

Zusammenfassung CN1

0	Basics	2
0.1	ISO/OSI und TCP/IP Modell	2
0.2	Organisationen	2
1	Layer 1	2
1.1	Protokolle & Geräte	2
1.2	Kabel	2
1.3	Manchester Encoding gemäss IEEE802.3 (Self-Clocking)	2
1.4	Return to Zero Encoding (Self-Clocking).....	3
1.5	Not Return to Zero Encoding (Non-Self-Clocking).....	3
1.6	8B/10B Encoding (Self-Clocking)	3
1.7	Wireless	3
1.8	Fiber	4
2	Layer 2	5
2.1	Protokolle & Geräte	5
2.2	Kollisionsdomäne / Broadcastdomäne	5
2.3	Ethernet Standards	5
2.4	802.2 Logical Link Control (LLC) Sublayer.....	5
2.5	802.3 Media Access Control (MAC) Sublayer	5
2.6	Carrier Sense Multiple Access / Collision Detection (CSMA/CD).....	5
2.7	Half-Duplex / Full-Duplex.....	6
2.8	Power over Ethernet (PoE).....	6
2.9	Twisted Pair / RJ45 PINs.....	6
2.10	Auto-Negotiation	6
2.11	Switching.....	6
2.12	Address Resolution Protocol (ARP)	6
2.13	Wireless	7
2.14	802.1D Spanning Tree Protocol (STP).....	8
2.15	802.3ad Link Aggregation Protocol (LACP): Port Aggregation with EtherChannel	8
2.16	VLANs.....	9
3	Layer 3	9
3.1	Protokolle & Geräte	9
3.2	ICMPv4.....	9
3.3	IPv4	9
3.4	IPv6	10
3.5	ICMPv6.....	12
3.6	Statisches Routing.....	12
3.7	Dynamic / Static Network Address Translation (NAT).....	12
3.8	Port Address Translation (PAT)	12
3.9	NAT64	13
3.10	Vor/Nachteile NAT/PAT	13
3.11	Open Shortest Path First (OSPF)	13
4	Layer 4	14
4.1	Protokolle & Geräte	14
4.2	Ports.....	14
4.3	User Datagram Protocol (UDP)	14
4.4	Transmission Control Protocol (TCP).....	14
5	Layer 5	17
5.1	Protokolle	17
6	Layer 6	17
6.1	Protokolle	17

7	Layer 7	17
7.1	Protokolle	17
7.2	DNS	17
7.3	DHCP	18
8	Network Management.....	19
8.1	ITIL	19
8.2	FCAPS.....	19
8.3	Protokolle	19
8.4	Flow Protokolle	20
8.5	Syslog.....	20
8.6	Simple Network Management Protocol (SNMP).....	20
8.7	Dokumentation.....	20
8.8	Software Defined Networking (SDN).....	20

0 BASICS

0.1 ISO/OSI UND TCP/IP MODELL

Layer	Englischer Name	Deutscher Name	TCP/IP Modell
7	Application Layer	Anwendungsschicht	Application
6	Presentation Layer	Darstellungsschicht	Application
5	Session Layer	Sitzungsschicht	Application
4	Transport Layer	Transportschicht	Transport
3	Network Layer	Vermittlungsschicht	Internet
2	Data Link Layer	Sicherungsschicht	Network access
1	Physical Layer	Bitübertragungsschicht	Network access

0.2 ORGANISATIONEN

- Internet Society (ISOC): Fördert die offene (Weiter-)Entwicklung des Internet
- Internet Architecture Board (IAB): Verantwortlich für die Verwaltung und Entwicklung von Internetstandards
- Internet Engineering Task Force (IETF): Entwickelt (weiter) und verwaltet Internet- und TCP/IP-Technologien
- Internet Research Task Force (IRTF): Macht Langzeit-Forschung zu Internet- und TCP/IP-Technologien
- Internet Corporation for Assigned Names and Numbers (ICANN): Koordiniert die Verwaltung von IPs, Domains und Ports
- Internet Assigned Numbers Authority (IANA): Verwaltet IPs, Domains und Ports
- IP-Adressverwaltung: Nordamerika ARIN, Europa RIPE, Asien APNIC, Afrika AfriNIC, Südamerika LACNIC

1 LAYER 1

1.1 PROTOKOLLE & GERÄTE

Protokolle: Keine Protokolle, lediglich Encoding, Daten sind Bits

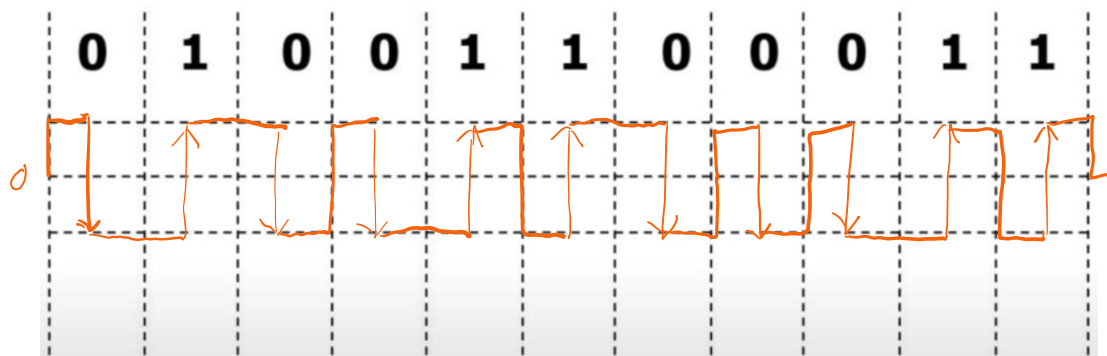
Geräte: Hub, Netzwerkkarte, WLAN-Antenne

1.2 KABEL

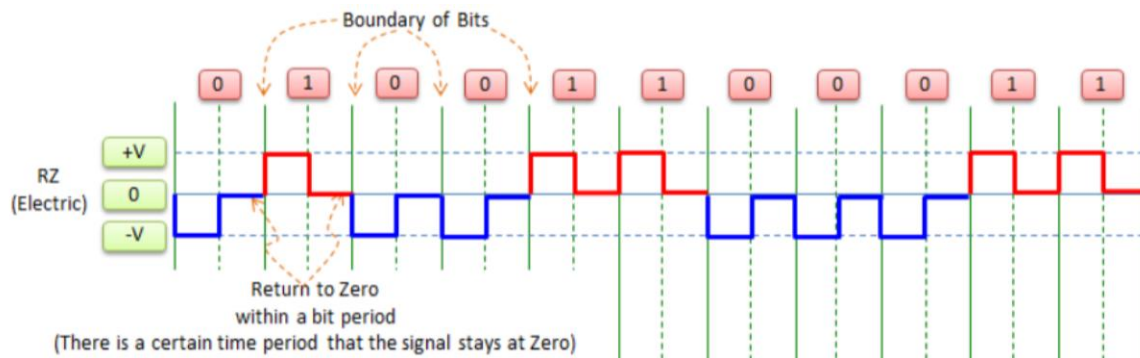
Unshielded Twisted-Pair (UTP) Kabel, Shielded Twisted-Pair (STP) Kabel, Koaxial Kabel, Fiber Kabel

1.3 MANCHESTER ENCODING GEMÄSS IEEE802.3 (SELF-CLOCKING)

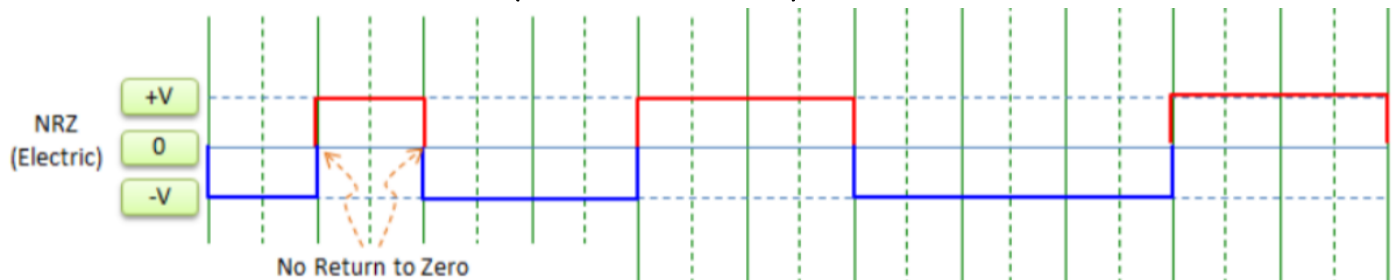
Es startet bei 0, bei 0 geht es nach unten, bei 1 geht es nach oben



1.4 RETURN TO ZERO ENCODING (SELF-CLOCKING)



1.5 NOT RETURN TO ZERO ENCODING (NON-SELF-CLOCKING)



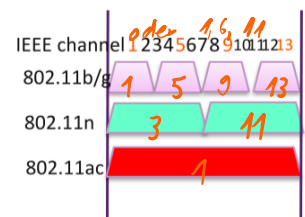
1.6 8B/10B ENCODING (SELF-CLOCKING)

Dabei werden 8-Bits gemäss einer Tabelle zu 10-Bits gemappt. Dadurch hat man Gleichstromfreiheit und eine Clock.

1.7 WIRELESS

1.7.1 Frequenzen/Channels

Die Frequenz wird in Hertz = Anzahl Schwingungen pro Sekunde gemessen. WLAN sendet auf 2.4 oder 5 GHz. Ein 2.4 GHz Channel ist jeweils 22 MHz breit.



5 GHz Channel Allocations

Frequency (GHz)	5.150	5.250	5.470	5.600	5.640	5.725	5.850
802.11 Allocations	UNII-1	UNII-2a	UNII-2c (Extended)	TDWR		UNII-3	
Center Frequency	5180, 5200, 5220, 5240	5260, 5280, 5300, 5320	5500, 5520, 5540, 5560, 5580, 5600, 5620, 5640, 5660, 5680, 5700, 5720			5745, 5765, 5785, 5805, 5825	
20 MHz	36, 40, 44, 48	52, 56, 60, 64	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144			149, 153, 157, 161	165
40 MHz	38, 46	54, 62	102, 110, 118, 126, 134, 142			151, 159	
80 MHz	42	58	106, 122, 138			155	
160 MHz	50		114				
FCC	1,000 mW Tx Power Indoor & Outdoor No DFS needed	250 mw w/6dBi Indoor & Outdoor DFS Required	250mw w/6dBi Indoor & Outdoor DFS Required 144 Now Allowed	120, 124, 128 Devices Now Allowed		1,000 mW EIRP Indoor & Outdoor No DFS needed	165 was ISM, now UNII-3
DFS Channels			DFS Channels				

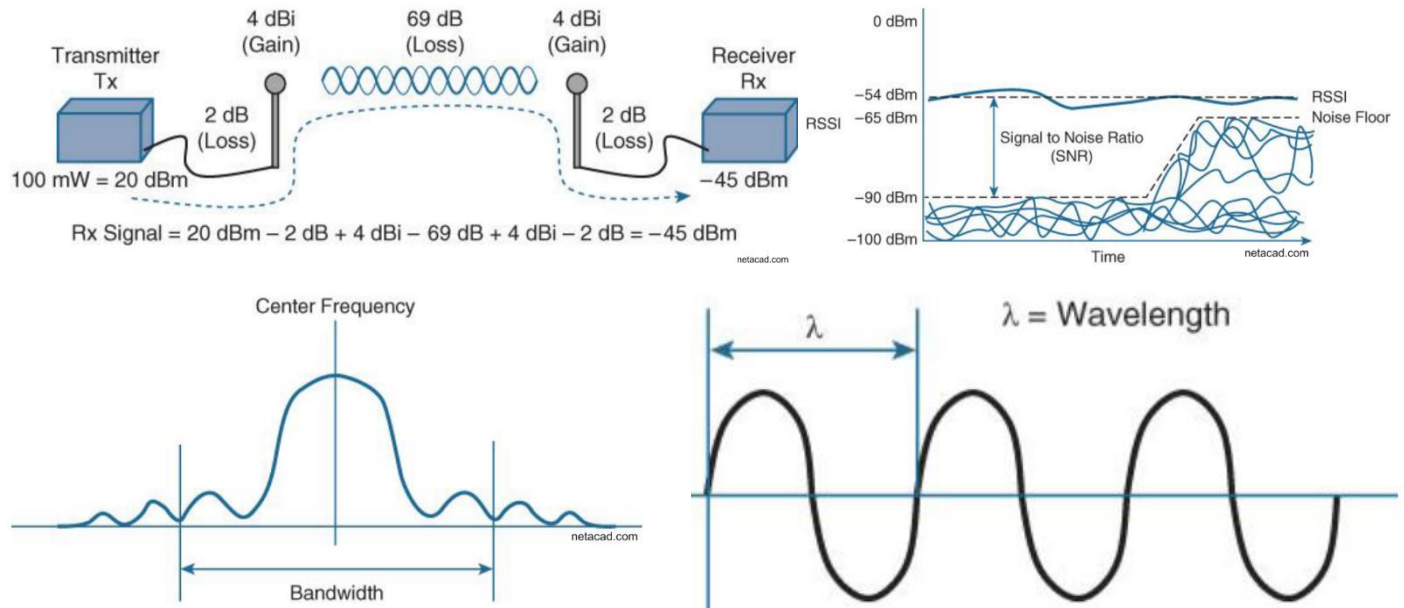
UNII = Unlicensed National Information Infrastructure, TDWR = Terminal Doppler Weather Radar, DFS = Dynamic Frequency Selection

1.7.2 Berechnungen

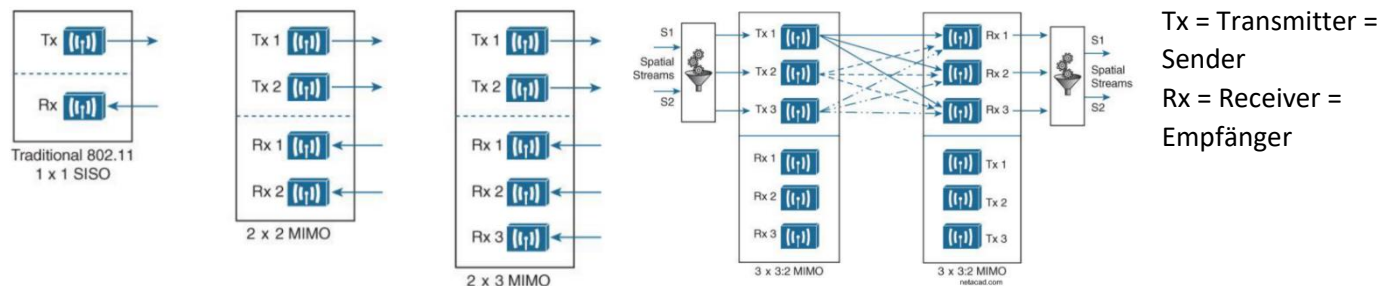
Einheit	Beschreibung	Formel
Dezibel (dBm)	Signalstärke Law of 3s: $mW \cdot 2 \Rightarrow dBm + 3$	$dBm = 10 \cdot \log_{10}(mW)$
Watt (1000 mW = 1 W)	Leistung Law of 10s: $dBm + 10 \Rightarrow mW \cdot 10$	$mW = 10^{\frac{dBm}{10}}$

1.7.3 Begriffe

RSSI = Received Signal Strength Indicator, SNR = Signal to Noise Ratio, dBi = Antenna Gain



1.7.4 Single-in Single-out (SISO) und Multiple-input Multiple-Output (MIMO) und Multiplexing



1.8 FIBER

1.8.1 Single-Mode vs. Multi-Mode

Single-Mode: Sehr kleiner Glaskern, braucht teure Laser, für lange Distanzen

Multi-Mode: Etwas grösserer Glaskern, etwas günstigere Laser, bis zu 10Gbit/s über 550m

1.8.2 Eye-Diagram

Das Auge im Diagramm muss möglichst weit und offen sein.

1.8.3 Mögliche Störungen

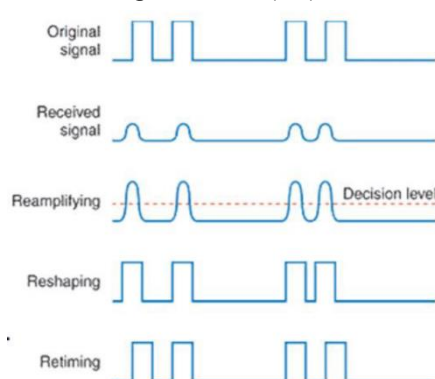
- Microbends: Kleine Beschädigungen am Glas von der Herstellung (Rayleigh Scattering)
- Macrobends: Beschädigungen am Glas durch zu starkes Biegen des Kabels
- Back Reflections: Reflektionen an den Enden des Kabels
- Splices: verursacht durch Dreck oder schlechte Verlegung
- Mechanical connections: physische Lücken zwischen Kabeln

1.8.4 Dispersion

Chromatic Dispersion: Signal wird mit verschiedenen Wellenlängen gesendet, welche unterschiedlich schnell reisen

Polarization Mode Dispersion: Signal wird in eine langsame und schnelle Achse getrennt

1.8.5 Regeneration (3R)



- Reamplifying: Signal stärker machen
- Reshaping: Originale Form zur Unterscheidung von 0/1 wiederherstellen
- Retiming: Die Abstände zwischen den Pulsen wiederherstellen

1.8.6 Berechnungen

Geschwindigkeit des Lichts im Fiber-Kabel: 200'000 km/s

Maximaler Eintrittswinkel: $\alpha = \arcsin(n_{\text{Glas}}/n_{\text{Mantel}})$

Maximale Kabellänge bei gegebener Tx-Power (10dBm), Rx-Sensitivity

(-5dBm) und Dämpfung des Kabels (2dB pro km): $\frac{10\text{dBm} - (-5\text{dBm})}{2\text{dB pro km}} = 7.5\text{km}$

2 LAYER 2

2.1 PROTOKOLLE & GERÄTE

Protokolle: Media Access Control (MAC) Adresse, Address Resolution Protocol (ARP), Daten sind Frames

Geräte: Switch, Netzwerkkarte, WLAN-Antenne

2.2 KOLLISIONSDOMÄNE / BROADCASTDOMÄNE

Hubs erstellen eine **Kollisionsdomäne**. Switches, Bridges oder Router sind immer eine Grenze der Kollisionsdomäne.

Broadcastdomänen hingegen werden durch Hubs, Switches und Bridges erstellt und durch Router begrenzt.

2.3 ETHERNET STANDARDS

Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Maximum Length
Ethernet	10Mbps	10BASE-T	802.3	Copper, 100 m
Fast Ethernet	100Mbps	100BASE-TX	802.3u	Copper, 100 m
Gigabit Ethernet	1000Mbps	1000BASE-LX	802.3z	Fiber, 550 m
Gigabit Ethernet	1000Mbps	1000BASE-T	802.3ab	Copper, 100 m
10GigE (Gigabit Ethernet)	10Gbps	10GBASE-T	802.3an	Copper, 100 m

2.4 802.2 LOGICAL LINK CONTROL (LLC) SUBLAYER

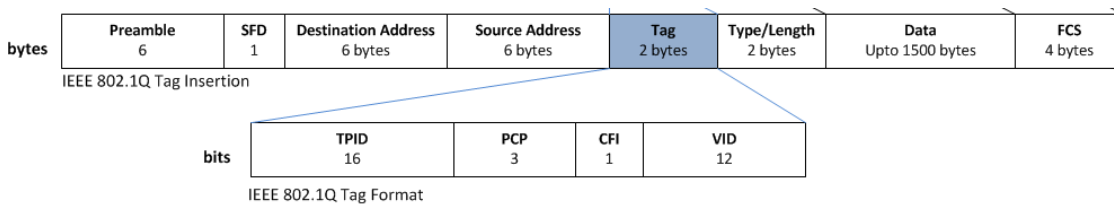
Bindeglied zwischen Layer 2 und 3. Es kann als Treibersoftware für NICs angeschaut werden.

2.5 802.3 MEDIA ACCESS CONTROL (MAC) SUBLAYER

Die MAC-Adresse ist eine 6 Byte lange Adresse mit 12 hexadezimalen Zahlen, welche durch den Hersteller auf dem NIC fixiert wird. Die Ersten 3 Bytes (= 6 Zahlen) sind der Organizationally Unique Identifier (OUI), welcher an die Hersteller vergeben wird. Die Grösse des MAC Headers ist 16B + 4B Trailer, Preamble und SFD zählen nicht dazu.

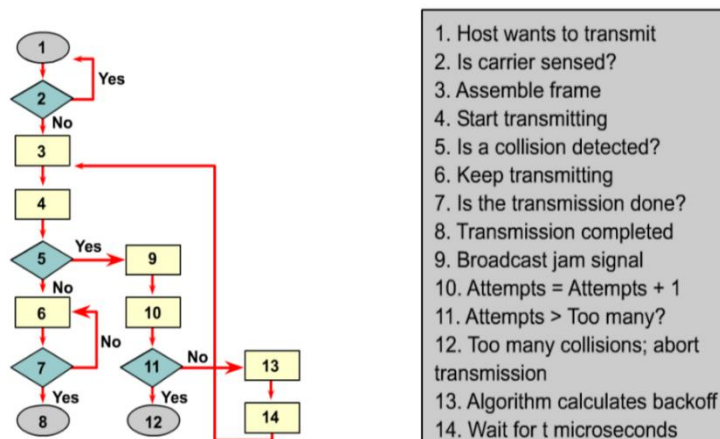
Frames an die Broadcast MAC-Adresse ff:ff:ff:ff:ff:ff erhalten alle Station der gleichen Broadcastdomäne.

2.5.1 Header



- Preamble: Immer gleiche Bitfolge zur Synchronisation
- Start Frame Delimiter (SFD): Immer gleiche Bitfolge zum Signalisieren des Starts des Frames
- Destination: Ziel-MAC-Adresse, Source: Sender-MAC-Adresse
- Type (bei Ethernet II Frame, LLC): Protokoll, welches im Layer 3 verwendet wird, meist IPv4, IPv6 oder ARP
- Length (bei 802.3 Frame statt Type): Länge der Daten in Bytes des Frames, Wert zwischen 46 und 1500
- Frame Check Sequence (FCS): Checksumme wird von Sender und Empfänger berechnet, stimmt sie nicht überein, wird das Frame verworfen (nur Detection, keine Corection)
- TPID: Tag Protocol Identifier (802.1Q für VLANs)
- PCP: Priority Code Point für Class of Service (CoS)
- CFI: Canonical Format Indicator, VID: VLAN ID

2.6 CARRIER SENSE MULTIPLE ACCESS / COLLISION DETECTION (CSMA/CD)



Nach 16 Versuchen wird das Frame verworfen. An diesem Punkt wird das Netzwerk als überlastet oder kaputt angesehen.

2.7 SLOT TIME/ BIT TIME

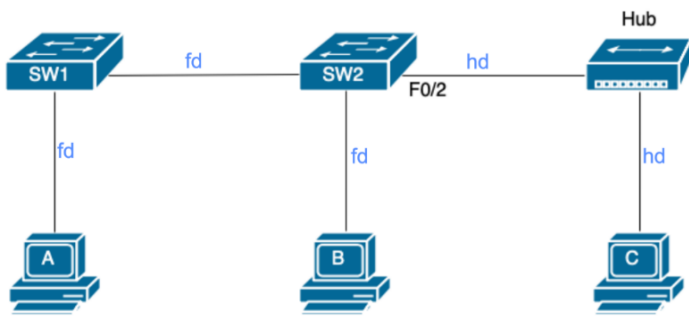
Slot time: längstmögliche Zeit für ein Signal, um durch das ganze Netzwerk zurück zum Startpunkt zu reisen

Bit time: Zeitdauer, um ein Bit aufs Medium zu platzieren.

Speed	Slot Time	Time Interval
10 Mbps	512 bit time	51.2 µs
100 Mbps	512 bit time	5.12 µs
1 Gbps	4096 bit time	4.096 µs
10 Gbps	not applicable	not applicable

Ethernet Speed	Bit time
10 Mbps	100 ns
100 Mbps	10 ns
1000 Mbps = 1 Gbps	1 ns
10,000 Mbps = 10 Gbps	.1 ns

2.8 HALF-DUPLEX / FULL-DUPLEX



Half-Duplex verwendet ein Twisted-Pair. Das Signal geht dabei in beide Richtungen durch das gleiche Paar, daher hat es eine schlechtere Bandbreite als Full-Duplex.

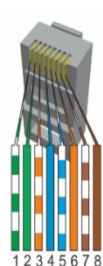
Bei Full-Duplex werden zwei Twisted-Pairs oder vier Twisted-Pairs verwendet. Die Hälfte der Twisted-Pairs wird zum Senden und die andere Hälfte zum Empfangen verwendet. So können keine Kollisionen entstehen und CSMA/CD wird deaktiviert.

2.9 POWER OVER ETHERNET (PoE)

Damit kann elektrischer Gleichstrom (DC) direkt über Twisted Pair Kabel übertragen werden, man spart sich so das Stromkabel, beispielsweise für IP-Telefone, WLAN Access Points oder Kameras. Es gibt zwei offizielle Standards:

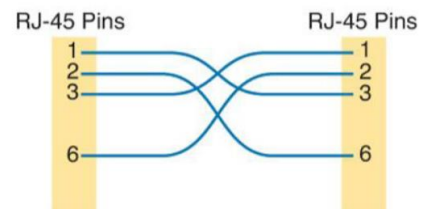
- 802.3af: PoE mit bis zu 15.4W, 802.3at: PoE+ mit bis zu 34.2W
- Proprietäre Lösungen, z.B. Cisco UPoE mit bis zu 60W

2.10 TWISTED PAIR / RJ45 PINS



RJ45 Pin #	Wire Color (T568A)	Wire Diagram (T568A)	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	White/Green		Transmit+	BI_DA+
2	Green		Transmit-	BI_DA-
3	White/Orange		Receive+	BI_DB+
4	Blue		Unused	BI_DC+
5	White/Blue		Unused	BI_DC-
6	Orange		Receive-	BI_DB-
7	White/Brown		Unused	BI_DD+
8	Brown		Unused	BI_DD-

Crossover



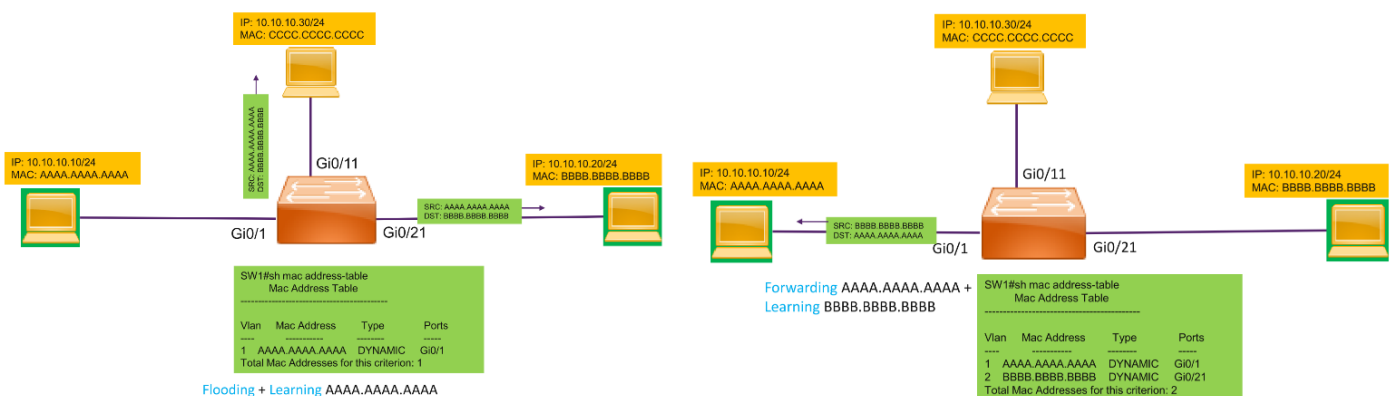
Die Tabelle oben gilt in der Spalte 10/100 für PC NICs, Router und WLAN APs. Bei Hubs und Switches hingegen ist Receive und Transmit vertauscht, daher muss ein Crossover Kabel verwendet werden, um beispielsweise Switches miteinander zu verbinden. Cisco Switches haben auto-mdix, welches ein falsches Kabel erkennt und umschaltet.

2.11 AUTO-NEGOTIATION

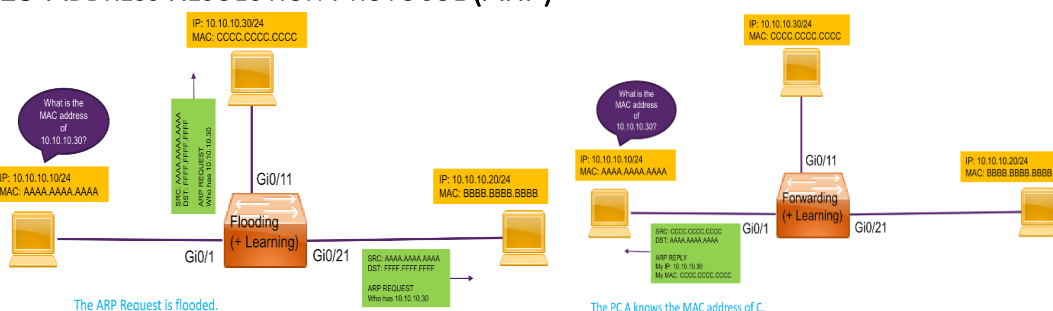
Dieses Protokoll handelt automatisch die Geschwindigkeit (10/100/1000 Mbit/s) und Full-/Half-Duplex aus.

2.12 SWITCHING

Switching basiert auf MAC-Adressen. Es wird eine Tabelle geführt, welche MAC Adressen an welchen Switchports angeschlossen sind.



2.13 ADDRESS RESOLUTION PROTOCOL (ARP)



Jeder Host und Router führt selbst einen ARP-Cache (Tabelle mit IPs und zugehörigen MACs). Ein Sicherheitsrisiko ist ARP Spoofing. Dabei sendet der Angreifer eine ARP-Antwort, obwohl er diese IP nicht hat und bekommt so Traffic, der für eine andere IP bestimmt war, beispielsweise für den Default Gateway.

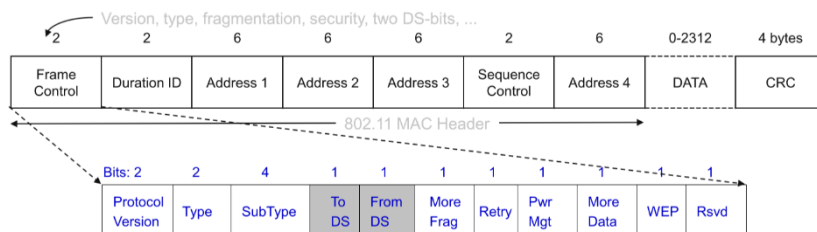
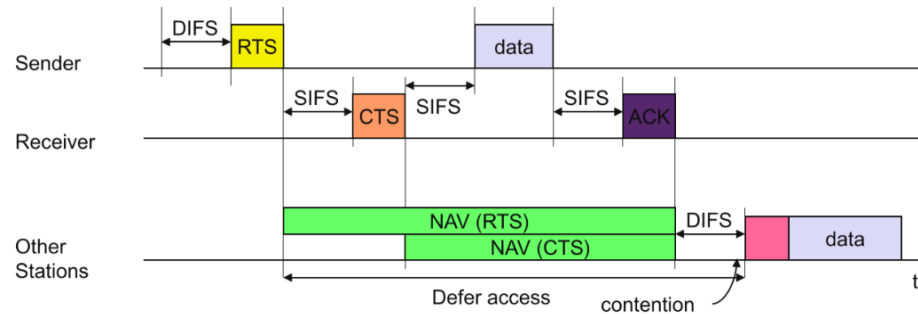
2.14 WIRELESS

2.14.1 Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)

Bei WLAN reicht CSMA/CD nicht aus, weil es ein Hidden Node geben könnte, welches zwar mit dem AP kommunizieren kann, aber nicht mit dem Client. Daher müssen Client und AP das OK zum Senden geben.

2.14.2 Distributed Coordination Function (DCF) & Network Allocation Vector (NAV)

Wenn eine Station kein ACK empfängt, wird das Frame erneut gesendet.



Scenario	To DS	From DS	Address 1	Address 2	Address 3	Address 4
Ad-hoc network	0	0	DA	SA	BSSID	-
From AP	0	1	DA	BSSID (AP)	SA	-
To AP	1	0	BSSID (AP)	SA	DA	-
Within DS	1	1	RA (AP 1)	TA (AP 2)	DA	SA

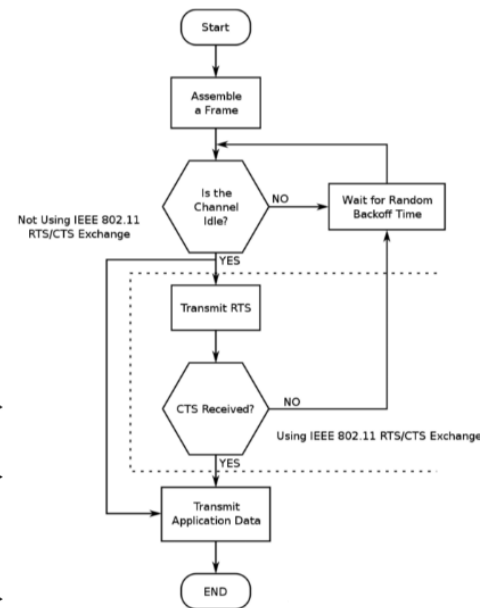
2.14.4 802.11 Management Frames

- Beacon: Timestamp, Beacon Interval, Capabilities, ESSID, (Extended) Supported Rates, Channel, Traffic Indication Map (TIM), Country, Indoor/Outdoor, Parameters
- Probe Request: ESSID, Capabilities, Supported Rates
- Probe Response: das gleiche wie ein Beacon, TIM fehlt jedoch
- Association Request: Capability, Listen Interval, ESSID, Supported Rates
- Association Response: Capability, Status Code, Station ID, Supported Rates
- Reassociation Request: Capability, Listen Interval, ESSID, Supported Rates, Current AP Address
- Reassociation Response: Capability, Status Code, Station ID, Supported Rates
- Disassociation: Reason Code
- Authentication: Algorithm, Sequence, Status, Challenge Text
- Deauthentication: Reason

2.14.5 Roaming von Access Point A zu Access Point B

Probe Request an A & B, Probe Response von A & B, Client merkt, dass B besser ist, Reassociation Request an B, Reassociation Response von B, Disassociation an A

Da dieser Vorgang langsam ist, gibt es Fast Roaming (802.11r). Der Handshake mit AP B wird gemacht bevor der Client roamed. Das erlaubt dem Client und AP, die Pairwise Transient Key (PTK) Berechnung im Voraus zu machen, was die Roaming-Zeit reduziert, der Client hat den PTK dann schon, wenn er die Reassociation macht. Fast Roaming funktioniert Over-the-Air oder Over-the-DS (Kabel zwischen APs).



2.14.3 802.11 Frame MAC Header

Type: Control Frame, Mgmt Frame oder Data Frame

Sequence Control: Schutz v. doppelt. Frames
CRC: Cyclic Redundancy Check (Checksumme)

AP: Access Point

SSID = ESSID: WLAN-Name

BSSID: Basic Service Set Identifier (AP MAC)

DS: Distribution System

DA: Destination Address

RA: Receiver Address

SA: Source Address

TA: Transmitter Address

2.15 802.1D SPANNING TREE PROTOCOL (STP)

Immer wenn es mehr als einen möglichen Pfad zu einem Switch gibt, würden Loops entstehen, welche das Netzwerk lahmlegen. Da Ethernet keinen eingebauten Schutz hat, ist STP standardmässig aktiviert auf Switches. Per-VLAN Spanning Tree (PVST) funktioniert für jedes VLAN separat, in den 2 Bytes Priority der Bridge ID befinden sich 12 Bits für den VLAN-Tag. Bestimmungs-Algorithmus (betrifft jeweils das Gegenüber):

1. Tiefste Root Path Cost (Summe Verbindungen bis Root Bridge, 1Gbit/s: 4, 100Mbit/s: 19, 10 Mbit/s: 100)
2. Tiefste Bridge ID (4 Bit Priority (Default 32768) + 12 Bit VLAN Tag + 6 Bytes MAC-Adresse)
3. Tiefste Port ID (4 Bits Priority + 12 Bits Port Nummer)

STP-Algorithmus:

1. Alle Switches denken sie sind Root Bridge und senden Bridge Protocol Data Units (BPDU) mit ihrer Bridge ID an die Multicast MAC-Adresse für Switches 01:80:c2:00:00:00
2. Die niedrigste Bridge ID wird Root Bridge, es kann nur eine Root Bridge pro Netzwerk geben, alle Ports der Root Bridge werden Designated Ports (DP)
3. Alle Non-Root Switches berechnen für jeden ihrer Ports die Root Path Cost
4. Die Non-Root Switches **bestimmen** genau einen Root Port (RP)
5. Alle Ports gegenüber einem RP werden DP
6. Bei der restlichen Verbindung vergleichen sich die verbundenen beiden Switches mit dem **Bestimmungs-Algorithmus**, der Verlierer bekommt einen Non-Designated Port (NDP)
7. Alle Ports gegenüber einem NDP werden DP

Port States:

- Blocking: Port erhält BPDUs, versendet aber keine. Daten werden keine übertragen.
- Listening: Port erhält und sendet BPDUs. Daten werden keine übertragen.
- Learning: ähnlich wie Listening, Port lernt aber die angeschlossenen MAC-Adressen
- Forwarding: Port erhält und sendet BPDUs. Daten werden übertragen.
- Disabled: Gerät ist ausgesteckt oder Port ist manuell deaktiviert

Timers (Cisco Default Wert in Klammer):

- Hello (2s): In diesem Intervall versendet die Root Bridge BPDUs
- Max age (20s): Wenn so lange keine BPDU gekommen ist, wird der STP-Algorithmus ausgeführt
- Forward delay (15s): Zeit, während der der Port im Listening und Learning State bleibt

Ablauf Gerät einstecken: 20s Blocking – 15s Listening – 15s Learning – Kommunikation (insg. 50s)

Wenn Links up/down gehen oder ein neuer Switch eingesteckt wird passiert folgendes:

1. Betroffener Switch sendet einen Topology Change Notification (TCN) BPDU via RP an die Root Bridge
2. Root Bridge setzt Topology Change Flag in BPDUs, welche alle *Hello Timer* an alle Switches gesendet werden
3. Alle anderen Switches setzen das TTL ihrer Bridge Table von Default 300s auf den *Forward Delay Timer*
4. STP-Algorithmus wird ausgeführt

Direkter Link Failure: 2x Forward Delay Unterbruch (Listening → Learning → Forwarding)

Indirekter Link Failure (wird von Timers bemerkt): Hello + Max age + 2x Forward Delay Unterbruch

PortFast: Kann bei Clientports aktiviert werden, keine TCNs und Port geht direkt in Forwarding State

2.16 802.3AD LINK AGGREGATION PROTOCOL (LACP): PORT AGGREGATION WITH ETHERCHANNEL

2 – 8 parallele Verbindungen zwischen Switches können zu einer logischen Verbindung (Port channel interface) zusammengefasst werden, es können auch bis zu 16 Verbindungen zusammengefasst werden, dann bleiben aber bis zu 8 im Standby (nach Port ID). Die Last wird auf die Verbindungen verteilt & bei einem Link Failure hat man nur einen Unterbruch von wenigen ms.

LACP active: Switch fragt Partner an für EtherChannel, LACP passive: EtherChannel wird nur aktiviert, wenn der Partner anfragt

Die Frames werden nicht gleichmässig verteilt sondern aufgrund eines LB-Algorithmus. Folgende Optionen gibt es: dst-ip, dst-mac, src-dst-ip, src-dst-mc, src-ip, src-mac

2.17 VLANs

Access Port: Ports werden einem VLAN zugewiesen. Nur Ports im gleichen VLAN können miteinander kommunizieren.

Trunk Port: Mehrere VLANs sind diesem Port zugewiesen, die Pakete werden mit einem 802.1Q VLAN tag versehen, damit der andere Switch die Pakete zuordnen kann.

Native VLAN (Cisco Default 1): Frames in diesem VLAN werden auf einem Trunk Port ohne Tag versendet

Pro VLAN wird ein anderes Subnet verwendet, Kommunikation wird durch einen Router oder L3-Switch ermöglicht.

Bei Routern wird oft Router-on-a-Stick verwendet, dabei ist der Router über nur ein Kabel an einen Trunk Port angeschlossen.

3 LAYER 3

3.1 PROTOKOLLE & GERÄTE

Protokolle: Internet Protocol (IP) Adresse, Internet Control Message Protocol (ICMP), IPsec, Daten sind Pakete

Geräte: Router

3.2 ICMPv4

Types: 0: Echo reply, 3: Destination unreachable, 8: Echo, 11: TTL exceeded, 30: traceroute

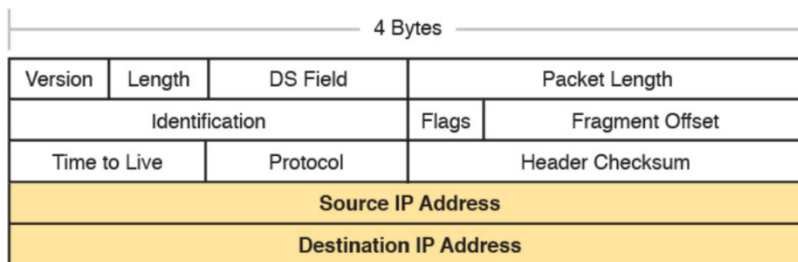
Codes: 0: Network unreachable, 1: Host unreachable, 2: Protocol unreachable, 3: Port unreachable

Traceroute: Host schickt ICMP Type 8 Code 0 mit TTL=1, Router antwortet mit Type 11 Code 0, dann TTL=2, usw.

3.3 IPv4

IPv4 ist ein Best-Effort Protokoll. Es ist nicht zuverlässig, weil es den Flow nicht tracken kann und Fehler nicht erkennt oder behebt, dafür ist L4 mit TCP zuständig. Es ist Medium-unabhängig, L2 kümmert sich darum.

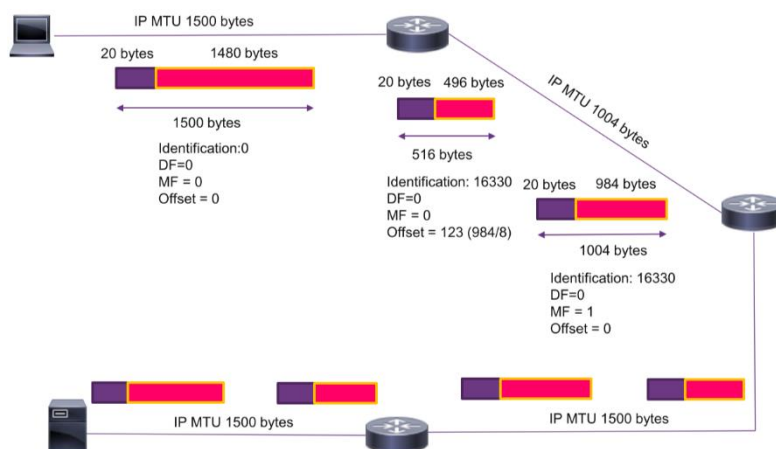
3.3.1 Header



- Version: 4
- Length: Headerlänge inkl. optionale Fields
- DS Field: Differentiated Services für Quality-of-Service (QoS)
- Packet Length: gesamte Grösse des Pakets inkl. Header und Daten

- Identification, Flags, Fragment Offset: IP Fragmentierung
- TTL: Time-to-Live (Default 255) bei jedem Hop (Router) wird -1 gerechnet, bei 0 wird das Paket verworfen
- Protocol/Next Header: Verwendetes Protokoll bei den Daten (TCP 0x06/UDP 0x11/ICMP 0x01)
- Header Checksum: Checksumme über den Header

3.3.2 Fragmentierung



- Identification: alle Pakete mit der gleichen ID sind Fragmente des gleichen ursprünglichen Pakets
- Flags: 1. Bit immer 0, 2. Bit = 1 = Don't Fragment (DF), 3. Bit = 1 = More Fragments on the way (MF)
- Fragment Offset: Daten in Bytes der vorherigen Fragmente addiert / 8
- Achtung: Gesamtlänge der Fragmente muss immer ein Vielfaches von 8 sein, evtl ist sie also kleiner als die MTU.

3.3.3 Subnetting

Jede IP-Adresse hat einen Netz- und Hostanteil. Die Verteilung der beiden Anteile wird durch die Subnetz Maske oder Prefix Length (z.B. /24) definiert. Bei jedem Subnetz ist die erste Adresse die Netzadresse und die letzte Adresse die Broadcast Adresse, man muss also bei den Anzahl Hosts zwei abziehen.

Früher, als es noch genug IPv4 Adressen gab, wurden classful Netzwerke an Unternehmen verteilt:

- Klasse A: 1.0.0.0/8 – 126.0.0.0/8 (bis 16 Mio. Hosts)
- Klasse B: 128.0.0.0/16 – 191.255.0.0/16 (bis 65K Hosts)
- Klasse C: 192.0.0.0/24 – 223.255.255.0/24 (Bis 254 Hosts)

Bei der heutigen Adressknappheit wurden private Adressblöcke eingeführt, welche hinter einem NAT/PAT sind:

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

Loopback-Adressen: 127.0.0.0/8, 127.0.0.1 für localhost

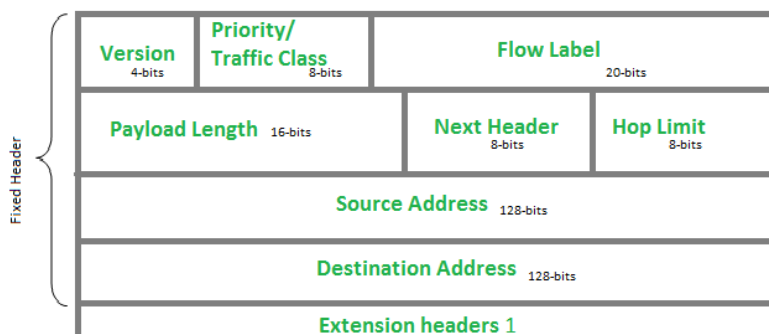
Link-Local Adressen: werden von Windows generiert für lokale Kommunikation ohne DHCP

Prefix Length	Subnet Mask	# of hosts	# of subnets in /8	# of subnets in /16	# of subnets in /24
/8	255.0.0.0	16'777'214	1	-	-
/9	255.128.0.0	8'388'606	$2 = 2^{(9-8)}$	-	-
/10	255.192.0.0	4'194'302	4	-	-
/11	255.224.0.0	2'097'150	8	-	-
/12	255.240.0.0	1'048'560	16	-	-
/13	255.248.0.0	524'286	32	-	-
/14	255.252.0.0	262'142	64	-	-
/15	255.254.0.0	131'070	128	-	-
/16	255.255.0.0	65'534	256	1	-
/17	255.255.128.0	32'766	512	$2 = 2^{(17-16)}$	-
/18	255.255.192.0	16'382	1024	4	-
/19	255.255.224.0	8'190	2048	8	-
/20	255.255.240.0	4'094	4096	16	-
/21	255.255.248.0	2'046	8192	32	-
/22	255.255.252.0	1'022	16384	64	-
/23	255.255.254.0	510	32768	128	-
/24	255.255.255.0	254	65536	256	1
/25	255.255.255.128	126	131072	512	$2 = 2^{(25-24)}$
/26	255.255.255.192	62	262144	1024	4
/27	255.255.255.224	30	524288	2048	8
/28	255.255.255.240	14	1'048'562	4096	16
/29	255.255.255.248	6	2'097'152	8192	32
/30	255.255.255.252	2	4'194'304	16384	64

3.4 IPv6

3.4.1 Header

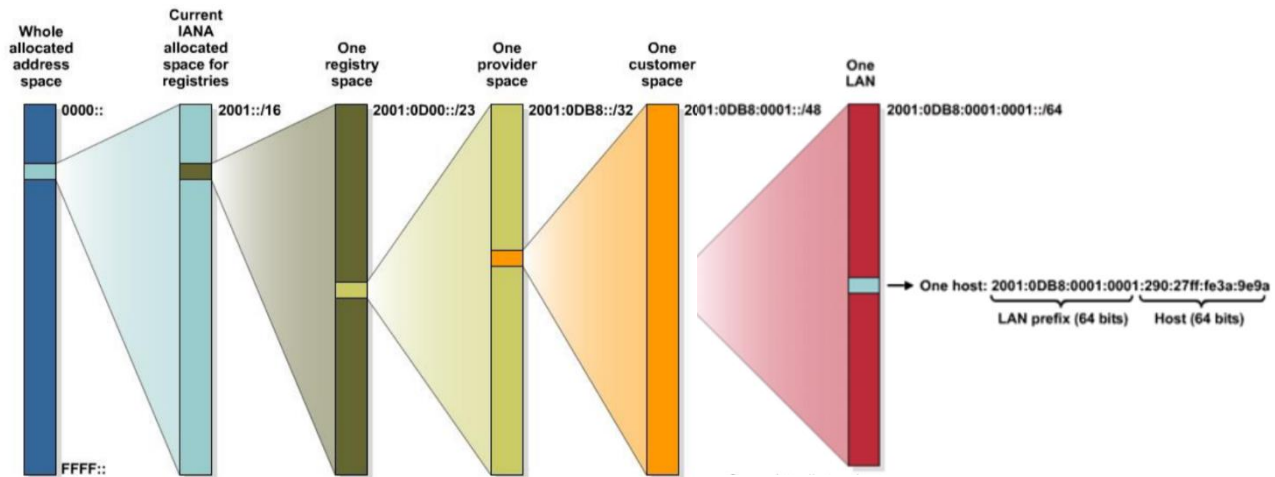
Vorteile gegüb. V4: Genug Adressen, einfacheres Subnetting, kein NAT, End-to-End Transparenz, fördert Innovation



- IPv6 Header Grösse: fix 40 Bytes
- Version: 6
- Traffic Class: DS Field von IPv4 (für QoS)
- Flow Label: für spezielle QoS Rules, normalerweise 0
- Payload Length: Grösse Paket ohne Header
- Next Header: Gibt an, ob TCP/UDP oder ein bestimmter Extension Header kommt
- Hop Limit: TTL von IPv4

- Fragmentation gibt es nicht, stattdessen führt jeder Host eine PATH MTU Discovery durch, so weiss er was für eine MTU er verwenden muss für jede IPv6 Adresse. Ein IPv6 Router schickt dem Client eine ICMPv6 Packet Too Big message (type 2 code 0), wenn das Package zu gross ist.
- Checksumme gibt es nicht, weil das TCP/UDP schon haben

3.4.2 Adressen

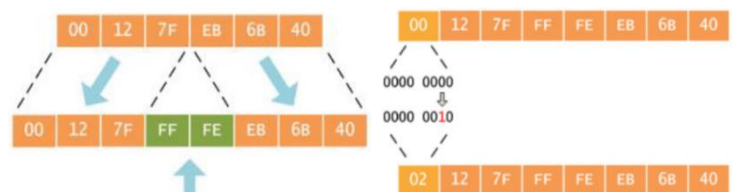


Vereinfachung: Führende Nullen können weggelassen werden, Nullerblöcke nacheinander können einmal pro Adresse mit :: ersetzt werden

Beispiel: 2001:0DB8:0000:1133: 0000:0000:0000:0200 → 2001:DB8:0:1133::200

Bei EUI-64 wird aus der MAC-Adresse die 64 Host Bits der IPv6 Adresse generiert:

1. FFFE in der Mitte einfügen
2. Siebtes Bit flippen (0→1, 1→0)



Ein IPv6 Gerät hat meist mehrere Adressen:

- Global Unicast: weltweit einzigartig und routable, stammt aus dem Range 2000::/3, Generierungs-Optionen:
 - Manuell
 - EUI-64
 - Stateless autoconfiguration (SLAAC): Prefix und Prefix Length kommt von RA, der Rest von EUI-64
 - SLAAC+ stateless DHCP: gleich wie SLAAC, jedoch ist DHCPv6 vorhanden für Optionen wie DNS
 - Stateful autoconfiguration: Normales DHCPv6
- Link Local: muss für jedes NIC vorhanden sein, kommt aus dem Range fe80::/10 (meist fe80::/64), Scope ist auf das lokale Netz beschränkt, Generierungs-Optionen: EUI-64 oder manuell, wird gebraucht für NDP
- Unique local address: wird verwendet für Kommunikation in mehreren Netzwerken, ist aber nicht im Internet routable, aus Range fc00::/7

Spezielle Unicast Adressen:

- Localhost: ::1
- Unspecified address: ::/128
- Dokumentations-Prefix: 2001:0db8::/32
- Discard-Prefix: 0100::/64
- Default Route/Unspecified: ::/0

Spezielle Multicast Adressen:

- Ff02::1: alle Nodes (MAC dazu: 33:33:00:00:00:01)
- Ff02::2: alle Router (MAC dazu: 33:33:00:00:00:02)
- Solicited Node: ff02::1:ff: + letzte 24 Bit der Unicast Adresse
Beispiel: FE80::200:CFF:FE3A:8B18 → FF02::1:FF3A:8B18
ist für JEDE IPv6 Ad. vorhanden, wird für ND/DAD verwendet

3.4.3 Neighbor Discovery (ARP-Ersatz zur MAC-Adressenfindung)

1. A möchte ein IPv6 Paket an die globale oder Link-local IPv6 Adresse von B schicken
2. A berechnet die Solicited Node (SN) Multicast Adresse von B
3. Neighbor Solicitation senden (Src=IPv6 Adresse von A, Dst=SN von B, Data=MAC von A, Query=MAC von B?)
4. Neighbor Advertisement senden (Src=IPv6 Adresse von B, Dst=IPv6 Adresse von A, Data=MAC von B)

Duplicated Address Detection (DAD) funktioniert ähnlich wie Neighbor Discovery. Bei Schritt 3 ist die Destination jedoch die SN von sich selbst, wenn keine Antwort kommt, ist die Adresse unique.

3.4.4 Autokonfiguration

Die Autokonfiguration wird mit Router Solicitations (RS) und Router Advertisements (RA) gemacht:

- Hosts senden RS beim Booten, um RAs zu erhalten (Src=unspecified, Dst=alle Router)
- RA: Router Konfiguration, wird periodisch und nach RS gesendet (Src=Router Link local Adresse, Dst=alle Nodes, Data=options, prefix, lifetime, autoconfig flag)

3.5 ICMPv6

Types: 9: RA, 10: RS

Codes: 0: No route to destination, 1: Communication with the destination is administratively prohibited (e.g. firewall), 2: Beyond scope of the source address, 3: Address unreachable, 4: Port unreachable

Darf nicht blockiert sein, sonst funktioniert nichts mehr, weil ND, DAD und Autokonfiguration nicht mehr funktioniert

3.6 STATISCHES ROUTING

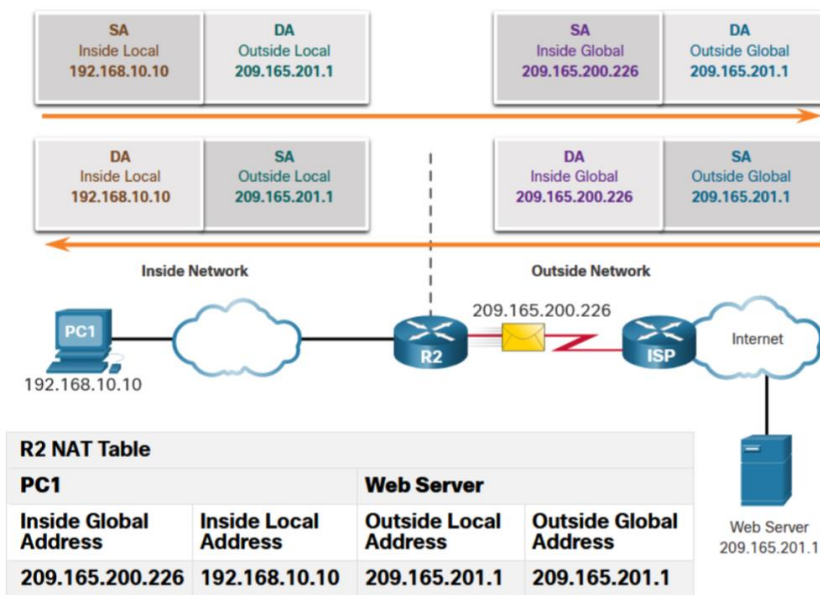
Es gibt drei Arten von Routen:

- Directly-connected: Diese Netzwerke sind direkt am Router angeschlossen.
`ip route <netzwerk-adresse> <subnetz-maske> <interface-name>`
`ipv6 route <prefix>/<prefix-length> <interface-name>`
- Remote: Diese Netzwerke sind an einem anderen Router angeschlossen.
`ip route <netzwerk-adresse> <subnetz-maske> <next-hop>`
`ipv6 route <prefix>/<prefix-length> <next-hop>`
- Default Route: Wenn ein Netzwerk nicht gefunden wird, geht das Paket dorthin.
`ip route 0.0.0.0 0.0.0.0 <next-hop>`
`ipv6 route ::/0 <next-hop>`

Routen können auch zusammengefasst werden. Beispiele:

192.168.0.0/24 + 192.168.1.0/24 = 192.168.0.0/23 (passt gerade perfekt)

2001:db8:ABBA:0::/64 + 2001:db8:ABBA:FFF::/64 = 2001:db8:ABBA::/48 (Zusammenfassung ist breiter gefasst)



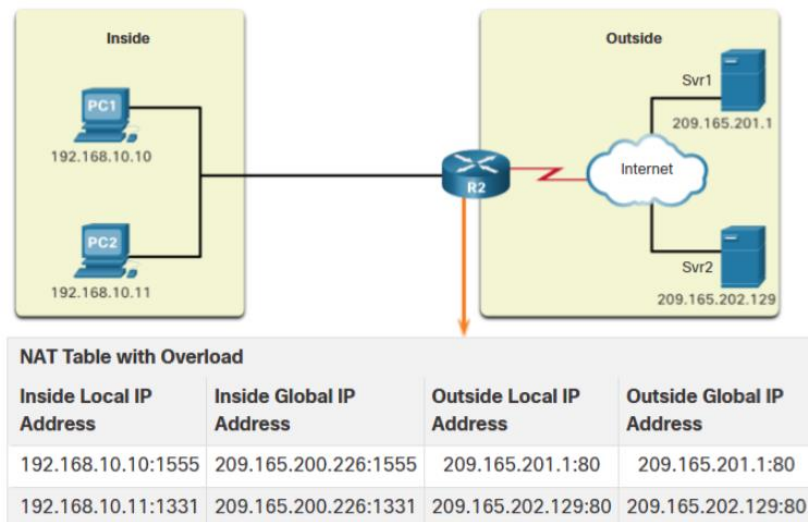
3.7 DYNAMIC / STATIC NETWORK ADDRESS TRANSLATION (NAT)

Beim static NAT ist für jede private Adresse eine öffentliche Adresse in der NAT-Tabelle eingetragen.

Beim dynamic NAT hat man einen Pool von öffentlichen IPs. Wenn ein interner Client ins Internet möchte, wird ihm eine öffentliche IP zugeteilt. Man braucht somit so viele public IPs, wie es gleichzeitig User Sessions hat.

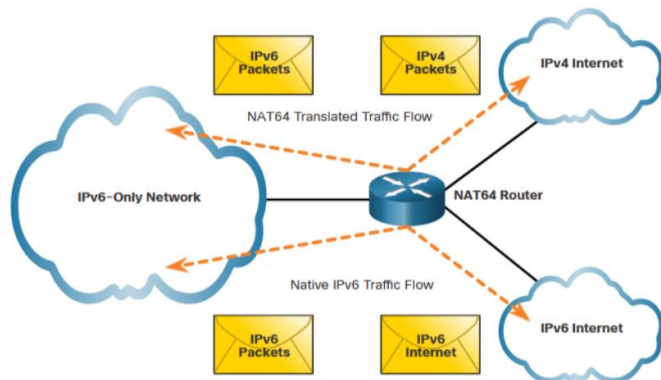
3.8 PORT ADDRESS TRANSLATION (PAT)

Das kommt meistens zu Hause zum Einsatz, es können mehrere private IPs hinter eine einzelne öffentliche IP gemappt werden.



PAT probiert, den ursprünglichen Source Port beizubehalten. Wenn dieser bereits besetzt ist, wird der der nächste freie Port der Gruppe (0-511, 512-1023, 1024-65535) genommen. Wenn alle Ports besetzt sind, kann auch die nächste public IP verwendet werden, sofern man einen Pool konfiguriert hat. Wenn kein Port verwendet wird, beispielsweise bei ICMP, muss das speziell behandelt werden. Bei echos wird beispielsweise aufgrund der Query ID entschieden.

3.9 NAT64



3.10 VOR/NACHTEILE NAT/PAT

Nachteile:

- Forward Delay wird erhöht
- End-to-End Adressierung und Verfolgbarkeit geht verloren
- Einsatz von Tunneling Protokollen wie IPSec wird erschwert
- Applikationen, bei denen die Verbindungsinitiiierung von aussen passiert, können gestört werden

Vorteile:

- IPv4 Adressen sparen
- Konsistenz bei internen Adressen
- Wahre IP der Geräte wird verborgen
- Öffentliche IP kann ändern ohne Einfluss auf die privaten Adressen

3.11 OPEN SHORTEST PATH FIRST (OSPF)

OSPF ist ein offener Standard für dynamisches Routing, der von fast allen Herstellern unterstützt wird. Es ist ein Interior Gateway Protocol (IGP) und Link-State Protokoll. OSPFv3 supportet IPv6 im Gegensatz zu OSPFv2, sie sind nicht kompatibel.

Schritt 1: Jeweils zwei Routern bilden eine OSPF Neighbor Beziehung

Dritter Punkt im Bild und folgendes nur, wenn die Anforderungen erfüllt sind: Area, Timers, Stub Flag, Network Type, MTU, Authentication, Subnet (unless P2P)

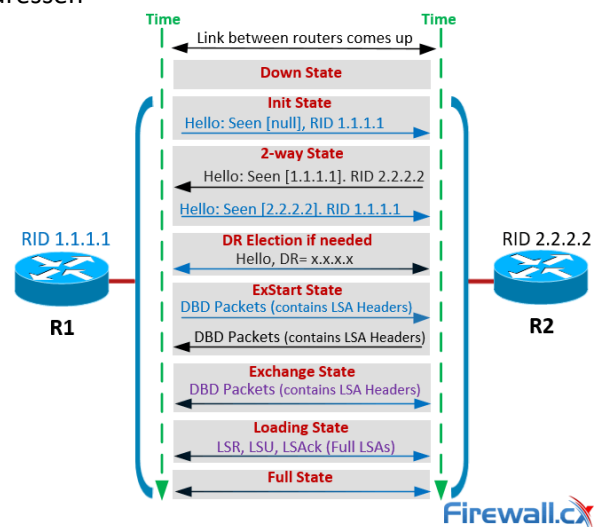
Schritt 2: Die Neighbors tauschen ihre Link-State Database (LSDB) aus. Eine LSDB hat die Spalten Router ID, Neighbor ID, Cost

- Database Descriptor (DBD): alle angeschlossenen Netzwerke
- Link State Request (LSR): ich sehe ein unbekanntes Netzwerk in deinem DBD, sende mir dieses
- Link State Update (LSU): okay, ich sende dir dieses unbekannte Netzwerk
- Link State Acknowledgement (LSAck): Danke habe erhalten

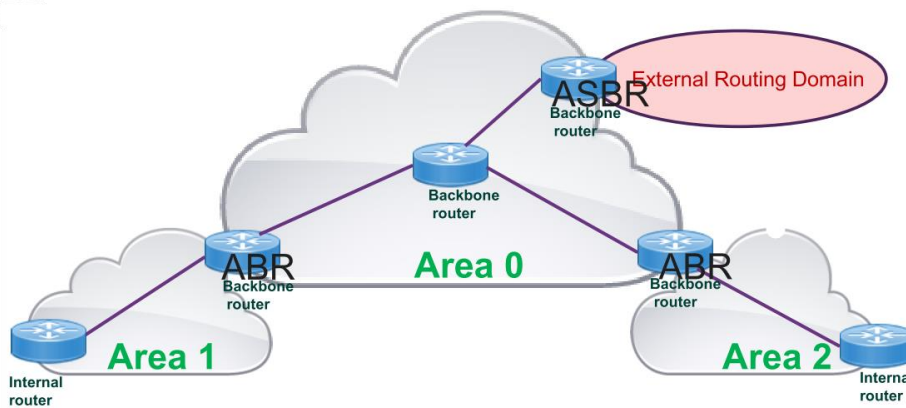
Schritt 3: Der shortest Path wird bestimmt mit dem Dijkstra Algorithmus

1. Beginn der Tabelle (aus Perspektive R9, R9 ist root)
2. Alle Neighbors von R9 in die Candidates schreiben (wenn der zweite Router bereits im Tree ist nicht adden)
3. Die Cost to Root ablesen und in diese Spalte schreiben
4. Niedrigste Cost in den Tree übernehmen
5. Candidates werden aus 2 Gründen gestrichen:
 - a. Der zweite Router (z.B. bei «R1, R2, 3» ist R2 der zweite) ist bereits bei einem Eintrag im Tree zweiter Router
 - b. Es sind zwei Einträge in den Candidates mit dem gleichen zweiten Router, dann werden alle Einträge ausser dieser mit der niedrigsten Cost gestrichen
6. Das Ganze wird wiederholt, bis die Anzahl Einträge im Tree gleich der Gesamtanzahl Router ist

Candidate	Cost from the Root to the Candidate	Nodes within the Tree
R9	R9, 0 ✓	R9, 0
R9, R1, 5 R9, R3, 7	R9, R1, 5 ✓ R9, R3, 7	R9, 0 R9, R1, 5



3.11.1 Router Roles



4 LAYER 4

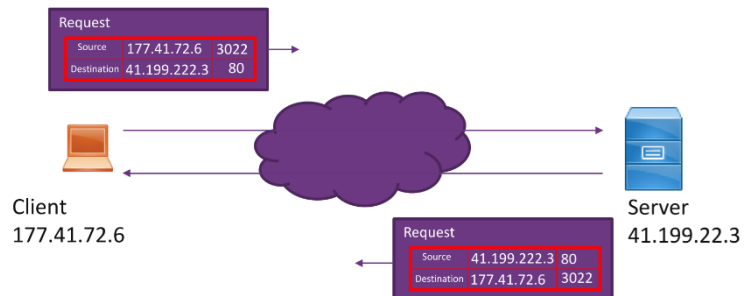
4.1 PROTOKOLLE & GERÄTE

Protokolle User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Daten sind Segmente

Geräte: Firewall

4.2 PORTS

Da Clients gleichzeitig Mails empfangen, surfen und VoIP-Telefonie machen, reicht es nicht, sie nur mit IPs zu adressieren, es braucht zusätzlich noch Ports. Serverdienste laufen normalerweise auf Well-Known Ports und der Client wählt einen zufälligen Port aus dem ephemeral Port Range, welcher irgendwo zwischen 1024 – 65535 liegt. Ein Socket ist die Kombination von IP und Port, z.B. 192.168.1.10:80.



Multiplexing: Daten von mehreren App-Prozessen auf der Senderseite zusammentragen, mit Header versehen und an Empfänger senden

Demultiplexing: Erhaltene Daten dem richtigen App-Prozess zuordnen

Well-Known / Privileged / IANA-manged Ports für Applikationen mit RFC: 0 – 1023

z.B. 20/21 FTP Data/Control, 22 SSH, 23 Telnet, 25 SMTP, 53 DNS, 69 TFTP, 80 HTTP, 161/162 SNMP/Trap, 443 HTTPS

IANA-registrierte Ports für Applikationen ohne RFC: 1024 – 49151

Private / dynamische Ports ohne Registrierungen: 49152 – 65535

4.3 USER DATAGRAM PROTOCOL (UDP)

Sehr simples Transport Protokoll, keine Connections, unidirektional, nicht zuverlässig, Daten können verloren gehen, stream-orientiert, Beispiele: DNS, BOOTP, DHCP, TFTP (hat selbst Acks), SNMP, RIP

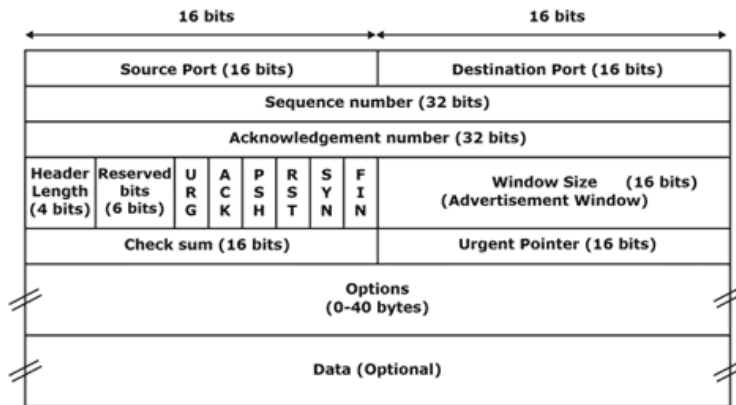
- Src/Dst Port
- Length: Grösse des gesamten Datagramms, also Header + Daten
- Checksum: Checksumme über das gesamte Datagramm



4.4 TRANSMISSION CONTROL PROTOCOL (TCP)

Verbindungsorientiert, bidirektional (Partner können senden, egal wer die Verbindung erstellt hat), mehrere Verbindungen zwischen den gleichen Partnern möglich, zuverlässig, mit ACKs, Daten können nicht verloren gehen, nimmt einen Block von Daten und teilt ihn in TCP-Segmente, damit Messages für IP entstehen

4.4.1 Header

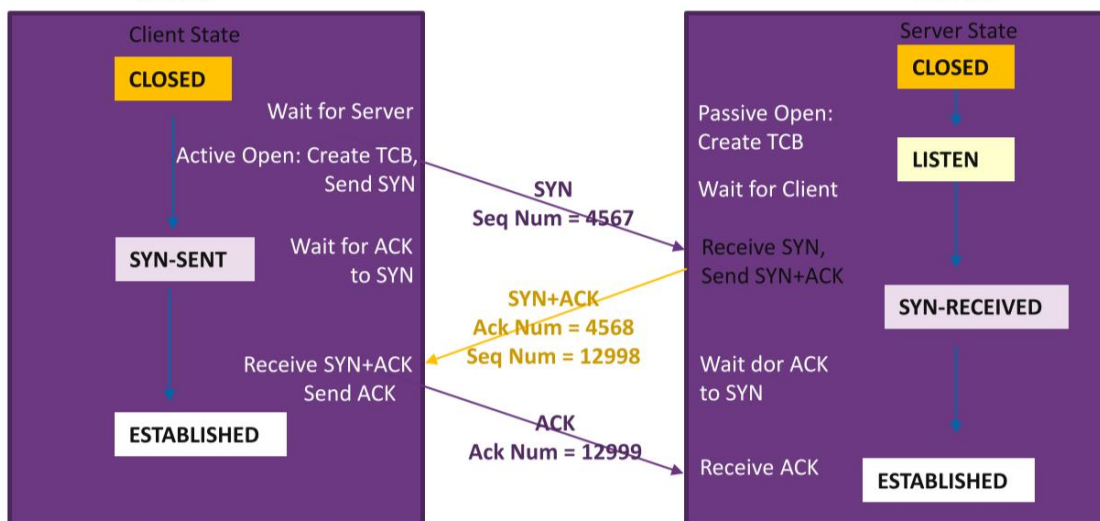


- Src/Dst Port
- Sequence Number: hilft bei Sortierung der Segmente, da diese in falscher Reihenfolge ankommen könnten
- Ack Number: Sequence Number, die der Sender als nächstes erwartet
- Header Length
- Reserved Bits: für Zukunft, alles 0
- URG: 1 = Urgent
- ACK: 1 = aktiviert Auswertung Ack number
- PSH: 1 = Push, nicht buffern und Sliding

Window deaktiviert, z.B. bei Telnet

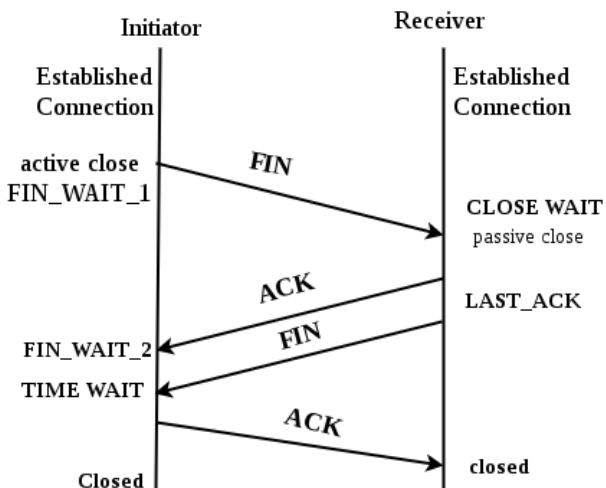
- RST: 1 = Reset, Verbindung abbrechen nach technischen Problemen
- SYN: 1 = Sync, Verbindung initiieren
- FIN: 1 = Finish, Verbindung beenden
- Advertisement Window
- Checksum: Checksumme über Header + Daten
- Urgent Pointer: Gibt Position des ersten Bytes des Datenstroms an
- Options: optionale weitere Verbindungsdaten

4.4.2 Connection Establishment



- TCB = Transmission Control Block
- 4567 & 12998: Initial Sequence Numbers (ISN) von Client bzw. Server, zufällig vom OS generiert

4.4.3 Connection Termination



In der Grafik links sieht man eine saubere Termination. Es kann jedoch manchmal zu Problemen kommen, beispielsweise halb-offene Connections oder unerwartete Messages. Dann sendet das Gerät, welches ein Problem erkannt hat, ein Segment mit der RST Flag gesetzt.

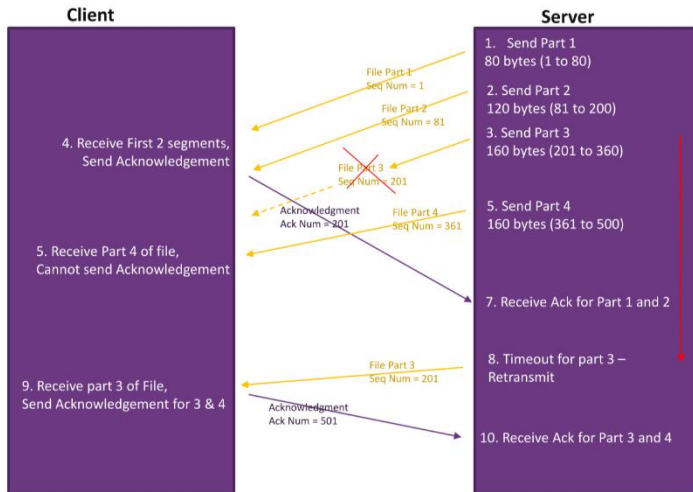
4.4.4 Maximum Segment Size (MSS)

Gewisse schwache Geräte haben einen limitierten Buffer und möchten die Segment-Grösse limitieren. Kompromiss zwischen:

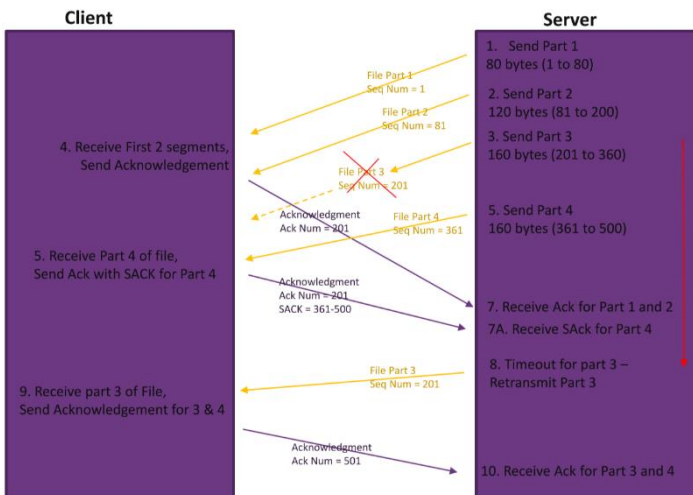
- **Overhead:** MSS=40B, IP-Header=20B, TCP-Header=20B, also 50% Header, 50% Header-Overhead, je grösser desto effizienter
- **Fragmentation:** Wenn MSS > MTU – 40B IP/TCP-Header, dann werden Segmente fragmentiert, zu gross = Fragmentation

Die Default MSS ist 536B. Der Grund ist, dass die minimale MTU 576B ist, 40B für TCP/IP-Header abgezogen sind 536.

4.4.5 Acknowledgement & Retransmission



1. Von jedem gesendeten Segment wird eine Kopie in die Retransmission Queue platziert
2. Wenn ein ACK vor dem Retransmission Timeout ankommt, wird das Segment aus der Retransmission Queue entfernt
3. Wenn kein ACK ankommt, wird nach dem Retransmission Timeout automatisch retransmitted



Wenn jedes Segment Acknowledget werden muss, generiert das sehr viel Overhead, daher gibt es Selective Acknowledgement (SACK).

4.4.6 Sliding Window

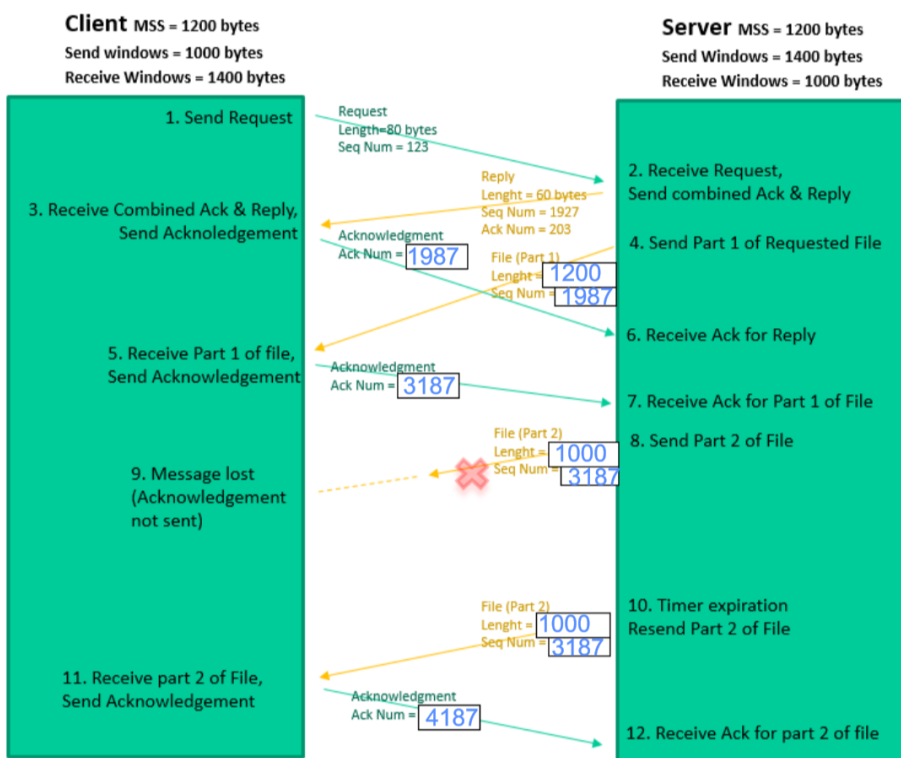
Es gibt vier Kategorien von Bytes:

- 1: Bytes gesendet und Acknowledged
- 2: Bytes gesendet und noch nicht Acknowledged
- 3: Bytes noch nicht gesendet, für die der Empfänger bereit ist
- 4: Bytes noch nicht gesendet, für die der Empfänger noch nicht bereit ist

Send window: Kategorien 2 + 3

Usable window: Kategorie 3

Wenn ein Gerät alle Bytes im usable window gesendet hat, wurden alle Bytes von Kategorie 3 zu 2 verschoben. Die Grösse des Send window ist also immer gleich und die Grösse des usable window kann 0 sein. Für jedes acknowledged Byte (Verschiebung von 2 zu 1) kommt dann ein Byte aus 4 zu 3.

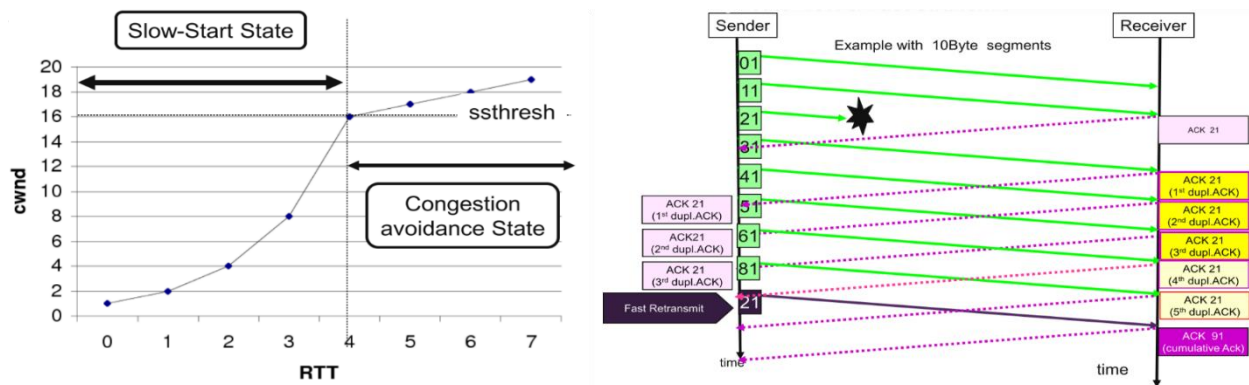


4.4.7 Slow Start, Duplicate ACK, Fast Retransmit, Fast Recovery

Das Ziel von Slow Start ist, das congestion window (cwnd = send window) so gross wie möglich zu machen, ohne das Netzwerk zu überlasten. Für jedes angekommene ACK wird ein oder mehr MSS addiert. Immer wenn ein Packet Loss (kein ACK) auftritt, wird das cwnd halbiert.

Sobald der slow start threshold (sssthresh) erreicht ist, wird für jede Round Trip Time (RTT) ein MSS addiert. Halbiert wird nicht mehr.

Wenn Fast Retransmit verwendet wird, um ein verlorenes Segment nochmals zu senden, verwendet das Gerät Congestion Avoidance, benutzt aber vorher nicht Slow Start. So wird die Performance verbessert.



5 LAYER 5

Dieses Layer erstellt und verwaltet den Dialog zwischen Source und Destination Applications.

5.1 PROTOKOLLE

Internet Small Computer System Interface (iSCSI), Interprocess Communication, Secure Socket Layer (SSL), Transport Layer Security (TLS)

6 LAYER 6

Dieses Layer ist für die Formatierung, Darstellung, (De-)Komprimierung, Verschlüsselung und Entschlüsselung von Applikationsdaten verantwortlich.

6.1 PROTOKOLLE

MOV, GIF, JPG und PNG, ASCII

7 LAYER 7

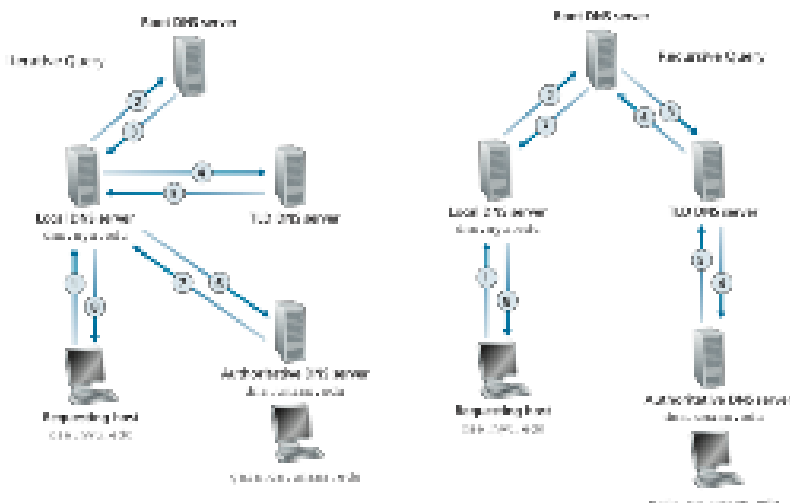
Dieses Layer ist die Schnittstelle zwischen Applikationen.

7.1 PROTOKOLLE

HTTP, FTP, TFTP, IMAP, DNS, DHCP, IP-Telefonie, Firewall L7 Deep Packet Inspection

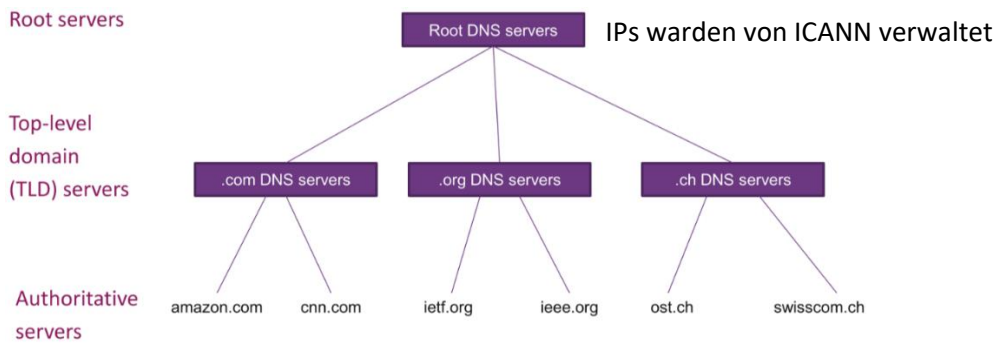
7.2 DNS

7.2.1 Iterative und Recursive Queries



12 Bytes Header

Reverse-DNS ist Anti-Spam



7.2.2 Resource Records

DNS Resource Records (RRs) enthalten die Informationen, die bei einem DNS Query abgefragt werden. Er besteht aus 6 Elementen:

- Name: Der Domainname (z.B. www)
- Time To Live (TTL, optional): Wie lange der Record gecacht werden soll in Sekunden, 0 um Caching zu verhindern
- Class=pref: Protokollgruppe, mögliche Werte: IN (meistens), CH (selten), HS (selten), CSNET (deprecated)
- Type: RR-Type, wichtigste Types:
 - A: Name=Hostname, Value=IPv4 Address
 - AAAA: Name=Hostname, Value=IPv6 Adresse
 - CNAME: Name=Alias-Hostname, Value=Hostname
 - MX: Name=Domainname, Value=Priorität, Hostname des Mailservers
 - NS: Name=Domainname, Value=Hostname des autoritativen Nameservers (bei TLD und Auth Serv.)
- Value=RDATA: unterschiedlicher Value je nach Type

Typen von DNS messages: query, reply, zone transfer

7.2.3 Beispiel Zone File

\$ORIGIN example.com.

\$TTL 86400

```

@      IN      SOA      dns1.example.com.  hostmaster.example.com. (
                                2001062501 ; serial
                                21600      ; refresh after 6 hours
                                3600       ; retry after 1 hour
                                604800    ; expire after 1 week
                                86400 )   ; minimum TTL of 1 day

      IN      NS       dns1.example.com.
      IN      NS       dns2.example.com.
      IN      MX       10    mail.example.com.

dns1    IN      A       10.0.1.1
dns2    IN      A       10.0.1.2
server  IN      A       10.0.1.3
www     IN      CNAME   server
  
```

7.3 DHCP

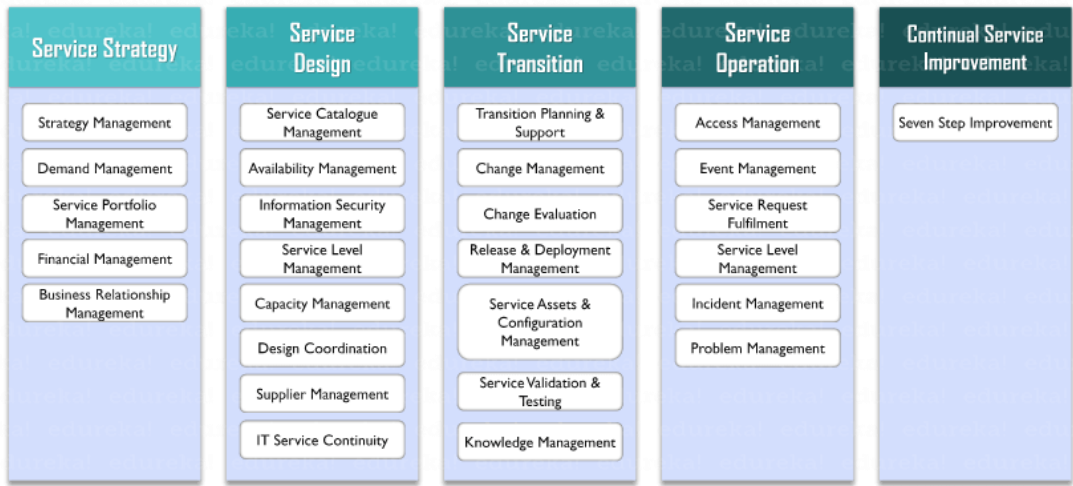


- Discover: L2-Src=Client-MAC, L2-Dst=ff:ff:ff:ff:ff:ff, L3-Src=0.0.0.0, L3-Dst=255.255.255.255
- Offer: L2-Src=Server-MAC, L2-Dst=Client-MAC, L3-Src=Server-IP, L3-Dst=Client-IP, UDP-Src/Dst=67/68
- Request: L2-Src=Client-MAC, L2-Dst=ff:ff:ff:ff:ff:ff, L3-Src=0.0.0.0, L3-Dst=255.255.255.255, UDP-Src/Dst=68/67
- Ack: L2-Src=Server-MAC, L2-Dst=Client-MAC, L3-Src=Server-IP, L3-Dst=Client-IP, UDP-Src/Dst=67/68

Wenn der DHCP-Server sich nicht im gleichen Subnetz befindet wie der Client, muss ein DHCP-Relay konfiguriert werden. Dabei wird das Router-Interface und die IP-Adresse des DHCP-Servers angegeben.

8 NETWORK MANAGEMENT

8.1 ITIL



Messbare Daten im Accounting:
Bandbreite,
Datenvolumen,
Transaktionen,
Priorisierung,
Ressourcenverbrauch

8.2 FCAPS

Fault Management	Configuration Management	Accounting Management	Performance Management	Security Management
Fault Detection	Resoure Initialization	Track Service	Performance data collection	Selective resource access
Fault Correction	Network provisioning	Resource usage	Performance data analysis	Access logs
Fault Isolation	Auto-discovery	Accounting limits	Utilization & error rates	Security alarms
Network recovery	Backup & Restore	Combine costs for multiple resources	Consistant performance level	Event reporting
Alarm generation	Resource shut down	Set quotas for usage	Problem Reporting	User access rights checking
Alarm handling	Change Management	Audits	Capacity planning	Compliance
Alarm filtering	Pre-provisioning	Fraud reporting	Maintaining historical logs	Security related information distributions
Alarm correlation	Inventory / asset management			
Diagnostic Tests	Remote Configuration			
Error logging	Software distribution			
Error handling	Job initiation			
Error statistics	Job tracking			

Fault Mgmt Tools:
Syslog, SNMP,
SNMP Traps, Test robots, Intelligent Syslog e.g. Splunk, Alerting und Monitoring Tool e.g. Nagios, Checkmk, PRTG etc., Pikett-Organisation, Ticketing Tool mit Zuweisung und Parent-Child

8.3 PROTOKOLLE

- Simple Object Access Protocol (SOAP): XML-Datenaustausch
- Syslog: Log-/Eventdaten über 514/UDP an zentralen Server senden
- Link Layer Discovery Protocol (LLDP): Identifikation von Nachbargeräten
- Cisco Discovery Protocol (CDP): automatische Auflistung von angeschlossenen Geräten, die ebenfalls CDP unterstützen
- IP SLA: Cisco Feature zum Performance-Monitoring in Echtzeit
- Telnet: Remote Shell
- Secure Shell (SSH): Telnet in sicher
- NETCONF: Konfiguration auf Netzwerkgeräten verwalten
- RESTCONF: NETCONF via HTTP
- gNMI: NETCONF via gRPC
- BGP Monitoring Protocol (BMP): Routes von BGP-Routern erhalten
- Network Time Protocol (NTP): Zeitsynchronisierung
- Precision Time Protocol (PTP): präzise Zeitsynchronisierung

8.4 FLOW PROTOKOLLE (Z.B. ZUM FINDEN VON OVERLOAD-URSACHE)

- NetFlow: L3-Flow Infos von Routern
- IPFIX: Cisco Weiterentwicklung von NetFlow
- sFlow: L2-7-Flow Infos

Definition Flow: Src-IP, Dst-IP, Src-Port, Dst-Port, L3 Protokoll, Type of Service (ToS), Input logical Interface

8.5 SYSLOG

Log-/Eventdaten über 514/UDP an zentralen Server senden

Message Format <PRIORITY>HEADER: MESSAGE

<164>May 16 2022 01:59:59: %ASA-4-106100: abcdef

Cisco Message Format: %FACILITIES-SEVERITY-MNEMONIC: DESCRIPTION

%LINK-3-UPDOWN: Interface Port-channel1, changed state to up

8.6 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

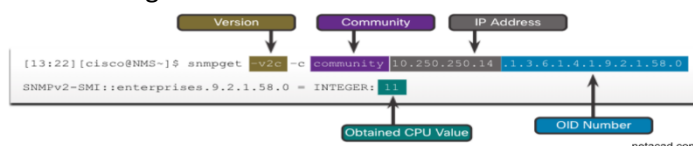
SNMPv1: Auth mit Community String, SNMPv2: v1 + Bulk Request, SNMPv3: User-Auth, Hashing, Encryption

Management Information Base (MIB): Hierarchische Collection von Object Identifiers (OID)

8.6.1 Pull/Push

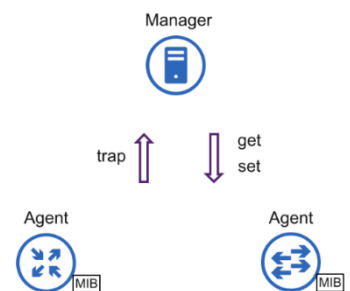
Pull: Der Manager holt sich in einem fixen Intervall die Daten beim Agenten

Push: Der Agent sendet Daten bei einem bestimmten Event an den Manager (SNMP-Trap)



iso(1).org(3).dod(6).internet(1).mgmt(2).mib(1).
system/ip/interfaces/at(1/4/2/3)

1.3.6.1.private(4).Cisco(6)



8.7 DOKUMENTATION

Topologie: L1, L2 und L3

Geräte: Hersteller, Modell, Firmware, Standort

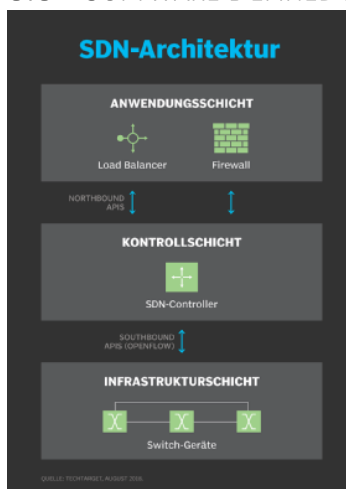
Verbindungen: Medium, Technologie, Geschwindigkeit, Eigenschaften, SLA

Schwierigkeiten: alles wichtige beinhalten, aktuell halten, synchronisieren

Lösungen: geeignete Tools verwenden, automatisieren von Planning, Testing, Implementation und Operation

Die meisten Fehler passieren auf Layer 1: Defekte, Wackelkontakt, zu wenig Strom, Interferenzen

8.8 SOFTWARE DEFINED NETWORKING (SDN)



Application Layer / Anwendungsschicht: Unterstützt die Kontrollschicht mit Services wie Load Balancer oder Firewalls

Control Layer / Kontrollschicht: Gehirn des SDN, der Controller befindet sich auf einem Server, der den Flow und Policies verwaltet

Infrastructure Layer / Infrastrukturschicht: die physischen Geräte des Netzwerks

Funktionen: Functional Isolation (Netzwerkvirtualisierung), Network Control Plane (Entscheidet den Flow der Pakete), Data Plane (realisiert den Flow der Pakete)

Vorteile: ändern der Rules aller Switches zum Upgraden, Downgraden und Blockieren von Paketen, Konfiguration von Kontrolle und Security, End-to-End Sichtbarkeit, Konfiguration passiert nur beim zentralen Controller, Dienste welche normalerweise Hardware erfordern können virtuell betrieben werden