Base

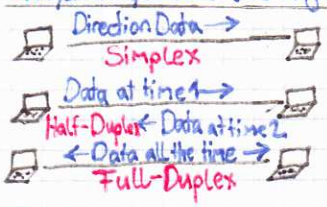
65535 = FFFF

Numbers 1 Byte = 8 bit, 1 Mbit = 1'000'000 bit, 1 Mibit = 2^{20} bit

Data Rate ① convert to bit ② divide by bandwidth Bsp: 750 kB over 10 Mbit/s
③ (750 · 8) bit ⇒ 6 Mbit ② 6 Mbit / 10 Mbit/s ⇒ 0.6 s ⇒ 600 ms

OSI-Model

Layer	Funktion	Protokolle	DNS (123)	Package	Device
7 Application:	Wahl Anwendungsprotokoll / Dienste	ssh, http, DHCP, VoIP, Mail, FTP, RTP (12B)		Message	Gateway
6 Presentation:	Message Encoding/Decoding including compression, presentation interpretation	ASCII, JPG			
5 Session	: Aufbau und Verwaltung von Sitzungen	iSCSI, TLS, SSL			
4 Transport	: virtuelle End-zu-End verbindung (clients)	TCP (reliable, 20B) UDP (unreliable 8B)		Segment	
3 Network	: Weltweite Adressierung, Routing in Web, Data Flow Control	IP (4/6) (20/40B), Routing (RIP/OSPF) ping (ICMP)		Datagram	Router
2 Datalink (Datensicherung)	: bereitstellen fehlerfreier Kommunikations-verbindung (Lokal)	Ethernet (14B, 4B), WLAN, LTE, Arp, MAC Broadcast, PPP		Frame	Switch / Bridge
1 Physical (Physikalisch)	: Übertragung von bits über physikalisches Medium	Modulation, Cabling, NIC, Collision		Bits	Hub / Repeater



⊕ Komplexität in Ebenen geteilt
⊕ Unabhängige Weiterentwicklung

⊖ Schlechtere Performance
⊖ Overhead

Service Data Unit (SDU): Data from/passed to UPPER Layer
Protocol Data Unit (PDU): Data from/passed to LOWER Layer

Division Multiplexing (DM): Technology to send Streams
- Time DM: Sending Data after each other
- Space DM: Sending on different Cables
- Freq. DM: Sending on different Frequencies
- Code DM: Gleichzeitige Nutzdatenströme auf gemeinsamem Freq. Bereich (3G)
- Wavelength DM: Sending with different Wavelengths

Unicast: Communication with a single Recipient
Multicast: Communication with multiple Recipients in specific Group
Broadcast: Communication with everyone in range and listening

Internet Organizations: Maintain IPv4-Adresses for respecting region
American Registry for Internet Numbers (ARIN)
Réseaux IP Europeans (RIPE)
Asia Pacific Network Information Centre (APNIC)
African Network Information Centre (AfriNIC)
Regional Latin-American and Carribean IP Address Registry (LACNIC)

Topologies

Vollvermascht (Core) 1.
K1 K2 K3 K4 K5 K6 K7 K8 K9 K10 K11 K12 K13
K1-Knoten
K-Kante

Ring

(Distribution) 2.

Stern

Bus

(LAN Access) 3.

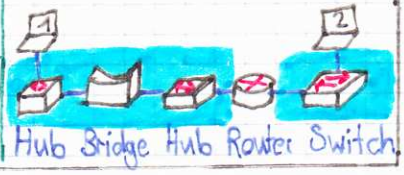
Hierarchical: Almost all big Networks
⊕ Summarization, traffic/capacity planning, scalability, domain separation, troubleshoot

Non Hierarchical (Flat-designs)
Best for small Networks / Any-to-Any

Broadcast and Collision Domains
Routers, switches and bridges separate LANs into Collision Domains

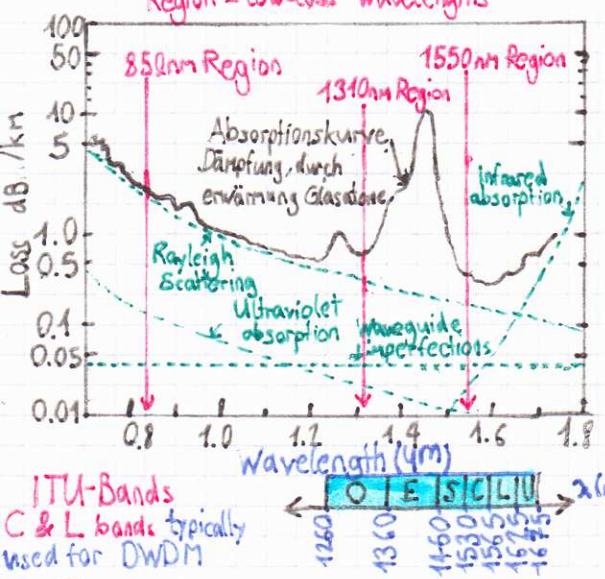
Routers separate LANs into separate Broadcast Domains

Collision Domains

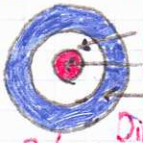


Physical Layer

Optical Networks



C & L bands typically used for DWDM



Cladding: Designed for optimal reflective Index
Core: medium where the signal travels
Coating: Protects cable from external factors
Dimensions: measured in µm = 10^{-6} m Hair = 50µm
Refractive Index (n): $n = c/v$: $n_{Luft} \approx 1.46$ n(core) > n(cladding)
Luft: $n_L \approx 1$, Wasser $n_W \approx 1.33$, Glas: $n_G \approx 1.5$

Decibels (dB): unit of level (relative measure): X dB is $10^{-X/10}$

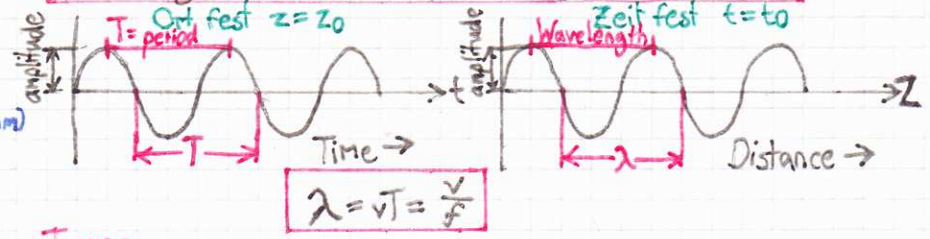
Decibels-milliwatt (dBm): decibel referenced to a milliwatt
dBm used for output power and receive sensitivity (absolute value)
dB used for power gain or loss (relative value)
X mW is $10 \cdot \log_{10}(X)$ in dBm, Y dBm is $10^{Y/10}$ in mW

Wavelength (λ): Length of a wave in a particular medium, Common unit nm = 10^{-9} m

Frequency (f): The number of times a wave is produced within a particular period

Velocity (v): speed of electromagnetic wave

Wavelength • frequency = speed of light ⇒ $\lambda \cdot f = C$

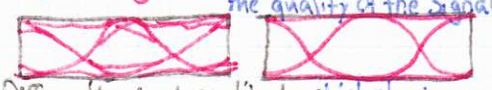


$$\lambda = vT = \frac{v}{f}$$

Typen

Wavelength	Type	Diameter	Refraction	Bit-rate Distance
650nm	Multimode	980/1000 µm (Plastic)	Stufenindex	N/A
850nm		50/125 µm (Glass) or 65/125 µm (Glass)	Gradienten-Index	>500 MHz-km
1300nm				
1550nm	Mono/single Mode	9/125 µm (Glass)	Stufenindex	>100 THz-km

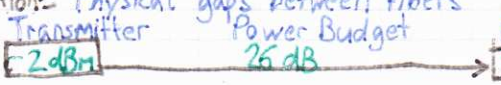
Eye-Diagramm: The wider open the eye is the better the quality of the signal



Differently sized amplitudes: hint at noise or great runtime differences
Horizontal differences (Jitter): can be caused by imprecise clocks

Attenuation: Caused by the following problems:
- Rayleigh Scattering: Scattering of light in the fiber. (due to e.g. impurities)
- Absorption by the fiber material
- Micro-Bend = caused by small distortions of the fiber in manufacturing
- Macro-Bend = caused by wrapping fiber around corners with too small bending radius
- Back reflection = caused by reflections at fiber ends, like conectors
- Fiber splice = caused by poor alignement or dirt
- Mechanical Connection = Physical gaps between fibers

Optical Power Budget = Power Sent - Receiver Sensitivity → Example



Calculate using minimum transmitter power and min. receiver Sensitivity
Attenuation/loss in the link, greater than Power Budget causes bit errors
Allow for two to three dBm power loss in Budget. If Budget = 15 design for 12

Short Reach (SR): 6dB (75% loss) Intermediate Reach (IR): 13dB (95% loss) Long R (LR) 26dB

3 dB difference equal 50% loss

Dispersions

Both CD & PMD

Chromatic Dispersion (CD): Different wavelengths travel at different Speeds, Causes spreading of light pulse
Polarization Mode Dispersion (PMD): Single Mode fiber supports two polarization States, fast and slow axes have different group velocities.

How far can I go without Dispersion Issues: Lower Speeds Travel further

$$\text{Distance} = \frac{\text{Specification of transponder (ps/nm)}}{\text{Coefficient of Dispersion of Fiber (ps/nm*km)}}$$

Calculate Maximal Cable Length:
Optical Power Budget / Attenuation per kilometer

(Reconfigurable) Optical Add Drop Multiplexer (OADM):
Devices built into wire, capable of adding or removing specific frequencies. Allows construction of Ring-Networks

Three R's

Re-Gen: optically amplify signal (e.g with Erbium-doped Fiber Amplifiers (EDFA). Results in up to 30dB gain of Signal And Noise. Hence deploy as early as possible. Optically transparent
Re-Shape: Cromatic Dispersion exists as long as lasers are incapable of sending at one exact wavelength, since the the speed of light is different for different frequencies and media. This spread must be Reversed / Re-shaped before its too high
Done with special Dispersion shifted fiber (DSF)
Dispersion Compensating Fiber (DCF): specially crafted fiber to compensate CD. Directly embedded into the fiber optic cable.
Re-Time: While Re-shape and Re-gen work, it is still necessary to simply read and retransmit signals onto the wire

Wavelength Division Multiplexing (WDM)
WDMs are different Devices capable of joining and splitting different Wavelengths from respectively into different cables
Coarse WDM (CWDM): low cost implementation. Drawbacks: Max 2.5gbps throughput, incapable to amplify (Re-gen), limited to 20 Channels
Dense WDM (DWDM): optimised for bandwidths, supports Re-gen. DWDM operates in the C-Band. 80 channels not uncommon

Eigenschaften Passive Optical Network (PON)
PONuses multi-mode fiber with OADM to reduce number of cables
- Weniger Glasfasser im Feeder nötig - Keine aktiven komponenten beiden Quartierverteilern - (CPE) Customer Premises Equipment werden individuell auf mode konfiguriert - Austausch von allen bei speed änderung - Effizienter für Verteildienste - Günstigere POI kosten - Security issues

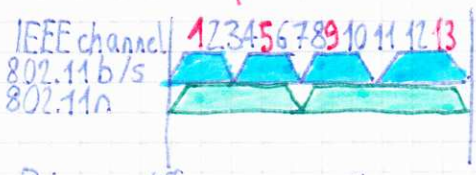
Eigenschaften Point-to-Point (P2P)
Jeder anschluss eigene Fiber → Mehr Glasfasern → Probleme im Feeder
- In den POPs müssen mehr faser gespleist werden und ports bereitgestellt werden - höher Infrastruktur/Bauarbeits-kosten

Fiber to the Curb (FTTC): Fiber ins quatier dann letzte 550m Kupferkabel 100 Mbit/s
Fiber to the Street (FTTS): Fiber bis ans Gebäude letzte 200 m Kupferkabel 500
Fiber to the Building (FTTB): Fiber bis in Keller von Gebäude Steigzone 500
Fiber to the Home (FTTH): Fiber bis zur Steckdose bis zu 1 Gbit/s

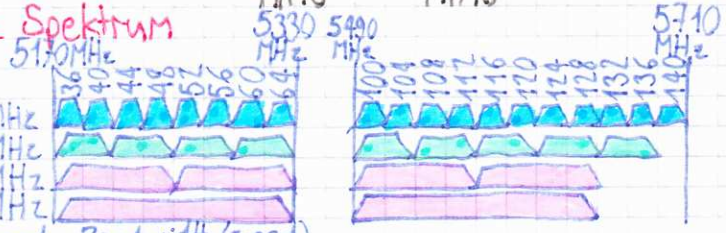
Physical Layer

WLAN	Standard	802.11	802.11b	802.11g	802.11a	802.11n	802.11ac	802.11ad
	Ratifiziert	1993	1999	2003	1999	2009	3013	2013
	Max Data Rate	0.5 Mbps	11 Mbps	54 Mbps	54 Mbps	65-600 Mbps	78-6930 Mbps	6.76 Gbps
	Kanalbreite	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	40/80/160 MHz	2 GHz
	Antenna	1x1 SISO	1x1 SISO	1x1 SISO	1x1 SISO	bis zu 4x4 MIMO	bis zu 8x8 MIMO	1x1 SISO

2.4 GHz Spektrum



5 GHz Spektrum



Primary differences are the range (coverage) and Bandwidth (speed)

2.4 GHz Band has a better range but lower speeds

5 GHz Band provides less coverage but transmits data at faster speeds. The range is lower because higher frequencies cannot penetrate solid objects

Channel Bonding: Combining channels with the goal to optimise throughput. Doubling the Bandwidth → reserving twice the space, limiting the number of collision free coexisting Access Points

Dynamic Frequency Selection (DFS): In 5 GHz some channels are used by weather radars or the military. To prevent interferences only empty channels are selected and if an interference is detected the channel is switched

Multiple in Multiple Out (MIMO)
MIMO uses multiple Spatial Streams (data Streams) on the same frequency to transmit data. With multiple Antennas the streams can be differentiated. Both the Access-Point (AP) and the client need multiple Antennas. This works only if there are enough and not to much Objects in the Room that refract the WLAN-Signal.
Depending on the amount of sending (a) and receiving (b) antennas the name changes according to "a x b MIMO"

Multi-User Multiple in, Multiple out (MU-MIMO)
Because many Clients dont have multiple Antennas with MU-MIMO each antenna of the AP can send a stream for a different Client.

Carrier Sense Multi-Access/Collision Avoidance (CSMA/CA)
Algorithm used to enable reliable communication in a wireless network. Relies on two basic parts: first start a timer for random interval, listen on the medium to determine if occupied. If someone transmitting stop timer until free again, then when timer ran out, send the data. If data simultaneously sent, this is detected if package was not Acknowledged → Reason for ACK on each package.
Backoff Algorithm: chose random time interval and send after.

WLAN-Management Frames

Beacon (Advertisment of AP)
- Sends Capabilities, ESSID, Supported Rates

Probe (Client asks AP)
- Sends Capabilities, ESSID, Supported Rates

Probe Response
- Sends Capabilities, ESSID, Supported Rates
- Same as Beacon without Traffic Indication Map (TIM)

Association Request
- Capability, Listen Interval, ESSID, Sup. Rates

Association Response
- Capability, status Code, Station ID, Supported Rates

Reassociation Request
- Capability, Listen Interval, ESSID, Supported Rates, Current AP Address

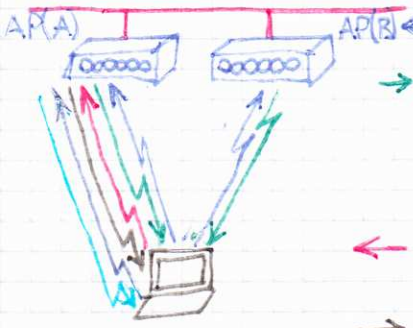
Reassociation Response
- Capability, Listen Interval, ESSID, Station ID, Supported Rates

Disassociation
- Reason Code

Authentication: Algorithm, Sequence, Status, Challenge Text

Deauthentication: Reason

Association Process



Initial Connection to an Access Point

← Client Sends Probe

→ AP Sends Probe Response

Client Evaluates AP Response Selects best AP

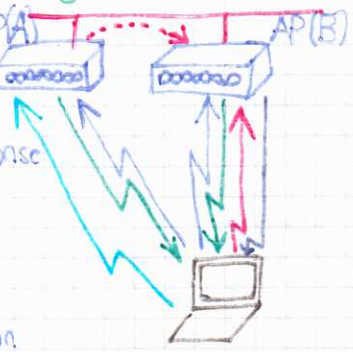
← Client sends Authentication Request to selected AP(A)

→ AP(A) Confirms Authentication and Registers Client

← Client Sends Association Request to Selected AP(A)

→ AP(A) Confirms Association and Registers the Client

Roaming Process



← Station Sends Probe

→ AP Sends Probe Response

Client Evaluates AP Response Selects Best AP (B)

← Client Sends a Reassociation Request

→ AP B Sends a Reassociation Response

← Client Sends a Dissassociation Request to AP(A)

⇢ The old AP send the unacknowledged data to the new one using Inter Access Point Protocoll (802.11f)

WLAN Addition — Physical Layer

Distributed Coordination Function (DCF): Check whether Media Air is free, before WLAN-data can be sent. After the medium is free, a contention window is started, where a station that wants to send can start sending after a random amount of time. Is another term for CSMA/CA

Maximal Ratio Combining (MRC): Signals of different origins overlay each other and they add up. Either signals can get erradicated or enhanced this way. If multiple receiving antennas are equiped this can be used as an advantage

Beamforming: If data is sent by multiple antennas. This can enhance the signal at a certain spot that can be calculated with the help of MRC.

Quadrature amplitude Modulation: is a optimization technique, with which the signal gets transmitted in a sinus curve which can be modulated into a higher bit transmission possibility. Since 802.11 a/g all newer WLAN standards include this feature. Through 64 QAM, there are 2^6 possibilites this means 6 bits can be transmitted with a sinus-wave instead of 1 bit Only works when a good Signal is available. 802.11ac uses 256QAM, 802.11ax upto 1024 QAM

Packet Aggregation: Multiple packets with one header sent, → reduces overhead

Antenna gain: Key performance figure, combines directivity and electrical efficiency

Effective Isotropically radiated power (EIRP): Amount of power a theoretical isotropical Antenna (distributes power in all directions evenly) emits to produce peak power density in direction of maximum antenna gain. EIRP (Real power) = P_T (Power of transmitter dBm) − L_C (cable loss dB) + G_a (Antenna gain dBi)

EIRP Limitations Switzerland:

$$dBm = 10 \cdot \log \frac{\text{power out}}{1\,mW} \qquad X\,mW = 10^{dBm/10}$$

2400 - 2483.5 Mhz Frequency range Max EIRP = 100 mW

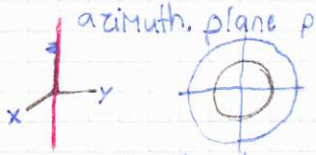
5150 - 5350 Mhz Frequency range Max EIRP = 200 mW

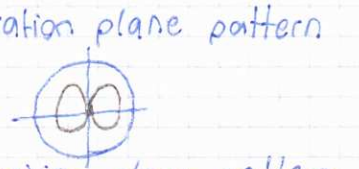
5470 - 5725 Mhz Frequency range Max EIRP = 1000 mW

dBm to mW Table:
- 14 dBm → 25 mW
- 17 dBm → 50 mW
- 20 dBm → 100 mW
- 23 dBm → 200 mW

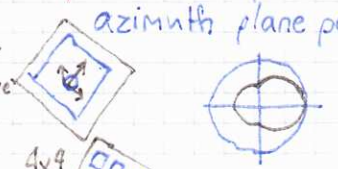
Antenna patterns: Gaphical representation of radiation properties.
Principal plane patterns: Two slices through 3D pattern. Azimuth plane pattern = Horizontal
Elevation plane pattern = Vertical
Lobes: Any part of the patter that sticks out, Main Lobe: Lobe with highest reach. Lobes at the side of the Main Lobe are called Side Lobes / Lobe on opposite side of Main Lobe are Back Lobes

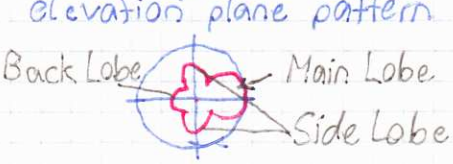
Dipole antenna: two thin wires oriented vertically along the z-axis



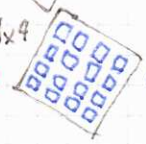


Patch antenna single rectangular or circular conductive plate located above a ground plate



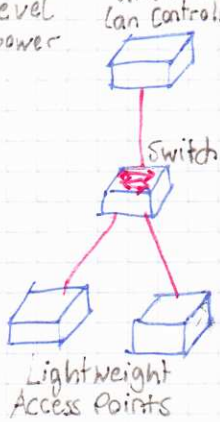


Patch array antenna



Signal to Noise Ratio (SNR): measure used that compares level of desired signal to level of background noise. Ratio of signal to noisepower expressed in dB

WLAN Centralization



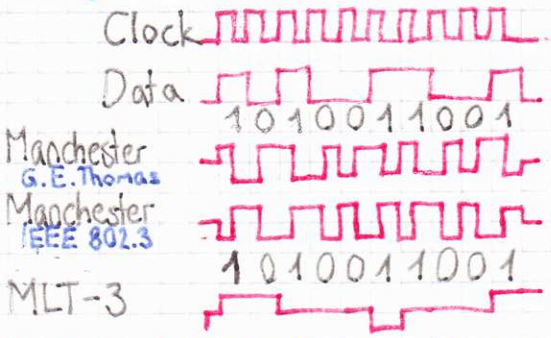
Lightweight Access Point Protocol (LWAPP): communication protocol for communication between Wireless LAN Controller and Lightweight Access Points

Controller MAC Functions
MAC Management: (Re)association requests and action frames; Data encapsulation and transmission to access point; Authentication and key exchange

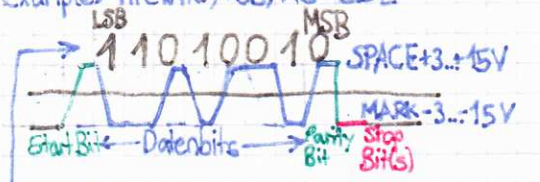
Access Point MAC Functions:
Beacons, probe response (authentication if open)
Control: Packet acknowledgement and transmission
Queuing and packet prioritization
Encryption in access point

Physical Layer

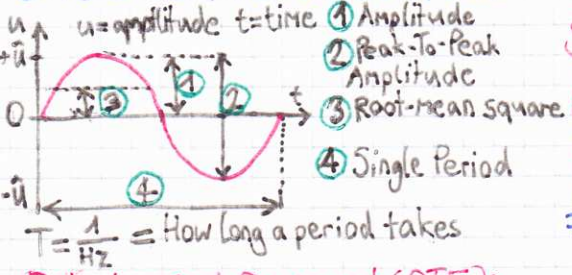
Signale



Serial ports: Serial = 1 bit at a time transmitted
Examples: FireWire, USB, RS-232



RS-323 Sequenz
0 1 0 0 1 0 1 1 b → 0x4B → "K" Ascii



1. Amplitude
2. Peak-To-Peak Amplitude
3. Root-mean square
4. Single Period

Data terminal Equipment (DTE):
either dumb terminal or Serial port
Data Communications Equipment (DCE):
Modem, DSU/CSU

Manchester: Developed for 10Base-T, now used for RFID & NFC
The clock rate is embedded into the Signal → Self clocking Signal

In IEEE 802.3 **1** is defined by a voltage shift from low to high
0 are a voltage shift from high to low.
Multiple successive 1/0 require the signal to shift from high/low to low/high for each bit

Higher Data-Rates than 10 Mbit/s are difficult to achieve → Frequency related Problem

Multi-Level Trasmission with 3 levels (MLT 3): The 100Base-TX standard defines a lookup-table which maps 4bit Data to 5 bits for transmission (4B5B)
This ensures enough transitions occur to enable a self-clocking Signal.
3 instead of two Voltage levels. Every 1 changes the level. NO DATA → Idle Symbols 11111

Start bit: The Initial state on the line is on MARK. A level change to SPACE indicates the start of a transmission
Framing bits: Signs framed in between start and stop bit. → The transmission Data
Parity bit: Optional bit. Used to detect failures. **Odd Parity bit** → Parity bit is set to 0 or 1 to ensure the total amout of ones is uneven. **Even Parity bit** → Ensures even total of 1
Stop bit: Marks the end of a sign. At least 1. can be 1,5 or 2 aswell

Signal Bandwidth: Range where the frequency portions lie. Difference $\frac{\text{Highest Freq.}}{\text{Lowest Freq.}}$

Sampling: Used to digitalize Signalwave. **Sampling Frequency (Abtastrate)** ⇒ Rate in der gesamplet wird. $1/Ts = fs$ / Ts = time between samples
Quantication: Number of different States / bit possibilities. Level described with a bit value of n-Bits. Amount of bits defines amount of Levels $N = 2^n$
High- and Low-pass filters: Allow removal of signal Frequencies. Software / Hardware
If a signal gets filtered Freq. under/over certain Threshold get attenuated.
From 3dB beyond the filter is the **Cut-off Freq.** and the Rate it gets attenuated → **Roll-off Rate**

Standards Overview

Physical Layer

Name	10BaseT (thin)	10Base5 (thick)	10BaseT	100BaseT	1000BaseT
Cable	Coaxial	Coaxial	Twisted	Twisted	Twisted
Data Rate	10 Mbit/s	10 Mbit/s	10 Mbit/s	100 Mbit/s	1 Gbit/s
Reach	185 m	500 m			
Duplex	Half	Half	Full	Full	Full
Encoding		Manchester		MLT-3 4B5B	PAM5 8B1B
Propagation Speed	0.65*c	0.67*c	0.59*c	0.59*c	

Max Transmittable Unit (MTU)
Ethernet limits the MAC size to 1500 B
MAC PDU ⇒ 1500 + 14 B header + 4 B trailer = 1518 B
In GBit SDU can be 9000 B MTU max.

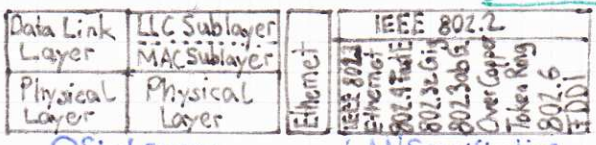
Auto Negotiation
used to find parameters for twisted pair Cables (speed, duplex, mode, etc) Implemented with Fast Link Pulse Bursts (FLP-Bursts)

Duplex Mismatch: if ends at cable are in different modes full-half or full-auto ⇒ low throughput, collisions, FCS errors

Carrier Sense Multi-Access with Collision Detection (CSMA/CD)
1. A jam signal informs all devices that a collision occured
2. The collision invokes a random backoff algorithm
3. Each device on the Ethernet segment stops transmitting for a short time until timers expire
4. All hosts have equal priority to transmit after the timers have expired

Twisted Pair Cables Router >< Host = Switch >< S = R >< H >< H

Data Link Layer



OSI-Layers LAN Specification

Logical Link Control (LLC): The LLC Sublayer IEEE 802.2 handles communication between the Network-layer and MAC-Sublayer, provides way to identify passed protocol. Takes network protocol data (e.g. IPv4 Packet) and adds control information to help deliver the packet. The LLC can be considered as the Driver Software for the Network Interface Card (NIC)

Media Access Control (MAC): MAC-Sublayer has two primary responsibilities implemented in the NIC. Communicates with physical components which send the information and prepare the Data for the transmission over the medium.
Data Encapsulation: frame assembly before transmission & frame parsing after the reception
- **Frame delimiting:** Preamble consists of a 7 Byte long 10101010 series which is used for bit synchronization Start Frame Delimiter (SFD) sequence is 10101011 and signals the beginning of a frame (transmitted MSB-first)
- **Addressing:** Each Ethernet-Header contains a MAC adr.
- **Error Detection:** Each Ethernet frame contains a Frame Check Sequence (FCS) in the trailer. After reception the Receiver creates a Cyclic Redundancy Check (CRC) and compares it with the FCS. Match ⇒ no error occurred

MAC: Controls the placement & removal of frames on media
- **Interframe Gap (IFG):** Is a break of 12 Bytes where nothing is transmitted

Ethernet II (DIX) Frame

MAC size 64 ... 1518 Bytes

IFG	Preamble	SFD	DA	SA	Type	Data (MAC SDU, MTU)	FCS	IFG
>=12B	7B	1B	6B	6B	2B	0(+46B padding) 1500B	4B	>=12B

Type: IPv4 = 0x8000; IPv6 = 0x86DD; ARP = 0x0806

Ethernet 802.3 Frame:

Length 2B	LLC 802.2	LLC SDU

Ethernet II (DIX) vs. IEEE 802.3: DIX uses Type to communicate the SDUs type. 802.3 encodes payload length. To differentiate the two from each other the actual number in the length field must be considered. If it's below the MTU value of 1500 its a 802.3 Frame otherwise a Ethernet II Frame

MAC-Address: Identifies devices in the Network. It is also known as Hardware-Address or Physical-Address and is generally programmed in the controller-board hardware

Common OUIs:
00 00 0C = Cisco Systems Inc.

Organizationally Unique Identifier (OUI)	Vendor Assigned (NIC, Interfaces)
24 Bits	24 Bits
6 Hex Digits	6 Hex Digits
00 60 2F	34 07 BC

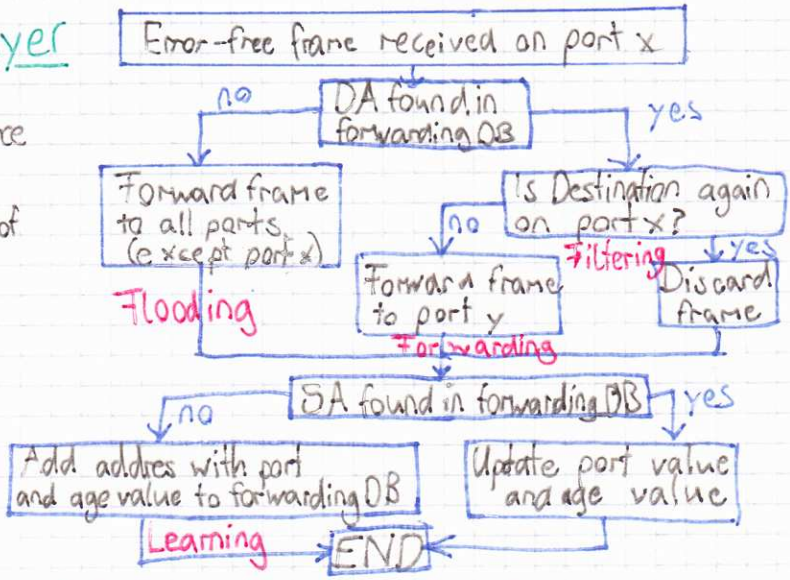
Format MAC:
Length: 48 bit (6 Byte)
Hex Notation: xx-xx-xx-xx-xx-xx oder mit (:) anstatt (-)
Two Parts (3 Byte each
- OUI uniquely identify vendor, manufacturer, ORG
- NIC specific part

Individual address bits have special meaning:
- **Individual / Group (I/G) Bit:** The first transmitted bit (LSB of first octet) is the Unicast/Multicast bit
- **Universally / Locally Administered Address (U/L) Bit:** The bit which is transmitted in the second place LSB. Globally Administered Addr. include a OUI in the first 3 bytes whereas Locally Administered Addr. can be managed by the Admin

Data Link Layer

Switching/Bridging states

Learn: Layer 2 switches & Bridges remember the source MAC-Address of each Frame received
Flood: If the switch does not contain the destination MAC-Addr. in its MAC-Table the frame gets flooded out of every interface, but the one it was received on.
Filter: If a switch receives a frame with the destination mapped to the interface that he received the frame on, he discards the frame.
Forward: If the switch knows the destination MAC address he forwards the frame out of the respective interface



Types

Cut-Through Switching/Fast-Forward: As soon as the MAC-Destination Address is read, the switch starts forwarding
Store-and-Forward: Whole frame gets received, buffered and forwarded only after the whole frame was received
MAC-table: Used by the Switch to map MAC-addresses to a specific interface on the switch. Usually expires after 5min Are updated by reading the Source Address of received frames
ARP-Table: Used to map MAC-address to IP-address If no ARP-entry exists an ARP broadcast is sent out and the table is updated with the response. Usually expire after 2-4h Each Host connected to the Network should maintain its own ARP-Table

Address Resolution Protocol (ARP):

Is used to map addr. to data link layer addr. Most common method for ARP is to resolve IPv4 addresses to MAC-adresses (Bcast)
Process: Acts on data link layer, has two functions: Resolving IPv4 to MAC-addresses, maintaining a cache of Mappings
Destination outside the network: Since ARP works with broadcast Messages it can only work within the same LAN/ Broadcast domain. For this purpose, the sender XORs the IP-address with the subnet mask and can find out whether the IP is in the same LAN. If not the Datagram is sent to the Default Gate-Way (GW).

ARP-Types

Reversed ARP (RARP): Protocol was used by a client to request an IPv4-address from the GWs ARP-Table. Protocol was replaced by Dynamic Host Configuration Protocol (DHCP) and Bootstrap (BOOTP)
Inverse ARP (InARP): Instead of using IP-addr. to find the MAC-address, Inverse ARP uses the MAC-address to find an IP-adress.
Proxy ARP: Was implemented to enable devices which are separated into network segments connected by a router in the same IP-Network or sub-Network to resolve IP-adresses to MAC-Adresses
Gratious ARP: When a computer boots up for the first time it automatically Broadcasts its MAC-Address to the entire Network. That is the reason why Broadcast-storms can happen when multiple devices boot up.

Port-Aggregation with Etherchannel:

If a network has multiple parallel Links between two switches/Routers, STP would block all the links except one. To prevent this, Etherchannel can bundle multiple (2-8) interfaces into one Logical Interface

Link Aggregation Protocol (LACP) IEEE 802.3ad:

LACP packets are exchanged between switches over EtherChannel capable ports. LACP can be configured in Active mode (Actively trying to establish EtherChannel) or Passive mode (negotiating EtherChannel if the other side is active)
16 potential Links can be defined but only 8 can be active at a given time and the rest are failover connections.

Load Balancing

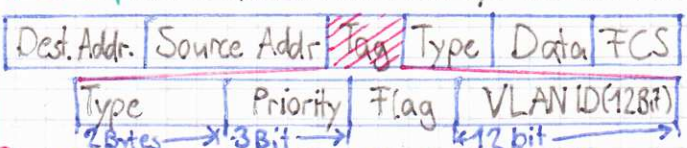
A hash algorithm computes a binary pattern that selects a link number in the bundle to carry each frame. This way the load gets spread over all links, but not necessarily equally.

Possible Load Balancing Criteria:
- dst-ip Destination IP Address
- dst-mac Destination MAC Address
- src-dst-ip Source XOR Destination IP Address
- src-dst-mac Source XOR Destination MAC-Address
- src-ip Source IP Address
- src-mac Source MAC Address

Port-based Load balancing: possible if TCP/UDP port-based load balancing is supported

VLAN

4 Byte Tag: VLANs get identified by a 4 Byte tag that is added within the Layer 2 Ethernet Frame



Type: Specifies the type (for 802.1Q value = 0x8100)
Priority: Class of service functions **VLAN ID:** Source VLAN of the frame

VLAN: Is a Bcast/STP-domain. Used to create multiple Bcast Domains Reduces complexity, increases Security. Without VLAN different Network would have to be created physically. VLAN 0, 1, 4095 Reserved
Inter VLAN Routing: Devices of different VLANs cannot communicate unless they are routed, since they are technically in another Network. (Option: trunk between switch & router = router-on-a-stick)
Per VLAN STP (PVSTP): Individual separate instances of STP running on different VLANS and can be configured independently. Each BPDU contains VLAN ID written into last 12 bits of the priority field. Only the left 4 bits can be used to prioritize them.
Unique Bridge ID for VLAN in PVST (extended system ID + STP MAC + switch priority)

Trunk IEEE 802.1Q: Communication between 2 switches with the same VLANs require a physical Link for each VLAN that wants to communicate over the switches. To also virtualize this, trunking was created. With Trunking multiple VLANs can communicate over the same Logical interface
Native VLAN: VLAN that remains untagged on a trunk to allow older Switches, that don't support VLAN or trunking to remain functioning. Default number is 1. Cannot be changed on cisco devices.
Default VLAN: VLAN to which all Access Ports are assigned to until they are explicitly placed in another VLAN.
Default VLAN ID on cisco is 1 and cannot be changed

Data Link Layer

Spanning Tree Protocol (STP) IEEE 802.1D

Eliminates loops by blocking ports

Bridge Protocol Data Units (BPDU)

Destination MAC: 01:80:c2:00:00:00 (Multicast)

Hello/Config BPDU: Sent by the rootbridge. In the Interval of the Hello-Timer

Topology Change Notification (TCN) BPDU:

- Announces Changes in the network
- A switch sends a TCN back to the root
  - Expiration of the max age timer
  - Addition or removal of a switch
  - Links going up/down
  - Receipt of new information via a BPDU
- If the root bridge receives a TCN it next Config BPDU has the Topology Change Flag set. This causes all other bridges to shorten their Bridge Table Aging times from the default (300s) to the Forward Delay value (default 15s)

Elements:

Root-Bridge: The Root Switch gets elected after the criteria Lowest bridge ID (Priority Nr + MAC Addr)

Root Port: Per switch that is a non-root bridge, there is one segment that is the root-port. Indicates fastest way to Root

Designated Port: is the port that has the lowest path Cost on a particular LAN segment. Each segment has exactly one single port that is used to reach the Root Bridge

Non-Designated Port: All left over ports in the network are non-designated and go into Blocking state. Prevents Loops

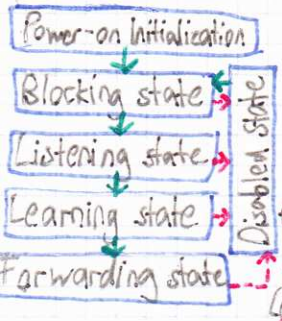
Election Process

The comparison algorithm will define:

- The Root bridge
- The root ports
- The designated ports

All ports that are neither root ports nor designated ports are blocked. The comparison algorithm has the following Criteria:

1. Lowest bridge ID (Default Priority 32768)
2. Lowest root path cost
3. Lowest sender bridge ID
4. Lowest sender port ID



States: In any state but "Disabled" BPDUs get forwarded to the system Module of a Switch

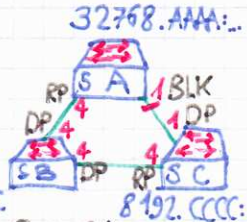
Blocking: Interface does not forward frames

Listening: First state. Until Forward-delay expires

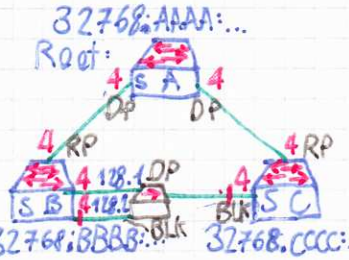
Learning: Port still blocks frame forwarding but is now learning the end-station-location for the forwarding-DB. Awaits till Forward-delay expires again.

Forwarding: Ports in this state, have both Learning and frame forwarding enabled

Disabled: Does not receive anything.



3rd. Criteria decided because 2nd was equal for both. Bridge ID of Switch C was lower



3rd and 4th Criteria decided Same advertised cost=4 Switch with lower BID=Switch B 128.1 has lower Port ID → is designated port rest blocking

Timers

Hello Timer (2s): Specifies the Interval in which the Root Bridge broadcasts Hello messages to switches

Forward-Delay Timer (15s): Determines how long the Listening and Learning states last

Maximum-Age Timer (20s): Is the numer of seconds a switch has to wait before attempting a reconfiguration when not receiving Hello-messages

Topology Changes

Direct Topology Changes:

Is when a link goes from up to down. The Blocking port in the network then needs to receive the TCN before changing its state.

Listening and Learning states

2x forward delay period (15 seconds) = 30seconds

Indirect Topology Changes:

Is when a link only partially breaks and data gets filtered

The switch that lost its connection realices the loss of connectivity only after the Max Age timer ran out. (20 seconds), the next Hello-message was received (BPDU) (2seconds) and the time spent in the Listening (15seconds) and the Learning (15 seconds) states = 52s

Insignificant Topology Changes:

If Clients are attached to the network that boot up and shutdow regularly the STP Portfast feature can be enabled. This means, that the port is brought right into Forwarding state, when the link comes up.

STP Costs:

Ethernet (10 Mbps): 100
Fast Ethernet (100Mbps): 19
Gigabit Ethernet (1000Mbps): 4

Network-Layer

IPv4

Network Adress Translation (NAT): Used to translate private IP addr. to global allowing for specific IP addr. to be reused (priv. Network) NAT runs on a device connected to two networks usually an internal network connected by a router to the internet
Static NAT: Mapping unregistered (private) IP addr. to a registered on a static one-to-one basis. Useful when device needs to be accessible from outside the network.
Dynamic NAT: Maps unregistered IP to registered IP from a group of registered IPs dynamically, meaning that public IP of device can change.
Overloading NAT, PAT (Port & Address Translation): form of Dynamic NAT that maps Multiple private IPs to a single public IP by using different Ports. Also known as PAT. A packet from a host leaves the network with the public IP of the router and a dynamically assigned Port Nr. Router holds Record of mappings in NAT-Table. When Receiving a packet the mapping is reversed.
Overlapping NAT: Used if two hosts share the same IP address. Maintains a Lookup Table of duplicate addresses. Intercepts traffic and replaces these IPs with a unique registered IP
Inside Local, outside Local, inside Global, outside Global

IPv4

Classful Unicast Networks:

Class	Address	Subnet	Range	
A	0.0.0.0	/8	10.0.0.0/8 - 10.255.255.255/8	1 Class A
B	128.0.0.0	/16	172.16.0.0/12 - 172.31.255.255/12	16 Class B
C	192.0.0.0	/24	192.168.0.0 - 192.168.255.255	256 Class C
D (multicast)	224.0.0.0	N/A	Not routed; implemented because of IPv4	
E (reserved)	240.0.0.0	N/A	Addr. shortage. Need to be replaced by public	

Private Networks (RFC 1918)

Special Reserved Addresses:
127.0.0.1/8 - Loopback, Class A, Address for communicatin with one-self
169.254.0.0/16 - Link local addr., Class B, Broadcast Domain wide network

IPv4 Header: Fields:

Version: decimal value 4 = 0100b; **IHL:** Internet Header Length, tells Length of header in 4 Byte increments; Min 20 Bytes, at least 5 (5·4)=20, max 15 → max 60 Bytes (15·4=60). **Type of service:** DS field (Differentiated Services), used for Quality of Service (QoS), defines packet priority; **Total Length:** Entire size of packet (header + data) in Bytes, min 20B max 65535B; **Identification:** contains fragmentation ID, shows to which packet the fragment belongs to; **Flags:** First bit always 0, Second bit called 'Dont fragment' bit if set, packet sent without fragmenting it, can be rejected because of this. **Fragment Offset:** Specifies Byte position of the fragmentation, 65528 (2^13-1); **TTL:** when packet passes through router TTL is decremented by 1; if TTL reaches 0, packet gets dropped; **Protocol:** Contains a value which stands for the used transportation Protocol (Most common: UDP, TCP, OSPF, ICMP); **Options:** used for network testing, debugging, security ect. field is usually empty; **Padding:** Because the Options field is variable in size the padding field is used to bring the Header to multiple of 32 bits.

Version	IHL	Type of Service	Total Length
Identification		Flags	Fragment Offset
Time to Live	Protocol	Header Checksum	
Source Address			
Destination Address			
Options ←|→ Padding			

IPv6

IPv6 Header: Fields:

Version: 4 bit inter Protocol version nr=6; **Traffic Class:** 8 bit traffic Class. Differentiated Services (Quality of Service QoS) comparable to TOS in IPv4. **Flow Label:** 20 bit, Each source chooses its own flow label values; routers use Source Address and Flow Label to identify flows. Flow label value = 0 = no special QoS is requested (common case today). **Payload Length:** 16 bit unsigned integer. Rest of the packet following IPv6 header in octets, but without 40 Byte header in calculation comparable to Total Length in IPv4; Max Payload 64 Kbytes; **Next header:** 8 bit selector: identifies type of header immediately following the IPv6 Header. comparable to Protocol field in IPv4 and uses the same values as the IPv4 Protocol field [RFC 1700] is either is either the Upper Layer (TCP/UDP layer 4) or the Extension Header **Hop Limit:** 8 bit unsigned integer. Decides Lifetime of package. If TTL=0, ICMP Packet is sent to sender. comparable to TTL in IPv4. **Source Addr:** 128 bit of originator of the packet. **Destination Addr:** 128 bit Addr. of the intended recipient of packet. (possibly not the ultimate recipient if a routing header is present.) **Extension Headers:** 0: Hop-by-Hop option; 43: Routing, 44: Fragment, 50: Encapsulating Security Payload, 51: Authentication Header (AH), 59: no next Header, 60: Destination option, 62: Mobility Header. Extension headers important for the router come at the beginning

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

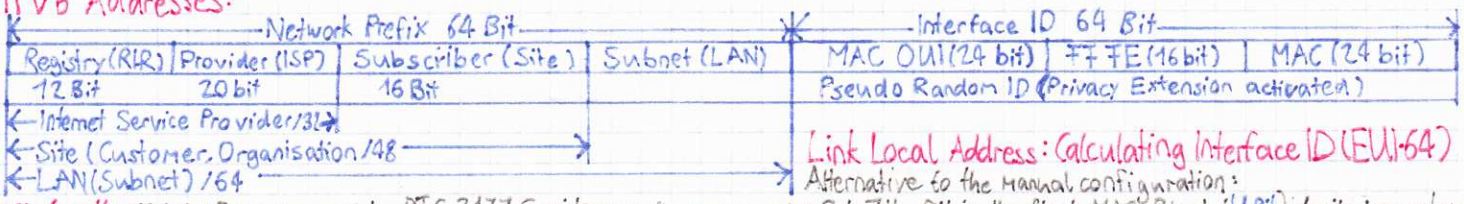
IPv6 Changes:

- 40 Bytes IPv6 Header. Bigger than IPv4 Header (20-60 Bytes). But strongly simplified on the contrary to the IPv4 Header
- Enhancement of the Addr. range from IPv4 with 2^32 (4,3·10^9) to IPv6 with 2^128 (3.4·10^38) adresses. Grow with the factor 2^96
- Address: 8 Blocks with 4 Hexadecimal digits. Each block is 16 Bit. Total of 128 bit
- Simplification of the header information, this decreases the burden on the router
  - → Removed Fields: Fragment Offset (Segmentation was removed), Header Checksum (Layer 3 Errors nearly impossible), Traffic Class instead of Type of Service, Next Header Field instead of Protocol Field (Specifies which protocol is used on higher Layer)
- Segmentation was removed. Only possible with extension headers. Oversized MTUs get Discarded and Error Message is sent
- Stateless automatic configuration of IPv6 Addresses. In many cases DHCP is obsolete
- Usage for mobile Devices easier (Mobile IP)
- Encryption and Authentication check built in. (Implementation of IPSec as a part of IPv6)
- Support of Quality of Service and Multicast
- No NAT needed anymore because there are more than enough IP addresses

Mechanism to prevent fragmentation: MTU Path Discovery

IPv6 — Network Layer

IPv6 Addresses:

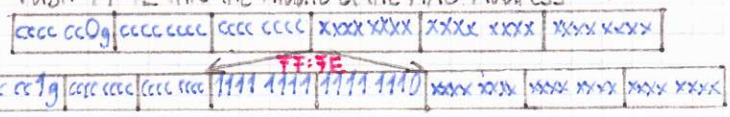


Prefix length: 64 bits: Recommended by RFC 3177. Consistency makes management easy. Must for SLAAC/MSFT DHCPv6; More than 64 bits: Enables more host per broadcast domain. Considered bad Practice. 64 bits offers more space for hosts than the media can support efficiently.; Less than 64 bits: Address space conservation. Special Cases: /126 /127 valid for p2p (RFC6164) /128 loopback complicates Address Management

Link Local Address: Calculating Interface ID (EUI-64)

Alternative to the manual configuration:

- Set 7th Bit in the first MAC-Block (U/L Bit): to its inverted value
- Push FF:FE into the middle of the MAC-Address



Address-types: IPv6 Interfaces have multiple IP addresses — 1 or many global Unicast Adresses and 1 link Local Address.

Unicast:

Link-local:	FE80::/10	Inside of closed Network, don't get routed, Pendant to MAC-Address, For Next Hop-Calculation in routing, Cannot Communicate with Internet
Unique local:	FC00::/7-FDFF/7	Only in local network, Only within 1 Routing Domain Routed
Loopback	::1/128	
Global Unicast:	2000::/3	Assigned by IANA e.g. for ARIN, RIPE; Components in Graphic above; Host-Address Assigned with EUI64, Pseudo Random, DHCP, Manually; Configuration: EUI64, SLAAC + DHCP for e.g. DNS) Stateful Autoconfig or DHCP

IPv4 Pendant
169.254.0.0/16
private/local Adresses RFC 1918
Loopback address 127.0.0.1
Public IPv4 Address

Multicast: FF00::/8

Addressing of all Interfaces that belong to a Multicast group. Assigned by IANA. First 32 bit relevant. The FF-Prefix follow 4 bits for Flags and 4 bits for the Scope: Node local (1), Link Local (2), Site Local (5), Organisation local (8), Global (8)

Node local	FF01:	Packet never leave Interface, Loopback
Link Local	FF02:	Don't get Routed
	FF02::1	All nodes/hosts on a segment
	FF02::2	All routers on a segment
FF02::5 /	FF02::6	OSPFv3
	FF02::9	RIP (v2)
	FF02::A	EIGRP
	FF02::D	All Protocol-Independent-Multicast (PIM) routers
	FF02::1:2	DHCP Relay Agents / DHCP-Server

Subnet Broadcast-Address
Not existing
224.0.0.5, 224.0.0.6
224.0.0.9

No Multicast Address

Solicited-Node Multicast

FF02::1:FF... (... lowest 24 bits of Link local Adr.)

For each configurated Unicast and Multicast address a repeating Solicited-Node-Multicast Address exists. Is a Multicast Address that is on a IPv6 Address of a interface. Usage: Replacement of ARP, Duplicate Address Detection (DAD), Neighbor Detection Protocol (NDP)
Composed of Prefix + lower 24 bits from Unicast Link Local Adr.
Example: Link Local is FE80::200:CFF:AA3A:8B18 → Solicited-Node Multicast is FF02::1:FF3A:8B18
An IPv6 Multicast FF02 gets converted to 33:33

Anycast:

Address that can be assigned to more than one interface..
Multiple Devices can have the same Anycast Address.
Usage: Load Balancing, DNS Rootserver, Content Delivery Network

Special:

2002::	Adresses for 6to4 Tunneling mechanisms
2001:db8::/32	For documentation
::	Unspecified, used as a placeholder

Protocols ICMPv6 and Neighbor-Discovery-Protocol:

Neighbor Discovery: Nodes can find their respective neighbors; Finding out Link-Layer-Address of neighbors; Finding Routers; Maintaining Neighbor Reachability Information (NUD) **Router Discovery:** With Router Discovery the default GW can be found
Replacement of ARP

ICMP Package Groups: Group 1: (Messages between Router and IPv6 Devices): ICMP Type Field 133 = Router Solicitation (RS) Host requests advertisements by sending an RS to all-Router Multicast Address FF02:2. Sent automatically when station starts up.
ICMP Type Field 134 = Router Advertisements (RA): Routers advertise themselves in the network and send information for IP-Autoconfiguration. Routers periodically send these packages to the All-Nodes Multicast Address FF02:1.
Group 2: (Messages between IPv6-Devices): ICMP Type Field 135 = Neighbor Solicitation (NS): Host searches for all Neighboring Hosts and their MAC-Address by sending a packet to the All-nodes Multicast Address FF02:1. In IPv4 the Broadcast address was used. Can also be used to discover Duplicate Address with Duplicate Address Detection (DAD)
ICMP Type Field 136 = Neighbor Solicitation Advertisement (NSA): Is the response to the NS and contains MAC Addr. of the Host.
Group 3: (Redirects): Redirect: Is used to see whether the packets could have a better first Hop. Can occur if there are multiple routers in the network.

Subnetting

IP/CIDR	Borrowed Host B.I.	Decimal Mask	Binary Notation	Add for BCast	Add for Subnet ID	Host Values -2 for Valid
/32	8	255.255.255.255	. . . 1111'1111	+ 0. 0. 0. 0	+ 0. 0. 0. 1.	1
/31	7	" . " . " .254	. . . 1111'1110	+ 0. 0. 0. 1	+ 0. 0. 0. 2.	2
/30	6	" . " . " .252	. . . 1111'1100	+ 0. 0. 0. 3	+ 0. 0. 0. 4.	4
/29	5	" . " . " .248	. . . 1111'1000	+ 0. 0. 0. 7	+ 0. 0. 0. 8.	8
/28	4	" . " . " .240	. . . 1111'0000	+ 0. 0. 0. 15	+ 0. 0. 0. 16.	16
/27	3	" . " . " .224	. . . 1110'0000	+ 0. 0. 0. 31	+ 0. 0. 0. 32.	32
/26	2	" . " . " .192	. . . 1100'0000	+ 0. 0. 0. 63	+ 0. 0. 0. 64.	64
/25	1	" . " . " .128	. . . 1000'0000	+ 0. 0. 0. 127	+ 0. 0. 0. 128.	128
/24	0	255.255.255. 0	. . . 1111'1111.0	+ 0. 0. 0. 255	+ 0. 0. 0. 0.	256
/23	7	" . " .254. 0	. . . 1111'1110.0	+ 0. 0. 1. 255	+ 0. 0. 1. 0.	512
/22	6	" . " .252. 0	. . . 1111'1100.0	+ 0. 0. 3. 255	+ 0. 0. 0. 0.	1'024
/21	5	" . " .248. 0	. . . 1111'1000.0	+ 0. 0. 7. 255	+ 0. 0. 8. 0.	2'048
/20	4	" . " .240. 0	. . . 1111'0000.0	+ 0. 0. 15. 255	+ 0. 0. 0. 0.	4'096
/19	3	" . " .224. 0	. . . 1110'0000.0	+ 0. 0. 31. 255	+ 0. 0. 32. 0.	8'192
/18	2	" . " .192. 0	. . . 1100'0000.0	+ 0. 0. 63. 255	+ 0. 0. 0. 0.	16'384
/17	1	" . " .128. 0	. . . 1000'0000.0	+ 0. 0. 127. 255	+ 0. 0. 128. 0.	32'768
/16	0	255.255. 0. 0	. . . 1111'1111.0.0	+ 0. 0. 255. 255	+ 0. 1. 0. 0.	65'536
/15	7	" .254. 0. 0	. . . 1111'1110.0.0	+ 0. 1. 255. 255	+ 0. 2. 0. 0.	131'072
/14	6	" .252. 0. 0	. . . 1111'1100.0.0	+ 0. 3. 255. 255	+ 0. 4. 0. 0.	262'144
/13	5	" .248. 0. 0	. . . 1111'1000.0.0	+ 0. 7. 255. 255	+ 0. 8. 0. 0.	524'288
/12	4	" .240. 0. 0	. . . 1111'0000.0.0	+ 0. 15. 255. 255	+ 0. 16. 0. 0.	1'048'576
/11	3	" .224. 0. 0	. . . 1110'0000.0.0	+ 0. 31. 255. 255	+ 0. 32. 0. 0.	2'097'152
/10	2	" .192. 0. 0	. . . 1100'0000.0.0	+ 0. 63. 255. 255	+ 0. 64. 0. 0.	4'194'304
/ 9	1	" .128. 0. 0	. . . 1000'0000.0.0	+ 0. 127. 255. 255	+ 0. 128. 0. 0.	8'388'608
/ 8	0	255. 0. 0. 0	1111'1111.0.0.0	+ 0. 255. 255. 255	+ 1. 0. 0. 0.	16'777'216
/ 7	7	254. 0. 0. 0	1111'1110.0.0.0	+ 1. 255. 255. 255	+ 2. 0. 0. 0.	33'554'432
/ 6	6	252. 0. 0. 0	1111'1100.0.0.0	+ 3. 255. 255. 255	+ 4. 0. 0. 0.	67'108'864
/ 5	5	248. 0. 0. 0	1111'1000.0.0.0	+ 7. 255. 255. 255	+ 8. 0. 0. 0.	134'217'728
/ 4	4	240. 0. 0. 0	1111'0000.0.0.0	+ 15. 255. 255. 255	+ 16. 0. 0. 0.	268'435'456
/ 3	3	224. 0. 0. 0	1110'0000.0.0.0	+ 31. 255. 255. 255	+ 32. 0. 0. 0.	536'870'912
/ 2	2	192. 0. 0. 0	1100'0000.0.0.0	+ 63. 255. 255. 255	+ 64. 0. 0. 0.	1'073'741'824
/ 1	1	128. 0. 0. 0	1000'0000.0.0.0	+127. 255. 255. 255	+128. 0. 0. 0.	2'147'483'648
/ 0	0	0. 0. 0. 0	0000'0000.0.0.0	+ N/A	+ N/A	4'294'967'296

c

b

a

Network-Layer

Routing

Host/PC requires: IP-Address, Subnet Mask, Default Gateway (GW)
Router Main Functions: forwards from inbound to outbound interface, learns the surrounding network topology and memorizes it via Routing Table
Forwarding Functions: Routing table association of Destination Address with the outbound Interface and therefore the next-hop Device
Routing Protocol Types: Purpose (IGP, EGP), Operations (Distance Vector Protocol, Link State Protocol, Path Vector Protocol), Behaviour (Classful or Classless)
Routing-Algorithm-Tasks: Delivery & reception of availability information, determining optimal path using availability info, recalculating routing table after Network changes in the lowest cost path to any destination and readvertising the updated info; Router will always choose the most specific route with more subnetmask-bits set.

Routing Table:

```
I 172.16.8.0 [100/118654] via 172.16.7.9, 00:00:23, Serial0
```

I	How route was learned (IGRP)
172.16.8.0	Destination logical network or subnet
[100	Administrative Distance (trustworthyness factor)
/118654]	Metric value (Reachability)
via 172..9	Next-hop logical address (next Router)
00:00:23	Age of entry (in hours:minutes:seconds)
Serial 0	Interface through which route was learned and through which the packet will leave

Possibly Included Info: Host address, Subnet, subnet-group, Major Network Nr. (A,B,C), Supernet, Default addr. 0.0.0.0

Dynamic Routing

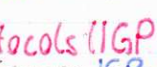
Routing tables are periodically updated with infos from other routers, is done by routing protocols.
Targets of dynamic routing: Discovery of current and removed networks, first updating neighboring topology then sending information to neighbors; Choosing lowest path cost to each network (using metrics); keeping the routing table up-to date; rechoosing lowest path cost after current one has gone down;
Protocol Types: Link state (OSPF, IS-IS), Distance Vector (RIPv1/2, IGRP, EIGRP), Path Vector (BGP)
Routing Protocol: Discovers current network topology at low maintenance labor costs; Determines the best path to every reachable network using metric infos; Stores information about best paths in the routing table; Decides on content, format, recipients and frequency of updates
Metric Information: Preconfigured values like 'hop-count', costs, bandwidth, delay, etc.

Classful Updates: Used by classful routing protocols (RIPv1). Does NOT send subnet mask along with updates
Example:
172.16.2.0/24; 172.16.0.0/24 → 172.is Class B network (/16 SM)
→ Update will be shortened to → 172.16.0.0
⊖ Lacks preasion and causes problems, therefore OUTDATED

Classless Updates: Used by classless routing protocols (e.g. OSPF, RIPv2). DOES send subnet mask along with updates. Classless Updates are NOT summarized. For every network there will be one entry advertised.

Routing Structure/Hierarchy:
Autonomous Systems (AS): Group of routers under a common administrative domain. IGPs discover paths beetween networks, EGPs discover paths between autonomous systems.
Interior Routing Protocols (IGP):
Are used inside AS. Common IGPs are: RIP, RIPv2, IGRP, EIGRP, IS-IS, OSPF, etc.
Exterior Routing Protocols (EGP):
Are used between AS. Common is Border Gateway Protocol (BGP)

Process Link failure (direct)



A-F are Routers. What happens when link C goes down
RIP: C awaits hold down timer (~120s) sends info with next update (~30s) to B & D until F. F knows it after over >600s, worst case
OSPF: C sends LSA directly to B & D, and calculates new topology, B & D send LSA directly to A & E and so on until they reach F, F uses SPF Algorithm and sends packets accordingly. takes > 1-12 seconds

Network-Layer

Static-Routing

Directly connected routes: Routes coming from directly connected interfaces with configured IP adresses
Remote Routes: Routes coming from remote networks connected to other routers. config manually or learned through a dynamic routing protocol

IP-Route command: Command on Cisco Internetwork Operating System (IOS) to configure static routes.
Directly connected routes:
ip route [destination Network Address] [Subnet Mask] [interface] [priority] [permanent]

Remote routes:
ip route [destination NA] [Subnet Mask] [IP addr of Next-hop] [priority] [permanent]

(priority range: 0 (highest) to 255 (never enter))

(permanent: optional parameter; without permanent, the route is removed from the routing table once an associated link goes down)

Load Sharing: Load sharing between multiple routes can be established by creating to-routes to same destination with the same priority

Default routes: If nothing in the Routing table matches, a default route can be configured, that is used in this case. It gets used as last option because it is the most unspecific route

dest NA Subnet Mask
ip route 0.0.0.0 0.0.0.0 [IP addr of Next-hop/Interface]

Alternative routes: Configuration of a backup route in case of a link failure with lower priority

Example (no priority equals priority 0 (highest))
ip route 10.1.9.0 255.255.255.0 192.168.128.33

ip route 10.1.9.0 255.255.255.0 192.168.96.1 50

Connectivity Verification

Ping (ICMP): ICMP (Internet Control Message Protocol) is used to test ability to reach a host on networks. Provides the Round Trip Time (RTT) → Time the packet takes to reach host and return.
ICMP TTL exceeded error: Indicates that an intermediate communication server/Switch has seen and discarded the package (TTL expired → too many Hops → TTL reached zero)
ICMP destination unreachable error: Indicates that destination node has received packet destined to an unreachable part and it discarded it because it could not deliver it.

Traceroute: Lists hops a packet takes on its way to destination host and the time the packet needs for each hop forth and back.

Network Layer

Distance Vector Routing:

Distance Vector Protocols (RIP, IGRP, EIGRP): Routes are advertised as vectors (distance → hop counts; direction → next hop router); Protocol calculates fastest path; **Routing by rumor:** router doesn't if the received info is correct; if there is a topology change, the whole Routing table is shared among the routers; **Iterative:** continues until no routers are sharing infos; **self terminating:** no stop signal; **Scales badly** for big networks, only used in laboratories or Universities

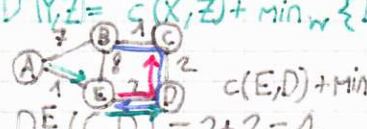
Disadvantages: router shares routing table every 10-90s. this results in a huge amount of traffic in big networks; **Slow convergence:** Network updates spread slowly in the network (multiple minutes) because of **Hold-down timers**; **Triggered/Flash updates:** If a link-cost-change happens, the router immediately shares the updated routing table **before** the exceeding of the **Hold-down timer**; Table entries have a limited Life-time (normally after 3-6 update cycles); Routers are **vulnerable** to **accidental** or **intentional misdirection**; The network can **maximally** be **15 hops** big.

Distance Vector Routing Flow: 1. when a router starts up it only knows directly connected networks; 2. router puts cost to the neighbors into his **Distance table**; 3. router creates his **Routing Table** from the Distance table and shares it with his neighbors; 4. with the received infos he updates his **Distance Table** & updates his **Routing-Table**; 5. If min. cost to a router changes, second step is invoked

Distance Vector Algorithm:
Iterative: continues until no nodes exchange info; **Self-Terminating**
Asynchronous: Nodes don't need to exchange infos/iterate in lock-step
Distributed: Each Node communicates only with directly attached Neighbors
Distance Table data structure: each node has its own row for each possible destination; column for each directly-attached neighbor to node; example: In node X, for dest. Y via neighbor Z

$D^X(Y,Z)$ = distance from X to Y via Z as next hop

$D^X(Y,Z) = c(X,Z) + \min_w \{D^Z(Y,w)\}$

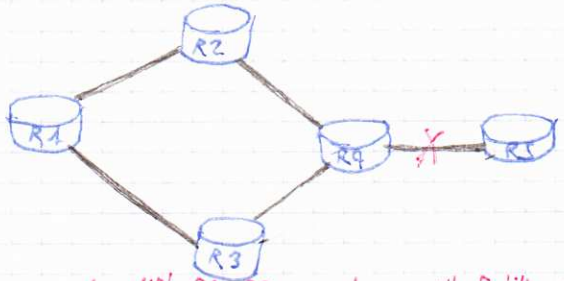


$c(E,D) + \min_w \{D^D(C,w)\}$

$D^E(C,D) = 2+2 = 4$
$D^E(A,D) = 2+3 = 5$ Loop
$D^E(A,B) = 8+(1+2+2+1)$ Loop

$D^E()$ — cost to dest via

destination	A	B	D
A	1	14	5
B	7	8	5
C	6	9	4
D	4	11	2



What happens when link R4-R3 goes down, with Splithorizon poisoned reverse and triggered updates?
Because of triggered updates all routers receive the information simultaneously and inform the source with **poisoned reverse**. The Holddow timer is per default two minutes and now gets started. Only after expiration the Routing-Entry gets deleted. During the two minutes the ICMP-Error message "Destination Unreachable. All not directly connected routers have a metric 16, but still send packages to R4.

RIPv1 vs. RIPv2

both: distance vector with hop count metric; **Hold-down timers** to prevent routing loops (default 180s); **Split horizon** to prevent routing loops; **16 hops** as metric for **infinite distance**
RIPv1: Classful; No authentication; Updates are sent as **Broadcasts**; Max hop count 15; No support for **Variable Length Subnet Mask (VLSM)** or **Classless Interdomain Routing (CIDR)**
RIPv2: Classless (Prefix-routing = subnetmask is in Updates VLSM); Authentication possible; Uses **Multicast** (224.0.0.9); Tags external routes; Routing Update **includes Next Hop**

Distance Vector Problems and solutions:

Problem: Count-to-Infinity: Path-cost gets incremented into infinity.
- In a network with the Routers A-B-C, C goes offline
- B marks C as offline in his routing table.
- A shares its routing-table with the information, that it can reach C over B
- B updates its routing-table with this information, but does not know that the Path from A to C goes over itself.
- B now shares that he has found a new way to reach C
- With the new information of B, A now updates his cost and increments by the cost from A to B. This creates a loop because A and B now continue to share their routing tables until they reach infinity (16), thus a count to infinity

Solution: Split Horizon: Router-information doesn't get sent back to the interface on which the router received them
Solution: Poison Reverse: Split Horizon prevents the router from sending information back to the interface that it came from. If a router receives a poisoned route, he sends this route back to the interface he received the information and therefore breaks the rule of split horizon. This ensures that the sender of the poisoned route knows not to change the poisoned routes metric.
Solution: Route Poisoning (RIP, IGRP, etc.): A router with a unreachable neighbor shares a routing update with an infinite hop-count to all other neighboring routers.
Hold-down-Timers: Prevents Loops, Default 180s.
If a router receives the information that a link is down, he starts the hold-down-Timer and discards any information that the route is available again. Only if the Router behind the link that is down sends routing-information, the Holddown Timer is stopped. The unreachable route is published with an infinite cost during this time.
Triggered Updates: Router sends updates, as soon as there is a change in the routing-table without the awaiting of the usual update interval. Prevents Count-to-infinity. Does not override the Hold-down timer.
Thanks to Triggered Updates all routers receive the information of upcoming links immediately. If good news are received the Hold-down-Timer is overriden.

Timers:
Update timer: Controls interval between Updates Broadcast to all RIP Enabled Interfaces. Default 30Sec
Invalid timer: Determines how long entry can be in Routing table without being updated. Also called Expiration Timer. After Timer expires Metric 16 Default 180Sec
Flush timer: Controls time of invalidated route to removal of route. Default 240Sec must be > than Invalid Timer
Holddowntimer: Is started per route entry when hop count changes from lower to higher value. Allows stabilization of route. During this time no update can be done to route entry. Default value 180 Seconds

Network-Layer

Link State Routing

Link State Routing (OSPF, IS-IS): Each router must know the whole network topology; each router creates his own topology-DB (Map) in which all LSAs he received from other routers are saved; ⊕ Link state protocols are more reliable, easier to debug & use less Bandwidth than Distance Vector Protocols; ⊖ They require more memory space & more Processing Power. They burden the network more because of LSA flooding; in order to tell all nodes about the network topology & to find the best path, 3 steps are required: 1. Hello Protocol, 2. LSAs, 3. Path calculation (shortest Path first algorithm)

Hello Protocol: In the first step the router finds out his neighbors & exchanges the info until their DBs are identical. Keep-alive Messages (every 10s) ensure that a neighbor is still up. If neighbor doesn't answer for 30-40s its marked as down. Negotiates parameters such as the election of a designated router. IS sent as IP Multicast: 224.0.0.5 (point-to-point, point-to-multipoint) or Unicast packets in Non-broadcast mode.

Link State Advertisments (LSA): Mechanism to distribute knowledge gained from the Hello Protocol to all other routers. Sends updates to other nodes and assures that only the youngest info is accepted.

- Whole network flooded with the logical sight of the routers (router ID, neighbor ID, cost)
- Each topology change invokes LSAs to inform the whole network of the topology change.
- When all routers have synced their DB, flooding is stopped

↳ if a router gets started he needs to know its last sequence number, that is needed to ensure network security. for this he asks neighboring routers for his last sequence Nr.

↳ With the sequence Nr. a router can recognize whether an info that he has received is up to date or if there is more recent info

↳ if the Maximal sequence number is reached, the router starts at 0. This would mean that preceeding updates are 'older'. But the Max is 2^{32} • updateInterval (10s) = 1361y (30Min)

Open Shortest Path First (OSPF): fast convergence time, scalable; OSPFv2 for IPv4, OSPFv3 for IPv6/4; Uses Hello protocol for neighborhood, LSA, Dijkstra (building neighborhood with Hello, LSA exchange via LSA flooding, building Link-state-DB according to LSAs, shortest path first execution, building the routing table); Classless routing with VLSM, sends SubnetMask with updates; authentication with MD5, Cleartext, SHA; When OSPF recognizes a topology change it distributes a complete update with all Link-state infos; All routers of an OSPF-Area need to have identical & synced Linkstate info in their DBs. Selective updates: If the OSPF network is converged and a new link is up, only this is sent as an update to the neighbors; Metric: Cumulative Cost of all outgoing interfaces from source to destination, Bandwidth, Delay Uses Multicast and Unicast instead of Broadcasts.

IPv4: Multicast 224.0.0.5 to all OSPF routers, Multicast 224.0.0.6 to DR/BDR Router. MAC: 01-00-5e-00-00-05

IPv6: Multicast FF02::5 to all OSPFv3 routers, FF02::6 to all DR/BDR Router;

Bundles Network into Areas: smaller logical subnets. This holds the networks stable (From 5000 routers unstable), → faster convergence, smaller routing tables, SPF-Algorithm is faster.

2 Routing types:

- Inter-Area Routing: each Inter-Area-Traffic has to go through Area 0
- Intra-Area Routing: Connects enduser and ressources

Area Border Router (ABR): ABR-Routers have at least one interface connected to Area 0. If this is physically impossible it can be done Logically with a OSPF virtual Link.

Autonomous system Boundary Router (ASBR): ASBR routers have one interface in the OSPF Domain and another interface in any other Routing Protocol Domain (RIP, EIGRP).

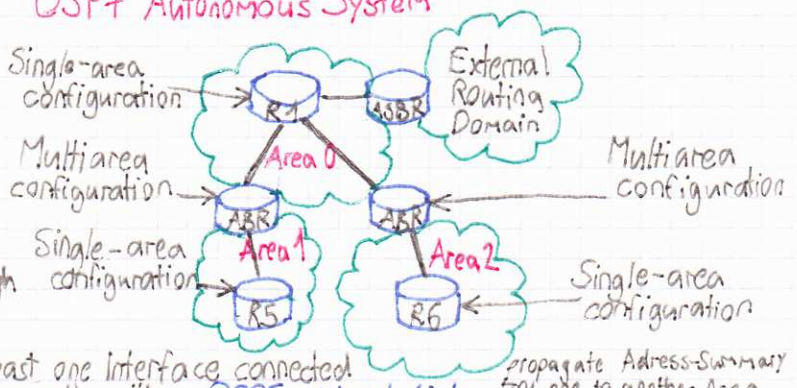
Shortest-Path-First-Algorithm (Dijkstra):

After all tables were shared over the network, the cost can be calculated. This is done with the Dijkstra Algorithm. A tree with minimal length is calculated. The aim is to find the shortest possible path for each router. A table is used with three columns: Candidates, Cost from the Candidates to the Root, Nodes within the tree

1. → First the Router itself into the column "Nodes within tree" with the cost of 0.
2. → All direct neighbors, of the router that was added to the tree most recently, are added to the "Candidate List" column from the Link-state-DB in the form of a triple: <ROUTER_ID>, <NEIGHBOR_ID>, <COST>. This describes the link of last added router to his direct neighbor with the cost of the direction.
3. → The Candidate List is now moved into the column "Cost from Root to Candidate" but with the cost from the Root (Initial) Router to the newly added candidate. Now Duplicates get checked and all but the way with the lowest cost get removed. The Candidate with the Lowest cost from root now gets added into the Tree
4. → All remaining Candidates in the "Cost from Root" column now get moved into the "Candidate" column
5. → The Iteration starts back at Step 2. The most recently added is now the Candidate that was added to the Tree in Step 3.
6. → When only one Candidate is left, this one is also added to Tree

The Algorithm is invoked each Time the Topology changes.

OSPF Autonomous System



Transport Layer

Protocol:	TCP	UDP
Characteristics:	Reliable/Acknowledged, Transport Layer Addressing (Allows multiple Apps to use single IP), virtual connection (bidirectional), sliding window system	Simple, Fast, Transport Layer Addressing, Unreliable, Connection-less

Header:

0	15	16	31
Source Port 16		Destination Port 16	
Sequence Number 32			
Acknowledgement Number 32			
Header Length 4	Reserved 6 / Control Bits 6	Window 16	
Checksum 16		Urgent 16	
Options 0/32			
Application Layer Data variable			

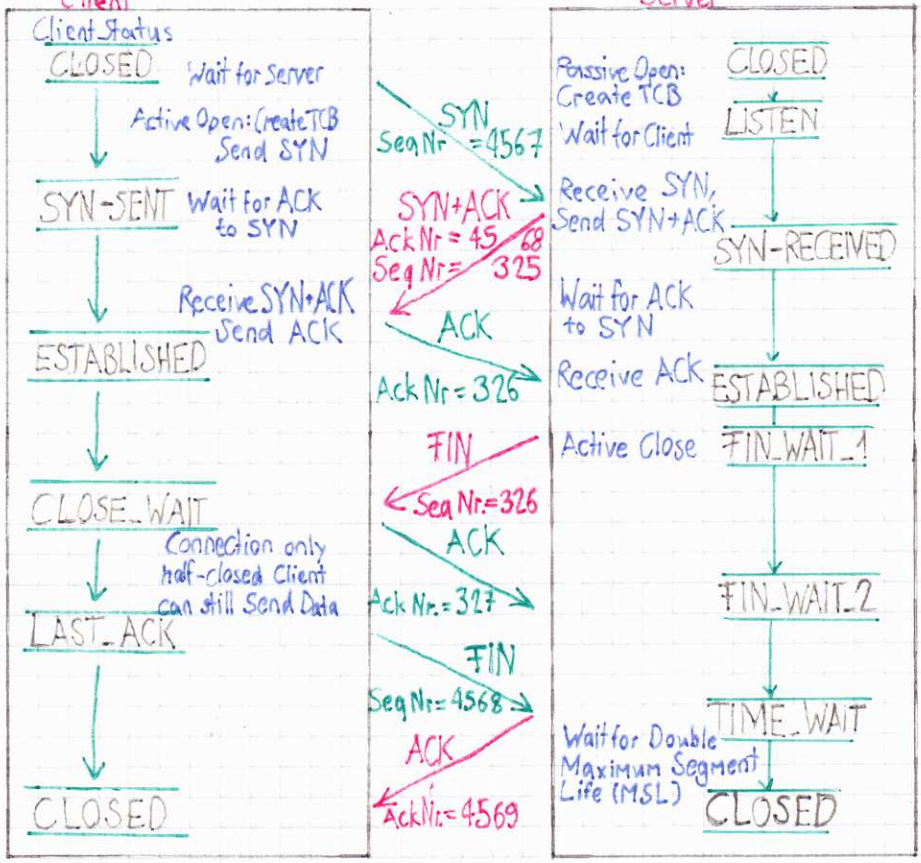
0	15	16	31
Source Port 16		Destination Port 16	
Length 16		Checksum 16	
Application Layer Data variable			

Use of Checksum Field optional; Pseudo Header for Checksum Calculation generated by UDP Software with IP Source port, IP Destination Address Field, IP Protocol Field and UDP Length Field. Total Length 11 Bytes plus 1 Byte of Zeros

Overhead:	Low, but higher than UDP	Very low
Transmission Speed:	High, but not as high as UDP	Very High
Data Quantity:	Small to very large amounts (up to few gigabytes)	Small to moderat (few 100 bytes
Types of Applications:	Most protocols and applications sending data must be received reliably, including most file and message transfer protocols	Where data delivery speed matters more than completeness, where small amounts of data are sent or where multicast/broadcast are used

TCP:

Control Bits: Urgent-bit (URG): Indicates invocation of priority data transfer feature and validity of Urgent Pointer field
Acknowledgement-bit (ACK): Indicates carriage of an acknowledgement in the segment and validity of Acknowledgement Nuber Field
Push-bit (PSH): Usage of the TCP Push feature, requests that data in segment is immediately pushed to the receiving Device
Reset-bit (RST): Sender has encountered a Problem and wants to reset the connection
Synchronize-bit (SYN): Segment is a request to synchronize sequence number and establish a connection. Sequence Number bit contains the initial sequence Number (ISN) of the sender of the segment
Finish-bit (FIN): Request to close the connection



3-Way Handshake: Open

To establish a connection each device must send a SYN message and receive a respecting ACK

Initial Sequence Number Selection
32-bit initial Sequence number chosen through timed counter. "Random" Nuber because of Security concerns

TCP Sequence Number Synchronization
Establishment involves Synchronization
ACK of SYN contains received Number + 1

Reset
Feature to deal with half-open Connections or unexpected message types

4-Way Handshak: Close

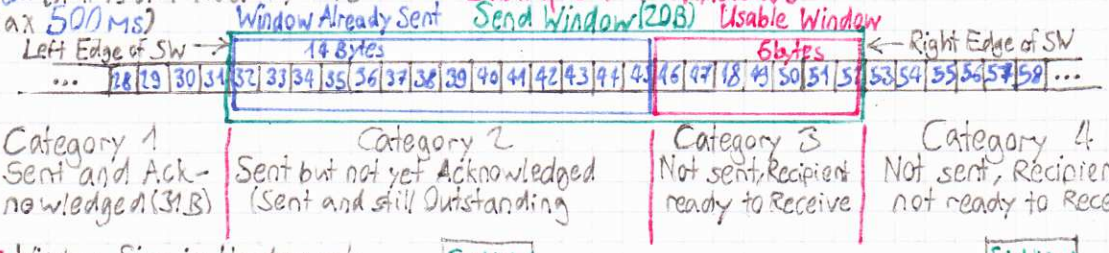
To close a connection each device must send a FIN message and receive an ACK from the other device.
FIN and ACK are not combined, thus it is a 4-Way Handshake

TCP: Transport-Layer

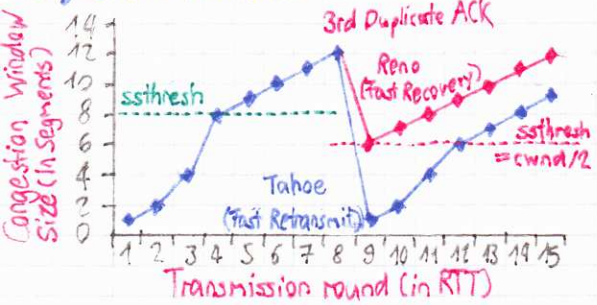
Retransmission Timeout (RTO): Time that the sender waits on ACK, before a segment counts as lost and gets resent
Cumulative ACK: Only every other segment gets confirmed. The highest Sequence Number acknowledged counts.
Duplicated ACK: If a sender receives 3 duplicate ACKs (4 ACKs for a packet), the packet will be resent. The Retransmission Timer is not awaited → "Fast Retransmit"
Sent when a receiver sees a gap in the packets it receives.
Delayed ACK: With delayed ACK the receiver has to send an ACK only in an interval that is defined by the Delayed-ACK-Timer (Max 500 ms)
Selective ACKs: Declares range of received packets, therefore only missing segments get resent.

Maximum Segment Size (MSS): Maximum size of payload of a single TCP-Segment. Default value 536 Bytes, but should be enlarged during initial TCP Handshake
Sliding Window: Participants of a TCP connection inform each other about the possible Window-size, this is the payload a participant can handle.
The window size can be set to 0, then the connection is called half-open. If an ACK which resizes the window is lost, it gets sent again after a certain time.

Example TCP Windows:

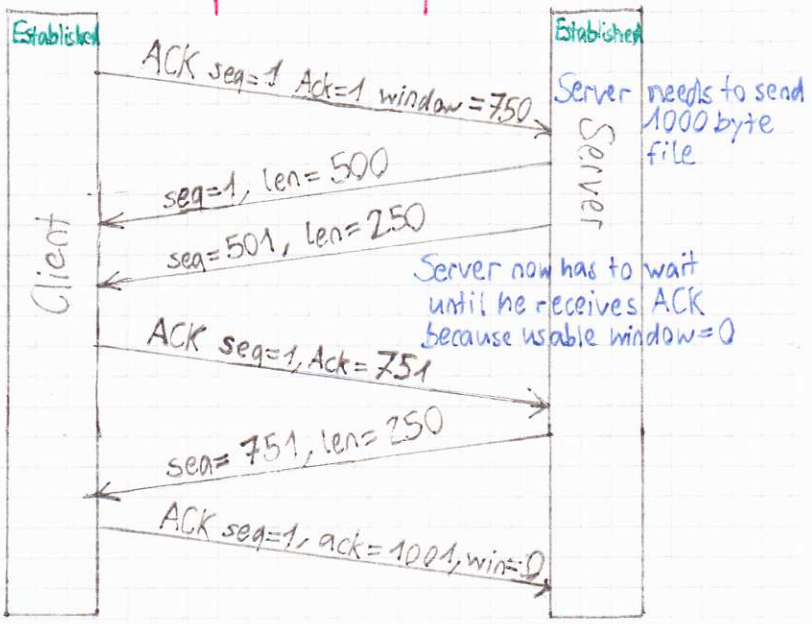


Window Scale Option: Window Size in Header only allows (2^16)-1 bits. Because of this an additional optional part offers a scaling option. The scaling factor is a left-shift by up-to 14 bits. Both sides need to support this feature in order to work. Max (2^30 - 2^14)
Flow Control: After the connection has been established data is transmitted in the flow described above (each packet get acknowledged). The data flow must be controlled by both workstations in order to further optimize it. The Optimization are the different types of ACK and the sliding window mechanism mentioned above.
Congestion Control: Avoids the overload of the network by the sender. Algorithm includes: Slow Start & Congestion Avoidance. Builds up on the sliding window. It redefines the window size constantly.
Slow Start: The congestion window get exponentially increased until it reaches a certain threshold. Then Congestion Avoidance takes over



Congestion Avoidance: When the threshold is reached, the congestion avoidance algorithm increases the window linear (Window only grows in MSS/Congestion Window). If 3 duplicate ACKs get detected the Window Size gets reduced to half and then does a Slow Start again.

Ephemeral Port:
Temporary communication Hub used for IP communications. It is created from a set range of port numbers and used as an end-clients port assignment in direct communication with a well-known port used by a server.

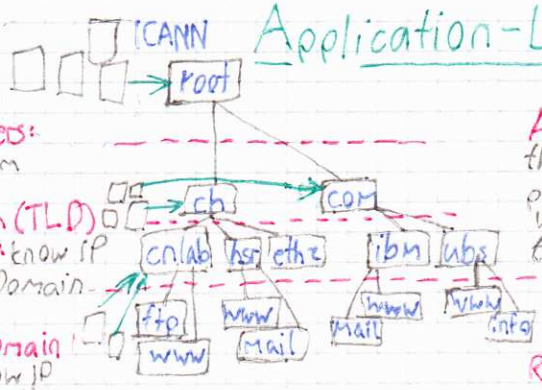


TCP-Ports: 16 bit, From 0 - 65535
Well known (Privileged): Port 0 - 1023
Managed by IANA, only standardized RFC Protocols
Registered (User): Port 1024 - 49151
For unstandardized applications, anyone can register a port number at IANA.
Private/Dynamic: Port 49152 - 65535
Unreserved and unmaintained

Most Important Registered Port Numbers:

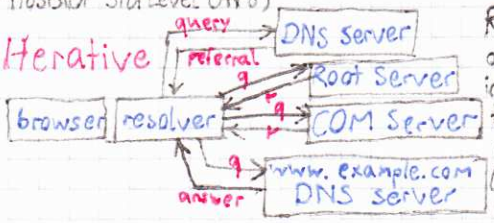
Protocol	Port	Protocol	Port
FTP data port (active)	TCP 20	NetBIOS (TCP rare)	TCP/UDP 137
FTP control port	TCP 21	NetBios	UDP 138/139
SSH (SCP, SFTP)	TCP 22	IMAP 4	TCP 143
Telnet	TCP 23	LDAP	TCP 389
SMTP	TCP 25	Https	TCP 443
TACACS	TCP 49	SMTP SSL/TLS	TCP 465
DNS name queries	UDP 53	IPSec (VPN with IKE)	UDP 500
DNS zone transfer	TCP 53	LDAP SSL/TLS	TCP 636
TFTP	UDP 69	IMAP SSL/TLS	TCP 993
http	TCP 80	POP SSL/TLS	TCP 995
Kerberos	UDP 88	L2TP	UDP 1701
POP3	TCP 110	PPTP	TCP 1723
SNMP	UDP 161	RDP (Remote Desktop)	TCP/UDP 3389
SNMP trap	UDP 162	MSSQL-Server	TCP 1433

DNS: Application-Layer

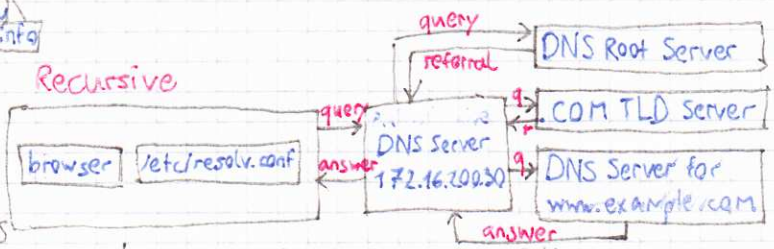


Root Name Servers: know IP of TLD nam servers
Top Level Domain (TLD) Name Servers: know IP of Second Level Domain Name Servers
Second Level Domain Name Servers: know IP of Hosts(or 3rd Level DNS)

Authoritative DNS Server: Is a nameserver that holds the actual DNS records (A, CNAME, PTR etc.) for a particular domain / address. A Recursive Resolver would be a DNS Server that queries a Authoritative DNS to resolve a domain / address



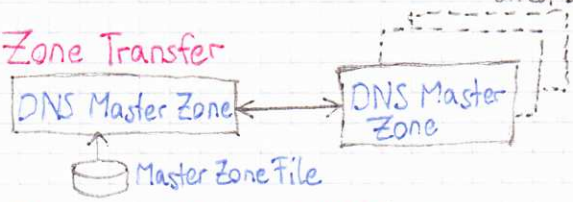
Request to DNS only returns own info and referral to next higher DNS in hierarchy. The Client has to do another request to the referred DNS Server



In a recursive Query the DNS Server, who received the query does the whole job and manages the communication with the higher level DNS Servers

DNS Messages: Query, Reply, zone transfer

Zone Transfer



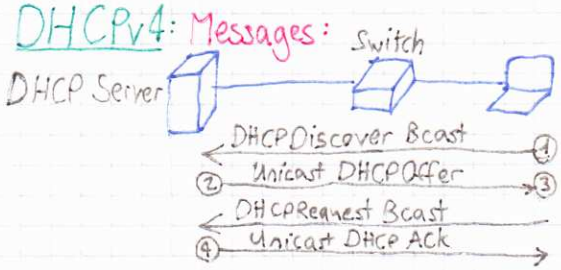
DNS servers synchronize their zone files with zone transfers to the other Slave name Servers. Terms, Master and Slave define which name Server has the master copy of the zone file loaded from a local file system and which has a copy loaded via zone transfer

Resource Record (RR): RRs contain the information requested by DNS queries. They are stored in a universal format. The formats employed for these Resource records are:
Format 1: (name, [pref], value, type, [TTL])
Format 2: name [TTL] [class] type [pref] value
TTL (Time to Live) is the Lifetime of the cached RR and is stored in a 32bit unsigned integer. 0 = no caching

RR Types

Type	Name	Value	Description / Example:
A	Hostname	IP-Address	Type is hostname-to-IPAddress mapping (ns1.cn is the worst.com, 152.96.37.51, A)
NS	Domain	Hostname of Authoritative DNS of Domain	Type used as a routing function for queries (cnisthe worst.com, ns1.cnistheworst.com, NS)
CNAME	Alias name	Canonical Name	Type provides the canonical name when requested (cnistheworst.com, www.cnistheworst.com, CNAME)
MX	Domain Name	Name of Mail-Server associated with Domain	A preference value is designated for each Mail-Server if multiple MX-Records in Domain Mail-Server with smallest preference value is used. No CNAME RR allowed for multiple Mail servers (cnistheworst.com, 10, mx1.cnistheworst.com, MX) (mx1.cnistheworst.com, 152.96.37.55, A)

DHCPv4: Messages:



DHCPv4:
The DHCP client protocol has two roles: Discover a DHCP server, and Request to lease an IPv4-address. Server has a configured range of addresses (Pool) and assigns those to a client for a set period. If the Lease has expired Client sends another Lease or IP is returned into the pool

Discover: Sent by DHCP client to find a DHCP Server
Ethernet: source = sender MAC; Dest = FF:...:FF
IP: source = 0.0.0.0; Dest = 255.255.255.255
UDP: source port = 68; Destination port = 67

Offer: Sent by a DHCP server to offer a lease of a IP-Addr
Ethernet: source = sender MAC; Dest = Client MAC
IP: source = 192.168.1.1; Dest = 255.255.255.255
UDP: source port = 67; Destination port = 68

Request: Sent by a DHCP Client to accept the offer of the DHCP Broadcast so other DHCP Servers know their offer was declined
Ethernet: source = Senders MAC; Dest = FF:...:FF
IP: source = 0.0.0.0; Dest = 255.255.255.255
UDP: source port = 68; Destination port = 67

Acknowledgement: Sent by the DHCP Server to assign the address and to send the Subnet Mask and DNS Server IP Addr.
Ethernet: source = Senders MAC; Dest = Client MAC
IP: source = 192.168.1.1; dest = 192.168.1.100
UDP: source port = 67; Destination port = 68

UCC & SIP: Application Layer

Vergleich SIP, H.323, Media Gateway Control Protocol (MGCP):

SIP: Decentralized Intelligence, Textbased, SDP
H.323: Decentralized Intelligence, Binary, Own Media Protocol (H.450), Telephony Protocol, Call Admission Control
MGCP: Centralized Intelligence, Voice, SDP

Session Initiation Protocol (SIP) RFC5411:

Overview: Cleartext, SIPS encrypted; SMTP-similar addressing format like MIME. Status codes like HTTP: ASCII and Linebased; IP address in header → OSI-Model not fulfilled; Transaction Protocol: SIP only describes Signalisation, rest is SDP; Layer 5-7
TCP/UDP Port 5060-5061; URI instead of Tel-Nr;

5 Facets establishing & terminating multimedia Communications:
User Location: Determination of the end system for communication
User Availability: Willingness of callee to engage in communication
User Capabilities: Determination of media and media parameters
Session Setup: "ringing" establishment of session parameters at both called and calling party
Session Management: Including transfer and termination of session, modifying session parameters and invoking services

Aufbau Messages:

SIP-Request
INVITE: Session Request
ACK: Terminal answer to INVITE
BYE: Ends a session
CANCEL: Terminates all pending Requests
REGISTER: Registers the Client according "To" Header Field. Binds SIP URI
OPTIONS: Asks for Server Capabilities
INFO: Sends info during a session that don't change session state

SIP Responses (like HTTP Status)
1xx = Informational
2xx = Success; ACK for INVITE
3xx = Redirection
4xx = Client Error (Request fail)
5xx = Internal Server Error
6xx = Global Failure
488 = Not acceptable here, sent when codec isn't supported

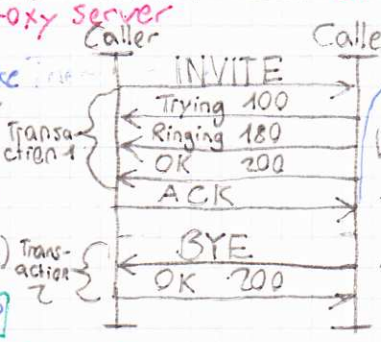
Components:

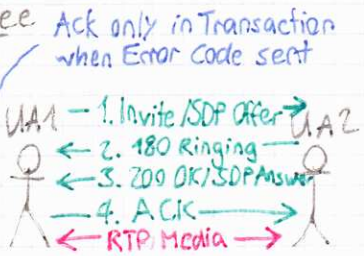
Physical Devices can unify multiple of these components.

- User Agents (UA) Mandatory: Endpoint, Can initiate or end SIP Sessions, Client and Server simultaneously on different ports
  - User Agent Client (UAC): Establishes connection, generates requests
  - User Agent Server (UAS): Listens to incoming connections
- Gateway: Translates between SIP and non-SIP protocols. Translates between mobile network and classic telephones
- Proxy Server (PS): Routes and connects 2 Endpoints. Receives Session Requests of UAs and ask Registrar Server for Receiver information. Forwards the Session Invitation directly to the UA (if in same domain) or Proxy Server / Redirect Server (if the UA is in another Domain)
- Registrar Server: Maps a SIP URI of a user to a certain IP-address. Receives SIP REGISTER requests to actualize Location Database (where all UAs of the domain are saved.
- Redirect Server: Address book. Accepts SIP Requests, Maps the address to a new one, and returns it to the UA. Does not Route SIP-Messages. Does not receive calls. Initiates no Requests. Enables Proxy Server to forward their SIP sessions to an outer domain. Regularly in the same hardware as the SIP Registrar Server and the Proxy Server

Call-Flow: There must be 3 packets to create a handshake

1. Sender sends Receiver an INVITE (can also go over proxy
2. Receiver responds with a 100 (Trying), 180 (Ringing) and status code 200 (OK)
3. Sender responds with ACK → connection is established
4. The UA that cancels the connection sends a BYE and the opposite responds with the status code 200 (OK)





Transaction Stateless: The proxy Server forwards all UDP messages and responses without maintaining any state
Transaction Stateful: A proxy Server that receives TCP a SIP Request retains state of that transaction until that server Receives a final Response (meaning a 2xx, 3xx, 4xx, 5xx or 6xx Response). Transaction stateful has no knowledge of a termination Request (BYE)
Dialog Stateful (really Stateful): When both VIA and Record Route Headers are utilized by a Proxy during the first SIP Request to ensure all remaining messages traverse that Proxy; this applies to each proxy that is in the signaling path between UAS
Record-Route Header: Phone providers need to know when a Connection was terminated, to know how much a user has to pay for his call. For this Record Route Headers can be used that ensure that the Call-Termination will also go through the Proxy

SIP Planes:

Service Plane: AAA, Address Resolution → Application Directory, Authentication, etc.
Call Control Plane: Signaling Entities and Protocols → e.g. SIP User Agent, Proxy, etc.
Connection Control Plane: Switch, Router, Transcoding, Media Control, etc.

Service Resource Record (SRV):
Used to resolve SIP URI

Leitungsvermittlung (circuit switched): Wegschaltung für traffic über reservierte Teilstrecken bei aufbau der Verbindung ⊕ Garantiert QoS, Optimiert Sprachübertragung, sehr stabil, Möglichkeit zu Lastabwehr ⊖ Durch feste Ressourcenbindung kosten über Reservierungszeit. Ungenützte Übertragungszeit.
Packetvermittlung (packet switched): wegesuche anhand der Destination Addresse für jedes Packet, daher Unterschiedlicher Delay der Packete → Jitter, out-of-order
⊕ einfacher, robuster und flexibler Netzaufbau, für Datenübertragungen Optimiert, Übertragungskosten nicht über zeit, sonder Datenvolumen oder flat rate

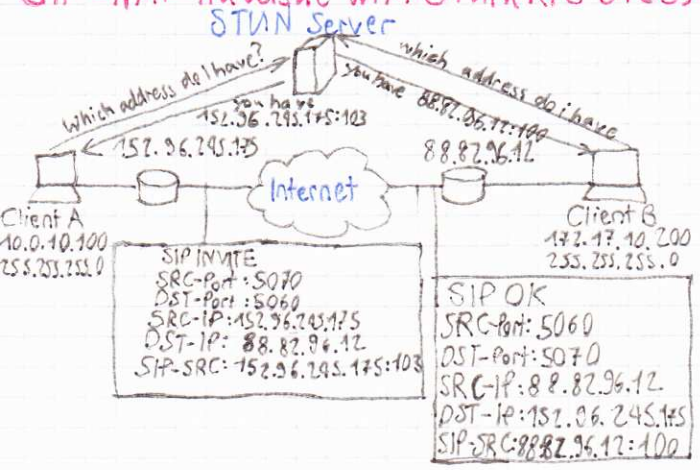
UCC & SIP — Application Layer

Session Description Protocol (SDP) RFC 2327: Standard representation for media information: media details, transport address and other descriptors for session-metadata; Transmits media type (video, audio, ...) transport protocol (RTP/UDP/IP), media format (H.261 video, MPEG-video, etc), Textbased, extendable; Format: <character>=<value>, case-sensitive, whitespaces not allowed; Three Main Sections: Sessions, Media, Timing; Names only unique within Section

Section	Param	Description
Session Description	v=	protocol version number, currently only 0
	o=	originator and session identifier: username, id, version number, network address
	s=	session name: Mandatory at least one UTF-8-encoded character
Media Description	m=	media name and transport address
Time Description	t=	time the session is active
RTPMap Payloads	Rtpmap:0 ⇒ PCMU/Audio/8000Hz; Rtpmap:3 ⇒ GSM/Audio/8000Hz; Rtpmap:5 ⇒ DVI4/Audio/8000Hz; Rtpmap:8 ⇒ PCMA/Audio/8k	

Real-Time Transport Protocol (RTP): Transmits audio-visual media-streams unencrypted in real-time, SRTP is encrypted
Real-Time Transport Control Protocol (RTCP): Handles QoS monitoring of Audio/Video packets, Send timing info to recipients

SIP-NAT-Traversal with STUN (RFC 3489): STUN = Simple Traversal of UDP through NATs = Session Traversal Utilites for NAT
Enables device to find out Public IP and the type of NAT service it's sitting behind. STUN operates on TCP and UDP port 3478
Not universally supported by VoIP devices yet. Works with three of four Main Types of NAT: Full cone, restricted Cone, port-restricted cone. Does not work with Symetric (bidirectional) NAT



STUN client sends a request to a STUN server. The server then reports back to the STUN Client what his public address outside the NAT is.

Quality of Service (QoS): Primary goal is to provide priority (including Bandwidth, jitter control, Latency) to selected types of traffic.

Problems:
Low Throughput: The Bandwidth assigned to any given data stream might be too low for the service to be useful. Video streaming with continous breaks is just one example
Dropped packets: If a router is under heavy load it might decide, or worst case is forced to drop packages. TCP applications will retransmit the dropped the dropped data, but significant delays will occur.
Errors: Sometimes packets get corrupted due to noise or interference, especially in wireless communication. The effects are similar to those of dropped packets in that the missing packages sometimes have to be retransmitted.
Latency: Depending on which route a package take and how full a routers queue is, the time it takes for a package to arrive varies. Excessive latency can render Applications like VOIP or multiplayer gaming unusable.
Jitter: Packages even of the same stream will reach their destination with different delays. This variation in delay is known as jitter and can seriously affect the quality of Streaming.
Out-of-order Delivery: Not every package from the same stream may take the same route through a network. In some cases, this can result in some later sent packages to arrive first (aka out-of-order). This is in many cases problematic and must be dealt with at some level. TCP reorders its packages on the Network Layer already whilst other protocols require higher layers to do so.

Approaches:
Parameterized system: Developed in early days of networking. Base on exchange of application requirements to the network which in turn manages all requirements and the traffic.
Integrated services (IntServ): Uses Resource Reservation Protocol (RSVP) for communication of application requirements. Due to Overhead of RSVP this approach does not scale well.
Prioritized System: Package identifies desired service level in headers. This information can be used directly to routers and switches to determine QoS.
Differentiated Services (DiffServ): In this approach packages can be classified based on for example IP source and destination, protocol etc. Based on this the packages are then placed in any number of queues. Finally, a scheduler uses a queuing strategy to write the packets back onto the wire. A great amount of Queueing strategies exist, two of which are now described.
Priority Queuing: Good for low Bandwidth links, can cause issues (starvation) if the workload is too much to handle. Works by always sending highest priority packages first.
Weighted Fair Queuing: As in pronity queuing packages are sorted in queues from which scheduler selects the next package to send. For each queue a weight is defined telling the scheduler how many packages to send In WFQ the scheduler goes from queue to queue in circles and sends from that queue until it's either empty or as many packages have been sent as the weight defines. The Advantage is that low-priority packages do get their turn and hence don't get starved out.