Understanding Protocols, Ports and Sockets

Understanding Protocols, Ports, and Sockets

Protocols

- Computers communicate with each other with network protocols.
- Protocols are rules governing how machines exchange data and enable effective communication.
- In an operating system (OS), a protocol runs as a process or service.

Ports

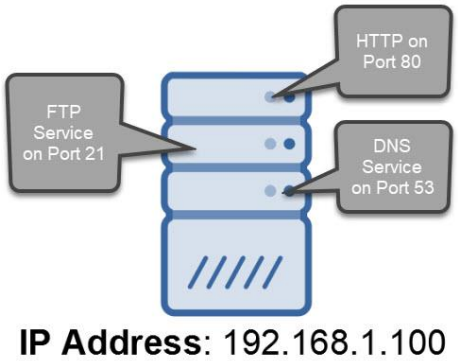
- Ports are logical constructs that bind a unique port number to a protocol process or service.

Sockets

- Sockets are a combination of an IP address and a port number, for example, 192.168.1.1:80.

Why We Need Ports and Sockets

- Computers require ports because of network application multitasking.
- Because a computer may have only one IP address, it needs ports to differentiate network protocols and services running on it.
- TCP/IP has 65,536 ports available



Port Type	Port Numbers	Description
Well Known Ports	0 – 1023	Assigned to well-known protocols.
Registered Ports	1024 – 49,151	Registered to specific protocols.
Dynamic Ports	49,152 – 65,535	Not registered and used for any purpose.

INSTRUCTOR ALTON

Protocols & Port Numbers

Service, Protocol, or Application	Port Number(s)	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
Secure FTP (SFTP)	22	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System)	53	UDP
DHCP (Dynamic Host Configuration Protocol)	67, 68	UDP
TFTP (Trivial File Transfer Protocol)	69	UDP
HTTP (Hypertext Transfer Protocol)	80	TCP
POP3 (Post Office Protocol version 3)	110	TCP

INSTRUCTOR ALTON

Protocols & Port Numbers

Service, Protocol, or Application	Port Number(s)	TCP or UDP
NTP (Network Time Protocol)	123	UDP
IMAP4 (Internet Message Access Protocol version 4)	143	TCP
SNMP (Simple Network Management Protocol)	161	UDP
LDAP (Lightweight Directory Access Protocol)	389	TCP
HTTPS (Hypertext Transfer Protocol Secure)	443	TCP
Server Message Block (SMB)	445	TCP
LDAPS (Lightweight Directory Access Protocol Secure)	636	TCP
RDP (Remote Desktop Protocol)	3389	TCP
ITU Telecommunication Standardization Sector A/V Recommendation (H.323)	1720	TCP
Session Initiation Protocol (SIP)	5060, 5061	TCP

TCP vs UDP

INSTRUCTOR ALTON

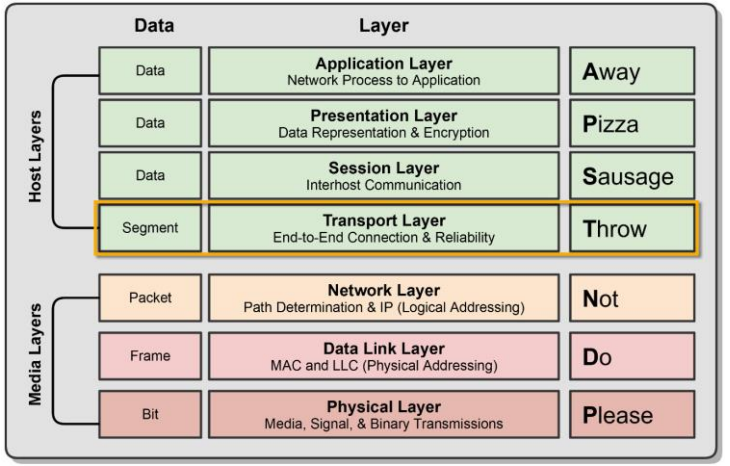
TCP vs. UDP

Transport Layer Protocols

- **TCP** (Transmission Control Protocol): Connection-Oriented
- **UDP** (User Datagram Protocol): Connectionless

TCP is the most widely used Transport Layer protocol because it is connection-oriented, which provides packet delivery reliability, i.e., guaranteed delivery.

UDP, being connectionless, is considered to be unreliable; however, it is more lightweight than TCP and often used for streaming or real-time data.



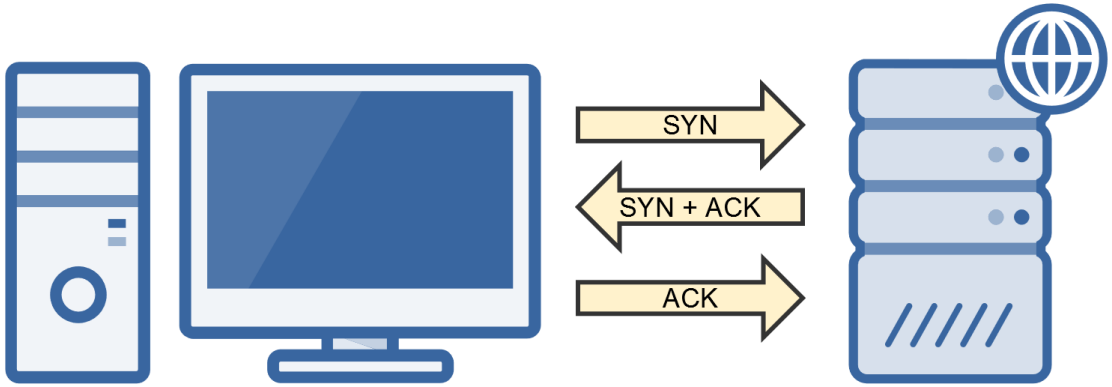
TCP Reliability

- TCP utilizes the following features to ensure reliable delivery of data.
  - **3-Way Handshake** creates a virtual connection between the source and destination before data is sent.
  - **Acknowledgment** is required before the next segment is sent.
  - **Checksum** that detects corrupted data.
  - **Sequence Numbers** that detect missing data and reassemble them in the correct order.
  - **Retransmission** that will retransmit lost or corrupt data.

- **Note**: TCP header is 20 bytes in size, whereas the UDP header is only 8 bytes.

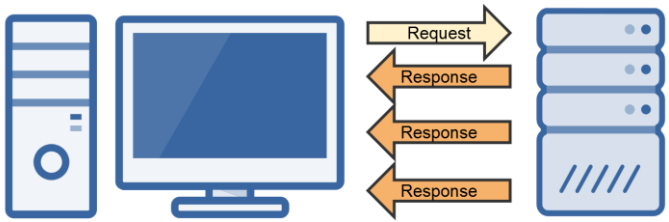
TCP Three-Way Handshake

- A connection must be established before data is transmitted, called the three-way handshake.
  - SYN → SYN / ACK → ACK
- Creates a Virtual Connection Between 2 Devices



"Best Effort" UDP

- A scaled-down, economic version of TCP
  - Connectionless & Unreliable
  - No Data Retransmissions
  - "Best Effort"
- Faster than TCP
  - Smaller Header & Connectionless
- Primarily used for protocols that favor:
  - Low-Latency, i.e., Faster Speeds
  - Can Tolerate Data Loss



"Best Effort" UDP

- Example UDP Use-Cases
  - VoIP Phone Calls
  - Live Video Streams
  - Live Audio Streams
  - Online Gaming
  - Certain Network Management Protocols
    - DNS
    - DHCP
    - NTP