.

Session layer network protocols

RPC: Remote Procedure Call protocol

RPC is a protocol for requesting a service from a program in a remote computer through a network, and can be used without having to understand the underlying network technologies. RPC uses TCP or UDP for carrying the messages between communicating programs. RPC also works on client-server model. The requesting program is the client, and the service providing program is the server.

Advantages

- RPC omits many protocol layers to improve performance.
- With RPC, code rewriting or redeveloping efforts are minimized.

Disadvantages

- Not yet proven to work effectively over wide-area networks.
- Apart from TCP/IP, RPC does not support other transport protocols.

Transport layer network protocols

1. TCP: Transmission Control Protocol

TCP is a transport layer protocol that provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgement. TCP is a connection-oriented protocol, as it requires a connection to be established between applications before data transfer. Through flow control and acknowledgement of data, TCP provides extensive error checking. TCP ensures sequencing of data, meaning the data packets arrive in order at the receiving end. Retransmission of lost data packets is also feasible with TCP.

Advantages

- TCP ensures three things: data reaches the destination, reaches it on time, and reaches it without duplication.
- TCP automatically breaks data into packets before transmission.

Disadvantages

- TCP cannot be used for broadcast and multicast connections.

2. UDP: User Datagram Protocol

UDP is a connection-less transport layer protocol that provides a simple but unreliable message service. Unlike TCP, UDP adds no reliability, flow control, or error recovery functions. UDP is useful in situations where the reliability mechanisms of TCP are not necessary. Retransmission of lost data packets isn't possible with UDP.

Advantages

- Broadcast and multicast connections are possible with UDP.
- UDP is faster than TCP.

Disadvantages

- In UDP, it's possible that a packet may not be delivered, be delivered twice, or not be delivered at all.
- Manual disintegration of data packets is needed.

Network layer protocols

1. IP: Internet Protocol (IPv4)

IPv4 is a network layer protocol that contains addressing and control information, which helps packets be routed in a network. IP works in tandem with TCP to deliver data packets across the network. Under IP, each host is assigned a 32-bit address comprised of two major parts: the network number and host number. The network number identifies a network and is assigned by the internet, while the host number identifies a host on the network and is assigned by a network admin. The IP is only responsible for delivering the packets, and TCP helps puts them back in the right order.

Advantages

- IPv4 encrypts data to ensure privacy and security.
- With IP, routing data becomes more scalable and economical.

Disadvantages

- IPv4 is labor intensive, complex, and prone to errors.

2. IPv6: Internet Protocol version 6

IPv6 is the latest version of the Internet Protocol, a network layer protocol that possesses addressing and control information for enabling packets to be routed in the network. IPv6 was created to deal with IPv4 exhaustion. It increases the IP address size from 32 bits to 128 bits to support more levels of addressing.

Advantages

- More efficient routing and packet processing compared to IPv4.
- Better security compared to IPv4.

Disadvantages

- IPv6 is not compatible with machines that run on IPv4.
- Challenge in upgrading the devices to IPv6.

3. ICMP: Internet Control Message Protocol

ICMP is a network layer supporting protocol used by network devices to send error messages and operational information. ICMP messages delivered in IP packets are used for out-of-band messages related to network operation or misoperation. ICMP is used to announce network errors, congestion, and timeouts, as well assist in troubleshooting.

Advantages

- ICMP is used to diagnose network issues.

Disadvantages

- Sending a lot of ICMP messages increases network traffic.
- End users are affected if malicious users send many ICMP destination unreachable packets.

Data link layer network protocols

1. ARP: Address Resolution Protocol

The Address Resolution Protocol helps map IP addresses to physical machine addresses (or a MAC address for Ethernet) recognized in the local network. A table called an ARP cache is used to maintain a correlation between each IP address and its corresponding MAC address. ARP offers the rules to make these correlations, and helps convert addresses in both directions.

Advantages

- MAC addresses need not be known or memorized, as the ARP cache contains all the MAC addresses and maps them automatically with IPs.

Disadvantages

- ARP is susceptible to security attacks called ARP spoofing attacks.
- When using ARP, sometimes a hacker might be able to stop the traffic altogether. This is also known as ARP denial-of-services.

2. SLIP: Serial Line IP

SLIP is used for point-to-point serial connections using TCP/IP. SLIP is used on dedicated serial links, and sometimes for dial-up purposes. SLIP is useful for allowing mixes of hosts and routers to communicate with one another; for example, host-host, host-router, and router-router are all common SLIP network configurations. SLIP is merely a packet framing protocol: It defines a sequence of characters that frame IP packets on a serial line. It does not provide addressing, packet type identification, error detection or correction, or compression mechanisms.

Advantages

- Since it has a small overhead, it is suitable for usage in microcontrollers.
- It reuses existing dial-up connections and telephone lines.
- It's easy to deploy since it's based on the Internet Protocol.

DIsadvantages

- SLIP doesn't support automatic setup of network connections in multiple OSI layers at the same time.
- SLIP does not support synchronous connections, such as a connection created through the internet from a modem to an internet service provider (ISP).