Network Notes

Computer Networks

Basics of Networks

A Computer Network → A system of two or more computers that are connected together by a
transmission medium for the exchange of data.

LAN

Local Area Network → Network of devices in a small location. Due to close proximity, data transfer speeds are very high. A WLAN is simply a wireless version of a LAN.

MAN

Metropolitan Area Network → Network of devices in a larger geographical area. Generally owned by companies, cities or governments.

WAN

Wide Area Network → Network of devices in large-scale geographical area. Generally consists of many smaller MANs and LANs. It uses more expensive technology, and can span very long range. WANs can be public (like the internet) or private (used by companies and governments).

Intranet

Intranet → Private network built within an organization. Access is restricted to authorized users to share information in a controlled and secure environment.

Internet

Internet → Global public network accessible to anyone with an internet connection. It is a network of networks that is connected through multiple wired and wireless means. It functions through a layered system, with data travelling in

packets using IP Addressing. Routers guide the traffic while ISPs provide the communication devices.

Intranet VS Internet Summary

Feature	Intranet	Internet
Scope	Private network within an organization	Public network accessible globally
Access	Restricted to authorized users within the organization	Open to anyone with an internet connection
Content	Internal resources relevant to the organization (documents, portals, tools)	Diverse content from various sources (news, social media, entertainment)
Security	More secure due to restricted access	Less secure due to open nature
Connection	Can be isolated from the internet or connected with security measures	Connects devices across the globe
Purpose	Internal communication, collaboration, secure resource sharing	Global communication, information sharing, access to online services

Network Hardware

Basics of Network Hardware

Network Hardware → Physical components that make up a computer network.

NIC

Network Interface Cards → A chip that provides the hardware interface for any data transfer between a device and a network. Most devices have one for ethernet and one for WiFi. It comes with driver software that auto-updates. Each NIC has a unique MAC address that won't change.

Cable

Unshielded Twisted Pair cables are the standard, and fiber optic cables are used for high speeds.

Hub

Simplest way to connect multiple devices in the same network. When a hub receives a packet, it shouts it to all other devices connected to it. It is cheap as it

does not store any information about the devices connected. However, the shouting can bottleneck and slow down the whole network.

Switch

Connect multiple devices within a limited area and manage data flow. Switches can function as hubs but can also keep track of the addresses of connected devices. They receive data packets from devices, examine the destination address and forward it to the recipient without shouting it out.

Router

Connect to other LANs and assign IP addresses to your devices. They connect multiple networks and direct data packets to their final destination across different networks using routing protocols.

WAP

Wireless Access Points → Devices that create WLANs

Modem

Facilitates signal conversion and reversion (analog to digital and VV). They act as translators to turn data into electrical pulses for wires or cables. Modem comes from MOdulation + DEModulation.

Network Addresses

MAC

Media Access Control → Identifier assigned to a NIC. Never changes. When a device in a local network transmits data, the MAC address is included in the packet header. It can look like “A4:B3:55:EF:01:7E”. It takes up 48 Bits.

IP

Internet Protocol → Unique numerical label given to devices connected to a network that uses IP for communication. Allows you to identify devices over a network, such as home network or the internet. Static IP Addresses wont change but dynamic IP Addresses can. IPV4 and IPV6 can coexist, the latter was created

because of scarcity. IPV4s can look like “33.44.56.123” and IPV6s can look like “A343:E434:3477:B343:4445:E43F:0347:134E”. IPV4s take up 32 Bits while IPV6s take 128 Bits. Each subshell in an IPV6 can be rewritten “00DE” → “DE” or “0000” → “0” to save space,

DNS

Basics of DNS

Domain Name Service → System that allocates readable domain names to host IP Addresses. It is set up as a hierarchical distributed database which is installed on a large number of domain name servers covering the whole internet. Root servers are replicated so multiple copies of all their data are kept at all times. DNS name space is then divided into non-overlapping zones. Each zone has a primary name server with the database stored on it. Secondary servers get information from this primary server.

DNS Request Process

1. Computer checks DNS Cache to see if you have recently visited. If not, a DNS request is made.
2. A recursive DNS Server (given by ISP) will be searched for popular visits. If not, the request is sent to the internet’s root DNS servers.
3. The root servers check the top level domain (.com) and refer you to the correct TLD server.
4. The TLD server refers you to the authoritative server which can answer the request. This authoritative DNS server is responsible for storing the DNS records for a particular domain name and where any updates to your domain name DNS records would be made.
5. The DNS record is then sent back to the Recursive DNS Server, where a local copy will be cached for future requests and then relayed back to the original client that made the request.

TCP/IP Model

TCP/IP Layers

1. Application Layer: It provides high-level functionality to end-users.
   It provides services directly to applications we use every day, such as web browsing
   (HTTP), email (SMTP), file transfer (FTP), and video conferencing.
2. Transport Layer: This layer provides functionality to transmit messages between any
   two programs.
   Two key protocols operate here:
   a. TCP (Transmission Control Protocol): Ensures reliable and ordered delivery of
      data. It acts like a reliable courier service, establishing a connection, checking for
      errors, and guaranteeing packets arrive in the correct order.
   b. UDP (User Datagram Protocol): Focuses on speed over guaranteed delivery.
      It's suitable for applications where speed is more critical than perfect accuracy,
      like online gaming or streaming media.
3. Internet Layer: This layer provides functionality to determine a route between any two
   devices. It is the heart of routing, handling addressing and routing data packets across networks
   using the Internet Protocol (IP). Imagine IP addresses like zip codes for devices on the
   internet; this layer ensures packets are delivered to the correct destination.
4. The Link Layer: This layer provides functionality to transmit packets from one device to
   an adjacent device.
5. The Physical Layer: This layer provides functionality to transmit individual bits through
   a transmission medium.

Layer	Description	Protocols	Hardware/Software
Physical Layer	Handles physical transmission of data packets over the network medium cables, wires, or wireless signals.	Ethernet	Network cables, Wireless adapters, Network Interface Cards (NICs), Modems
Data Link Layer	Packages the data into frames and ensures error-free transmission between devices on the same network segment.	Ethernet, Wi-Fi, PPP (Point-to-Point Protocol) ARP (Address Resolution Protocol)	Network Interface Cards (NICs), Switches
Internet Layer	Routes data packets across different networks, determining the best path to reach the destination device	IP (Internet Protocol), ICMP (Internet Control Message Protocol)	Routers
Transport Layer	Manages reliable data transfer between applications	TCP (Transmission Control Protocol), UDP (User Datagram Protocol)	Not directly associated with specific hardware, but relies on the functionality of the Network Access Layer
Application Layer	Provides services directly to applications like web browsing, email, and file transfer.	HTTP (Hypertext Transfer Protocol), HTTPS (Secure Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System)	Web browsers, Email clients, FTP clients, Operating Systems (for application support)

Transmission Protocols

As a summary :

- Application layer: HTTP, SMTP, DNS, FTP, POP3
- Transport layer: TCP, UDP, SCTP
- Network layer: IP, IGMP, ICMP, ARP

Specific Protocols :

▼ Communication Protocols

▼ HTTP

▼ Hyper Text Transfer Protocol

▼ Makes a request for a webpage, server responds with either HTML webpage or error

▼ Normally status code 200 is returned, errors return other codes like 404

▼ Sample HTTP Request

```
GET /index.html HTTP/1.0
User-agent: Mozilla
Accept: text/html, text/plain, image/jpeg, image/gif,
Host: foo.com
```

▼ Sample HTTP Response

```
HTTP/1.0 200 OK
Server: Sun-Java System-Web-Server/6.1
content-type: text/html
Content-length: 83

<HTML>
<HEAD><TITLE>Hello World</Title></HEAD>
<BODY>Hello World</BODY>
</HTML>
```

▼ HTTPS

▼ Hyper Text Transfer Protocol (Secure)

▼ Makes encrypted request for webpage, server responds with encrypted HTML webpage or error

▼ More secure than HTTP

▼ FTP

▼ File Transfer Protocol

▼ Used to upload or download a file from a server, and send an error if process fails

- Not secure, use SFTP (Secure File Transfer Protocol)

- SMTP
  - Simple Mail Transfer Protocol
  - Used to send an email to an email server, and returns a code indicating success of process
  - For red@orangemail.com, all orangemail.com accounts are managed by the same email server
  - If the mail is for someone in the same organization, the mail is stored until that users connects. If not, the domain name of the destination is resolved using the DNS and the email is forwarded to the destination mail server using SMTP.
- POP
  - Post Office Protocol
  - Used to request any new emails for a specific email account
  - Once the new emails are requested, they are deleted from the server, which is inconvenient when multiple people have to access one account
- IMAP
  - Internet Message Access Protocol
  - Used to request for any new emails for a specific email account as well as deletes emails that have been locally deleted (basically synchronization)
  - Once the new emails are requested, they are copied from the server instead of deleted, so the old news is always traceable from the server
- DHCP
  - Dynamic Host Configuration Protocol
  - Used to assign IP addresses to other device in a network
- TCP
  - Transmission Control Protocol

▼ When data is transmitted, it is split into packets, each of which has a sequence number. At the end, all packets are accounted for, and missing packets are resent, making the protocol reliable.

▼ UDP

▼ User Datagram Protocol

▼ Same as TCP, but but packets are ignored if they fail transmission or are out of order. This makes it unreliable but very fast.

▼ IP

▼ Internet Protocol

▼ Packages packet with host IP and destination IP to be transmitted across the internet

▼ Ethernet / WiFi Protocols

▼ Encapsulates the data from the previous layer into frames with a source and destination MAC address

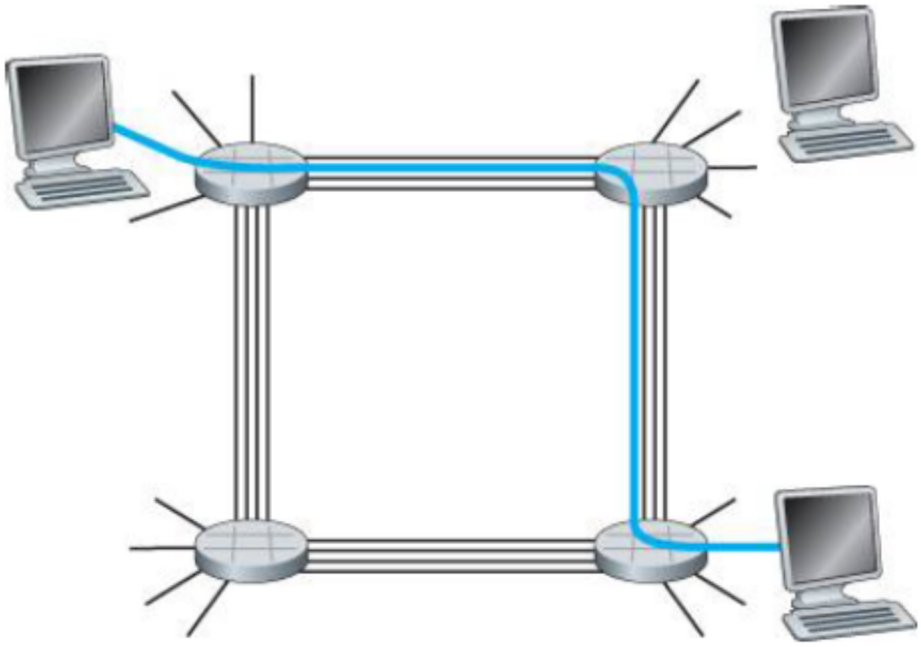
Transmission

▼ Circuit Switching

▼ What is Circuit Switching

▼ The resources needed (buffers and the link transmission rate) are reserved for the duration of the session

▼ Circuit Switching Diagram



▼ In a Circuit, a number of switches have a number of connections going into and out of the switches.

▼ Choosing a combination of these connections allows one switch to send information to another switch.

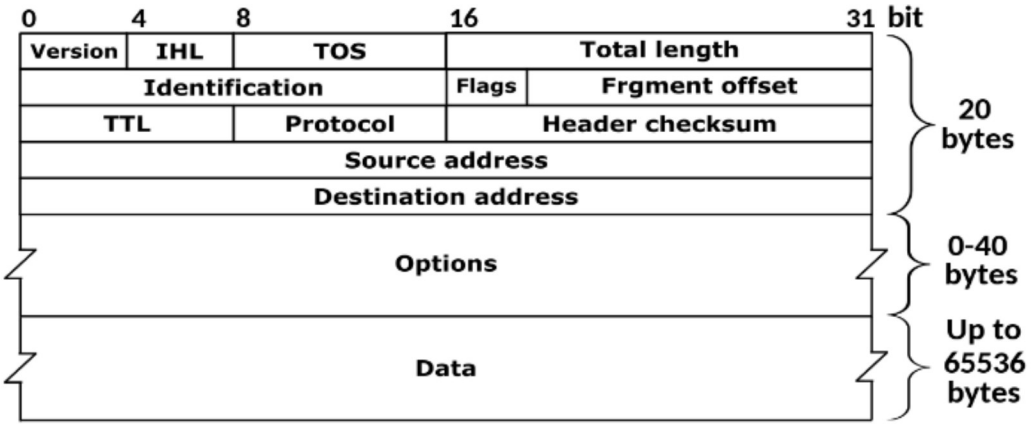
▼ However, the transmission rate of data is divided by the number of connections.

▼ Packet Switching

▼ What is Packet Switching?

▼ The resources needed (buffers and the link transmission rate) are not reserved as each session’s messages use them on demand. Thus, if a link is congested (traffic jam), packets need to wait in a buffer

▼ Anatomy of a Packet



- IHL indicates the header length.
- Packets use Type of Service (TOS) to request special treatment (e.g. being put at the front of any queues).
- The identification, flags, and fragmentation offset fields keep track of each fragment when an IP packet is split up into smaller packets.
- The Time To Live (TTL) is set when the IP packet is sent off, and the number is reduced by 1 each time the packet goes through a router. When the time to live gets to 0, the packet is deleted. This stops packets from circulating in a loop.

▼ Store and Forward Transmission

▼ Most switches are like primary school teachers leading a learning journey. Each switch will wait for all bits of a packet (all children in a class) before moving to the next destination (next switch).

▼ We assume propagation delay (time taken for electricity to travel through a wire) to = 0

▼ Queuing Delays and Packet Loss

▼ A switch is like immigration at an airport. There are multiple immigration counters (multiple links) attached to it. Each immigration counter (link) has a queue (buffer). People will queue up for each counter until they get their chance to go, and then one at a time they will finish immigration. Similarly, packets will queue up for each link until it can be transmitted.

▼ However, if the queues are full at immigration, people will hate the long queues and decide to grab lunch first instead. Similarly, if the queues are full at a switch, the packets will be dropped.

▼ Busy Internet

▼ If routers receive packets faster than they can route them, they are buffered in memory, which is what causes game lags or video lags

▼ IP packets contain ToS (Type of Service) fields in their headers, which makes it easier to mark packets according to priority levels. Routers can choose whether or not to use it.

▼ Lost Packets

▼ If a destination is unreachable, sometimes packets are sent away to a default device

▼ A packet could theoretically get caught in a loop of being sent away again and again, causing the data to infinitely cycle through devices

▼ Packets come equipped with a TTL (Time To Love) counter which tells it to kill itself after a long period of time

▼ Forwarding Tables

▼ On the internet, every destination address has an IP address. The source of a packet includes the IP address of the destination in the packet header

▼ Every router has a table of destination addresses and corresponding IP addresses

▼ These tables are set using some algorithm

▼ Packet VS Circuit Switching

▼ Packet switching is not useful for real time services such as video or voice calling as there are many delays caused by buffering and queueing delays.

▼ Packet switching offers better sharing of transmission capacity than circuit switching and is simpler, faster and cheaper.

▼ Circuit switching might waste transmission link time. Link transmission capacity will be shared on a packet-by-packet basis only among those users who have packets that need to be transmitted over the link.

▼ Mostly the world is migrating to packet switching.

Client-Server Processes

Basics of Client-Server Processes

An app has a pair of processes that send messages to each other over a network. One is a client and one is a server.

- In a webapp, a browser is the client process and the web server is the server process.
- In a P2P file sharing system, downloading is a client process and uploading is a server process.
- For simplicity, we call the FIRST communication a client, and the RESPONSE, a server.

Client-Server Architecture

- There is an always-on host (server) which services requests from other hosts (clients).
- The server has a fixed, well known IP address.
- The server is usually hosted on a data center to handle a large number of requests.
- The service providers must pay recurring interconnection and bandwidth costs.

P2P Architecture

- Minimal or no reliance on data centers.
- Uses processing power of both host computers.

Hybrid Architecture

- In some apps, servers track IP addresses but user-user messages are P2P.
- This has the scalability and cost effectiveness of P2P while remaining secure and reliable.

Process-Network Interface

Basics of Process-Network Interface

- Any message sent from one process to another goes through the underlying network.
- Socket → Software interface through which processes receive data from and send it to server.
- Sockets are bidirectional, and can carry data both to and from.
- Internet sockets use TCP/IP to transmit data over the internet.
- Internet sockets can pass through multiple devices before reaching the destination (vulnerable).

Socket Communication

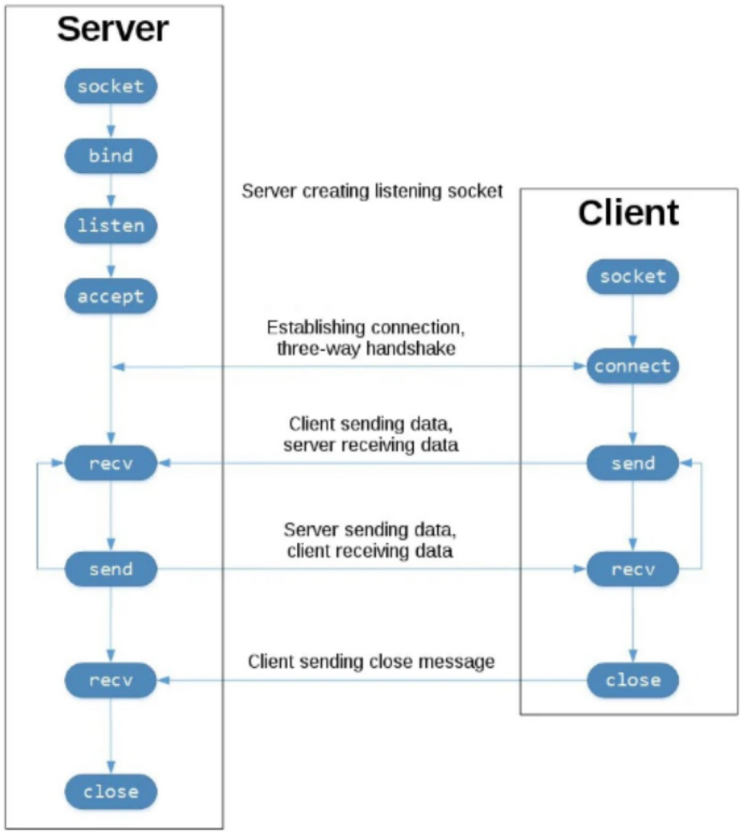
- Data might lag or be chopped up in transmission, protocols help identify the start and end of it.
- Sockets are the interface between application and transport layer, known as the API between an application and a network.
- The application dev can control everything on the application layer, but only protocol choice and some parameters on the transport layer.

IP Addresses and Ports

- To identify the receiving process, we must know the host IP and an identifier like a port number.
- The IP address identifies the device while the port number identifies the program on the device.
- Port numbers can range from 0-65535. However, the first 1024 are reserved for specific programs, and should not be used for other purposes.

TCP Socket API

- Diagram of TCP Socket API



1. Server creates passive socket, binds it to pre-chosen port number, listens for connection.
2. Client initiates a connection request using server IP and port. If no-one is listening, it refuses.
3. The server accepts and creates a new socket for client using dynamically assigned port.
4. Old socket goes back to listening for new connections, new socket used for communication.