Computer Networks

Computer Network - connection of at least 2 devices in order to exchange information

Host - device with asigned IP which recives and send data from and to other devices.

Server - computer providing services like www, mail, files exchange to other computers

Client - computer (software) using services provided by server.

Communication protocol - way of communication and data exchange described by rules

Internet - colection of wide networks creating global computer network

Intranet - private network using the same communications standards as internet with constrained acces

Extranet - expanded kind of net intranet network to which more users have acces

DNS (Domain Name System) - network service changing names understable to humans to IP addresses of devices in network.

DHCP (Dynamic Host Configuration Protocol) - protocol of automated configuration of network settings asigning IP addresses, address masks, gateway addressed to host

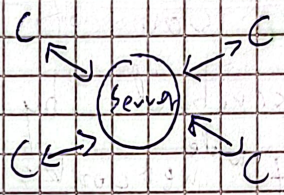
- 1 bajt [B] = 8 bit [b]

ex. 100 [B] = 8bit [b]

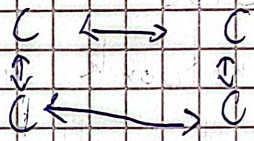
Network types:

- LAN (local area network) - network having the smallest area ex. house
- MAN (Metroplitan area network) - network having bigger area like citylies
- WAN (Wide area network) - wide network of connected together LAN and MAN networks

-
- Client - Server



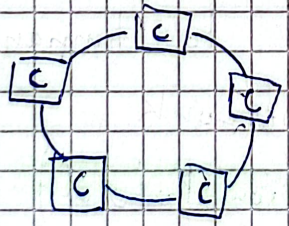
- P2P (Peer-to-Peer)



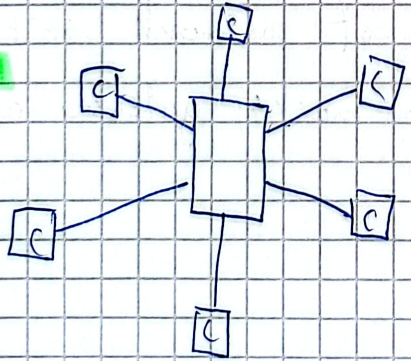
Network topologies:

- Bus

- Ring:



- Star



TCP/IP

4-layer model

	Application	allows users to use network
[port]	Transport	responsible for communication service
[IP]	Internet	determines the data transfer route
[MAC]	Network Access	code the data and transfer it to medium

ISO/OSI

Application	Human-computer interaction
Presentation	Ensures that data is in usable format and is encrypted here
Session	Maintains connections and is responsible for controlling ports and sessions
Transport	Transmits data using protocols
Network	Decides which physical path the data will take
Data Link	Defines the format of data on the Network
Physical	Transmits raw bit stream over the physical medium

PDU - (Protocol data unit) - data send through network

IPv4 (internet protocol version 4)

ex. 192.168.1.120

4 octets, each have 8 bits it means that each octet can represent number from 0 to 255

First part (that octet) can be 1, 2, 3 of ~~address~~ IP is network address and the rest is host address.

Subnet mask ex. 255.255.255.0 - determines network size and number of hosts

Mask must be a set of 1s in binary and 0 can't appear between 1.

ex1.

IP - 192.168.1.145, subnet mask - 255.255.255.128
short form /25

Calculate:

a) network address

b) broadcast address

c) host number (+ first and last host address)

a)

I) 192.168.1.145

↓

11000000.10101000.00000001.10010001

255.255.255.128

11111111.11111111.11111111.10000000

II) We multiply them binary (make operation and)

11000000.10101000.00000001.10000000

III) convert to decimal

b)

i) change 1 to 0 and 0 to 1 in subnet mask (make operation not)

00000000|00000000|00000000|01111111

ii) we convert it to decimal

0.0.0.127

iii) we add decimaly network address

```
  0.0.0.127
+ 192.168.1.128
---------------
  192.168.1.255
```

c)

host number:

$2^{(\text{number of bits in IP} - \text{short form of mask})} - 2$

$2^{(32-25)} - 2 = 2^7 - 2 = 126$

i) First host: add 1 to network address

```
  192.168.1.128
+             1
---------------
  192.168.1.129
```

ii) Last host: we subtract 1 from broadcast address

```
  192.168.1.255
-             1
---------------
  192.168.1.254
```

16 min

ex 2 IP - 172.16.160.200 subnet mask - 255.255.192.0 /18

a) Network address

b) broadcast address

c) host number (+ 1st and last host number)

a)

172	
86	0
43	1
21	1
10	0
5	1
2	0
1	1
0	

16	0
8	0
4	0
2	0
1	1
0	

160	0
80	0
40	0
20	0
10	0
5	1
2	0
1	1
0	

200	0
100	0
50	0
25	0
12	1
6	0
3	0
1	1
0	1

192	
96	0
48	0
24	0
12	0
6	0
3	0
1	1
0	1

128 64 32 16 8 4 2 1

10101100.00010000.10100000.11001000

× 11111111.11111111.11000000.00000000

10101100.00010000.10000000.00000000

172.16.128.0

b) 00000000.00000000.00111111.11111111

0.0.63.255

\+ 172.16.128.0

172.16.191.255

c) $2^{(32-18)} - 2 = 2^{14} - 2 = 16382$

1st: 172.16.128.1

last: 172.16.191.254

ISP = Internet Service Provider

NAT (Network Address Translation) - translate private addresses to public and vice versa

Network Interface Card (NIC) - a Nic physically connects the end device to the network

Physical port - a connector or outlet on a networking device where the media connects to an end device or another networking device

Interface - specialized ports on a networking device that connect to individual networks. Because routers connect networks, the ports on a router are referred to as network interfaces.

Terms port and interface are often used interchangeably

End devices: ex. Computer, Laptop, Printer, Tablet, TV

Intermediary Devices: Router, LAN switch, wireless router

Network Media: LAN media, WAN media, Wireless media

Physical Topology diagram - illustrate the physical location of intermediary devices and cable installation. Rooms in which these devices are located are labeled in this topology diagram.

Logical Topology diagram - illustrate devices, ports, and addressing scheme of the network. You can see on it which end devices are connected to which intermediary devices and what media is being used

A fault tolerant network is one that limits the number of affected devices during a failure. Such a network depends on multiple paths between the source and destination. Having many paths to a destination is known as redundancy.

A scalable network expands quickly to support new users and applications without degrading the pe performance for existing users.

Quality of service (QoS) is a ~~primary~~ mechanism for managing congestion and ensuring reliable delivery of content to all users. Congestion occurs when the demand for bandwidth exceeds the available amount. Network bandwidth is measured in bits that can be transmitted in a second (bps)

Network administrators must address 2 types of network security concerns: network infrastructure and information security. To achive network security, there are 3 primary requirements:

- Confidentiality; only the intended and authorized recipients can access and read data
- Integrity; assures that the information has not been altered in transmission, from origin to destination
- Availability - assures users of timely and reliable access to data services

Bring Your Own Device (BYOD) - enables end users the freedom to use personal tools to access information and communicate across a business or campus network. BYOD means any device, with any ownership, used anywhere.

Cloud computing allows us to store personal files, even backup an entire drive on servers over the internet. Cloud IT extends the capabilities of IT without requiring investment in new infrastructure, personel or licensing new software. Cloud computing is posible because of data centers. Data centers are facilities used to house computer systems and associated components.

Cloud Types:

- Public clouds; available to the general population, services are free or are offered on pay-per-use model, or use internet to provide
- Private clouds; intended for a specific organization or entity eg. government, can be set up using private network. Can be expensive to build and maintain.
- Hybrid clouds; made up of 2 or more clouds eg. part private, part public, each part is a distinct object, but both are connected using single architecture.
- Community cloud; created for exclusive use by specific organizations or entities

~~Power line~~ Powerline networking for home networks uses existing electrical wiring to connect devices. Using a standard powerline adapter, devices can connect to the LAN wherever there is an electrical outlet. Only cables and interfaces

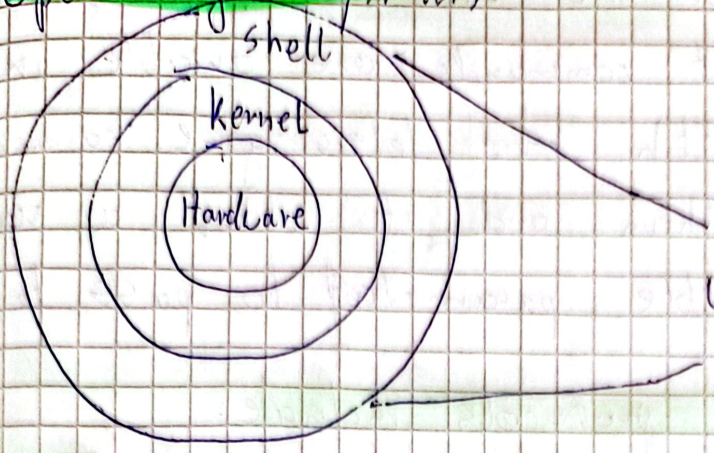
A Wireless Internet service Provider (WISP) is an ISP that connects subscribers to access point or hot spot using similar technologies found in home wireless local area networks (WLANs)
WISPs are more common in rual areas where DSL or cable services aren't available.

Several common external threats to networks:

- Viruses, worms, and Trojan horses; malicious software or code running on a user device
- Spyware and adware; software installed on user's device that secretly collects information about the user
- Zero-day attacks; occurs on the 1st day that a vulnerability becomes known
- Threat actor attacks; malicious person attacks user devices or network resources
- Denial of service attacks (DoS) attacks that slow or crash applications and processes on a network device
- Data interception and theft; captures private information from an organization's network
- Identity Theft; steals log in credentials of user to access private data

The internet is a network of networks that

Operating Systems



Shell - user interface that allows users to requests specific tasks from the computer. Can be done by CLI or GUI

Kernel - communicates between the hardware and software and manages how hardware resources are used to meet software requirements.

Hardware - the physical part of a computer including underlying electronics

CLI - command-line interface

GUI - grafical user interface

Most popular access method is **SSH** (secure shell) - it is for remotely establishing a secure CLI connection through a virtual interface, over a network.

API - application programming interface

CLI commands:

enable ; enter privileged EXEC mode

disable ; leave privileged EXEC to enter user EXEC mode

configure terminal ; enter global configuration mode

exit ; leave

Switch>show ip protocols

Prompt | Command | Space | Keyword(s) or Agruments

Switch > ping 192.168.10.5

"?" - is of very broad use in CLI if given alone returns what commands are aviable in that mode, if with some letters give commands that starts with them and if after a comma it returns possible parameters to pass to

Comomon computer protocols include:

- message encoding
- message formating and encapsulation
- message size
- message timing
- message delivery options

Encoding is the process of converting information into another acceptable form, for transmission. For ex. converting bits to pattern of voltages on copper wires, infrared light in optical fibers or microwaves in wireless system. Decoding reverses this process to read the informat

Message timing include:

- Flow Control
- Response Timeout
- Access method

Delivery Options

- Unicast; info transmited to only 1 end device
- Multicast; ——,,—— to 1 or more end devic
- Broadcast; ——,,—— to all end devices

Functions of protocoles:

1. Addressing
2. Reliability
3. Flow control
4. Sequencing
5. Error detection
6. Application interface

Hypertext transfer protocol (HTTP) - governs the way a web server and web client interact.

Transmition Control Protocol (TCP) - manages individual conversations, guarantee reliable delivery of info and manage flow control.

Internet Protocol (IP) - Delivering messages from sender to reciver, used by routers to forward msg across multiple networks.

Ethernet - delivering msgs from one NIC to another NIC on the same ethernet LAN

A protocol suite is a set of protocols that work together to provide versatile network communication services. Eg. TCP/IP, ISO/OSI

TCP/IP is the protocol suite used by the Internet and the networks of today

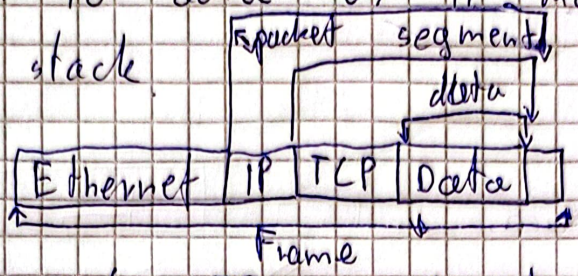
Segmentation is the process of dividing data into smaller pieces for transport over the network.

Benefits of segmentation:

- increased speed
- increased efficiency

TCP is responsible for sequencing the individual segments so they are delivered to proper address and

Encapsulation is the process of adding protocol information to data as it moves down the protocol stack



Data - term for PDU used at application layer

Segment - Transport layer PDU

Packet - Network layer PDU

Frame - Data link PDU

Bits - Physical layer PDU

PDU - Protocol Data Unit; simply a piece of da

Layer 3 - IP Packet

Source IP	Destination IP	...
ex. 192.168.1.110	ex. 172.16.1.99	

IP addresses have 2 parts:

Network portion (IPv4) or Prefix (IPv6)

Host portion (IPv4) or Interface ID (IPv6)

The subnet mask (IPv4) or prefix-length (IPv6) is used to tell those apart.

Data link - Ethernet Frame

Destination MAC address	Source MAC address	IP packet
ex. AA-AA-AA-AA-AA-AA	ex. CC-CC-CC-CC-CC-CC	

MAC - (Ethernet) Media Access Control

Destination MAC	Source MAC	Source IP		Destination IP		Data
		Network	Device	Network	device	
AA-AA-AA-AA-AA-AA	11-11-11-11-11-11	192.168.1	110	172.16.1	99	

Data Link
Ethernet Frame Header

Network Layer

When sender and reciver of the IP packet are on different networks, the Ethernet data link frame cannot be sent directly to the destination host. The Ethernet frame must be sent to another devise ~~switch~~ router as router or default gateway

Physical Layer

Bandwidth - capacity at which a medium can carry a data. Usually measured with ~~bits~~ kbps, Mbps, Gbps

Latency - refers to the amount of time, including delays, for data to travel from one given point to another

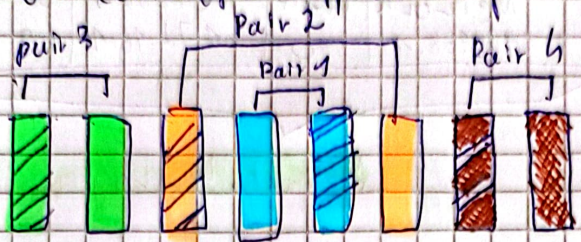
Throughput - measure of the transfer of bits across the media over a given period of time Usually smaller than bandwidth cause it is influenced by traffic and latency

Goodput - measure of usable data transfered in a given period of time. Usually smaller than Throughput

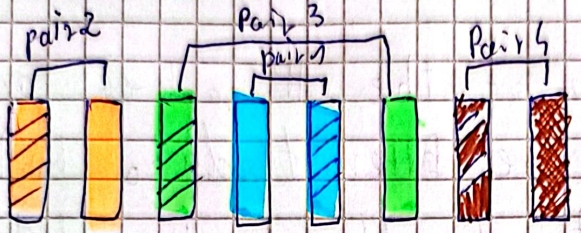
3 types of copper cabling

1. Unshielded Twisted-pair (UTP) - most popular cheapest usually ended with RJ-45
2. Shielded Twisted-pair (STP) - also RJ-45 better protection more expensive, need to be grounded
3. Coaxial cable - almost replaced with UTP, used in

UTP cabling consists of four pairs of color-coded copper ~~cabling~~ wires that have been twisted together to counter effects of EMI and RFI



- T568A



- T568B

Fiber Optic cable

- Single-mode fiber: long distance (~100km), high cost
- Multimode Fiber: short distance (~560m), low cost

Wireless Media

limitations

- coverage area
- interference
- security
- shared medium

WLAN requires following devices

- Wireless Access Point (AP)
- Wireless NIC adapter

WLAN operate in half-duplex mode, which means only 1 device can send or recive at a time

Data link layer

It does:
- enables upper layers to access the media
- accepts data, usually L3 packets and encapsulates it to L2 frames
- controls how data is placed and received on the medium
- exchanges frames between endpoints over media
- receives data, usually L3 packets and direct it to proper upper-layer protocol
- performs error detection and rejects corrupted frames

It consists of 2 sublayers:
- Logical Link Control (LLC) - communicate between the networking software and upper layers
- Media Access Control (MAC) - data encapsulation and media access control.

half-duplex communications restrict the exchange of data to one direction at a time

Full-duplex allows the sending and receiving of data to happen simultaneously.

A multiaccess network can have 2 or more end devices attempting to access network simultaneously

Contention-based access - all nodes operate in half-duplex, competing for the use of the medium.

Controlled access - each node has its own time to use the medium

Today, ethernet networks operate in full-duplex and don't require an access method

WLAN use half-duplex

Each frame has 3 basic parts:

- Header
- Data
- Trailer

There is no one frame structure that meets the needs of all data transportation across all types of media.

In a process called error detection, the trailer determines if a frame arrived without error.

The MAC address table - the swich examines its MAC table to make forwarding decisions for each frame. If the source MAC address isn't in the table the swich adds it, if it is it refreshes its timer here (usually up to 5 minuts). Then it checks if the destination address is here, if it is it forwards the frame only to this port and if it isn't here it flood it to every port except the origin.

2 Frame Forwarding Methods:

- Store-and-forward switching - recives entire frame and check if there are no errors in it by computing It is forwarded to proper port if no error is detected
- Cut-though switching - it forward frame before it is fully recived
  - Fast forward switching - forward immediatly after reading the destination address
  - Fragment-Free switching - stores first 64 bits and checks them, because in 64 first bits errors occures

Ethernet switch may use buffering technique to store frames before forwarding them:

2 types of buffering methods:

- Port-based memory
- Shared memory

A crossover cable is used when connecting alike devices, and a straight-through cable is used when connecting unlike devices.

The process of encapsulating data layer by layer enables the services at different layers to develop and scale without affecting the other layers.

Network layer protocols perform:

- Addressing end devices
- Encapsulation; adds IP header to transport layer segment making it a packet.
- Routing; provides services to direct packets to destination hosts on another network
- De-encapsulation; If destination IP address maches its own IP then it removes header from packet and pass it to transport layer

Characteristics of IP

- **Connectionless**; there is no connection with destination before sending packets (~~was~~ similar to sending a letter to someone without notifying them in advance)
- **Best Effort**; packet delivery isn't guaranteed by this protocol, it doesn't check if every thing was correctly send and another other protocols have to look for that.
- **Media Independent**; it can be transmitted by different media (i.e. copper, fiber-optic, wireless)

There is one major characteristic which network layer considers: max size of PDU, routers sometimes have split up PDU to smaller pieces this is called **Fragmentation**

Significant fields in IPv4 header:

- **Version**
- **Differentiated Services (DS)** - handle prioritization
- **Time to Live (TTL)**; it limits the lifetime of packet, each time a router gets this header it reduces TTL
- **Protocol**; identifies next layer protocol, and what data type it is carrying i.e. UDP, TCP, ICMP
- **Header Checksum**; detect if header is corrupted
- **Source IPv4 address**
- **Destination IPv4 address**

Major issues of IPv4:

- IPv4 address depletion; limited num. of addresses
- Lack of end-to-end connectivity

Improvements in IPv6 over IPv4:

- Increased address space
- Improved packet handling: IPv6 header has been simplified with fewer fields
- Eliminated the need for NAT

Fields in IPV6 header:

- version
- Traffic Class; equivalent to IPv4 DS field
- Flow Label; suggest that all packets with the same flow label receive the same type of handling by routers
- Payload Length; length of data portion of IPv6 packet
- Next Header - equivalent to IPv4 Protocol field
- Hop Limit - equivalent to IPv4 TTL field
- Source IPv6 address
- Destination IPv6 address

Another role of network layer is to direct packets between hosts. A Host can send a packet to:

- itself
- local host
- remote host

The default gateway is the network device that can route traffic to other networks

on windows `netstat -r` or `route print` to display routing table of host

The routing table of router contains:

- directly-connected networks
- remotel networks
- default route

in PT
show ip route
in exec mode

A router can learn about remote networks in 2 ways:

- Manually
- Dynamically

ARP - device uses ARP when it knows the IPv4 address of destination but don't know MAC address. If IP is in another network it tryies to find MAC of a router. To do so it sends ARP request to all devices.

ARP main functions:

- resolving IPv4 to MAC
- maintaining a table of IPv4 + MAC mappings.

Neighbor Discovery (ND) - It is similar to ARP but for IPv6 addressing. ND provides:

- address resolution,
- router discovery,
- redirection services

Tasks that should be completed when configuring initial settings on a router:

1. device name
2. secured privileged EXEC mode
3. secure user EXEC mode
4. secure remote Telnet/SSH access
5. secure all passwords in config file
6. legal notifications
7. save configuration

IPv4 addresses

There are private IPv4 addresses which can't be used in internet and public IPv4 addresses which can. There is such division due to lack of IPv4 addresses.

VLSM (variable length subnet masking) - allows dividing IPv4 a network space to unequal parts by varying the subnet mask size. This enable more efficient address allocations.

Migration techniques on migrating from IPv4 to IPv6

- Dual stack - allows IPv4 and IPv6 to coexist on the same network segment
- Tunneling - method of transporting IPv6 packet over an IPv4 network, IPv6 is encapsulated inside IPv4 packet
- Translation - allows IPv6 devices to communicate with IPv4 devices, it is similar to NAT for IPv4

Categories of IPv6 addresses:

- unicast
- multicast
- anycast

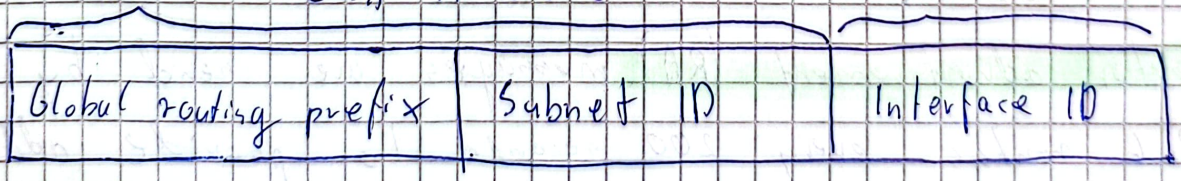
SLAAC - Stateless address autoconfiguration

IPv6 unicast addresses:

- Global unicast address (GUA)
- Link-local Address (LLA)

IPv6 GUA

globally unique, routable on IPv6 internet - equivalent to public IPv4 addresses



Global routing prefix - prefix or network portion of address which is assigned by provider ie. ISP

Subnet ID - used by organizations to identify subnets within its site

Interface ID - equivalent to host portion of IPv4

LLA enables a device to communicate other IPv6 devices on the same subnet (link) and only there

Using LLA of router as default gateway address is considered best practice.

ICMP - Internet Control Message Protocol

Types of ICMP:

- Host Reachability - local host send an ICMP echo on request to host, if host is avaible it reply with echo reply
- destination or service unreachable when a host or gateway recives message it cannot deliver, it use an ICMP destination unreachable message to notify the source. This message contain code that indicate why the packet couldn't be delivered
- Time excoeded - used when a packet couldn't be delivered because the time to live field or hop limit field was decremented to 0

ICMPv6 sends a router Solicitation (RS) message to acquire an IPv6 configuration when booting up

router advertisement (RA) messages are send by IPv6 routers every 200 seconds to provide addressing information to IPv6 hosts.

Neighbour Solicitation (NS) messages is send by host to other hosts to check if its address isn't dyplicated

Neighbor Advertisement (NA) message is send by device in order to determine MAC of destination

Ping the loopback (IPv4 - 127.0.0.1, IPv6 - ::1) - is used to test the internal configuration of IP on local host.

Ping the Default Gateway - used to test ability of host to communicate on the local network.

Ping the remote host - successful ping across the internetwork confirms communication on the local network, operation of router serving as default gateway and operation of all routers that might be in path between

Traceroute (tracert) is a utility that generates a list of hopes that were successfully reached along the path

7. Interference

Interference - when identical waves from 2 sources overlap at a point of space, the combined wave intensity at that point can be greater or less than intensity of either of 2 waves.

case of double sl.

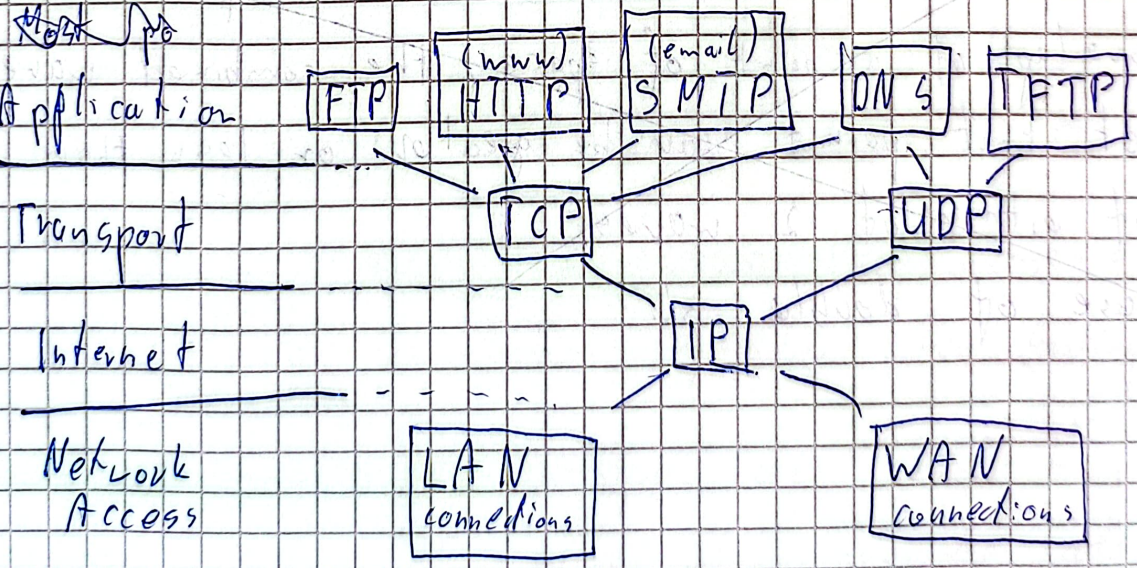
Role of Transport layer

Application layer programs generate data that must be exchanged between destination hosts. Transport layer is responsible for logical communications between applications running on diff. hosts. This

Each set of data flowing bet. a source and dest. application is known as a **conversation** and is tracked separately. It is responsibility of transport layer to maintain and track these conversations.

Other transport layer responsibilities

- segmenting data and reassembling segments
- add header info.
- identifying the applications
- conversation multiplexing (many at the same time)



Transport layer protocols:

- Transmission Control Protocol (TCP) - ensures that all data arrive to final dest.

  TCP provide reliabil. and flow using these operations:

  - number and track data segments
  - acknowledge received data
  - retransmit any unacknowledged data
  - sequence data that might arrive in wrong order
  - send data at efficient rate

- User diagram protocol (UDP) - doesn't provide reliability and flow control, requires fewer header files which means it can be processed faster

TCP Header fields

- Source Port
- Destination Port
- Sequence number ; for reassembly purposes
- Acknowledgment number ; indicate that data has been received
- Header length
- reserved ; for future use
- Control bits ; purpose and function of TCP segment
- Window size ; num of bytes that can be accepted at once
- checksum
- urgent ; if contained data is urgent

UDP Header Fields

- Source port
- destination port
- length
- checksum

Applications that use UDP:

- like vide multimedia applications ie. VoIP
- Simple request and reply app. ie. DNS, DHCP
- Applications that handle reliability themselfs ie. SNMP, TF

Combination of source IP and port or dest. IP and dest. port is known as **socket**

Together they form a socket pair

usually Represented 192.168.1.5 : 1099

IP Port

Port number groups:

- well-known ports 0 - 1023
- registered ports 1,024 - 49,151
- Private/Dynamic ports - 49,151 - 65,535

inetstat command to list the protocols in use

TCP uses 3-way handshake to establish a connection and 4-way to end connection

~~Host~~ source Dest

SYN →

ACK, SYN ←

ACK →

Source Dest

FIN →

ACK ←

FIN ACK ←

ACK →

Application Layer

closest layer to end user, provides interface between ~~users~~ application and underlying network over which messages are transmitted

Presentation layer

- formating and presenting data at source dev. to right form
- Compressing data
- Encrypting and decrypting data

Session layer

create and maintain dialogs between source and destination applications

HTTP and HTTPS

It is a request/response protocol. When client, typically a web browser, sends a request to a web server, HTTP specifies the message type. 3 common message types:

- GET - client request for data
- POST - uploads data files to the web server i.e. form data
- PUT - uploads resources or content to the web server ie image

Email supports 3 seperate protocols, the application layer process that sends email uses SMTP. A client retrieves email using POP or IMAP.

attenuation - loss of signal strength as distance increases

IMAP keep messages in mail servers until they are manually deleted POP: don't provide this. POP3 download the mail to local client

BOOTP - legacy app. enables workstation to discover its own IP address

adware - collect info about user

~~inspecting and~~

IPS - intrusion prevention system

Zigbee - low-data rate and low-power requirements. popular in IoT