Intro to Networks

Quick intro to computer networks

Nomenclature

- Data
- Bits
- Node
- Link
- Network
- Protocol
- Protocol Stack

OSI vs TCP/IP

LAYERS	OSI	TCP/IP
L7	Application	Application
L6	Presentation	↑
L5	Session	↑
L4	Transport	TCP/UDP
L3	Network	IP/ICMP
L2	Data Link	Network access
L1	Psysical	-

- OSI (Open Systems Interconnection) model: De jure / TCP/IP model: De facto

Protocol Layers

Layers	CLIENT	SERVER
App	show www.google.com	Google
L7	GET / HTTP/1.1 Host: www.google.com User-Agent: curl/8.9.1 Accept: /	HTTP/1.0 200 OK Date: Mon, 25 Nov 2024 06:57:24 GMT Cache-Control: private, max-age=0
L4	Source port: 31232 Destination port: 443 SEQ: 1	Source port: 443 Destination port: 31232 SEQ: 1
L3	Source IP: 172.31.3.4 Dest IP: 142.250.185.196	Source IP: 142.250.185.196 Dest IP: 172.31.3.4

IP

IP (Internet Protocol) is the fundamental communication protocol used to send data across a network. It ensures data packets are addressed, routed, and delivered between devices.

- Packet-Based: Data is broken into packets, which are sent independently and reassembled at the destination.
- Routing: Routers direct packets to their destination based on IP addresses.
- Stateless: Each packet is treated independently, without information about previous packets.
- Layer: Operates at the network layer (Layer 3) in the OSI model.

IP address

An IP address (Internet Protocol address) is a unique identifier assigned to a device on a network, allowing it to communicate with other devices. It acts as a virtual address, enabling data to be sent to the correct destination.

- IPv4: 32-bit address, written as four decimal numbers separated by dots (e.g., 192.168.1.1).
- IPv6: 128-bit address, written as eight groups of hexadecimal numbers separated by colons (e.g., 2001:0db8:85a3::8a2e:0370:7334).
- Public IP: Used for devices directly accessible on the internet.
- Private IP: Used within private networks (e.g., homes or businesses) and not routable on the internet.
- Static IP: Manually assigned, does not change.
- Dynamic IP: Assigned by DHCP, changes over time.

DHCP (Dynamic Host Configuration Protocol)

DHCP is a network protocol used to automatically assign IP addresses to devices (hosts) on a network.

- Simplified Management: Eliminates manual IP address configuration.
- Address Reuse: IP addresses are leased for a certain period and can be reused when no longer needed.
- Avoids Conflicts: Prevents duplicate IP addresses on the network, ensuring each device gets a unique address.

TCP

TCP (Transmission Control Protocol) provides reliable, ordered, and error-checked delivery of data between applications. Transport layer (Layer 4) of the OSI model.

- Connection-Oriented: TCP establishes a connection between the sender and receiver
- Reliable Delivery: It ensures that data is delivered accurately and in the correct order, using acknowledgments and retransmissions if packets are lost or corrupted.
- Flow Control: TCP manages data flow to prevent the sender from overwhelming the receiver.
- Error Detection: TCP uses checksums to detect and handle data corruption during transmission.
- Segmentation and Reassembly: It breaks large data into smaller packets (segments) for transmission and reassembles them at the destination.

TCP ports

TCP ports are a fundamental part of the TCP/IP protocol suite, used to identify specific processes or services on a device for communication.

- A port is a 16-bit number (0–65535) that serves as an endpoint for network communication.
- It allows a device to differentiate between multiple applications or services running on the same IP address.
- Source Port: The port number of the application initiating the connection.
- Destination Port: The port number of the service or application being accessed.

TCP ports

- Well-Known Ports (0–1023) Reserved for standard services (e.g., HTTP, FTP, SMTP).
- Multiple Services: Ports allow a single device to host multiple networked services simultaneously.
- Routing Traffic: They ensure the correct application receives the transmitted data.
- Security: Firewalls and intrusion detection systems can monitor or block traffic based on ports.
- For example, when you visit a website, your browser (source port) connects to the server's port 443 (HTTPS). After establishing the connection, data flows between these ports.