tech talks beach edition

Networking - moving data from one place to another.

Converting physical information into electrical impulses which are then send in the network.

OST Model

1. Physical layer - the physical connection between the different components (routers, servers, etc.) through wires and wireless signals. Most used cables - twisted pair cables. Coax cable is used to connect the cable modem to the Internet Service Provider. In the Internet fiber optics, wireless and copper cables are used for establishing connection.
2. Data link layer - ~~Mainly the Ethe~~ a set of protocols for establishing data transfer. Ethernet protocol is mostly used. Between the cable modem and the ISP the DOCSIS-3 protocol is used. An important fact is that the communication happens only between two connected devices for example between the PC and the router, between the router and the modem.
3. Network layer - Provides the communication between any two devices on the internet. Uses the IP protocol

which provides greater abstraction over the Ethernet protocol.

- IP addressing
- IP routing

4. Transport layer - Creates session for communication between two devices on the internet.
   - TCP (Transmission control protocol)
5. Session layer } antiquated layers
6. Presentation layer - It was used back in the days to convert between ASCII and EBCDIC representations.
7. Application layer - Uses the HTTP to encode the data (as hyper text) and transfer the data between machines.

Communication

4.1. Foundations

* The OSI (Open Systems Interconnection [Reference Model]) model
  ~~of 7 layers~~
  - communication ~~protocols~~ services
    - connection-oriented - first the two parties establish a connection, exchange data and terminate the connection
      - telephone
    - connectionless - no setup is needed
      - mailbox
  - 7 layers - each layer provides interface to the one above it

High-level:
- Application - high level protocols; e-mail protocols, web access protocols; FTP, HTTP
- Presentation - defines how data is represented
- Session - provides sessions between applications

- Transport - protocols for establishing reliable communication as well as streaming of data; TCP - reliable, connection-oriented, stream-oriented comm. UDP - unreliable datagram comm.

real-time →

Low-level:
- Network - protocols for routing messages to receiver through a network as well as protocols for congestion transmission
- Data link - detect and correct errors and keep sender and receiver in the same pace
- Physical - how the computers are connected and how bits are represented

- message goes down the layers in the ~~receiver~~ sender and headers are added and upward in the receiver, then downward again in receiver so that a response is sent

Protocols and Port numbers

1. HTTP or HTTPs - protocols for data transfer
   - distinction between a client and a server
   - client machine has browser installed (the software needed for HTTP communication)
   - server has Web Server installed like Apache, Nginx, IIS through which it serves resources
   - & data is sent as hypertext
   - port numbers are the layer 4 (Transport layer) representation of layer 7 protocols used for communication; 80-HTTP, 443-HTTPS; port numbers are used to identify which layer 7 protocol should be used at layer 4

2. FTP, SFTP, TFTP, SMB - protocols for file transfer
   ports: 20 21, 22, 69, 445
   authentication / file transfer
   SMB (Server Message block)
   - SFTP has port 22 which is the same as the SSH port number, because a FTP connection is put in a SSH session, making it secure and encrypted
   - SMB - used for easily sharing files between client and a server in an organization/network; maybe the blue that we used in Amexis has been relying on SMB

   * the browser can actually be used as ftp client if we put ftp:// in front of the url, but has limitations - no file upload, you can only view the file system

3. POP3, IMAP, SMTP - protocols for transfering email messages
   - POP3, IMAP - used by client for retrieving mail from server
   - SMTP - sends email from client to SMTP server

4. LDAP, LDAPs, DHCP

*LDAP, LDAPs - used for authentication

- used with the Microsoft Active Directory
- a client machine which has Windows 10 installed sends the credentials to an Active Directory server, which authenticates us and provides the workstation

*DHCP - provides IP addresses to client machines

- DHCP server could be our router

5. DNS

nslookup (url) - to get the IP address for the given URL

6. NTP (Network Time Protocol) - server provides concrete time to client; run by the government

7. Telnet, SSH - protocols for network management

- Telnet - uses clear text; not secure
- putty - Telnet or SSh client
- SSH connection can be established with servers and hardware devices

8. SNMP (Simple Network Management Protocol) - used for monitoring the status and of all devices in a network.

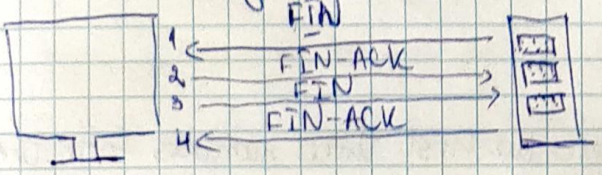
9. RDP (Remote Desktop protocol), Audio/Visual protocols communication with a machine

- RDP - used for remote
- H.323 - used for visual communication; web conference/chat?
- SIP (Session Initiation protocol) - used for sending audio data; used for establishing a phone call

TCP and UDP

1. 3-way handshake
   - syn (synchronized) message is sent to the server
   - the server sends syn-ack (acknowledgement) message back to the client to confirm receiving the message
   - the client sends ack message to the server and now a session is established between the client and the server
   - from now on layer 7 (application) protocol can be used to send another message (request if we are using HTTP)

2. 4-way disconnect
   - 4 messages are sent for ending the session



! it could start the other way around also - from client to server

   - RST - for breaking the communication immediately; used when there are problems with the communication
   - When the session is broken, no more messages can be sent

3. UDP (User Datagram protocol)
   - no 3-way handshake
   - no reliable communication
   - extremely efficient for small data transfer

4. Port numbers

Server (destination port)	Client (source port)
- Well-known - 0 - 1023	- Temporary (Ephemeral) - 49152 - 65,535
- Registered - 1024 - 49151	

Well-known: HTTP(80), HTTPS(443), SSH(22), FTP(20,21), etc.

IP Addressing

1. Introduction

95	87	12	186

↑ network portion ← host portion

host portion - unique identifier of the device

network portion - the larger group that we are part of

- the IPv4 address is a 32bit number that we convert to decimal

2. Classless addressing

- Subnet mask - address which specifies where the host portion is located in the IP address
  - marks all components of the network portion with 1s and uses 0s for the host portion

192.168.0.105

255.255.255.0

11111111 11111111 11111111 00000000

=> here the first three numbers form the network portion and the last one - the host portion

  - network and host portion can exist anywhere in the IP address
- Classless addr. is used since 1995 till now

3. Classful addressing

unicast addresses; the addresses which the public internet uses

A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	192.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	255.255.255.255

unicast - one device on the internet talking to another device on the internet.

multicast - talk from one device to many; used only in large enterprises, not in public internet

A - first 8 bit Network portion; B - first 16bit Network portion;

C - first 24bit Network portion

4. Address types

- Network address - identifies a group of IP addresses
  - also called 'Network prefix'
- Broadcast address - identifies all IP addresses on a network
  - used when we want to send a message to all devices on a network
  - not used much
- Host address - identifies the unique device on a network

5. Network address

- Network address - has only 0s in the host portion
- Broadcast address - has only 1s in the host portion
- Host address - has anything different than only 1s or only 0s in the host portion

Examples:

203.0.113.0	203.0.113.255	203.0.113.10
255.255.255.0	255.255.255.0	255.255.255.0
network	broadcast	host

! We are considering that the decimal numbers are converted to binary, that's why we are only speaking of 0s and 1s.

6. CIDR Notation

- used for shorter writing of the subnet mask

203.0.113.10
255.255.255.0 = 203.0.113.10 /24

/24 ↑ number of bits of the network portion

7. Private IP Address Ranges

10.0.0.0	10.255.255.255	/8
172.16.0.0	172.31.255.255	/12
192.168.0.0	192.168.255.255	/16

- These are the only ranges that we must use for our private IP addresses
- They can't be used for public IP addresses
- 127.0.0.1 - Loopback address
  - used for testing

- Default Gateway - The IP Address of the router; if this field is empty then ~~no router is present~~ there is no router on the network

- In order for two devices to communicate they have to be on the same IP network

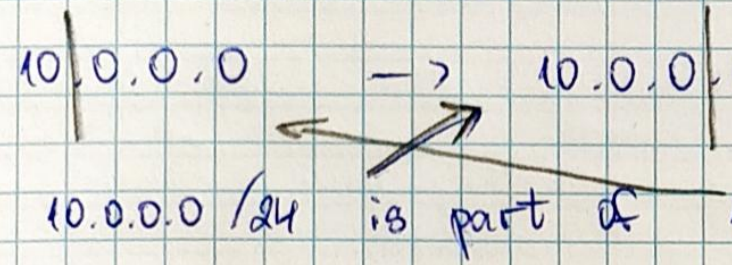
Subnetting networks

- Network IP Address
- Host IP Address
- Broadcast IP Address

→ Define a range for the host IP Addresses

- We can manipulate the subnet mask, for example if we have the 10.0.0.0/8 IP address, we have 24 bits for the host which makes 256^3 unique host addresses and we might want to decrease that number.

- We can move the subnet mask line and thus creating new subnetworks in the main network 10.0.0.0/8



Then we can find the network and broadcast addresses in that subnet and between them lie the host IP Addresses we can use.