-**Switch**:Saves to CAM table (Content addressable memory) pairs port number - MAC address -**Optic fibers**-Single-Mode, Multimode Fiber,Graded-Index Fiber,Step-Index Fiber,Polarization-Maintaining Fiber

-Reliability: reaction of layer to lost/corrupted block of data. Types of services:

- unacknowledged connectionless service acknowledged connectionless service acknowledged connection-oriented service.

-Link layer protocols ensure communication between neighboring devices:**-framing, -link access.**

-Bit error rate (BER) - number of bit errors per unit time

-CRC (Cyclic Redundancy Check)

-"bandwidth × delay—influences the selection of frame acknowledgment and resend methods.

-Link Layer(data transfer between "neighboring" devices) Sublayers

- **MAC (Medium Access Control)** – controls the access to shared medium, defines frame address (MAC address)
  - Random Access Methods:
    - **ALOHA**: whenever a sender has data, it transmits, in case error (higher layer), sender retransmits his message after some random time **Slotted ALOHA**: time is slotted and a packet can only be transmitted at the beginning of one slot **CSMA(Carrier *Sense* Multiple Access)**: before the station starts transmission, it listens to the link. if channel is idle, station transmits && if channel is not idle, three variants:
      - 1-persistent: wait for finish and send right away with probability 1
      - non-persistent: wait for random time
      - p-persistent: wait until the next slot and send with probability p
    - **CSMA with CD(collision detect)**: same with CSMA, just if collision stop. (could not listen during transmitting) **CSMA with CA(collision avoidance)**:(RTS-CTS: station- RTS – Request To Send packet……central- CTS – Clear To Send)
- **LLC (Logical Link Control)** – supports the coexistence of different network layer protocols in the same link, flow control and error control

-**Frames**: Stream of bits is divided into frames…..byte stuffing: start and stop flags

-**collision**: a situation where two or more wireless devices transmit data simultaneously, resulting data packets overlapping each other

-**AP (Access Point)**: a (central hub)device that enables wireless devices to connect and communicate with each other/a wired network

-WiFi: authentication protocols:- free access (no authentication): -WEP, –WPA, WPA2

-**Bluetooth: PAN (Personal Area Networks)**

-**VLAN = Virtual Local Area Network**- They are designed to be able to separate flows in networks at the link layer. implemented using tagged frames. VLAN division:

- By **ports** – a specific VLAN is selected according to which specific ports on the switch are assigned to it (can be used for smaller networks). By **addresses** – a specific frame is assigned to a specific VLAN group according to the link(MAC) address. By **protocol** – the frame is assigned to a specific VLAN according to the higher layer protocol it transmits (eg voice, video, etc.). By **tag** – by attaching a tag to a frame (most common today), it is commonly referred to as a tagged vlan. Multiple (VLAN within VLAN, Q-in-Q)

-IP = Internet Protocol

-ICMP = Internet Control Message Protocol-send error/information messages

-The mechanism for finding a path between a source and a destination station is called **routing**

-Network layer

- connectionless services, connection-oriented services,
- their diff—— **path registration** | no yes **addressing** | src/dest addr label **state information on the router** | no yes **routing** | individual only during the path registration **router failure** | small problem big problem **QoS & flow control** | difficult easy **congestion control** | difficult easy

-Types of addressing:

- **unicast**(dest-1 host) **broadcast**(dest-all hosts in local) **anycast**(dest-1 host in group) **multicast**(dest-groups of hosts)

  - **IGMP protocol** (Internet Group Management Protocol) for hosts registration **PIM protocol** (Protocol Independent Multicast) for multicast routing

-IPv4 address:

- **CIDR schema** (Classless Inter-Domain Routing) – RFC1518, RFC1519. network prefix length is arbitrary **Private IP address**: free to use in private networks

-**Fragmentation**: by MTU (Maximal Transmission Unit),packet with length > MTU will be divided to more smaller packets

-**ARP**-Address Resolution Protocol-resolution of network layer addresses into link layer addresses

-IPv6 header: changes

- **omitted**:fragmentation, options: replaced by extension headers header length: is fixed now checksum: get rid of recalculation on each router
- **New field**:Flow label (20b) – identification of data flow to make routing easier

-Types of IPv6 addresses-

- individual: **unicast** group: **multicast** selective: **anycast**

-IPv6 network ranges-

- ::1/128 - loopback fc00::/7 - unique local addresses (local network range) fe80::/10 - link local range ff00::/8 - multicast 2000::/3 - global addresses 2001:db8::/32 - used for documentation and illustration purposes

-**Jumbogram**: IPv6 allows larger packet – jumbogram – up to 4 GB

-Fragmentation: minimal MTU for IPv6 is 1280 bytes, performed by sender.

-**Neighbor Discovery Protocol**: extended replacement for ARP, uses ICMPv6…find out link addresses in the local network && routers discovery

-**MultiProtocol Label Switching (MPLS)**:adds label to layer 3 packets & implements end-to-end connection independent of link layer

-**MPLS network**:Label Edge Router(LER) attaches label to packet when it enters MPLS network, inside the MPLS network, packets are forwarded according labels by LabelSwitch Routers(LSRs),when packet exits the MPLS network, the edge router removes the label

-**DHCP service(statefull-auto network configuration):** (we have one more -dhcp is not connected for stateless(link-local))

- Client - discovery Server - offer Client - request Server - acknowledgment

-**Path** = the sequence of routers that a packet must pass between a source and a destination station.

-If the routing tables on the routers have to be set manually, this is **static routing**. When routing tables autonomously configure routing protocols during operation, this is **dynamic routing**.

-Types of routing:

- Optimal(metric)
  - **shortest path**, number of intermediate routers. **the cheapest** (different routes have different costs).
- **Redundant** (multi-path): The router chooses one path based on a certain criterion
  - Traffic can be conducted in different ways. It is suitable for backing up trips or load sharing.
- By symmetry
  - **symmetrical** (forward and reverse paths are the same). **asymmetric** (not symmetrical, e.g. satellite systems.. affects packet delivery time).
- According to the way-finding method
  - **flood** (simplest, but many technologies and protocols use them). The request is provided with an identifier (ID), to prevent loop **proactive** (path is calculated in advance and stored in the routing tables). **reactive** (path is created only when needed) adhoc/mobile networks (variable topology).

- According to the route calculation area
  - **Internal** (within one network).OSPF, RIP protocols **External** (between different networks).BGP protocol

-**ISP- Internet Service Provider**, connection provider with assigned specific IP ranges.

-Typical routing table entry entries

- **Destination**: IP (destination city analogy). **Gateway**: IP (an analogy to the next signpost on the route).Gateway 0.0.0.0 means it's a local network **Mask/GenMask**: by prefix (analogy: area).. **Flag**:--- **Metric**: price (analogy: distance in km). **Interface**: name (analogy: entrance to the road).

-Routing tables can be configured manually (statically)-not able to respond to changes. or dynamically-quickly respond…. types of dynamic routing algorithms

- **Distance Vector Algorithms** (DVA)-to optimize uses Distributed version of Bellman-Ford Algorithm (DBFA-used in RIP = Routing Information Protocol.). **Link State Algorithms** (LSA)-used Dijkstra's algorithm (DA) , protocol OSPF = Open Shortest Path First, IS-IS (Intermediate System to Intermediate System) protocol.. LSAs are less demanding on the link load due to data exchange **Path Vector Algorithms** (PVA)-using **BGP = Border Gateway Protocol**(BGP is used primarily for external routing). metric of a particular path-VH = vector of values. Between neighboring edge routers, data is delivered using the link layer

-**Link (L):** connection of two neighboring routers (X and Y) with a certain cost (C).

-**EIGRP (Enhanced Interior Gateway Routing Protocol)**:advanced distance-vector routing protocol. synchronizes routing tables at startup, sends specific updates only when topology changes occur to multicast address 224.0.0.10

-**Autonomous System (AS):** Group of all IP address ranges of a specific ISP. Each AS has its own specific identifier. Identifiers are used for external routing

- An AS receiving traffic only for its internal stations is referred to as **non-transient,** An AS forwarding traffic intended for a station belonging to another AS through its internal network is called **transient**.

-**Sample BGP routing table**:

- **Network** = target network **AS PATH** = path to destination **network, L(AS PATH)** = path length. **MED, LocPrf, Weight** - various attributes of the metric value vector. Rule: Weight > LocPrf > MED > L(AS PATH), i.e. if two paths to one destination have the same e.g. Weight, the decision is further made according to LocPrf.

-Transport layer:

- reliability flow control data segmentation correction of errors
- **Connection establishment**: three-way handshake: CONNECTION REQUEST, ACKNOWLEDGE, DATA…..conntect(->)->accept(<-)->data(->)->accept(<..-)
- **Connection termination: asymmetric termination**(one user terminates the connection , possible data loss when the other user sent data before receiving termination message), **symmetric termination**(both sides must agree, there is no fully reliable solution if communication is not secured) FIN(->)->ack(<-)..half closed. FIN(<-)->ack(->) total close

-**TSAP – Transport Service Access Point** port 80 for http

-The minimum transmitted unit is referred to as a **segment.**

-**TCP-Transmission Control Protocol**- connection-oriented, guarantees error free data transmission, duplex. **data delivery guarantee**: checksum, detection of duplicate packets, retransmission, correct ordering, timeout, good for applications which need reliable data channel

- **Sliding window**: receiver reserves buffer, receiver specifies the current window size in the reply
- **Acknowledgement**: receiver sends ACK, where is the sequence number of the byte, which is expected. if a packet does not arrive, but the following does, receiver repeats the last ACK it will indicate the packet might have been lost
- **MSS (Maximum Segment Size)** – maximum size of the packet to be sent, defined by the receiver
- **SSTHRESH (Slow-start Threshold)** – limit for likely congestion
- **CWND (Congestion Window)** – sender window.

Congestion Control:-slow start initial CWND 1,congestion window size is increased 2x: grows exponentially….packet or its acknowledgment is lost, if ACK did not come at all (timeout), is duplicate ACK comes 3x:

-**UDP(User Datagram Protocol):** connection-less, UDP datagram may be lost, used where packet losses are not be critical (eg. DNS)

-**RTP(Real-time Transport Protocol)**UDP**:** streaming data between endpoints in real time. header contains ”timestamp”.

-**RTP Control Protocol- RTCP:** provides statistics and control information for an RTP session, does not transport any media data itself, used to control quality of service

-Domain Name System (DNS): a system primarily intended for translating domain names into IP addresses. load sharing, access restriction. DNS runs on port 53 by default

-**DNSSEC** :secure DNS extension to prevent response forgery.

-**Name Server (NS):** a computer that takes care of translating domain names to IP addresses.

-**DNS Server** = NS working in the DNS system.

-**Domain =** a set of different domain records grouped under a common domain name

-**Resolver**: a program that communicates with the Name server by sending a request to translate a domain name to the corresponding IP address.

-DNS servers that manage RRs for specific domains are called **authoritative DNS servers** for those domains.translation: -**directly**(ip->domain), -**reverse**(opposite)

-Root DNS servers = Level 0 DNS servers.13 groups are there.

-Four types of TLD domains:

- **Generic Top Level Domains (gTLDs)** The **3-character code** indicates the function of the organization using this domain. Primarily used in the US. …. gov, mil, edu, org, com, net. **Country Code Top Level Domain (ccTLD)** I The **2-character code** indicates the state in which the servers listed in the RRs of the given domain are typically located: cz, us, va, jp, de. **New Generic Top Level Domains (ngTLD)** The domain name can be any string. This is how they mark e.g. cities .paris, .london, etc. **Reverse domain in-addr.arpa** Designed for converting an IP address to a domain name

-**Fully Qualified Domain Name (FQDN)**: concatenation of domain name into one string ‘.’ for separation. limited to 63 characters(specific level).overall 255 character.

-**Zone**: a specific subset of a set of domain names.

-**Zone Record** = SOA Record.{RRs}

-**SOA record**: record containing basic general information about the given zone. Only one exists.

-**Domain resource record**: a record containing specific information for a specific domain name. There are usually several mutually different RRs.

-The **general form of RR** is (Name, TTL, Class, Type, Value)

- **Name** = domain name of the given server. **TTL** = time in seconds, how long the RR can be stored in the cache of DNS servers, after which it must be loaded again. If the TTL is not specified in the record, it is taken as the MINIMUM value from the SOA record. **Class** = the protocol family to which the record relates (commonly IN, IN = Internet, other classes exist but are not used). **Type** = determination of the type of record. **Value** = IP address or domain name.
- **Selected types of RR**: **A** - IPv4 domain name **AAAA** = IPv6 domain name. **NS**= authoritative DNS server **MX** = server handles email delivery **CNAME** = canonical name **PTR** = reverse record of IP address **SRV** = server providing VOIP **TXT** = Text comment **CAA** = Certificate authorities **RRSIG** = public key to verify given record, uses DNSSEC extension record

-**DNS protocol** = a protocol that is used for sending queries and responses in the DNS system. transmitted in the DATA item of a UDP or TCP packet. uses port 53

-The DNS server sends DNS queries distributedly, in two ways: **iteratively** or **recursively**.

- An **iterative DNS server** that resolves a domain name to an IP address is querying step by step. It starts at the root DNS server and moves down one level at each step. **Recursive way of querying** in DNS: here root dns servre request TLD or authoritative DNS recursively. **Reverse query** = a query whose task is to find out the domain name for a given IP address.The reverse query for the IP AA.BB.CC.DD is formulated as a direct query for the domain name DD.CC.BB.AA.in-addr.arpa.

-Dynamic DNS- DynDNS server: DNS server that can change A records for domain names according to station instructions on the fly.(checking ip address regularly)

-**DNSSEC** = secure DNS where the authenticity of the response can be verified. Each DNS server signs its response with its private key. Using the public key, which is stored in the RRSIG record on the DNS server of the parent domain, it is possible to verify the authenticity of the answer.

-**DNS and load balancing**: The principle is that when the same domain name is requested repeatedly, the authoritative DNS server returns a different IP address each time.

-**Attack on DNS - Cache Poisoning**: when the DNS server detects the translation, the attacker generates a response that contains the identical response ID and the spoofed IP address. Since the response from the attacker arrives earlier than from the authoritative DNS server, the DNS server forwards the attacker's response to the user and stores it in its cache memory.

-**Attacker** = an Internet user who, on his own or through special programs or hardware, carries out attacks against other users.

-Computer **network security technologies**

- **Firewall IPS/IDS Honeypot Scrubbing center**

-**Firewall** = a device that controls, passes, filters, or modifies network traffic coming to the inbound network interface. The specific firewall activity for a specific type of network traffic is defined by firewall rules.

-Types of firewalls:

- **Packet(network)** Evaluate network traffic based on the source and destination IP addresses of the packet. More advanced firewalls also perform detailed in-depth analysis of individual packet headers and data, the so-called **Deep Packet Inspection (DPI).** DPI is not applicable to encrypted protocols, such as HTTPS. Unencrypted protocols can be identified by specific strings. **State(transport)** Throughput rates are comparable to packet firewalls. In advanced security systems, they are used with **Intrusion Prevention Systems (IPS)**. **proxy(application layer)** Devices or programs that control and forward traffic between the source station and the destination server. communication via the application layer protocol.

-**Signatures**: specific unique strings (fingerprints) of characters enabling the identification of headers of specific protocols with high probability.

-**DEEP Packet Inspection (DPI)**: DPI firewalls have so-called signatures defined for selected protocols, on the basis of which they recognize the protocols.

-**Packet firewall operation**: Firewalls perform specific actions on packets based on predefined rules. The well-known Linux packet firewall is called **iptables** (the newer version is called nftables).

-iptables - **chains of rules for working with packets**:

- **PREROUTING** = chain related to all packets before making a routing decision based on the packet's destination IP address. **POSTROUTING** = chain related to all packets after routing decision is made based on the destination IP address of the packet. **FORWARD** = chain related only to packets that are forwarded. **INPUT** = chain only for packets that are intended for local applications. **OUTPUT** = chain related only to packets that are generated by local applications.

-iptables distinguish three basic rule tables:

- **filter** = enable or disable packet delivery. **nat** = translation of IP addresses or ports in the packet header. **mangle** = edit items in the packet header for further processing.

-**Demilitarized Zone (DMZ)**: part of a network that is accessible from the external network (Internet). It makes a certain service available to any users, such as websites/mail forwarding.

-**Intranet**: internal part of the network that is accessible only to authorized users, e.g., file sharing server, non-public websites.

-**Application firewall** = firewall communicating through specific application protocol.

-**Application firewall (proxy)**: used for hiding the source IP address, reducing the amount of outbound traffic. AF copies the request, sets up itself as the originator of the request, and contacts the destination server (DS).

-**Intrusion Detection System (IDS)**: If a threat is detected, it informs the administrator, who will take action to eliminate the threat.

-**Intrusion Prevention System (IPS)**: If a threat is detected, the IPS sends an instruction to the Firewall requesting activation or generation of a rule

-**Honeypot** (demilitarized zone)= a device that serves as bait for an attacker in order to obtain information about attacker. gives the impression of running network service.The attacker who discovers the honeypot tries to attack it and it stores their info.

-**Scrubbing center** = a group of devices filtering a portion of network traffic that shows signs of various network attacks. Filtration phases:2 router. 1 for unfiltered, 1 for filtered.

-**Port scanning** = discovery of services running on a given computer. performed by establishing a connection (TCP). If the station responds to requests sent to the destination port, we speak of an **open port**, otherwise a **closed port**.

- **Horizontal**: scans a specific port with different IP addresses(pcs). **Vertical**: scans multiple ports with a single IP address(pc).

-**Password cracking** - the attack takes place via terminal services (SSH, RDP, TELNET)

- **Brute force attack**: tries all possible combinations of characters. **Dictionary attack**: uses a predefined list of passwords that used frequently.

-**Denial of Service (DOS)** = attack implemented to prevent access to the service.(send many ICMP queries, opening many TCP connections)

- **Distributed DOS (DDOS)**: DOS version run from different infected computers.(The attacker first attacks and controls several computers and attacks) **Reflected/Spoofed DOS (RDOS)**: The source IP address in the IP packet header is spoofed and used for sending many ICMP requests and therefore difficult to identify the attacker.

-exploit specific security vulnerabilities : Malicious applications that perform this type of attack are called **worms**. **attack Buffer overflow** = overwriting a specific area of main memory triggers a specific action

- **Sending spam**: attack by content is **Phishing** = an attack to capture a user's identity by opening a link to a fake login page.

-**Malware**: The application then performs specific actions without the user's knowledge.

- **Trojan horse** :behaves like a normal legitimate application, but contains malicious code. **Ransomware** = malware that encrypts the contents of the hard disk. **Spyware** = malware that tries to read various user information. **Adware** = malware that displays advertising offers.

-**VPN-Virtual Private Network**.The task of a VPN is to make the local network or its part available to user who is by network geographically separated from it.

- **Intranet** - within the same network of one organization. **Extranet** - allow access for an authorized set of customers to subset of services. **Remote Access** - connection of a certain employee to the company.

-**Access/VPN Server** = access server that mediates remote access to user connected via a data/telephone line. **VPN Device** = device that is used to connect a local network to surrounding networks via VPN. VPN protocols are used for communication. **VPN tunnel** = virtual connection realized between VPN devices.

-**Tunneling(network service does not have native encryption support)** = sending data through the created tunnel.

- -**Carrier Protocol** = a lower layer protocol that ensures the delivery of VPN protocol packet data. **VPN Protocol** = the protocol used to create the tunnel. **Encapsulated data** = packets/frames of the original protocol, are transmitted through the tunnel.

-Classification:

- ***CE**(customer edge):***IPsec GRE***(*transport layer,…* **C, R, K, S, s** = corresponding flags that indicate whether the given items (Checksum, Routing, Key, Sequence number, strict source route) are in the header. **Recursion** = number of additional encapsulations allowed. **Flags** - reserved bits must be set to 0. **Version** = GRE header version: 1 if it is a PPTP protocol, otherwise 0. **Protocol** = indication of the protocol whose data is encapsulated. **Checksum** (optional) = calculated checksum from the GRE header and payload. **Offset** (optional) = offset within the Routing field. **Key** (optional) = number that was entered together with the encapsulation. The receiving party uses them to authenticate the sender of the packet. **Sequence number** (optional)= number that was entered together with the encapsulation. The receiving side determines the order in which the packets were sent. **Routing** (optional) = list of source route entries.*)* ***PE**(Provider Edge): LX VPN = Layer X VPN: ***OpenVPN***(*app layer,* s implemented in the operating system through virtual network interface*),* ***PPTP(***used GRE,PPP, built on a client-server model…**Length**:size of the PPTP message in bytes. **Message type** = identifier taking the values 1 or 2. **Magic cookie** = the value of this field is always set to 0x1A2B3C4D.***)/SSTP(***app layer,* Secure Socket Tunneling Protokol, transmitted in HTTPS protocol.How to-**Establish a TCP connection-Start SSL encryption-Transmission via HTTPS***),IPinIP(**network layer,* interconnect networks that are located behind routers that perform address translation, original IP packets are packed into new IP packets, no encryption*), VPLS* ***Dial-Up:** ***PPP***(**Flag** (1 byte)frame's begin and end. **Address** (1 byte) = destination identification, always has value 255 (broadcast). **Control field** (1 byte) type of operation performed. **Protocol** (2 bytes) protocol whose data is transmitted in the Data field. **Data** (max. 1500 bytes) = specific transmitted information. **FCS** (2/4 bytes)-frame check sequence, protection against transmission errors.*)/L2TP (*link layer, **T, L, x, S, x, O, P = flags** (Type, Length, Sequence, Offset, Priority) and reserved (x) bits. **Version** = protocol version. **Length** = message size in bytes. **Tunnel ID** = unique identifier of the tunnel. **Session ID** = a unique session identifier within a given tunnel. **Ns** = sequence number for data/control message. **Nr** = sequence number expected in the next control message to be received. **Offset size** = specifies the number of bytes after the L2TP header where the start of the data is expected. **Offset Pad** = variable length, padding.*)* ***Broadband**: (**DSL(Digital Subscriber Line)**, VPN is implemented via a digital line. It is used for telephone lines/cable television): *IPsec(*IP Secured,network layer.*)*

  - **Internet Key Exchange (IKE)**:aims to negotiate encryption keys that are used in AH or ESP. **Authentication Header (AH)**: ensure mutual authentication between parties. **Encapsulating Security Payload (ESP)**: provides symmetric encryption of transmitted data.
  - two modes- **Transport mode** = IP header is kept and the data part of packet is encrypted. lower demands on the capacity of the transmission link. **Tunneling mode** = the IP packet is packed and protected. The new packet contains IP addresses of routers between which the tunnel is built. hides the IP address of the source&destination.

-**Browser fingerprint (BF)** = a set of specific attributes sent within an HTTP connection by a web browser.

-**Tor** = a network that aims to disable user tracking.

-**Darknet** = anonymous unregulated version of the WWW.

-Typical services that application protocols:

- **Terminal services (remote administration)**: ***SSH, Telnet,***(Protocols for remote management of stations or servers via a terminal, uses TCP, client-server model, ssh port 22, telnet port 23.) ***RDP(***Emulates access to a computer's graphical interface, Port 3389,TCP, written efficiently***), VNC.*** **File transfer**: ***FTP***(TCP, creates two different connections that differ in destination ports, contains a number of commands for working with the file system, works in **passive(**client is behind router that performs address translation**)(**AUTH, USER,PASS,PASSV(mode), server proposes port, client choose his port,(data transfer),QUIT**)** or **active**(AUTH,USER,PASS, PORT,(data transfer),QUIT), ***TFTP, SCP/SFTP*** **Electronic mail**: ***SMTP***(Simple Mail Transfer Protocol, forwarding emails between mail servers, or sending emails between UA and MTA, destination port 25), ***POP3,(***port 110***), POP3s*** (port 995), ***IMAP(***Internet Mail Access Protocol, port 143, protocols designed for reading mail through UA and MTA.***), IMAPs(***port 993***)*** **POP3vsIMAP**(pop3 copies to each pc, deletion does not affect all-imap just opposite)***SPAM EMAILS(***Two solutions -**Filtering on the server side, Filtering on the client side*****)*** **Website**: ***HTTP(s)***(Hyper-Text Transfer Protocol, used to transfer website content, port 80,transport layer, HTTP v1, 2, 3, Is stateless…HTTPS(secured) port 443), ***QUICK*** Requests: GET = loading a page from the server, HEAD = loading only the header from the server,POST/PUT sending data , DELETE – deleting information from the server **Cookie**:file with the settings of specific client parameters for a given website, client ID. HTTPS protocol,**how:** request, public/private key, random encryption key, encrypt REK, decrypt REK using private, use the REK to encrypt website to send to client, decrypt the message **time synchronization**: ***NTP(***Network Time protocol, uses UDP, port 123, most accurate time data can be obtained from atomic clocks***)*** P2P(peer-peer) sharing: ***Bittorrent***(creation of this protocol is the implementation of data sharing between users directly) **Communication via VoIP**: ***SIP(***Session Initialization Protocol, establish a connection between stations for the purpose of making voice call, simple open protocol, contains only signaling commands,for sending data containing voice it is necessary to use another protocol -**RTP** = Real Time Protocol, a simple unacknowledged voice transmission protocol, direct connection to the DNS protocol, not encrypted***), RTP(***communication are available to each other using routing. Devices: **User Agent** (UA) = client program/device enabling VoIP services. **SIP Server** = server that mediates SIP communication for group of UA belonging to the same domain name. **SIP Proxy** = node that communicates with the SIP server if it is not reachable directly. **SIP Registrar** – node that responds to requests to login to the SIP server. **Redirect server** – server that redirects registration requests to another server (typical code 3XX). **SIP Gateway** –place where connections to other operators (public telecommunications network) take place***), Skype.***

-**Mail Transfer Agent (MTA)**:program running on a mail server that sends/receives electronic mail.-**MTA relay (forward)**:server accessible from the Internet that fulfills the MTA function. It is used to protect the MTA from attack(located in the demilitarized zone).-**User Agent (UA)**:program running on the user's device that retrieves mail from a mailbox (**mailbox** = a file with mail content) on a mail server.

-**MX record** = IP address or domain name of the mail server (MS)

-**Wireless network**: transmission medium used is air or vacuum, Antennas are used,

-**Communication channels (CC)** = communication links of wireless networks. -**Radio Frequency Identification (RFID)**

-**Electromagnetic (EM) wave** = propagation of electromagnetic field through space at certain time.

-**Antennas** = elements in wireless networks that transmit and receive EM waves.(controls direction, intensity).parameters: **Antenna gain** = level of amplification of elmag intensity. waves after passing through the antenna. **Operating bandwidth**: frequency range for which the antenna was designed and has the highest gain. **Antenna directivity**: direction of transmission or reception of elmag. wave, is described by a radiation pattern.

-**Transmission channel** = antenna operating band on which the data is transmitted. Typical transmission channel parameters: frequency & width

-**Throughput(capacity) of the transmission channel** = number of bits/second that can be transmitted through transmission channel simultaneously.

-**Antenna polarization**: plane in which the electric component of EM wave propagates (circular polarization more resistant to interference)

-**Radiation pattern**: planar representation of the radiation directions of a given antenna. Beam angles are used to quantify the direction of propagation..**Main lobe** = primary radiation direction of the antenna, indicates the area covered by the antenna. **Back lobe** = opposite direction of the antenna, indicates the area that the antenna disrupts. **Side lobe** = the direction that the antenna covers or interferes with

-Types of antenna: ***radiation patter***: **Omnidirectional** ($360\circ$)-(10s and 100s meters). **Sector** ($30-180\circ$)(1s kilometers). **Directional** ($10-30\circ$)(100s meters to 1s kilometers). **Narrow-directional** ($<5\circ$)-(10s kilometers). ***type of construction:*** **Yagi antennas Zig-Zag antennas Dishes Spiral antennas(**circular polarization**)**

-**Antenna array**: system of antennas that connects each antennas into a homogeneous whole. -**Fresnal Zone**: one of series of ellipsoidal regions of space between transmitter & receiver

-**Transmission channel**: set of subchannels of the same width connected together.

-**Multiplex**: simultaneous sharing of same transmission medium by multiple stations. ***Types***: ***Frequency Division Multiplexing (FDM) Time Division Multiplexing (TDM) Space Division Multiplexing (SDM) Orthogonal Frequency Division Multiplexing (OFDM):*** same width for all sub-channel, data transferrred via separate subchannels. ***Frequency Hopping Spread Spectrum (FHSS):*** transmission channel divided into many subchannels, between it is retuned according to predetermined scheme, low interference

-**Modulation**: adaptation of signal that carries data information to the frequency band of antennas for which they are designed.***Types: Simple***(Amplitude, frequency, phase) ***Compound***(Combine more simple modulations, **Quadratic Amplitude Modulation (QAM)**, **Direct Sequence Spread Spectrum (DSSS)**)

-**Symbol**: data unit that is transmitted by a single EM wave. -**Modulator**: device that modulates the transmitted signal.-**Demodulator** = device that obtains original data information from the received signal.

-Hidden(C)/Exposed(B&C) Node(A&C are not reachable/A&D do not hear each other).

-802.11 division: **Infrastructure**: central unit (AP = Access Point) controls the communication.**Ad hoc**: Stations communicate directly, without AP

-Type: ***Management***: Used to connect the station to the network, Send parameters that stations must support to connect to the network: Beacon (also contains name + transmission parameters). ***Control***: Controls the access of stations to the medium. ***Data:*** Transfer data between the AP and the station/between stations.

-IEEE version diff:

	Frequency-GHz	Channel Width-MHz	Overlap	Total channel	modulation	through put-Mbit/s
802.11b	2.4	22	y	14	DSSS+BPSK	11
802.11g	2.4	22	y	14	OFDM+QPSK	**54**
802.11a	5.1-5.9	20	n		OFDM+QPSK+16QAM	5180-5320(Home), 5500-5700(Outdoor)
802.11n	2.4/5.1-5.9	MIMO supported	can use beamforming	can be combined(upto 4 antennas)	OFDM+QPSK+16QAM	600
802.11ac/ax - Wifi 6	2.4 and 5 both	20/40/80/160..MU-MIMO	spatial-multiplex. beamforming	upto 8 antennas	16, 64, 256 QAM	WPA3 security

-**Channel overlapping: 802.11b,** the transmission channels overlap. 5n+1(n=0,1,2)/5n+integer

-**IEEE 802.11 is called SISO** = Single Input Single Output, one antenna is used for reception and transmission. -**MIMO** = Multiple Input Multiple Output, multiple antennas are used for transmission and reception at the same time(how to use: **spatial multiplexing(**data is split before transmission and is transmitted in parts by different antennas**), maximal-ratio combining(**client does not support MIMO connects to AP supports MIMO. AP receives same signal from multiple antennas and chooses one that is best**)**).-**MU-MIMO** = part of the antennas is reserved for each user. AP communicates with each user in parallel

-**Beamforming** = broadcast EM waves in narrow direction that can be changed dynamically.(target and shoot)

-**Channel Bonding**: Multiple transmission channels used simultaneously to create single wide transmission channel. -**Stop-Wait**: if sliding window Wlm will be nominator

$$n_0=\begin{cases}\frac{l_m}{l_m+T_0C} & \text{: NACK without error}\\ \frac{l_m}{l_m+T_0C+P(l_m+l_a+2T_dC)} & \text{: NACK with error}\\ \frac{l_m}{l_m+l_a+2T_dC} & \text{: NACK\&PACK without error}\\ \frac{l_m}{l_m+l_a+2T_dC+P(l_m+l_a+2T_dC)} & \text{: NACK\&PACK with error}\\ \frac{l_m}{l_m+l_a+2T_dC} & \text{: PACK without error}\\ \frac{l_m}{l_m+l_a+2T_dC+P(l_m+T_0C)} & \text{: PACK with error}\end{cases}$$

$$P=\frac{1}{1-P_p}P_p=\frac{1}{errorRate}|P=\frac{1}{1-P_p},P_p=1-(1-p)^{l_m}$$