

Netztechnik

Inhaltsverzeichnis

1 - Empfehlungen, Standards und Normen.....	1
1.1 - Einleitung.....	1
1.2 - ANSI (American National Standards Institute).....	1
1.3 - ITU.....	2
1.3.1 - ITU-R.....	2
1.3.2 - ITU-T.....	2
1.3.3 - ITU-D.....	2
1.4 - Internet-Gremien.....	3
1.5 - ICANN.....	4
1.6 - ECMA.....	5
1.7 - IEC.....	5
1.8 - DBP.....	5
1.9 - EIA / TIA.....	6
1.10 - RIPE (Réseaux IP Européens).....	6
1.11 - BS (British Standard).....	6
1.12 - EN.....	7
1.13 - ISO.....	7
1.13.1 - OSI-Modell.....	7
1.14 - IEEE-Normen.....	8
1.15 - RFC's.....	9
1.15.1 - Allgemeines.....	9
1.15.2 - RFC-Lebenszyklus.....	10
1.15.3 - Beispiele bekannter RFCs.....	11
1.15.4 - RFC-Bezugsquellen.....	12
1.15.5 - FAQ's.....	12
1.15.6 - FYI's.....	12
2 - Netztechnik-Grundlagen.....	13
2.1 - Zusammenhang mit Wirtschaft.....	13
2.2 - Grundbegriffe bei der Informationsverarbeitung.....	14
2.2.1 - Informationssysteme.....	14
2.2.2 - Information.....	15
2.2.3 - Anforderungen an Informationssysteme.....	16
2.2.3.1 - Geschwindigkeit.....	16
2.2.3.2 - Verfügbarkeit.....	17
2.2.3.3 - Kosten.....	18
2.2.3.4 - Qualität.....	18
2.2.3.5 - Sicherheit.....	18
2.3 - Kommunikationsmodelle.....	18
2.3.1 - Terminal-Systeme.....	19
2.3.2 - Client-Server-Modell.....	19
2.3.3 - Peer-to-Peer-Modell.....	20
2.3.4 - E-Commerce.....	20
2.3.5 - Ubiquitous Computing.....	20
2.4 - Aufbau von Netzwerken.....	21
2.5 - Beziehungsarten.....	23
2.6 - Kommunikationsformen.....	23
2.7 - Verkehrsarten.....	24
2.8 - Betriebsarten der Nachrichtenübertragung.....	25
2.9 - Technisches Übertragungskonzept.....	26
2.9.1 - Broadcast-Netzwerke (Diffusionsnetze).....	26
2.9.2 - Punkt-zu-Punkt-Netzwerke (Teilstreckennetze).....	27
2.10 - Klassifikation von Rechnernetzwerken.....	28
2.10.1 - Betreiber des Netzzugangs.....	28
2.10.1.1 - Öffentlicher Netzzugang.....	28
2.10.1.2 - Privater Netzzugang.....	28
2.10.2 - Ausdehnung eines Netzwerks.....	29
2.10.3 - Ziele.....	30
2.10.4 - Verbindungstyp.....	31

2.10.4.1 - Vermittlungssysteme.....	31
2.10.4.1.1 - Leitungsvermittlung.....	31
2.10.4.1.2 - Speichervermittlung.....	31
2.10.4.2 - Rundfunksysteme.....	33
2.10.4.2.1 - Radiofunk.....	34
2.10.4.2.2 - Mikrowellen.....	34
2.10.4.2.3 - Frequenzzuteilung.....	35
2.10.4.2.4 - ISM-Bänder.....	35
2.10.4.2.5 - Infrarotübertragung.....	36
2.10.4.2.6 - Lichtwellenübertragung.....	36
2.10.4.2.7 - Kommunikationssatelliten.....	36
2.10.4.2.7.1 - VSAT.....	39
2.10.4.2.7.2 - CubeSat.....	39
3 - Schichtenmodelle.....	41
3.1 - Ansichten eines Schichtenmodells.....	41
3.2 - Grundelemente einer Kommunikations-Architektur.....	44
3.3 - Protokoll.....	44
.....	44
3.4 - Referenzmodelle.....	45
3.4.1 - Interaktion zwischen den Schichten.....	45
3.5 - Bestandteile von Referenzmodellen.....	47
3.5.1 - Primitive bei verbindungsorientierter Kommunikation.....	49
3.5.2 - Primitive bei verbindungsloser Kommunikation.....	50
3.5.3 - Globale und lokale Signifikanz.....	51
3.5.3.1 - Globale Signifikanz.....	51
3.5.3.2 - Lokale Signifikanz.....	51
3.5.4 - Zusammenfassung.....	52
4 - OSI-Referenzmodell.....	53
4.1 - Einführung.....	53
4.2 - Bitübertragungs-Schicht (1).....	55
4.3 - Sicherungs-Schicht (2).....	56
4.4 - Vermittlungs-Schicht (3).....	62
4.5 - Transport-Schicht (4).....	65
4.6 - Sitzungs-Schicht (5).....	65
4.7 - Darstellungs-Schicht (6).....	65
4.8 - Anwendungs-Ebene (7).....	65
5 - Abtastung.....	66
5.1 - Klassifizierung von Signalen.....	66
5.2 - Abgetastete Signale.....	66
5.3 - Begriffe der Abtastung.....	69
5.4 - Aliasing-Effekt.....	72
5.4.1 - Beispiel einer richtigen Abtastung.....	72
5.4.2 - Beispiel einer falschen Abtastung.....	73
5.5 - Darstellung eines Signals.....	74
5.6 - Fourier-Transformation eines periodischen Signals.....	74
6 - Digitale Datenübertragung.....	80
6.1 - Einleitung.....	80
6.2 - Maximale Kanalkapazität (C_N).....	80
6.3 - Kanalkapazität (C).....	81
6.4 - Message Cube.....	82
6.5 - Multiplex-Verfahren.....	83
6.5.1 - Zeit-Multiplex.....	83
6.5.2 - Frequenz-Multiplex.....	84
6.6 - Modem.....	85
6.6.1 - Modem-Standards nach ITU-T.....	86
6.6.2 - 2-Draht und 4-Draht Verbindungen.....	87
6.6.3 - Schaltungstechnisch.....	87
6.7 - Digitale Übertragung im Basisband.....	88
6.7.1 - Synchrone Übertragung.....	88
6.7.2 - Taktimpuls.....	88

6.7.3 - Scrambling und Descrambling.....	89
6.7.4 - Synchronisation.....	89
6.8 - Asynchrone Datenübertragung.....	90
6.9 - Grundbegriffe.....	91
6.9.1 - Alphabet.....	91
6.9.2 - Anforderungen an eine Datenübertragung.....	92
6.9.3 - Bandbreite.....	92
6.9.4 - Baud-Rate.....	92
6.9.5 - Bit.....	92
6.9.6 - Bit-Übertragungsrate.....	92
6.9.7 - Byte.....	92
6.9.8 - Code.....	92
6.9.9 - Entscheidungsinhalt.....	93
6.9.10 - Information.....	93
6.9.11 - Informationsgehalt.....	93
6.9.12 - Durchschnittlicher mittlerer Informationsgehalt (Entropie).....	93
6.9.13 - Redundanz und Relevanz (Zugehörigkeit).....	94
6.9.14 - Nachrichten-Ebene.....	95
6.9.15 - Informationsquelle.....	96
6.9.16 - Kanal.....	96
6.9.17 - Nachricht.....	96
6.9.18 - Schritt.....	96
6.9.19 - Schrittgeschwindigkeit.....	96
6.9.20 - Signal.....	96
6.9.21 - Symbol.....	96
6.9.22 - Zeichen.....	96
6.10 - Codierung.....	97
6.10.1 - Source-Coding.....	97
6.10.1.1 - Einleitung.....	97
6.10.1.2 - Huffmann-Codierung.....	100
6.10.1.3 - Beispiel für eine Huffmann-Codierung in Tabellenbearbeitung.....	100
6.10.1.4 - Beispiel für eine Huffmann-Codierung in graphischer Bearbeitung.....	103
6.10.2 - Channel-Coding.....	104
6.10.2.1 - Fehlererkennung.....	104
6.10.2.1.1 - Fehlererkennung durch Paritätsbits.....	104
6.10.2.1.2 - Hamming-Distanz.....	105
6.10.2.2 - Zweidimensionale Parität.....	107
6.10.2.3 - Echo.....	107
6.10.2.4 - CRC (Cyclic Redundancy Check).....	108
6.10.2.4.1 - Beispiel für eine CRC-Bearbeitung.....	109
6.10.3 - Wire-Codes.....	112
6.10.3.1 - Grundvoraussetzungen.....	112
6.10.3.2 - NRZ (Non Return to Zero).....	113
6.10.3.2.1 - NRZ-L.....	113
6.10.3.2.2 - NRZ-M.....	113
6.10.3.2.3 - NRZ-S.....	113
6.10.3.2.4 - RZ (Return to Zero).....	113
6.10.3.3 - Biphasic-Codierung.....	115
6.10.3.3.1 - Biphasic-L (Level).....	115
6.10.3.3.2 - Biphasic-M (Mark).....	115
6.10.3.3.3 - Biphasic-S (Space).....	115
6.10.3.3.4 - Manchester.....	116
6.10.3.3.5 - Differential Manchester.....	116
6.10.3.4 - Ternary-Wire-Codes.....	116
6.10.3.4.1 - AMI-NRZ.....	116
6.10.3.4.2 - AMI-RZ.....	116
6.10.3.4.3 - HDB3.....	116
6.10.3.4.4 - MLT3 (Multiple Level 3).....	116
6.10.4 - Bitfehlerrate.....	118

6.10.5 - Augenmuster.....	120
7 - Modulation.....	121
7.1 - Einleitung.....	121
7.2 - Lineare Modulation.....	124
7.3 - Analoge Modulationsverfahren.....	126
7.3.1 - Amplitudenmodulation (AM).....	126
7.3.1.1 - Modulationsindex.....	126
7.3.1.2 - 50%-Modulation.....	126
7.3.1.3 - 100%-Modulation.....	126
7.3.1.4 - Übermodulation.....	127
7.3.2 - Frequenzmodulation (FM).....	127
7.4 - Binäre Modulationsverfahren.....	128
7.4.1 - Unipolare Modulation.....	128
7.4.2 - Bipolare Modulation.....	129
7.4.3 - Orthogonale Modulation.....	130
7.5 - Mehrwertige digitale Modulationsverfahren.....	131
7.5.1 - Mehrwertige Amplitude Shift Keying (ASK).....	131
7.5.2 - Mehrwertige Frequency Shift Keying (FSK).....	132
7.5.3 - Mehrwertige Phase Shift Keying (PSK).....	132
7.6 - Quadrature Phase Shift Keying (QPSK, 4PSK).....	133
7.7 - Pulsmodulation.....	135
7.7.1 - Pulsamplitudenmodulation (PAM).....	135
7.7.2 - Pulsfrequenzmodulation (PFM).....	135
7.7.3 - Pulphasenmodulation (PPM).....	135
7.7.4 - Pulsweitenmodulation (PWM) Pulsdauermodulation (PDM).....	135
7.7.5 - Spektrum der Pulsmodulation.....	136
7.8 - Direkte Kodierung der Abtastwerte.....	137
7.9 - Deltamodulation (DM) / Differenz Puls Code Modulation (DPCM).....	138
7.10 - Zusammenfassung.....	139
8 - Leistungstheorie.....	140
8.1 - Unterschied zwischen Leitung und Kabel.....	140
8.2 - Stromkreis.....	140
8.3 - Ersatzschaltbild.....	141
8.4 - Wellenwiderstand.....	142
8.5 - Reflexion.....	146
8.6 - Ausbreitungsgeschwindigkeit.....	148
9 - Leitungsmessungen.....	149
9.1 - Link-Definitionen.....	150
9.2 - Messungen bei Twisted Pair-Leitungen.....	151
9.3 - NEXT, FEXT.....	152
9.4 - SNR.....	154
9.5 - BER Bit Error Rate.....	154
9.6 - Dämpfung.....	155
9.7 - ACR.....	157
9.8 - PSNEXT (Power Sum NEXT), PSFEXT (Power Sum FEXT).....	159
9.9 - PSACR (Power Sum ACR).....	160
9.10 - ELFEXT (Equalized Level FEXT).....	161
9.11 - PSELFEXT (Power Sum ELFEXT).....	162
9.12 - Propagation Delay.....	163
9.13 - Propagation Delay Skew.....	164
9.14 - HDTDR (High Definition Time Domain Reflectometry).....	165
9.15 - HDTDX (High Definition Time Domain Crosstalk).....	166
9.16 - Return Loss (RL).....	167
9.17 - DC Loop Resistance.....	167
9.18 - Alien Crosstalk.....	168
9.19 - Wire-Map-Fehler.....	169
9.19.1 - Split Pairs.....	169
9.19.2 - Anwendung unterschiedlicher Normen Normen von EIA/TIA 568.....	170
9.19.3 - Kurzschluss und Leitungsunterbrechung.....	170
9.20 - Güte / Qualitätseinteilungen von Kabel.....	171

9.20.1 - Amerikanischer Ansatz.....	171
9.20.2 - Europäischer Ansatz.....	171
9.20.3 - Bedingungen für die Einordnung in Qualitätsklassen.....	172
10 - Zugriffsverfahren.....	174
10.1 - Pure ALOHA.....	175
10.1.1 - Historisches.....	175
10.1.2 - Kollisionen.....	175
10.2 - Slotted ALOHA.....	178
10.3 - CSMA-Protokolle.....	179
10.3.1 - 1-persistent CSMA.....	179
10.3.2 - Nicht-persistentes CSMA.....	180
10.3.3 - p-persistent CSMA.....	180
10.3.4 - Vergleich der unterschiedlichen Zugriffsverfahren.....	180
10.3.5 - CSMA/CD.....	181
10.3.5.1 - Implementierung bei Ethernet.....	181
10.3.5.2 - Ablauf einer Kollision bei Ethernet mit 10Mbps.....	182
10.4 - CSMA/CA.....	185
10.5 - CSMA/CR.....	186
10.6 - Token-Zugriffsverfahren.....	187
11 - Topologien.....	189
11.1 - Allgemeines.....	189
11.2 - Merkmale.....	189
11.2.1 - Durchmesser.....	189
11.2.2 - Grad.....	189
11.2.3 - Bisektionsweite.....	189
11.2.4 - Symmetrie.....	189
11.2.5 - Skalierbarkeit.....	189
11.2.6 - Konnektivität.....	189
11.3 - Logische Topologie.....	193
11.4 - Physikalische Topologie.....	194
11.5 - Topologie-Vergleich.....	195
12 - Kupferverkabelung.....	196
12.1 - Symmetrische / Unsymmetrische Leitungen.....	196
12.1.1 - Symmetrische Leitungen.....	196
12.1.2 - Unsymmetrische Leitungen.....	197
12.2 - Koaxialkabel.....	198
12.2.1 - Yellow-Cable.....	198
12.2.2 - Cheapernet-Cable.....	199
12.2.3 - Twin-Koax-Leitung.....	200
12.3 - Sternvierer.....	201
12.4 - Twisted Pair Kabel (TP).....	201
12.4.1 - Unshielded-TP-Kabel (UTP).....	202
12.4.2 - Shielded-TP-Kabel (STP).....	202
12.4.3 - Unshielded Foiled TP (UFTP).....	202
12.4.4 - Screened shielded TP (SSTP/SFTP).....	203
12.5 - Übersicht über Kabeltypen nach IEEE-802.3 bei LAN's.....	204
12.5.1 - 10 Mbps - Verkabelung.....	204
12.5.2 - 100 Mbps - Verkabelung.....	205
12.5.3 - 1000Mbps / 1Gbps - Verkabelung.....	206
12.5.4 - 10Gbps - Verkabelung.....	206
12.5.5 - Aufbau der Topologie-Bezeichnung.....	207
12.5.5.1 - Datenraten.....	207
12.5.5.2 - Übertragungsverfahren.....	207
12.5.5.3 - Maximallänge.....	207
13 - Lichtwellenleiter.....	208
13.1 - Historisches.....	208
13.2 - Allgemeines.....	209
13.2.1 - Vorteile der Lichtwellenleiter gegenüber Kupferkabel.....	210
Nachteile der Lichtwellenleiter gegenüber Kupferkabel.....	210

13.2.2 - Multimode-Fasern.....	212
13.2.3 - Gradienten-Faser.....	213
13.2.4 - Monomode-Fasern.....	214
13.3 - Lichtquellen.....	215
13.4 - Lieferbare Formen.....	216
13.4.1 - Übersicht über die lieferbaren Einzelfasern.....	216
13.4.2 - Simplexkabel.....	217
13.4.3 - Duplexkabel.....	217
13.4.4 - Breakout-Kabel.....	217
13.4.5 - Bündelader-Kabel.....	217
13.4.6 - Bezeichnungscodes für Innenkabel nach DIN / VDE 0888.....	218
13.5 - Bezeichnungscodes für Aussenkabel nach DIN / VDE 0888.....	219
13.6 - Herstellung.....	220
13.7 - Verbindung von LWL-Fasern.....	221
13.8 - Messungen.....	222
13.9 - LWL Link-Klassen.....	223
13.9.1 - Link-Längen.....	223
13.9.2 - LWL-Faserklassen.....	223
13.9.3 - Linklänge in Abhängigkeit vom Standard und verwendeten Fasertyp.....	224
13.9.4 - Transceiver-Module.....	225
13.10 - SFP28.....	225
13.11 - Steckverbinder.....	227
13.11.1 - ST-Stecker.....	227
13.11.2 - FSMA-Stecker.....	227
13.11.3 - SC-Stecker.....	228
13.11.4 - FC-Stecker.....	228
13.11.5 - LC-Stecker.....	228
13.11.6 - E2000 Streeker.....	228
13.11.7 - MT-RJ Stecker.....	229
13.11.8 - ESCON-Stecker.....	229
13.11.9 - MIC-Stecker.....	229
13.11.10 - Pigtail mit ST-Stecker.....	230
13.11.11 - Patchkabel.....	230
13.11.12 - Übersicht über die unterschiedlichen Steckertypen.....	231
14 - Ethernet.....	232
14.1 - Historisches.....	232
14.2 - 10 Mbps-Ethernet.....	233
14.2.1 - 10 Mbps-Aufteilung auf die Schichten im OSI-Referenzmodell.....	234
14.2.1.1 - LLC.....	234
14.2.1.2 - MAC.....	234
14.2.1.3 - PLS.....	234
14.2.1.4 - PMA.....	234
14.2.2 - 10Mbps-Koaxiallösungen.....	235
14.2.2.1 - 10Base5.....	235
14.2.3 - 10 Mbps-Ethernet mit Twisted-Pair-Leitungen.....	237
14.2.4 - 10 Mbps- mit Glasfasern.....	240
14.2.4.1 - Kenngrößen für 10 Mbps-Ethernet.....	241
14.3 - 100 Mbps-Ethernet.....	242
14.3.1 - 100Base-TX (Fast Ethernet).....	242
14.3.1.1 - Reconciliation Layer.....	242
14.3.1.2 - PCS.....	243
14.3.1.3 - PMA.....	243
14.3.1.4 - PMD.....	243
14.3.1.5 - Auto-Negotiation-Handshake.....	247
14.3.1.6 - Flow-Control nach IEEE802.3x.....	250
14.3.2 - Weitere 100 Mbps-Kupfer-Varianten.....	251
14.3.2.1 - 100Base-T2.....	251
14.3.2.2 - 100Base-T4.....	251
14.3.2.3 - 100Base-FX.....	253
14.3.2.4 - 100Base-FX für große Distanzen.....	253

14.3.2.5 - Kenngrößen für 100 Mbps-Ethernet.....	253
14.4 - 1000 Mbps-Ethernet.....	254
14.4.1 - IEEE-802.3z.....	254
14.4.1.1 - Physical-Layer.....	256
14.4.1.2 - PCS.....	256
14.4.1.3 - PMA.....	256
14.4.1.4 - PMD.....	256
14.4.1.5 - 1000Base – LWL-Varianten.....	258
14.4.1.5.1 - Bandbreiten-Längenprodukt.....	258
14.4.1.5.2 - 1000Base-SX.....	258
14.4.1.5.3 - 1000Base-LX.....	259
14.4.1.5.4 - 1000Base-T.....	259
14.4.1.5.5 - 4D-PAM5-Leitungscodierung.....	261
14.4.1.5.6 - Hybridfunktion.....	267
14.4.1.5.7 - Echo Cancellation.....	267
14.4.1.5.8 - Crosstalk-Minimierung.....	267
14.4.1.5.9 - Startup einer 1000Bast-T-Schnittstelle.....	267
14.4.1.5.9.1 - MDI/MDIX -Erkennung und Einstellung.....	268
14.4.1.5.9.2 - Auto-Negotiation.....	269
14.5 - 10Gbps-Ethernet.....	271
14.5.1 - 10GBase-R.....	272
14.5.1.1.1 - 10GBase-SR.....	272
14.5.1.1.2 - 10GBase-LR.....	274
14.5.1.2 - 10GBase-LX4.....	274
14.5.1.3 - 10GBase-W.....	276
14.5.1.3.1 - STM-64/STS-192-Rahmen.....	277
14.5.1.4 - 10GBase-T.....	279
14.5.1.4.1 - 10GBase-PHY.....	280
14.5.1.4.2 - Master Slave Priorisierung.....	286
14.5.1.4.3 - Hinweis zur Verkabelung.....	286
14.5.2 - 10GBase-KX.....	287
14.5.2.1 - 10GBase-KX4.....	287
14.5.2.2 - 10GBase-KR.....	287
14.6 - 40/100Gigabit-Ethernet.....	288
14.6.1.1 - PCS.....	289
14.6.1.2 - FEC.....	289
14.6.1.3 - PMA.....	289
14.6.1.4 - 40GBase-CR4 und 100GBase-CR10.....	289
14.6.1.5 - 40GBase-SR4 und 100GBase-SR10.....	290
14.6.1.6 - 40GBase-LR4.....	291
14.6.1.7 - 100GBase-LR4 und 100GBase-ER4.....	291
14.6.1.8 - 40GBase-FR.....	291
14.6.1.9 - 40GBase-KR.....	291
14.6.1.10 - Auto-Negotiation bei 40/100GBit-Ethernet.....	291
14.7 - 200/400Gigabit-Ethernet.....	292
14.8 - Übersicht über die Historie.....	293
15 - Kupfer-Steckverbindungen.....	298
15.1 - BNC-Stecker.....	298
15.2 - Barrel-Stecker (N-Stecker).....	299
15.3 - SUB-D-Stecker.....	300
15.4 - RJ-Stecker.....	301
15.4.1 - RJ11-Stecker.....	301
15.4.2 - RJ12-Stecker.....	302
15.4.3 - RJ45-Stecker.....	302
15.4.3.1 - Aufteilung der Adernpaare einer Leitung nach TIA 568A.....	303
15.4.3.2 - Aufteilung der Adernpaare einer Leitung nach TIA 568B.....	303
15.4.3.3 - Aufteilung der Adernpaare bei verschiedenen Topologien nach TIA 568B.....	303
15.4.3.4 - Farbbelegung der verschiedenen Normungsgremien.....	304
15.4.3.5 - Funktionsbelegung des RJ45-Steckers bei 10BASE-T.....	304

15.4.3.6 - Funktionsbelegung des RJ45-Steckers bei Token Ring.....	304
15.4.3.7 - Zusammenfassung.....	305
15.4.3.8 - Nachfolger für den RJ45-Stecker.....	306
15.4.3.8.1 - GG45.....	306
15.4.3.8.2 - TERA-Stecker.....	307
15.4.4 - RJ21 TELCO -Stecker.....	308
15.5 - Stecker für IBM-Verkabelungs-System (IVS).....	308
16 - Strukturierte Verkabelung.....	309
16.1 - Grundlagen.....	309
16.2 - EN 50173.....	311
16.2.1 - Topologie.....	313
16.2.1.1 - Logische Topologie.....	313
16.2.1.2 - Verkabelungstopologie.....	313
16.2.2 - Leistungsvermögen der Übertragungsstrecke.....	314
16.2.3 - Anforderungen an Leitungen und Verbinder.....	314
16.3 - Backbone.....	315
16.3.1 - Distributed Backbone.....	315
16.3.2 - Collapsed Backbone.....	315
17 - PoE (Power over Ethernet).....	317
17.1 - Einleitung.....	317
17.2 - Stromversorgung.....	317
17.3 - Geräte.....	317
17.4 - Erkennung der PoE-Endgeräte.....	317
17.5 - Mögliche Konfigurationen.....	319
17.5.1 - Endspan-Versorgung mit Phantomspeisung.....	319
17.5.2 - Endspan-Versorgung über die freien Adernpaare.....	320
17.5.3 - Midspan-Versorgung.....	321
17.6 - Management.....	321
17.7 - PoE-Leistungsklassen.....	322
17.8 - Pinbelegung.....	322
18 - MAN / WAN.....	324
18.1 - Grundlagen.....	324
18.2 - PDH.....	324
18.3 - SDH.....	325
18.4 - MAN.....	327
18.4.1 - DQDB.....	327
18.5 - WAN.....	328
18.5.1 - X.25.....	328
18.5.2 - Frame-Relay.....	329
18.5.3 - ISDN.....	330
18.5.3.1 - ISDN-Dienste.....	330
18.5.3.2 - ISDN-Schnittstellen.....	331
18.5.3.3 - ISDN-S ₀ -Basisanschluss.....	332
18.5.3.4 - Kurzer Passiver Bus.....	333
18.5.3.5 - Erweiterter Passiver Bus.....	334
18.5.3.6 - Punkt-zu-Punkt-Verbindung.....	335
18.5.3.7 - Externer und interner S ₀ -Bus.....	336
18.5.3.8 - S ₀ -Rahmenaufbau.....	337
18.5.3.9 - Kollisionserkennung.....	338
18.5.3.10 - ISDN-S _{2M} -Primary Rate Interface.....	339
18.5.4 - xDSL.....	340
18.5.4.1 - ADSL.....	340
18.5.4.2 - HDSL.....	340
18.5.4.3 - SDSL.....	340
18.5.4.4 - UADSL.....	340
18.5.4.5 - VDSL.....	340
18.5.4.6 - Vergleich der unterschiedlichen DSL-Varianten.....	341
18.5.4.7 - Übertragung von POTS / Uplink / Downlink.....	342
18.5.4.8 - ADSL-Aufbau.....	343
18.5.5 - MPLS.....	344

18.5.5.1 - Einführung.....	344
18.5.5.2 - Funktionsweise.....	344
18.5.5.3 - VPN-Funktion.....	349
19 - Netzwerk-Komponenten.....	351
19.1 - Einleitung.....	351
19.2 - Repeater.....	352
19.2.1 - Einleitung.....	352
19.2.2 - Ausprägungen von Repeatern.....	353
19.2.2.1 - Local Repeater.....	353
19.2.2.2 - Remote Repeater.....	353
19.2.3 - Repeater-Regeln für 10 Mbps.....	354
19.2.4 - Repeater-Regeln für 100 Mbps.....	354
19.2.5 - Sicherheitsmechanismen.....	354
19.2.5.1 - Auto Partitioning.....	354
19.2.5.2 - Scrambling.....	354
19.2.6 - Repeater im ISO-RM.....	354
19.2.7 - Repeater-Bauformen.....	355
19.2.7.1 - Sternkoppler.....	355
19.2.7.2 - Hub.....	355
19.2.7.3 - Media-Konverter.....	355
19.2.7.4 - Switching Hub.....	355
19.2.8 - Probleme in Netzwerken, bei denen ein Repeater hilfreich ist.....	355
19.3 - Brücken (engl. Bridges).....	356
19.3.1 - Allgemeines.....	356
19.3.2 - Probleme in Netzwerken, bei denen eine Brücke hilfreich ist.....	357
19.3.3 - Brücke im ISO-RM.....	359
19.3.4 - Brückentypen.....	359
19.3.4.1 - Lokale Brücken.....	359
19.3.4.2 - Remote-Brücken.....	359
19.3.4.3 - Multiport-Brücken.....	359
19.3.5 - Adressbuchverwaltung.....	360
19.3.5.1 - Dynamisches Adressbuch.....	360
19.3.5.2 - Statisches Adressbuch.....	360
19.3.6 - Redundanz und Zyklendiffreiheit.....	360
19.3.7 - Spanning-Tree-Algorithmus.....	361
19.3.7.1 - Grundlagen.....	361
19.3.7.2 - Ablauf des Spanning-Tree-Algorithmus.....	362
19.3.7.3 - Beispiel für einen Spanning-Tree-Algorithmus-Durchlauf.....	363
19.3.8 - Rapid Reconfiguration Spanning Tree (RSTP) und Multiple Spanning Tree (MSTP).....	372
19.3.8.1 - Aufbau des RSTP.....	372
19.3.8.1.1 - Root Bridge.....	372
19.3.8.1.2 - Designated Bridge.....	373
19.3.8.1.3 - Ports.....	374
19.3.8.1.4 - Root Port.....	374
19.3.8.1.5 - Designated Port.....	374
19.3.8.1.6 - Edge Port.....	375
19.3.8.1.7 - Alternate Port.....	375
19.3.8.1.8 - Backup Port.....	375
19.3.8.2 - RSTP Port Modi.....	375
19.3.8.2.1 - Discarding Mode.....	375
19.3.8.2.2 - Learning Mode.....	375
19.3.8.2.3 - Forwarding Mode.....	375
19.3.8.3 - RSTP-Regeln.....	377
19.3.8.3.1 - RSTP-Regel 0.....	377
19.3.8.3.2 - RSTP-Regel 1.....	377
19.3.8.3.3 - RSTP-Regel 2.....	377
19.3.8.3.4 - RSTP-Regel 3.....	377
19.3.8.3.5 - RSTP-Regel 4.....	378
19.3.9 - Topologie Change.....	379

19.3.9.1 - Versand der TC-Meldung (Topologie Change).....	379
19.3.9.2 - Verarbeitung der TCN-Meldung.....	379
19.4 - Switches.....	382
19.4.1 - Allgemeines.....	382
19.4.2 - Merkmale.....	382
19.4.3 - Switching-Verfahren bezogen auf den Datenweitertransport.....	382
19.4.3.1 - Cut-Through.....	382
19.4.3.2 - Cut-Through (Collision-Free).....	382
19.4.3.3 - Store-And-Forward.....	382
19.4.4 - Kommunikationsarten.....	382
19.4.5 - Layer2-Switches.....	383
19.4.5.1 - Beispiel.....	383
19.4.5.2 - Layer-2-Switch im ISO-RM.....	383
19.4.6 - Layer-3-Switches.....	384
19.4.6.1 - Beispiel.....	384
19.4.6.2 - Layer-3-Switch im ISO-RM.....	385
19.4.7 - Layer2-Layer3-Switching-Methoden.....	385
19.4.8 - Layer-4-Switch.....	386
19.4.9 - Aufbau von größeren Netzwerken mit Switches.....	387
19.4.10 - Management.....	389
19.4.11 - Stackports.....	389
19.4.12 - Backplane.....	389
19.4.13 - Priorisierung.....	389
19.5 - Router.....	390
19.5.1 - Allgemeines.....	390
19.5.2 - Router im ISO-RM.....	393
19.5.3 - Protokolle im Zusammenspiel mit Routern.....	394
20 - Routingprotokolle.....	394
21 - Routebare Protokolle.....	394
22 - Nicht routebare Protokolle.....	394
22.1.1 - Funktionsweise von Routern.....	395
22.1.2 - Beispiele von Pakettransporten in verschiedenen Netzwerken.....	396
22.2 - Gateways.....	399
22.2.1 - Allgemeines.....	399
22.2.2 - Gateways im ISO-RM.....	400
22.2.3 - Mischformen von Netzwerkgeräten.....	401
22.3 - Collision-Domain / Broadcast-Domain.....	401
23 - Protokoll-Funktionen.....	402
23.1 - Vermittlung.....	402
23.1.1 - Verbindungsorientierte Übertragung.....	402
23.1.2 - Verbindungslose Übertragung.....	402
23.1.3 - Leitungsvermittlung.....	403
23.1.4 - Speichervermittlung.....	404
23.1.5 - Paketvermittlung.....	404
23.2 - Signalisierung.....	405
23.3 - Multiplexing.....	406
23.3.1 - Fehlerarten.....	406
23.3.2 - Fehler-Erkennung und -Korrektur.....	406
23.4 - Flusskontrolle.....	406
23.4.1 - Übertragungswiederholung.....	407
23.4.1.1 - Stop and Wait.....	408
23.4.1.2 - Sliding Window.....	409
23.4.2 - Fehlerbehandlung bei der Fenstertechnik.....	411
23.4.2.1 - Go back n.....	411
23.4.2.2 - Selective Repeat.....	412
23.4.2.3 - Selective Reject ARQ.....	412
23.5 - Zusammenfassung.....	413
24 - Protokolle.....	415
24.1 - Übersicht.....	415
24.2 - Einführung.....	415

24.3 - Aufbau eines Rahmens auf der Leitung.....	416
24.4 - Ethernet Protokolle.....	417
24.4.1 - NOVELL.....	418
24.4.2 - IEEE-802.3.....	418
24.4.3 - SNAP.....	418
24.4.4 - Ethernet V2.....	418
24.5 - IEEE-802.2.....	419
24.5.1 - Allgemeines.....	419
24.5.2 - Typen.....	419
24.5.3 - Dienste.....	419
24.5.4 - Aufbau von LLC-Frames.....	420
24.5.4.1 - I-Frames.....	420
24.5.4.2 - S-Frames.....	420
24.5.4.3 - U-Frames.....	421
24.5.4.3.1 - Kommandos.....	421
24.5.4.3.2 - Antworten.....	421
24.6 - Zusammenfassung der Ethernet-Protokolle.....	422
24.7 - Mögliche Protokollbindungen.....	423
24.8 - Token Ring.....	424
24.9 - FDDI.....	425
24.10 - CDDI.....	425
24.11 - Unterschiede im Frame-Aufbau bei den verschiedenen Topologien.....	426
24.12 - IP (v4).....	427
24.12.1 - IPv4-Adressen.....	429
24.12.2 - Classless-inter-Domain-Routing (CIDR).....	430
24.12.3 - Subnetting.....	434
2-Bit-Subnetting.....	434
24.12.4 - Beispiel eines 3-Bit-Subnetting.....	435
24.12.5 - Subnet-Arithmetik in einem C-Klasse-Netzwerk.....	436
24.12.6 - Interpretation der Subnetzmaske.....	441
24.12.7 - Beispiel für eine Anwendung der Subnetmask.....	442
24.12.7.1 - Broadcasts.....	444
24.12.7.1.1 - Limited Broadcast.....	445
24.12.7.1.2 - Net Directed Broadcast.....	445
24.12.7.1.3 - Subnet Directed Broadcast.....	445
24.12.7.1.4 - All Subnets Directed Broadcast.....	445
24.12.7.2 - Multicasts.....	446
24.12.7.2.1 - Multicast-ID.....	446
24.12.7.2.2 - Umsetzung der Multicast-ID in eine MAC-Adresse.....	447
24.12.8 - IP-Header.....	448
24.12.9 - Referenz-Netzwerke.....	450
24.12.10 - TOS für verschiedene Applikationen.....	451
24.13 - Network-Address-Translation.....	452
24.13.1 - Problemstellung.....	452
24.13.2 - Vorgehensweise.....	453
24.13.2.1 - Vorteile von NAT.....	453
24.13.2.2 - Nachteile von NAT.....	454
24.13.3 - Formen von NAT.....	455
24.13.3.1 - Full Cone.....	456
24.13.3.2 - Restricted Cone.....	457
24.13.3.3 - Port Restricted Cone.....	458
24.13.3.4 - Symmetric Cone.....	459
24.13.4 - Lösung der Probleme mit NAT.....	460
24.13.4.1 - VPNs.....	460
24.13.4.2 - Einstellen der Ports.....	460
24.13.4.3 - Manueller Porteintrag.....	460
24.13.4.4 - STUN.....	460
24.13.4.5 - Dynamisches DNS.....	461
24.13.4.6 - Application Layer Gateway.....	461

24.13.4.7 - Universal Plug'n'Play (UPnP).....	461
24.13.4.8 - MIDCOM.....	461
24.13.4.9 - TURN.....	462
24.14 - ARP-Request (Address Resolution Protocol).....	463
24.14.1 - Problemstellung.....	463
24.14.2 - Ablauf.....	464
24.15 - RARP-Request (Reverse Address Resolution Protocol).....	465
24.15.1 - Problemstellung.....	465
24.15.2 - Ablauf.....	465
24.16 - Proxy ARP.....	466
24.16.1 - Einleitung.....	466
24.16.2 - Abhilfe.....	466
24.17 - UNARP.....	467
24.17.1 - Allgemeines.....	467
24.17.2 - Problembeschreibung.....	467
24.17.3 - Ablauf.....	467
24.18 - BOOTP.....	468
24.18.1 - Ablauf.....	468
24.18.2 - Paket-Aufbau.....	468
24.19 - DHCP.....	469
24.19.1 - Allgemeines.....	469
24.19.2 - Ablauf eines DHCP-Lease.....	470
24.19.2.1 - IP-Adresse anfordern.....	470
24.19.2.2 - Angebot einer IP-Adresse von den vorhandenen DHCP-Servern.....	470
24.19.2.3 - Auswahl der IP-Adresse.....	470
24.19.2.4 - Bestätigung der IP-Adresse.....	470
24.19.2.5 - Lease-Erneuerung.....	470
24.19.3 - DHCP-Zustände.....	471
24.19.4 - DHCP-Nachrichten.....	471
24.19.4.1 - DHCP-Discover.....	471
24.19.4.2 - DHCP-Offer.....	471
24.19.4.3 - DHCP-Request.....	471
24.19.4.4 - DHCP-ACK.....	471
24.19.4.5 - DHCP-NAK.....	471
24.19.4.6 - DHCP-Release.....	471
24.19.5 - Kommandos auf DOS-Ebene.....	471
24.19.6 - Paket-Aufbau.....	472
24.19.7 - APIPA.....	474
24.20 - ICMP (Internet Control Message Protocol).....	475
24.20.1 - ICMP-Paket-Aufbau.....	476
24.20.2 - ICMP-Typen.....	476
24.20.2.1 - ICMP-Codes (Type 0).....	477
24.20.2.2 - ICMP-Codes (Type 3 = Destination unreachable).....	477
24.20.2.3 - ICMP-Codes (Type 4 = Source quench).....	478
24.20.2.4 - ICMP-Codes (Type 5 = redirect).....	478
24.20.2.5 - ICMP-Codes (Type 8 = Echo request).....	479
24.20.2.6 - ICMP-Codes (Type 11 = Time to live exceeded).....	479
24.20.2.7 - ICMP-Codes (Type 12 = Parameter Problem).....	479
24.20.2.8 - ICMP-Codes (Type 13 = Timestamp-Message (Zeitstempel-Meldung)).....	480
24.20.2.9 - ICMP-Codes (Type 15 = Information-Request-Message).....	481
24.20.2.10 - ICMP-Codes (Type 16 = Information-Reply-Message).....	481
24.21 - Namensauflösung.....	482
24.21.1 - Einleitung.....	482
24.21.2 - Internet Name Service.....	482
24.21.3 - DNS.....	483
24.21.3.1 - Domain Namensraum.....	484
24.21.3.2 - Nameserver.....	485
24.21.3.3 - Resolver.....	487
24.21.3.4 - Resource Records.....	488
24.21.3.4.1 - Resource Records Format.....	488

24.21.3.4.2 - Resource Records Typen.....	489
24.21.4 - Dynamisches DNS (DDNS).....	493
24.22 - IP-Version 6 (IPv6).....	494
24.22.1 - Historisches.....	494
24.22.2 - Neue Terminologie.....	495
24.22.3 - Header-Aufbau.....	496
24.22.3.1 - Allgemeines.....	496
24.22.3.2 - Unterschiede zum IPv4-Header.....	497
24.22.4 - IPv6-Adressen.....	498
24.22.4.1 - Scope.....	498
24.22.4.2 - Aufbau.....	500
24.22.4.3 - EUI-64 Adresse.....	501
24.22.4.4 - Adress-Typen.....	502
24.22.4.4.1 - IPv6-Unicasts.....	502
24.22.4.4.2 - IPv6-Anycast.....	502
24.22.4.4.3 - IPv6-Multicast.....	503
24.22.4.4.4 - Weitere Unterschiede zu IPv4-Adressen.....	504
24.22.4.5 - Aussehen einer IPv6-Adresse.....	505
24.22.4.5.1 - Die bevorzugte Form.....	505
24.22.4.5.2 - Mischformen von IPv4 und IPv6.....	506
24.22.4.5.2.1 - Unter IPv6 genutzte IPv4 -Adressen.....	506
24.22.4.5.2.2 - IPv4-mapped IPv6-Adresse.....	506
24.22.4.6 - Adress-Präfix.....	506
24.22.4.6.1 - Bedeutung.....	506
24.22.4.6.2 - Adress-Präfix-Schreibweise.....	506
24.22.4.7 - Adress-Typ-Darstellung.....	507
24.22.4.8 - Übersicht der vorgeschriebenen Adressen.....	508
24.22.4.9 - Aufbau von Multicast-Adressen.....	508
24.22.4.10 - Weitere Protokolle im Umfeld von IPv6.....	511
24.22.4.11 - RFCs im Zusammenhang mit IPv6.....	512
24.22.5 - Der Übergang von IPv4 zu IPv6.....	514
24.22.5.1 - Dual-Stack-Technik.....	514
24.22.5.2 - Tunnel-Techniken.....	516
24.22.5.2.1 - 6in4.....	516
24.22.5.2.2 - 6over4.....	516
24.22.5.2.3 - ISATAP.....	517
24.22.5.3 - Translation-Technik.....	517
24.22.5.3.1 - Teredo / Miredo.....	518
24.22.5.3.2 - 6to4.....	518
24.22.6 - Maßnahmen zur Migration von IPv4 zu IPv6.....	519
24.22.6.1 - Adress-Planung.....	519
24.22.6.2 - Router-Migration.....	519
24.22.6.3 - Server-Migration.....	519
24.22.6.4 - Endgeräte-Migration.....	519
24.22.6.5 - Firewall-Migration.....	519
24.22.6.6 - Funktionen.....	520
24.23 - GLBP (Gateway Load Balancing Protocol) HSRP / VRRP.....	521
24.23.1 - Einführung.....	521
24.23.2 - VRRP.....	522
24.23.2.1 - Grundlagen.....	522
24.23.2.2 - Definitionen.....	522
24.23.2.2.1 - VRRP-Router.....	522
24.23.2.2.2 - Virtueller Router.....	522
24.23.2.2.3 - Master Router.....	522
24.23.2.2.4 - IP Adress-Owner.....	523
24.23.2.2.5 - Prioritätszuordnung.....	524
24.23.2.2.6 - Höchste IP-Adresse.....	525
24.23.2.2.7 - Nutzung einer speziellen VIP-Adresse.....	526
24.23.3 - Betrieb.....	527

24.23.4 - VRRP-Packet-Format.....	529
24.24 - ICMPv6.....	534
24.24.1 - Allgemeines.....	534
24.24.2 - ICMPv6-Fehlermeldungen.....	534
24.24.3 - ICMPv6-Informationen.....	535
24.24.4 - Typ-Längen-Werte (TLVs) / Optionen für Neighbour Discovery ICMP Meldungen.....	537
24.25 - DHCPv6.....	538
24.25.1 - Allgemeines.....	538
24.25.2 - Autokonfiguration.....	538
24.25.3 - Bearbeitung der DHCP-Informationen.....	539
24.26 - Virtuelles LAN (VLAN).....	540
25 - Einführung.....	540
26 - VLANs portbasiert oder getagged.....	542
26.1.1.1 - Portbasiert.....	542
26.1.1.2 - Getaggt.....	542
27 - VLAN-Tagging.....	542
28 - VLANs in unterschiedlichen Ebenen.....	544
29 - Sicherheit von VLANs.....	544
30 - Beispiel 1:.....	546
31 - Beispiel 2:.....	547
32 - Eigenschaften von VLANs.....	549
32.1 - Software Defined Networks (SDN).....	550
32.1.1 - Einführung.....	550
32.1.2 - Veränderung der Netzwerk-Komponenten unter SDN.....	553
32.2 - UDP-Protokoll.....	558
32.2.1 - Allgemeines.....	558
32.2.2 - UDP im ISO-RM.....	558
32.2.3 - Header-Aufbau.....	558
32.3 - TCP-Protokoll.....	559
32.3.1 - Allgemeines.....	559
32.3.2 - TCP im ISO-RM.....	559
32.3.3 - Header-Aufbau.....	560
32.3.4 - Verbindungsstati.....	562
32.3.5 - Ablauf des Verbindungsaufbaus.....	563
32.3.6 - Ablauf des Verbindungsabbaus.....	565
32.3.7 - Half-Close.....	566
32.3.8 - RST(Restet).....	567
32.3.9 - Abbrechen einer Verbindung.....	567
32.3.10 - Erkennung von halb offenen Verbindungen.....	567
32.3.11 - Gleichzeitiger Open (engl.: simultaneous open).....	568
32.3.12 - Gleichzeitiger Close (engl.: simultaneous close).....	569
32.3.13 - Datenübertragung.....	570
32.3.14 - Bandwidth-Delay-Product.....	574
32.3.15 - URGENT-Mode.....	575
32.3.16 - Slow Start.....	576
32.3.17 - TCP-Timer.....	577
32.3.17.1 - Retransmission Timer.....	577
32.3.17.2 - Persist Timer.....	578
32.3.17.3 - Keepalive Timer.....	579
32.3.17.4 - 2MSL Timer.....	579
32.4 - RIP.....	580
32.4.1 - RIP Version 1.....	580
32.4.2 - Aufbau von RIPv1.....	581
32.4.3 - RIP Version 2.....	584
32.4.4 - Aufbau von RIPv2.....	585
32.5 - OSPF.....	586
32.5.1 - Einführung.....	586
32.5.2 - Autonome Systeme.....	586
32.5.3 - Topologie-Aufbau.....	589
32.5.4 - Aufbau.....	593

32.5.4.1 - Grundlagen.....	593
32.5.4.2 - Übersicht.....	593
32.5.4.3 - Ablauf.....	593
32.5.4.3.1 - Designated Router und Backup-Router.....	593
32.5.4.3.2 - Nachbarschaftsbeziehungen.....	594
32.5.4.3.3 - Austausch der Routing-Informationen.....	594
32.5.4.3.4 - Laufender Betrieb.....	595
32.5.5 - OSPF-Pakete.....	596
32.5.5.1 - OSPF-Header.....	596
32.5.5.2 - HELLO-Pakete.....	596
32.5.5.3 - Database Description (DD).....	597
32.5.5.4 - Link-State-Request.....	597
32.5.5.5 - Link-State-Update.....	597
32.5.5.6 - Link-State-ACK.....	597
32.5.5.7 - LSA-Header.....	597
32.5.6 - Zusammenfassung.....	597
32.6 - IGMP.....	598
32.6.1 - Encapsulation im IP-Paket.....	598
32.6.2 - Aufbau einer IGMP-Meldung.....	598
32.6.3 - Gruppen-Bearbeitung.....	599
32.6.4 - All-Hosts-Group.....	600
32.6.5 - Informationen.....	600
33 - Link Aggregation (LA).....	601
33.1 - Historisches.....	601
33.2 - Aufbau.....	602
34 - Static Link Aggregation.....	602
35 - Dynamic Link Aggregation.....	602
36 - Vorteile von LACP bietet gegenüber einer statischen Link Aggregation:.....	602
36.1 - Funktionsweise.....	603
36.2 - Voraussetzungen.....	604
37 - Verkehrsaufteilung innerhalb einer LAG.....	604
38 - Firewalls.....	606
38.1 - Allgemeines.....	606
38.2 - Unterscheidungsmerkmale.....	607
38.2.1 - Anbindung.....	607
38.2.1.1 - Dual-Homed Firewall.....	607
38.2.1.2 - Screened-Host Firewall.....	607
38.2.1.3 - Screened-Subnet Firewall.....	609
38.2.2 - Typen.....	610
38.2.2.1 - Paketfilter.....	610
38.2.2.2 - Zustandslose Filterung (stateless inspection).....	610
38.2.2.3 - Zustandsbehaftete Filterung (stateful inspection).....	610
38.2.2.4 - Proxy Firewall.....	610
38.2.2.5 - Application-Level-Gateways.....	611
38.2.2.6 - Personal Firewalls.....	611
38.2.3 - Accesslisten.....	612
38.2.3.1 - Einführung.....	612
38.2.3.2 - Definieren von Zugriffslisten.....	612
38.2.3.3 - Syntax für eine Standard-Zugriffsliste.....	612
38.2.3.4 - Zuordnung zu einer Schnittstelle.....	614
38.2.3.5 - Beispiel-Ablauf:.....	615
38.2.3.6 - Bearbeitungsschritte.....	615
38.2.3.7 - Erweiterte Zugriffslisten.....	616
38.2.3.8 - Benannte Zugriffslisten.....	617
38.2.3.9 - Syntax für benannte Standard Zugriffslisten.....	618
38.2.3.10 - Syntax für benannte erweiterte Zugriffslisten.....	618
38.2.3.11 - Dynamische Zugriffslisten.....	619
38.2.3.12 - Reflexive Zugriffslisten.....	619
38.2.3.13 - Zeit gesteuerte Zugriffslisten.....	619

38.2.3.14 - Ausgabe der Zugriffslisten.....	619
38.2.3.15 - Überprüfung der Zugriffslisten.....	619
39 - Netzwerk-Management.....	620
39.1 - Einführung.....	620
39.2 - SNMP.....	620
39.2.1 - Management-Konsole.....	621
39.2.2 - Zusammenspiel der SNMP-Komponenten.....	622
39.2.3 - Proxy-Agent.....	622
39.2.4 - MIB-Aufbau.....	623
39.2.5 - Community-String.....	625
39.2.6 - SNMPv1.....	625
39.2.6.1 - Paket-Aufbau unter SNMP.....	626
39.2.6.1.1 - Aufbau für Get, Getnext, Response Set.....	626
39.2.6.1.2 - Aufbau für Traps.....	626
39.2.6.1.3 - Aufbau der variablen Bindungen.....	628
39.2.6.2 - Einfache Datentypen.....	628
39.2.6.3 - Anwendungs-Datentypen.....	628
39.2.7 - SNMPv2.....	629
39.2.8 - SNMPv3.....	630
39.2.8.1 - Allgemeines.....	630
39.3 - RMON.....	630
39.4 - SMON.....	631
39.5 - Netzwerk-Management-Software.....	632
39.5.1 - Allgemeines.....	632
39.5.2 - CiscoView.....	633
39.5.2.1 - Beispiel.....	633
39.5.2.2 - Bearbeitung.....	634
39.5.3 - VLANDirector.....	634
39.5.4 - TrafficDirector.....	634
39.5.5 - ATMDirector.....	634
40 - Anwendungsprotokolle.....	635
40.1 - Einführung.....	635
40.2 - Electronic Mail (E-Mail).....	637
40.2.1 - Einführung.....	637
40.2.2 - Simple Mail Transfer Protocol (SMTP).....	638
40.2.2.1 - Ablauf.....	638
40.2.2.2 - E-Mail-Adresse.....	639
40.2.2.3 - SMTP-Character Code.....	639
40.2.2.4 - SMTP-Datentransfer.....	639
40.2.2.5 - SMTP-Kommmandos.....	640
40.2.2.6 - SMTP-Replies.....	641
40.2.2.6.1 - Erste Stelle.....	641
40.2.2.6.2 - Zweite Stelle.....	641
40.2.2.6.3 - Dritte Stelle.....	641
40.2.2.6.4 - Reply-Tabelle.....	642
40.2.2.7 - Ablaufbeispiel einer Session.....	643
40.2.3 - Post Office Protocol (POP3).....	644
40.2.3.1 - Allgemeines.....	644
40.2.3.2 - Ablauf.....	644
40.2.3.3 - POP3-Kommmandos.....	645
40.2.4 - Multipurpose Internet Mail Extensions (MIME).....	645
40.2.5 - Internet Message Access Protocol (IMAP4).....	646
40.2.6 - Hyper Text Transfer Protocol (HTTP).....	648
40.2.7 - File Transfer Protocol (FTP).....	650
40.2.7.1 - Aufbau.....	650
40.2.7.2 - FTP-Befehlssatz.....	651
40.2.8 - Network Virtual Terminal (Telnet).....	653
41 - IP-Telefonie (Voice over IP (VoIP)).....	654
41.1 - Einleitung.....	654
41.2 - Historisches.....	654

41.3 - Vorteile.....	655
41.4 - Nachteile.....	655
41.5 - Aufbau.....	656
41.5.1 - Spracherfassung mit einem Mikrofon.....	656
41.5.2 - Bearbeitung mit einem Codec.....	657
41.5.3 - Paketierung.....	658
41.5.4 - Datenübertragung über ein paketvermittelndes Netzwerk.....	658
41.5.5 - Signalisierungsprotokolle.....	658
41.5.5.1 - SIP.....	659
41.5.5.1.1 - Dialoge.....	659
41.5.5.1.2 - SIP Requests:.....	659
41.5.5.1.3 - Responses von SIP:.....	659
41.5.5.1.4 - Verbindlungsaufbau.....	661
41.5.5.1.5 - SIP im Redirect-Mode.....	662
41.5.5.1.6 - SIP im Proxy-Mode.....	662
41.5.5.6 - ENUM.....	663
41.5.7 - Verzögerung - Laufzeit.....	664
41.5.8 - Laufzeit mit Ping messen.....	664
41.5.9 - Jitter.....	665
41.5.10 - Paketverluste - Packet Loss.....	665
41.5.11 - QoS (Quality of Service) / ToS (Type of Service).....	665
41.6 - Zusammenfassung.....	666
41.7 - Quellen.....	667
42 - Anhang.....	669
42.1 - MAC-Adr. – Hersteller-Zuordnung.....	669
42.2 - Sonstige MAC-Adress-Zuordnungen.....	671
42.3 - Ethernet Typ-Kennungen.....	671
42.4 - Portnummern-Zuordnungen TCP -und UDP-Ports.....	672
42.5 - AWG-Tabelle.....	676
42.6 - Verwendete mathematische Zuordnungen.....	678
42.6.1 - Logarithmen.....	678
43 - Literaturhinweise.....	679
44 - Abbildungsverzeichnis.....	681
Abbildungsverzeichnis.....	681
45 - Stichwortverzeichnis.....	690
46 - Abkürzungsverzeichnis.....	704

1 - Empfehlungen, Standards und Normen

1.1 - Einleitung

Bei der Standardisierung sind nationale und internationale Interessengemeinschaften (Anwender, Hersteller und technische Fachgremien) mit der Erstellung von Dokumenten beschäftigt. Diese Dokumente enthalten für allgemeine und wiederkehrende Anwendungen Regeln und Leitlinien sowie für Tätigkeiten und deren Ergebnisse Merkmale. Diese Dokumente werden auch Standards genannt, die das Ziel verfolgen Produkte und Leistungen zu vereinheitlichen.

Dies bedeutet im Netzwerkbereich eine Gewährleistung für:

- Konnektivität (Anschlussfähigkeit)
- Interoperabilität (Fähigkeit zur Zusammenarbeit)
- Kompatibilität (Austauschbarkeit)

für alle Komponenten durch Protokolle und einheitliche Schnittstellen.

Standards sind oft die Vorstufen von Normen. Wird die Standardisierung durch eine anerkannte nationale oder internationale Institution durchgeführt spricht man von Normung und die erstellten Dokumente Normen.

In der Welt der Netzwerke haben sich im Laufe der Jahre mehrere Normen (engl. **standards**) entwickelt und verbreitet.

Zudem sind daneben noch de facto Standards entstanden, die man sich gar nicht mehr weg denken kann.

Für die Empfehlungen, Standards und Normierungen fühlen sich mehrere Gremien zuständig.

1.2 - ANSI (American National Standards Institute)

Die ANSI ist eine private, nichtkommerzielle Organisation. Sie hat ihren Sitz in Washington DC. Das Gremium wurde 1918 gegründet und hat für das US-Standardisierungssystem die Verwaltung und Koordination übernommen.

Es hilft bei der Entwicklung von nationalen und internationalen Standards. Sowohl bei der ISO als auch bei der IEC repräsentiert es die USA.



Bekannte Normen sind:

- ANSI X3T9.5 (FDDI-MANs: Fibre Distributed Data Interface)
- SONET (Synchronous Optical Network)
- ANSI-COBOL und ANSI-C (Programmiersprachen)

Viele der ANSI-Standards wurden von der ISO als Normen übernommen.

1.3 - ITU

Für die internationale Bearbeitung von Empfehlungen wurde die ITU (International Telecommunications Union) von 20 europäischen Staaten in Paris 1865 gegründet. Sie hat derzeit ihren Sitz in Genf und die Aufgabe die Standardisierung der internationalen Telekommunikation voranzutreiben. 1947 wurde die ITU eine Behörde der UN und kennt daher als vollwertige Mitglieder nur Staaten. Daher erklärt sich das Übergewicht der nationalen Netzbetreiber in der ITU.



Die ITU wird in drei Bereiche unterteilt:

1.3.1 - ITU-R

Steht für die Radiokommunikation. Hier werden z. B. weltweit die Radio-Frequenzbereiche vergeben.

1.3.2 - ITU-T

Steht für die Telekommunikation. Hier werden Empfehlungen für die Telefon- und Datenkommunikation abgehandelt. Von 1956 bis 1993 hieß die ITU-T CCITT (Comité Consultatif International Télégraphique et Téléphonique). So ist z. B. X25 eine bekannte Empfehlung der CCITT.



Für die internationale Bearbeitung von Normen ist die ISO (Die offizielle Bezeichnung lautet: International Organisation for Standardization) seit 1946 zuständig. Zur ISO gehören mehrere nationale Normungsgremien wie z. B. die deutsche DIN oder die amerikanische ANSI (American National Standards Institute). Die ISO ist Mitglied bei ITU-T.

Die ITU-T hat Recommendations (Empfehlungen) geschaffen, die von A bis Z geordnet sind. Bekannte Serien sind:

- G-Serie (Übertragungssysteme und -Medien) z. B. **G.711** für PCM (Pulse Code Modulation).
- H-Serie (Audiovisuelle und multimediale Systeme) z. B. H.323 für paketvermittelte Multimediakommunikation.
- I-Serie (Integrated Digital Services Network) z. B. **I.430** zur **S₀**-Schnittstelle oder **I.431** für die **S_{2M}**-Schnittstelle.
- Q-Serie (Switching and Signaling) **Q.920/21** und **Q.930/31** zur ISDN-Signalisierung.
- V-Serie (Datenkommunikation über das Telefonnetz) **V.24** für die serielle Schnittstelle zwischen **DEE** und **DÜE**.
- X-Serie (Datennetze und offene Kommunikationssysteme) z. B. **X.21** oder **X.25**.

1.3.3 - ITU-D

Steht für Entwicklung. (Development). Aktuelle Themen sind unter anderm Cybersecurity und Kommunikation im Katastrophenfall.

1.4 - Internet-Gremien

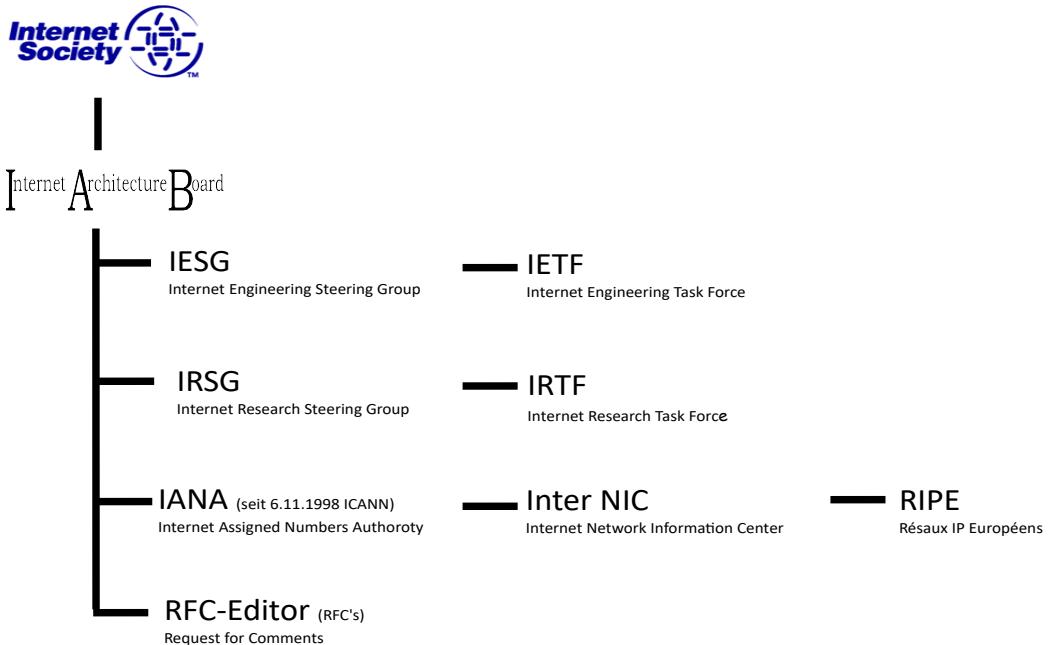


Abbildung 1: Internet-Gremien

Die Internet Society, kurz ISOC, bildet den Überbau der die gesamten Neuentwicklungen im Internet organisiert. Nähere Informationen sind unter www.isoc.org zu finden.

Die Entwicklung neuer Protokolle und Dienste, wird auch durch Industrie-Foren wie etwa die IETF (Internet Engineering Task Force; deutsch: Internet Engineering Sonderkommando) vorangetrieben. Hier sind auch wirtschaftliche Interessen der Antrieb und daher erklärt sich auch die größere Dynamik, im Vergleich zu den ITU-Bereichen in denen nationale Interessen vorrangig sind.

Laut eigenen Angaben ist die IETF ein offener, internationaler Zusammenschluss von Netzwerk-Designern, Verwaltern, Herstellern und Forschern.

Sie ist in Areas aufgeteilt, die von einem Area-Director verwaltet werden. Die Kommunikation wird über Mailing-Listen durchgeführt.

Dreimal jährlich werden Meetings abgehalten. Die Area-Directors sind Mitglieder der IESG (Internet Engineering Steering Group; deutsch: Internet Engineering Lenkungs Gruppe)

Die Aufsicht über das gesamte Gebilde hält die IAB (Internet Architecture Board). Die IAB ist auch für Beschwerden gegenüber der IETF zuständig. Für diese Zwecke werden IAB und IETF von der ISOC (Internet Society; deutsch: Internet-Gesellschaft) gechartert.

Die ISOC bedient sich auch der IANA (Internet Assigned Numbers Authority; deutsch: Internet Verwalter zugewiesener Nummern) bei der Verwaltung der Parameterwerte in Protokollen und Normen. Im RFC 1700 sind viele dieser Festlegungen veröffentlicht.

1.5 - ICANN

Die **ICANN** (Internet Corporation for Assigned Names and Numbers; deutsch: Internet-Gesellschaft für zugewiesene Namen und Nummern) ist eine Non-Profit-Organisation mit Sitz im kalifornischen Marina del Rey und verwaltet die begehrten Domänennamen sowie die IP-Adressräume. Dies bedeutet auch, dass unter ihrer Regie die 13 Root-DNS-Server betrieben werden. Die Aufgabe wurde am 6.11.1998 von der IANA übernommen. Die Organisation ist mit dem US-Handelsministerium verbunden. Damit hat das Ministerium ein Vetorecht bei Entscheidungen was immer wieder Anlass zu internationalen Verstimmungen beinhaltet.



Anfang 2001 wurden 7 neue so genannten „**Generic Top Level Domains**“ (gTLD's) für das weltweite Datennetz zugelassen.

Damit gibt es folgende Gerneric TDL's:

Domainkürzel	Domain-Bezeichnung
com	Kommerziell (eng: commercial)
edu	Bildung (engl: education)
gov	Regierungsorganisationen
mil	Militär
net	Netzwerke
org	Organisationen
name	Websites von Privatpersonen
prof	Bestimmte Berufsgruppen
museum	Museen
biz	Business
aero	Luftfahrt
info	Informationsanbieter
coop	Genossenschaftliche Organisationen

Für die einzelnen Länder gibt es natürlich noch die so genannten „**Country Code TLD's (ccTLD's)**“ wie de für Deutschland, us für USA , fr für Frankreich, it für Italien, se für Schweden usw.

Ab dem 12.01.2012 werden Bewerbungen um Branchen-TDLs (.reise), Geo-TDLs (.bayern) oder City-TDLs (.koeln) von der ICANN angenommen. Die neuen Domains sind seit 2013 verfügbar .

Weitere Gremien sind:

1.6 - ECMA

Die European Computer Manufacturers Association ist eine private internationale Organisation zur Normung von Kommunikations-, Unterhaltungs- und Informationssystemen.



Der Hauptsitz ist in Genf. Um der internationalen Ausrichtung Rechnung zu tragen wurde der Name 1994 geändert was allerdings dazu geführt hat, dass der Name seine ursprüngliche Bedeutung verloren hat. Beispiele für hier verfasste Normierungen sind:

Office Open XML, C#.

1.7 - IEC

Die International Electrotechnical Commission wurde 1906 in London gegründet und war wesentlich daran beteiligt Normierungen für Maßeinheiten zu vereinfachen. Die IEC hat als erstes Gremium das von Giovani Giorgi entwickelte System, aus dem später das SI-System entstand, vorgeschlagen.



1938 wurde das International Electrotechnical Vocabulary, ein Wörterbuch für Begriffe aus der Elektrotechik veröffentlicht. Heute ist dieses Wörterbuch (Electropedia) frei verfügbar und unter: <http://www.electropedia.org/> (IEC 60050) erreichbar. Die Sprachen Englisch, Französisch, Arabisch, Chinesisch, Deutsch, Italienisch, Japanisch, Portugiesisch, Russisch, Spanisch und Schwedisch werden unterstützt.

1997 wurde die bis dato veröffentlichten Normen neu durchnummerniert indem man 60000 hinzu addierte. Aus IEC50 wurde damit IEC 60050. Das Nummernband reicht somit von 60000 bis 79999.

Beispiel: IEC 60417 (Graphical Symbols for use on Equipment).

Wer sich für Spannungen, Frequenz, das Aussehen von Steckern und Steckdosen Betrieb von Elektrischen Geräten in Europa interessiert kann sich unter: <http://www.iec.ch/worldplugs> informieren.

1.8 - DBP

Die Deutsche Post, früher Deutsche Bundespost, hat zu ihren Monopolzeiten kräftig normiert. Hier wurden viele Protokolle und Verordnungen wie z. B. Die FO (Fernmeldeordnung) oder VfrsDx (Verordnung für den Fernschreib- und Datendienst) erstellt.



1.9 - EIA / TIA

1988 wurde die **EIA** (Electronic Industries Alliance) mit der **TIA** (Telecommunication Industries Association) zusammengelegt.

1991 wurde von der EIA/TIA der Standard „Commercial Building Telecommunications Wiring“ bekannt als EIA/TIA 568(1) veröffentlicht.

Darin sind die Grundlagen der strukturierten Verkabelung (siehe auch nächstes Kapitel) beschrieben.

In der **EN 50173** wurden diese Standards zur Europäischen Norm umgesetzt.



1.10 - RIPE (Réseaux IP Européens)

Zuständig für die IP-Adressvergabe in Europa.

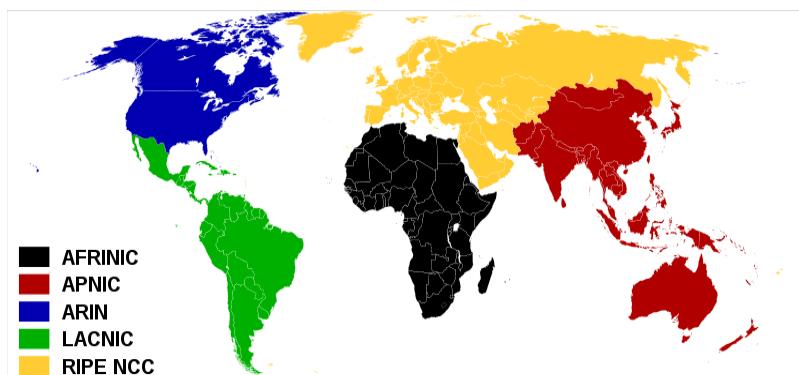


Abbildung 2: Bereiche der IP-Adressvergabe

1.11 - BS (British Standard)

Das BSI (British Standards Institution) wurde 1901 unter dem Namen Engineering Standards Committee von James Mansergh, mit der Aufgabe der Normierung von Stahlsektionen, gegründet. Die Normen werden unter der Bezeichnung BS xxxx oder in BSi xxxx veröffentlicht

In England wurden Normen entwickelt, die auch für den restlichen Europäischen Raum Bedeutung erlangt haben. Hierzu zählen mit dem BS 7799 als Basis für die Sicherheits-Zertifizierungen und dem BS 15000 als Basis für ITIL. Diese Normen wurden in die ISO-Normen übernommen. Der BS 15000 wurde zum DIN ISO 20000.



Produkte und Dienstleistungen, welche die nach BSI vorgegebene Standards erfüllen, werden vom BSI mit dem sog. Kitemark-Prüfsiegel versehen. Der kommt von der Ähnlichkeit mit einem Papierdrachen, englisch = kite.



1.12 - EN

Für Europäische Normen ist das CEN (Comité Européen de Normalisation) zuständig. 1962 wurde die CEN von Normierungsgremien der Staaten von EWG und EFTA gegründet.

Mit seinen EN (Europäische Normen) werden alle Bereiche außer Elektrotechnik und Telekommunikation abgedeckt.

Link: <http://www.cen.eu>



European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Für die Elektrotechnischen Normen ist die CENELEC (Europäisches Komitee für elektrotechnische Normung) zuständig. Link: <http://www.cenelec.eu>

Für die Telekommunikation ist die ETSI (Europäisches Institut für Telekommunikationsnormen)

Im europäischen Zusammenhang sind auch Normen entwickelt worden. Diese können aus nationalen oder internationalen Normen entlehnt worden sein. Link: <http://www.etsi.org>

Die CENELEC ist auch zuständig für das CE-Kennzeichen auf Elektrogeräten mit dem der Hersteller bestätigen, dass das Gerät den europäischen Richtlinien entspricht. Mit einer 4-stelligen Kennnummer ist dokumentiert, dass eine Benannten Stelle eingebunden war. Das CE-Kennzeichen ist kein rechtliches Gütesiegel! Trotzdem kann es mit dem China-Export-Kennzeichen verwechselt werden, welches nur auf die Herkunft hinweist und keine Rückschlüsse auf die Verwendbarkeit zulässt.

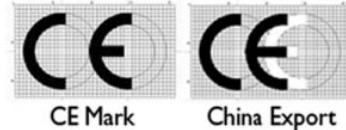


Abbildung 3: CE-Kennzeichen

1.13 - ISO

ISO steht für International Organisation for Standardization.

1946 trafen sich die Delegierten aus 25 Nationen in London um eine internationale Organisation zu schaffen, die das Ziel hat, die verschiedenen nationalen Standards zu koordinieren und zu vereinheitlichen.

Die ISO wurde am 23. 2. 1947 als nicht staatliche Organisation gegründet. Trotzdem hat es oft den Anschein als ob einige Länder über diese Organisation ihren Einfluss geltend machen wollen. Das liegt zum Teil auch an den Auswahlverfahren für die Mitglieder. Es kommt vor, dass die Mitglieder von staatlichen Organisationen ausgewählt und entsandt werden. Trotzdem versteht sich die ISO als Mittler zwischen den Staaten, Herstellern und der Gesellschaft.



Bis heute hat die ISO mehr als 13700 internationale Normen veröffentlicht.

Bekannt wurde z. B. Die ISO 9000 im Rahmen der Qualitätssicherung und im Netzwerk-Umfeld durch das Open Systems Interconnection Model, welches auch OSI-Referenzmodell (**OSI-RM**) genannt wird.

1.13.1 - OSI-Modell

Im Open Systems Interconnection Model der ISO wird die Bearbeitung der Übertragung von Informationen in ein Modell aus 7 Schichten aufgeteilt.

Es wurde von 1977 bis 1984 entworfen und 1984 von der ISO als ISO-Norm 7498 veröffentlicht. Jede Schicht stellt eine oder mehrere Funktionen zur Verfügung. Die Funktionen können von den überlagerten Schichten als Dienst genutzt werden. Näheres siehe Kapitel Schichtenmodelle.

1.14 - IEEE-Normen

Das **IEEE** (Institute of Electrical and Electronics Engineers) ist der größte Fachverband der Welt. Außer Fach-Konferenzen und Veröffentlichungen von Testberichten werden in einer Normierungsgruppe Normen im Bereich der Elektrotechnik und Informatik erarbeitet. Eine der wichtigsten Normen im Bereich der LAN ist IEEE-802. Diese Norm wurde von ISO als Grundlage für **ISO-8802** verwendet.



Die Bezeichnung hat ihren Ursprung im Gründungsdatum der Gruppe im Februar 1980.

Die **IEEE-802** wird in weitere Untergruppen mit folgenden Bedeutungen unterteilt:

Norm	Bedeutung
IEEE-802.1	Übersicht über die Normen
IEEE-802.1d	Spanning Tree
IEEE-802.1p	Spezifikation der QoS (Quality of Service)
IEEE-802.1q	Spezifikation von VLANs (Virtuelle LANs)
IEEE-802.1w	Rapid Spanning Tree
IEEE-802.1x	Authentifizierung
IEEE-802.2	Oberer Teil der Sicherungs-Schicht (2.2) Hier wird die LLC (Logical Link Control) abgehandelt
IEEE-802.3	Beschreibung des LAN mit dem Zugriffsverfahren CSMA/CD (Carrier Sense Multiple Access / Collision Detection)
IEEE-802.3a-t	Eigenschaften von 10Mbit-Ethernet
IEEE-802.3u	Beschreibung von 100Mbit-Ethernet (Autonegotiation 10/100Mbps FDX/HDX)
IEEE-802.3y	100Base-T2
IEEE-802.3z	1000Base-TX
IEEE-802.3ab	1000Base-TX mit CAT5-Kabeln mit 100m Reichweite
IEEE-802.3af	Power over Ethernet
IEEE-802.4	Beschreibung des LAN mit dem Zugriffsverfahren Token Bus
IEEE-802.5	Beschreibung des LAN mit dem Zugriffsverfahren Token Ring
IEEE-802.6	Beschreibung des MAN DQDB (Distributed Queue Dual Bus)
IEEE-802.7	Broadband
IEEE-802.8	Fibre-Optic
IEEE-802.9	Voice & Data
IEEE-802.10	Gruppenbildung und Tagging (SDE Secure-Data-Exchange) (VLAN's)
IEEE-802.11	Wireless LAN
IEEE-802.12	Beschreibung des LAN 100VGAnyLAN

Weiterentwicklungen oder Ergänzungen sind daran erkennbar, dass Buchstaben angehängt werden. Z. B. IEEE-802.11 → IEEE-802.11a → IEEE-802.11b. Ist man einmal bei z angekommen wird mit aa → ab → ac weiter gemacht. Für die Einführung eines Standards gibt sich die IEEE 4 Jahre Zeit.

1.15 - RFC's

1.15.1 - Allgemeines

Die schnelle Entwicklung der Netzwerktechnologie beruht größtenteils auf der Art und Weise, in der Innovationen vorgestellt, begutachtet, korrigiert und dokumentiert werden. Nämlich den RFC's.

Ein RFC (Request For Comment; deutsch: Anfrage auf Kommentierung) ist eine Beschreibung eines technischen Zusammenhangs, vornehmlich im Bereich der Netzwerke. Der Verfasser wendet sich an alle, um Kommentare, zu seiner vorgeschlagenen Lösung, zu bekommen.

Wer etwas Neues der Weltöffentlichkeit vorstellen möchte, kann sich an das IAB (Internet-Architecture-Board) wenden. Das IAB ist ein Bereich des IETF (Internet Engineering Task Force).

Dort kann man einen Text einbringen. Er bekommt, wenn das IAB meint es wäre ein guter Beitrag, eine RFC-Nummer unter der er der Öffentlichkeit vorgestellt wird. Damit hat der RFC den Status Proposed Standard (deutsch: vorgeschlagene Norm).

Dann wird der RFC in der Netzwerkwelt diskutiert.

Findet der RFC ausreichend Interesse und sind mindestens zwei funktionierende Implementierungen mehr als vier Monate in Betrieb, erreicht der RFC den Status Draft Standard (Norm-Entwurf).

Ist der IAB davon überzeugt, dass die Idee fundiert ist und stabil läuft, kann sie nach 6 Monaten zum Internet Standard ausgerufen werden.

Dies erscheint etwas umständlich in der Abwicklung, ist jedoch immer noch die schnellste Art und Weise, in der Innovationen von einer breiten Hersteller- und Anwenderbasis umgesetzt werden.

Wer sich mit RFC's beschäftigen will, sollte sich zuerst einen aktuellen RFC-Index besorgen. Darin sind alle RFC's, nach ihrem Erscheinen und somit der Nummer nach, geordnet aufgeführt. In diesem RFC-Index kann ermittelt werden, welcher RFC der aktuellste zu einem Thema ist. Es kann vorkommen, dass RFC's abgelöst oder ergänzt werden. Um aktuelle Informationen zu bekommen, ist also zuerst der RFC-Index zu bemühen.



1.15.2 - RFC-Lebenszyklus

Die Abwicklung der RFC's ist selbst in einem RFC beschrieben (RFC 1280 „IAB Official Protocol“ Standards). In der folgenden Abbildung, ist der Lebenszyklus eines RFC's beschrieben.

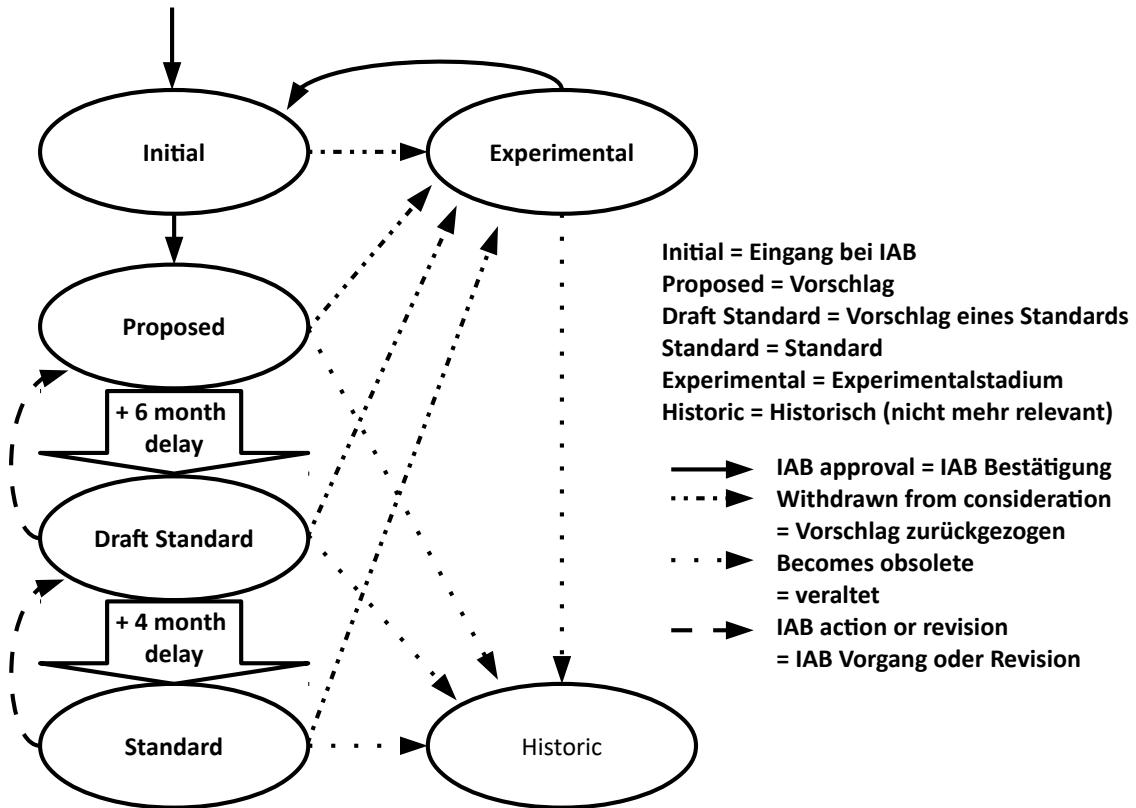


Abbildung 4: RFC-Lebenszyklus

1.15.3 - Beispiele bekannter RFCs

- RFC 1 (erster RFC von Steve Crocker)
- RFC 768 (UDP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 959 (FTP)
- RFC 1006 (Umsetzung des ISO/OSI-Protokolls auf TCP/IP)
- RFC 1034 (DNS – Concepts and Facilities)
- RFC 1035 (DNS – Implementation and Specification)
- RFC 1094 (NFS Version 2 Protocol Specification)
- RFC 1166 (IP-Adresse)
- RFC 1280 (Beschreibung der RFCs selbst)
- RFC 1321 (MD5 Message-Digest Algorithm)
- RFC 1459 (IRC)
- RFC 1661 (PPP)
- RFC 1738 (URLs)
- RFC 1813 (NFS Version 3 Protocol Specification)
- RFC 1855 (Netiquette)
- RFC 1939 (POP3)
- RFC 2131 (DHCP)
- RFC 2222 (SASL)
- RFC 2251 (LDAP)
- RFC 2440 (OpenPGP)
- RFC 2445 (iCalendar)
- RFC 2613 (Remote Network Monitoring)
- RFC 2616 (HTTP 1.1)
- RFC 2821 (SMTP)
- RFC 2822 (E-Mail-Format)
- RFC 3174 (SHA)
- RFC 3530 (NFS Version 4 Protocol Specification)

1.15.4 - RFC-Bezugsquellen

Bezogen werden können die RFC's aus dem Internet z. B.

<ftp://nic.ddn.mil/rfc>

www.rfc-editor.org – Offizielle Webseite (englisch)

www.rfc.net – RFC, FYI, STD und BCP als .html, .txt, .ps mit verschiedenen Indexen

www.rfc-editor.org/fyi-index.html – Auflistung der FYI-Dokumente (englisch)

www.rfc-ref.org – RFCs im HTML-Format

1.15.5 - FAQ's

Mit den FAQ's (Frequently Asked Questions (deutsch: Oft gestellte Fragen)) wird eine Liste mit Fragen und Antworten zu einem Thema, Gerät usw. der Öffentlichkeit zur Verfügung gestellt. In den Texten werden meist einführende Fragen, mit deren Antworten dargestellt, die von allgemeiner Natur sind. Tiefergehende Informationen sind hier oft nicht möglich.

1.15.6 - FYI's

(FYI bedeutet For Your Information (deutsch: zu Ihrer Information)) Um im Gegensatz zu den trockenen Texten der RFC's, eine leicht verdauliche Beschreibung der Internet-Themen zu veröffentlichen, wurden innerhalb der RFC-Reihe, eine Serie mit den FYI's erstellt und der Öffentlichkeit zur Verfügung gestellt. Diese Texte sind leicht verständlich und für ein breiteres Publikum gedacht.

2 - Netztechnik-Grundlagen

An die Netztechnik kann man sich mit unterschiedlichen Herangehensweisen annähern. In der technisch geprägten Literatur geschieht das im Allgemeinen über die Informationssysteme. Es gibt jedoch noch andere Ansätze. Zuerst ein Beispiel aus der Wirtschaft.

2.1 - Zusammenhang mit Wirtschaft

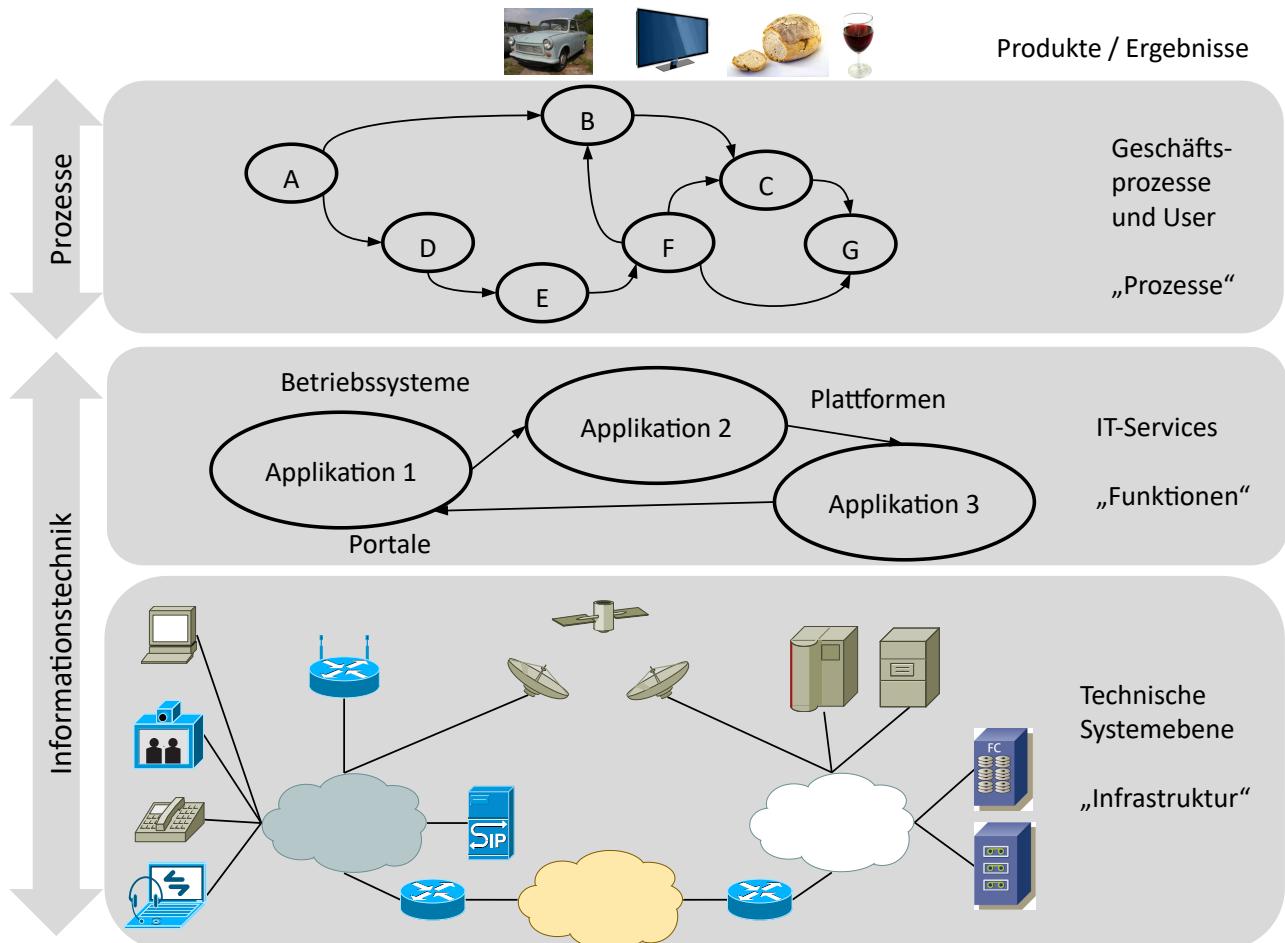


Abbildung 5: Einordnung der Netztechnik in die Ebenen der Wirtschaft

Im Gesamtzusammenhang der Wirtschaft kann die Netztechnik als Teil der **Informationstechnik (IT)** verstanden werden. Die Netztechnik gehört hierbei größtenteils in den Bereich der Infrastruktur, reicht jedoch auch bis in die Betriebssysteme hinein.

2.2 - Grundbegriffe bei der Informationsverarbeitung

2.2.1 - Informationssysteme

Eine andere Betrachtungsweise stellt die Netztechnik in den Zusammenhang der Informationssysteme. Information kann als Wissen über Sachverhalte und Vorgänge verstanden werden. Damit sind sie an Menschen zur inhaltlichen Informationsverarbeitung gebunden. Der Mensch benötigt Informationen um Situationen zu erkennen, Entscheidungen zu treffen und zu handeln.[Scherff-GCN-2010]

Alle Organisationen nutzen Informationssysteme. Informationssysteme erfüllen 3 Funktionen:

- **Übermittlung von Informationen**
Dabei wird zwischen räumlich nahen Informationserzeugern und Informationsnutzern kommuniziert, oder Informationen über große räumliche Distanzen zwischen Kommunikationspartnern ausgetauscht (Telekommunikation). Kommunikation bedeutet; Austausch von Informationen zwischen so genannten Kommunikationspartnern.
- **Netztechnik** bildet die technische Basis für den Austausch von Informationen.
- **Speicherung von Informationen**
Damit kann die Zeit zwischen Informationserzeugung und der Informationsnutzung überbrückt werden.
- **Verarbeitung von Informationen**
zur inhaltlichen Transformation

Akteure in diesem Zusammenhang sind auf der einen Seite Menschen als Erzeuger und Nutzer der Informationen und andererseits Maschinen in Form von Kommunikationssystemen und Computer für die Datenverarbeitung.

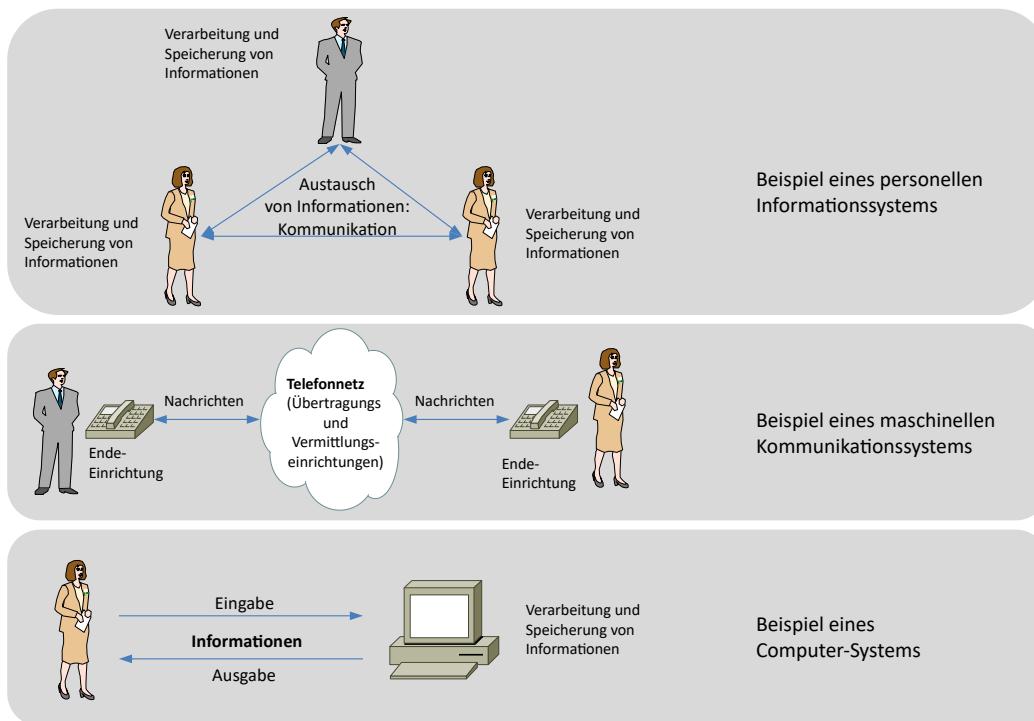


Abbildung 6: Informationssysteme

2.2.2 - Information

Im Zusammenhang Informationsverarbeitung gilt es einige Begriffe richtig einzuordnen.

- ➊ **Zeichen** sind einzelne Werte aus einem so genannten Zeichenvorrat, die mit einem Code definiert werden.
- ➋ **Daten** sind Zeichen, mit einer syntaktischen Zuordnung.
- ➌ **Informationen** sind Daten, die für eine Bedeutung für den Empfänger. Informationen sind für den Empfänger wichtig und neu.
- ➍ **Wissen** entsteht im Kopf wenn Informationen mit Erfahrung und Vernetzung in Zusammenhang gebracht werden.
- ➎ **Aktionen** können ausgelöst werden, wenn Wissen angewendet wird.

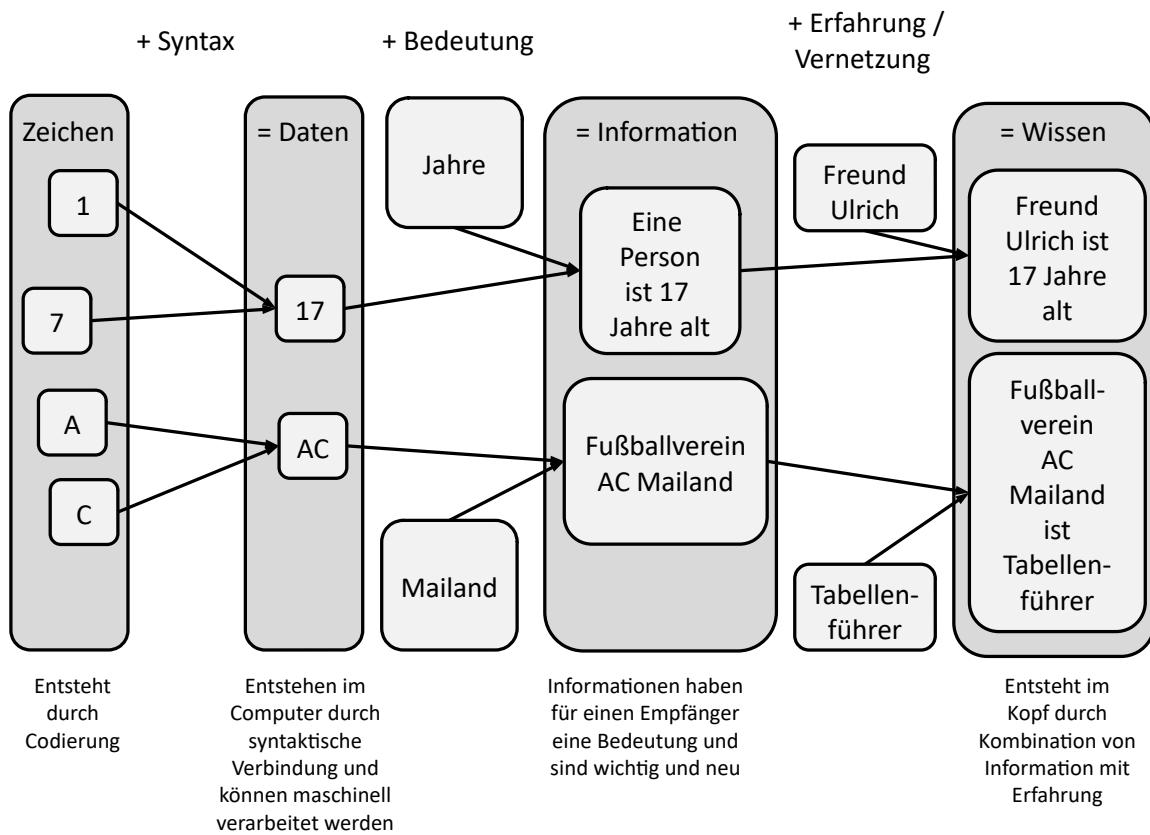


Abbildung 7: Einsortierung von Informationen in Wissen

2.2.3 - Anforderungen an Informationssysteme

Informationssysteme und Kommunikationssubsysteme unterliegen sich widerstreitenden Anforderungen.

- Geschwindigkeit
- Verfügbarkeit
- Kosten
- Sicherheit
- Qualität
- ???

2.2.3.1 - Geschwindigkeit

Eine der Hauptanforderungen an Informations- und Kommunikationssysteme ist die Geschwindigkeit. Der immer größer werdenden Datenmenge, die zu verarbeiten ist, kann durch Komprimierungsverfahren und einer schnelleren Bearbeitung bzw. einem schnelleren Transport begegnet werden. Tatsächlich können die Daten nicht schneller durch die Netzwerke gesendet werden. Stattdessen werden immer Bits parallel (also während einer Zeiteinheit) transportiert.

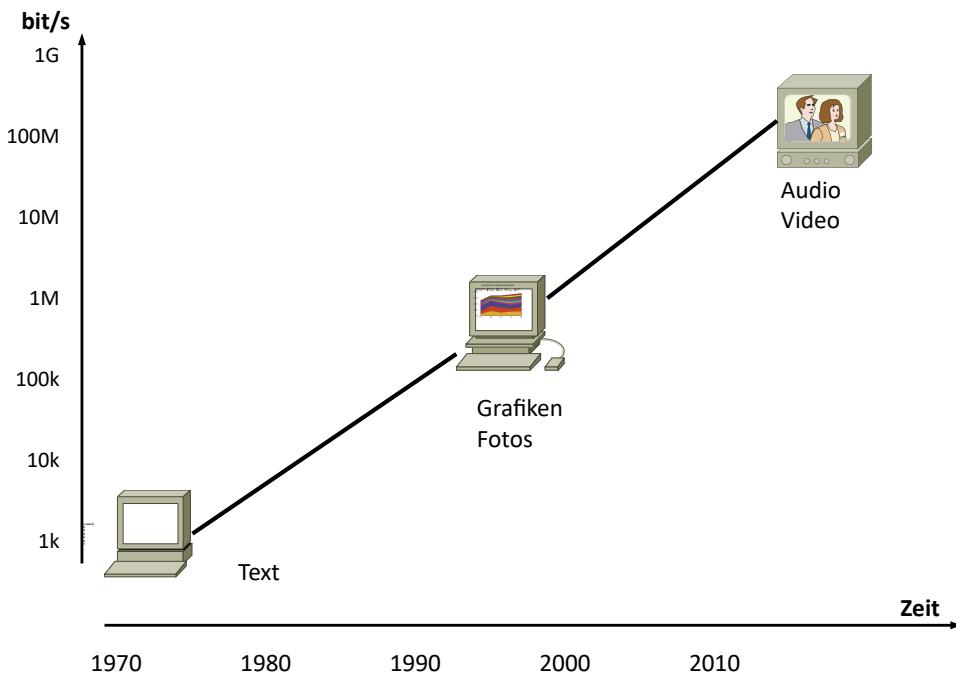


Abbildung 8: Bandbreitenbedarf über der Zeit

2.2.3.2 - Verfügbarkeit

Ein Kommunikationssystem sollte immer zur Verfügung stehen. Jedoch unterliegen auch Kommunikations-Systeme Ausfällen und Wartungsarbeiten.

Die Verfügbarkeit wird nach der folgenden Formel berechnet:

$$\text{Verfügbarkeit} = (\text{Gesamtzeit} - \text{Gesamtausfallzeit}) / \text{Gesamtzeit}$$

Die Berechnung erfolgt auf Basis eines Jahres. Sind keine Wartungszeiten zugelassen gilt:
24 Stunden/Tag * 365 Tage = 8760 Stunden

Verfügbarkeit [%]	Minimal erwartete Betriebszeit [Stunden]	Maximal erlaubte Ausfallzeit [Stunden]	Maximale erlaubte Ausfallzeit [Minuten]
98,5	8628,6	131,4	7884
99	8672,4	87,6	5256
99,2	8689,92	70,08	4204,8
99,4	8707,44	52,56	3153,6
99,6	8724,96	35,04	2102,4
99,8	8742,48	17,52	1051,2
99,9	8751,24	8,76	525,6
99,99	8759,124	0,876	52,56
99,999	8759,9124	0,0876	5,256
100	8760	0	0

Systeme, die mit 98,5 % Verfügbarkeit oder schlechter festgelegt wurden können mit einfachen Komponenten aufgebaut werden.

Systeme mit einer besseren Verfügbarkeit sind mit einem **Verfügbarkeits-Verbund** (also redundant) aufzubauen.

Hochverfügbare Systeme, sind Systeme mit einer Verfügbarkeit von mindestens 99,99 %.

2.2.3.3 - Kosten

Je nach Anwendungsfall können die Kosten sich in kleinen Rahmen halten (Verbindung zweier PCs), oder einen großen finanziellen Aufwand bedeuten (Kommunikation über Satelliten-Verbindungen). Grundsätzlich gilt natürlich, dass sich die Kosten so gering wie möglich halten sollen. Dies führt zeitweise dazu, dass nicht unbedingt die beste Möglichkeit zum Zug kommt.

2.2.3.4 - Qualität

Grundsätzlich gilt die Forderung nach maximaler Datenqualität. Allerdings gibt es Anwendungen bei denen es auch vorkommen kann, dass z. B. einzelne Datenpakete verloren gehen können, ohne dass die grundsätzliche Funktionalität leidet. Z. B. bei Voice über IP (VoIP)

2.2.3.5 - Sicherheit

Die Sicherheit der Datenübertragung ist in den letzten Jahrzehnten zu einer elementaren Forderung bei der Datenkommunikation geworden. Anfänglich war man froh, wenn die Kommunikation überhaupt zustande kam. Die Protokolle aus den ersten Tagen hatten keine Mechanismen zur Verschlüsselung. Heutzutage geht es nicht mehr ohne. (z. B. IPv4 im Vergleich zu IPv6)

2.3 - Kommunikationsmodelle

Kommunikationssysteme wurden ursprünglich entwickelt um **Nachrichten** zwischen Menschen zu übertragen (Telefon, Fernschreiber, ...). Nachrichten werden nach DIN 44 300 als Darstellung von Informationen durch Zeichen oder kontinuierliche Funktionen wie Sprache oder Schallwellen definiert.

Computer verarbeiten **Daten**. DIN 44 300 definiert Daten als Darstellung von Informationen durch Zeichen oder kontinuierliche Funktionen (z. B. analoges Foto).

Damit muss ein User seine Informationen als Daten darstellen damit ein Computer sie verarbeiten kann.

Computernetzwerke bestehen aus räumlich getrennt verteilten autonomen Computern die mit Übertragungseinrichtungen, Vermittlungseinrichtungen und Übertragungsmedien wie Kupfer oder Glasfasern miteinander verbunden sind. Da ein Computernetz Daten überträgt spricht man von **Datenübertragung** und nicht von Informationsübertragung. Computernetzwerke werden in der Literatur oft in Form einer Wolke (Cloud) dargestellt. Z. B. wie in Abbildung 5.

Die Kommunikation kann in Rahmen unterschiedlicher Modelle erfolgen. Je nach Anwendungsfall bieten sich unterschiedliche Ausprägungen an.

Grundsätzlich unterscheidet man:

- ➊ Terminal-Netz
- ➋ Client-Server-Modell
- ➌ Peer-to-Peer-Modell
- ➍ E-Commerce
- ➎ Ubiquitous Computing

2.3.1 - Terminal-Systeme

In den Anfängen der Computernutzung gab es Systeme mit Batchbearbeitung oder Prozessrechner für die Steuerung von Automatisierungssystemen.

Die ersten Systeme, die Computerleistungen mehreren Nutzern zugänglich machen, waren Terminal-Systeme. Die Terminals von der Größe einer Hundehütte mit 24*80 monochromen Zeichen auf dem Bildschirm konnten entweder direkt an den Host angeschlossen werden, oder über Multiplexer (auch Konzentratoren genannt) via

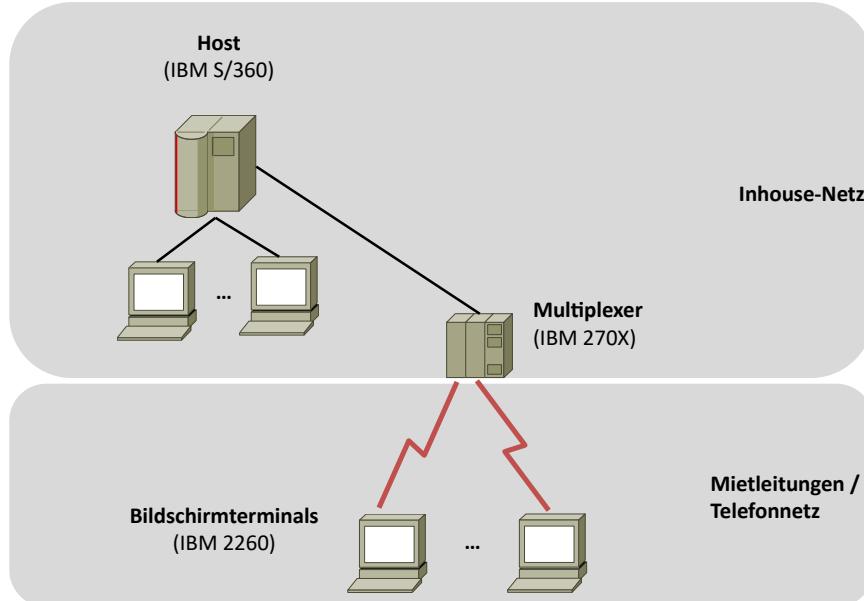


Abbildung 9: Terminal-Netzwerk

Telefonleitungen an entfernte Standorte angeschlossen werden.

2.3.2 - Client-Server-Modell

Hierbei werden die Informationen an zentraler Stelle auf einem Server z. B. in einer Datenbank gehalten. Initiiert wird ein Informationsaustausch durch den Client der den Client-Prozess dazu bringt eine Anfrage über das Netzwerk an den Server-Prozess auf dem Server zu senden. Der **Server-Prozess** sendet seine Antwort an den **Client-Prozess** wieder über das Netzwerk zurück. Ein klassisches Beispiel ist eine Internetabfrage bei Google, oder eine Datenbankabfrage.

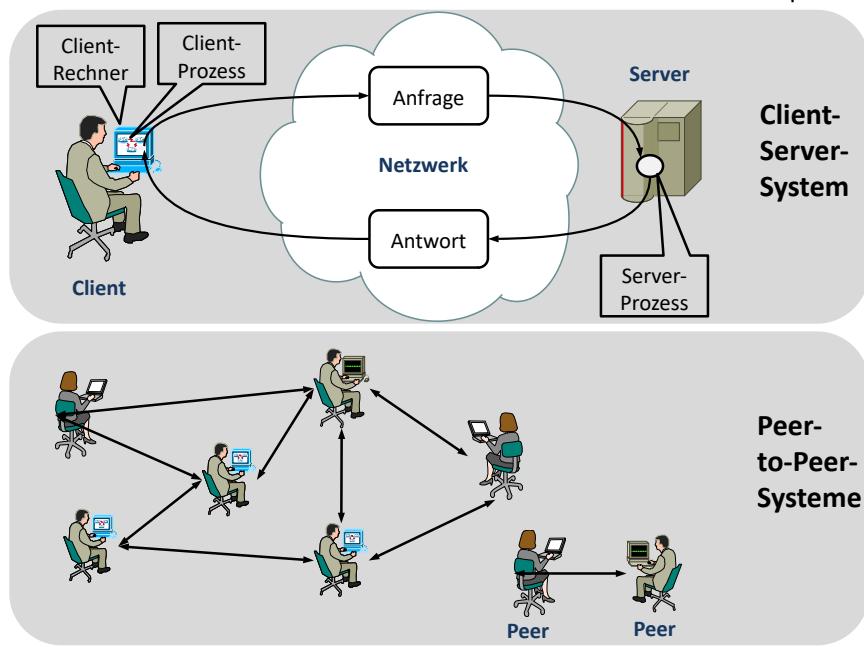


Abbildung 10: Client-Server und Peer-to-Peer-Systeme

2.3.3 - Peer-to-Peer-Modell

Im Peer-to-Peer-Modell gibt es keine festen Zuordnungen, sondern gleichberechtigte Kommunikationspartner, die sich gegenseitig Informationen zukommen lassen. Dabei interagiert ein Peer mit einem anderen oder einer Gruppe von Peers. Es gibt keine zentrale Datenbank. Jeder Peer verwaltet seine Daten selbst. Obwohl Server daran beteiligt sind, ist das Versenden von E-Mails eine Peer-to-Peer-Anwendung.

2.3.4 - E-Commerce

In diesem Bereich haben sich wirtschaftliche Zusammenhänge und Geschäftsmodelle etabliert.

Name	Abkürzung	Beispiel
Business-to Consumer	B2C	Onlinebestellung von Büchern
Business-to-Business	B2B	Kfz.-Hersteller bestellt Reifen beim Lieferanten
Goverment-to-Consumer	G2C	Lohnsteuerjahresausgleich via ELSTER
Consumer-to-Consumer	C2C	Onlineauktion gebrauchter Gegenstände bei Ebay
Peer-to-Peer	P2P	Gemeinsame Nutzung von Musik

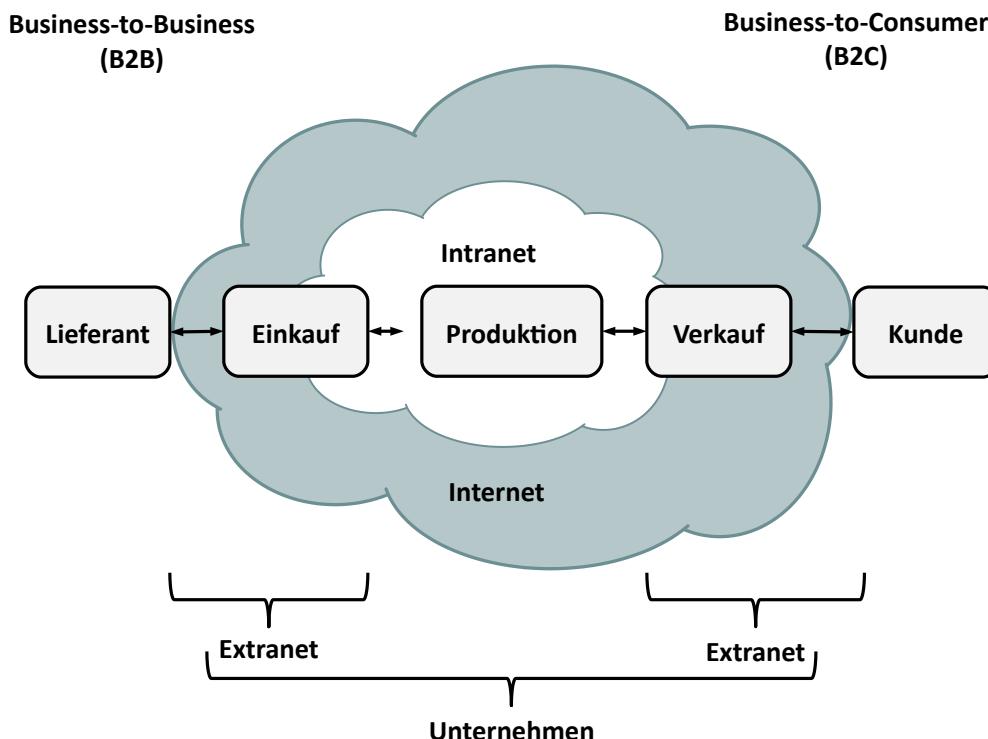


Abbildung 11: E-Commerce-Beispiel

2.3.5 - Ubiquitous Computing

Wie Mark Weiser bereits 1991 beschrieben hat, wird dabei die Rechnerallgegenwart dazu führen, dass die Datenverarbeitung überall stattfindet. Mit Smart Home und dem Internet of Things (IoT) nähert sich unsere Gesellschaft dieser Vision. Geräte wie Fernsehgeräte, Kühlschränke, Rauchmelder, Staubsauger, Strom-, Gas-, Wasserzähler und vieles mehr haben Sensoren und intelligente Systeme an Bord und sind miteinander verbunden.

2.4 - Aufbau von Netzwerken

Nach der Klärung warum kommuniziert wird, steht im folgenden die Übersicht darüber wie kommuniziert wird an.

Grundsätzlich erfolgt eine Übermittlung von Informationen von einer Informations- / **Datenquelle** hin zu einer Informations- / **Datensenke**. Dazwischen ist ein Sender geschaltet, der über einen **Informationskanal** die Daten an einen Empfänger überträgt.

Als **Informationsquelle** agiert im Allgemeinen ein Mensch, der Informationen in ein Informationssystem eingibt. Es kann aber auch ein Sensor sein der Messwerte erfasst.

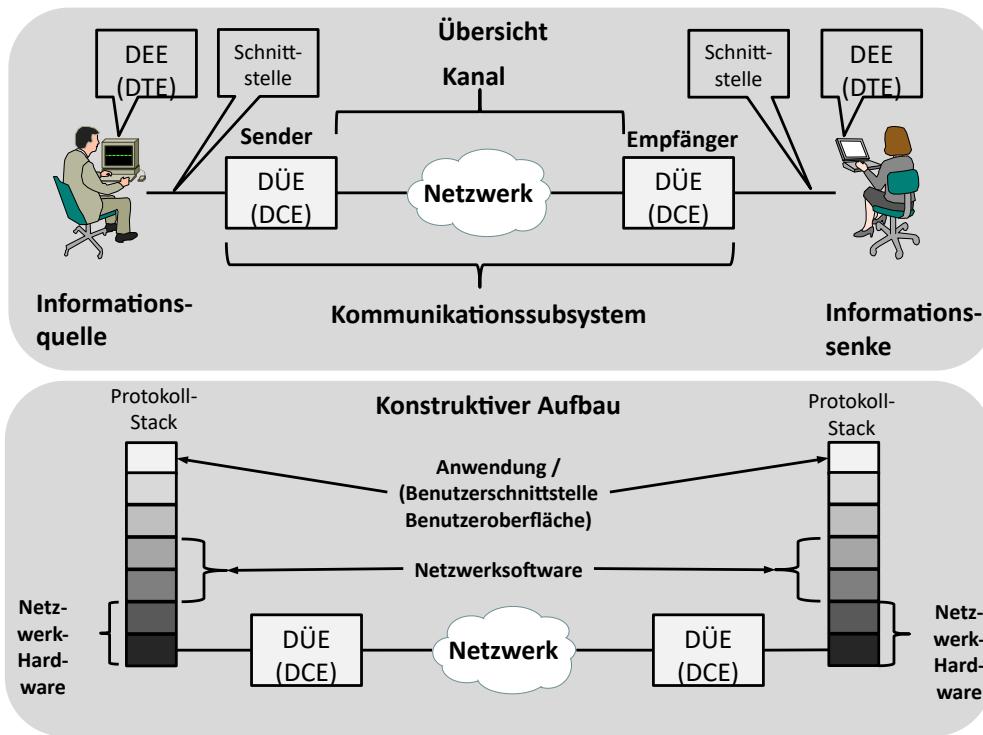


Abbildung 12: Kommunikationssystem

Der Aufbau eines Kommunikationssystems hat folgende Bestandteile:

- ➊ Rechner
- ➋ Kommunikationssubsystem

Ein Rechner, der mit einem Kommunikationssubsystem verbunden ist, wird auch als **Daten-Endeinrichtung (DEE)** (engl. **Data Terminating Equipment (DTE)**) bezeichnet.

Das Kommunikations-Subsystem dient als Datentransportsystem. Die **Daten Übertragungseinheit (DÜE)** (engl. **Data Communication Equipment (DCE)**) übernimmt den physikalischen Anschluss an das Netzwerk. Es leitet den Datenverkehr weiter und liefert Taktsignale zur Synchronisation mit der DEE.

Die Unterscheidung der Geräte ist bei der Steckerbelegung an den Schnittstellen-Leitungen wichtig, da hier in den Steckern zusätzliche Brücken verdrahtet sind. Ein beliebter Fehler ist das Vertauschen der Stecker, da die äußerlich gleich aussehen.

Netztechnik-Grundlagen

Als DÜEs werden die folgenden Geräte bezeichnet.

- ➊ **Modem**
Kunstwort aus Modulator und Demodulator. Dient als Abschluss des Telefonnetzwerks. Setzt digitale Computersignale in analoge Telefonsignale um und umgekehrt.
- ➋ **NTBA (Network Termination Basis Anschluss)**
Abschluss eines ISDN-Netzwerks. Setzt die 2-Draht-Leitung in eine 4-Draht-Leitung (S0-Bus) um.
- ➌ **Transceiver**
Kunstwort aus Transmitter und Receiver. Führt bei Ethernet das Senden und den Empfang der Bits durch. Dient zusätzlich zur Kollisionserkennung.
- ➍ **DSL-Modem**
Wird auch als NTBBA (Network-Termination-Breitbandanschluss) bezeichnet. Dient zum Senden und Empfangen von Daten über eine Teilnehmeranschlussleitung mit DSL-Technik.

Für die Schnittstelle zwischen DEE und DÜE gibt es mehrere Standards:

- ➊ **TIA/EIA-232**
Serielle Schnittstelle zur binären Datenübertragung (Früher RS-232)
- ➋ **ITU-T V.24**
Schnittstelle zur asynchronen Datenübertragung über das Telefonnetz (entspricht TIA/EIA-232)
- ➌ **ITU-T X.21**
Schnittstelle zur synchronen Datenübertragung über öffentliche Datennetze.
- ➍ **ITU-T I.430**
S0-Schnittstelle (siehe hierzu auch ISDN)
- ➎ **USB**
Universal Serial Bus. Universelle Schnittstelle des USB-Interface für eine Vielzahl von Geräten

Funktional gesehen schließt die Schnittstelle das Datentransportsystem ab und ist damit Bestandteil des Teilnehmeranschlusses (z. B. Bei T-DSL der Deutschen Telekom)

Bis 1995 war das auch die Grenze des Hoheitsbereichs der damaligen Deutschen Bundespost. Damals gehörten die DÜEs und die Telefonapparate zum deren Hoheitsbereich.

Erst die darauf folgende Steckerlösung gab dem Teilnehmer das Recht, selbstständig einen Netzabschluss zu installieren und damit sich ein DÜE auf dem Markt zu beschaffen.

Oben auf dem **Protokoll-Stack** dient die Benutzerschnittstelle dem Anwender als Schnittstelle zum Informationssystem. So ist z. B. ein Browser für den Zugriff auf eine Internetabfrage zu sehen.

Die **Netzwerksoftware** (als Bestandteil des Protokoll-Stacks) ist heutzutage Bestandteil des Betriebssystems. Hier sind Protokolle wie z. B. TCP/IP angesiedelt.

Als **Netzwerk-Hardware**, auch Netzwerk-Adapter genannt, (Engl. **Network Interface Controller (NIC)**) dienen heutzutage folgende Komponenten:

- ➊ **Serielle Schnittstellenkarte**
Anschluss an ein Telefonnetz mittels eines externen Modems
- ➋ **ISDN-Karte**
Anschluss über einen S0-Bus an ein NTBA
- ➌ **Ethernet-Karte**
Dient zum Anschluss an ein lokales Ethernet.

Es gibt Geräte bei denen DEE und DÜE in einem Gerät zusammengefasst sind. DIN 44 302 bezeichnet Geräte, die direkt an ein Übertragungsmedium angeschlossen sind, als **Datenstation**.

2.5 - Beziehungsarten

Je nach Anwendungsfall können die Beziehungen zwischen den logischen Diensten und den technischen Netzen folgende Ausprägungen haben:

- **1:1-Beziehung**
Telefondienst in einem früheren nationalen Telefonnetz.
- **1:N-Beziehung**
Weltweiter Datenkommunikationsdienst eines internationalen Konzerns über verschiedene nationale Teilnetze.
- **N:1-Beziehung**
Telefon, Fax, und Datenkommunikationsdienste im nationalen ISDN-Netz.
- **M:N-Beziehung**
Alle möglichen Dienste über alle möglichen Netze des Internets.

2.6 - Kommunikationsformen

Je nachdem welche Akteure an einer Kommunikation teilnehmen werden unterschiedliche Kommunikationsformen unterschieden:

- **Mensch-Mensch-Kommunikation**
Diese Form kann im direkten Gespräch erfolgen oder indirekt mittels Telefon oder auch E-Mail.
- **Mensch-Maschine-Kommunikation**
Wird direkt an einem Computer bei der Eingabe von Daten angewandt, oder indirekt über ein Kommunikationssystem auf einem entfernten Computer. (z. B. Bestellung auf einem entfernten Server)
- **Maschine-Maschine-Kommunikation**
Diese Form wird indirekt über ein Kommunikationssystem mit Datendirektverbindung, eine gemeinsam genutzte Verbindung oder ein Kommunikationsnetz abgewickelt.

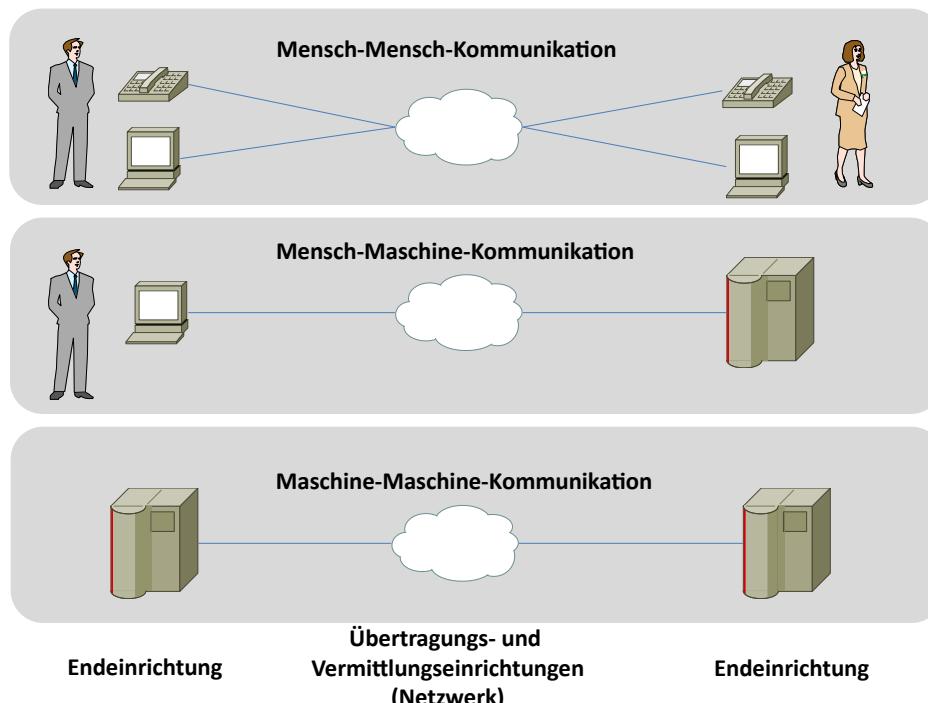


Abbildung 13: Kommunikationsformen

2.7 - Verkehrsarten

Je nach Anzahl der adressierten Empfänger eines Senders wird in unterschiedliche Verkehrsarten unterschieden.

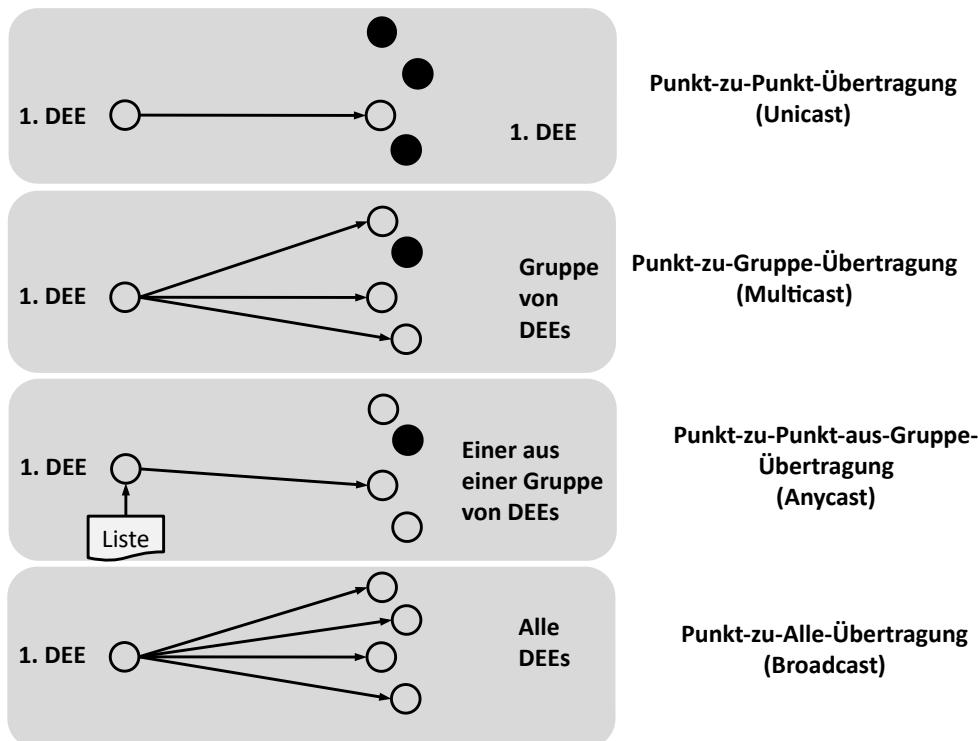


Abbildung 14: Verkehrsarten

Mit einem **Unicast** wird eine 1:1-Kommunikation durchgeführt. Bei einem **Multicast** wird eine Gruppe (mit einer bestimmten Funktion adressiert). Bei einem **Broadcast** werden alle möglichen Empfänger angesprochen. Mit der Einführung von IPv6 wurden die Broadcasts abgeschafft und die **Anycasts** eingeführt. Broadcasts werden als Multicasts abgehandelt und bei Anycasts wird der nächste Node aus einer Gruppe von Nodes angesprochen. Die Verwaltung der Nodes erfolgt mittels einer Liste.

2.8 - Betriebsarten der Nachrichtenübertragung

Die Betriebsart gibt an in welcher Richtung die Nachrichtenübertragung über der Zeit erfolgen kann.

➊ **Simplex-Betrieb**

Nachrichten können immer nur in einer Richtung (unidirektional) übertragen werden. Beispiele hierzu sind Radio und Fernsehen.

➋ **Halbduplex-Betrieb**

Nachrichten können abwechselnd (nacheinander) in beiden Richtung (bidirektional) gesendet werden. Ein Beispiel hierzu ist der Taxifunk.

➌ **Vollduplex-Betrieb**

Nachrichten können gleichzeitig in beide Richtungen (bidirektional) gesendet werden. Beispiele hierzu sind Telefon und moderne Computernetze.

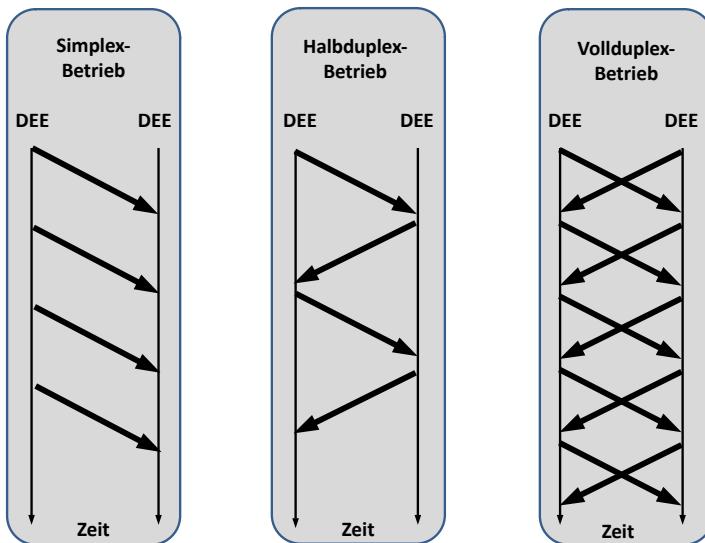


Abbildung 15: Betriebsarten der Nachrichtenübertragung

2.9 - Technisches Übertragungskonzept

Auf physikalischer Ebene kann in zwei unterschiedliche Netzwerk-Übertragungskonzepte unterschieden werden:

- Punkt-zu-Punkt-Netzwerke (Teilstreckennetze)
- Broadcast-Netzwerke (Diffusionsnetze)

2.9.1 - Broadcast-Netzwerke (Diffusionsnetze)

Bei **Broadcast-Netzwerken** überträgt ein Sender fast gleichzeitig Daten an alle Teilnehmer (Empfänger).

Das macht das Senden von **Broadcasts** einfach. Bei **Multicasts** jedoch muss sich jede Station damit beschäftigen, obwohl es möglicherweise nicht erforderlich ist. Noch schlimmer ist es bei **Unicasts**. Da muss die Hardware aller Station die Daten in Empfang nehmen, obwohl sie nur für einen Empfänger gedacht sind. Die gegenseitige Beeinflussung aller Netzteilnehmer ist offensichtlich. Da immer nur eine Station senden darf sind **Medien-Zugriffs-Verfahren** erforderlich. Diese Eigenschaften haben dazu geführt, dass dieses Übertragungskonzept, bis auf Wireless-Netzwerke, von Punkt-zu-Punkt-Netzwerken abgelöst werden.

Da alle Netzteilnehmer alle Daten empfangen können ist das Mitlesen von Daten relativ einfach möglich und muss mit zusätzlichen Methoden (wie z. B. Verschlüsselung) unterbunden werden, was den Betrieb dieser Netze zusätzlich aufwändig macht.

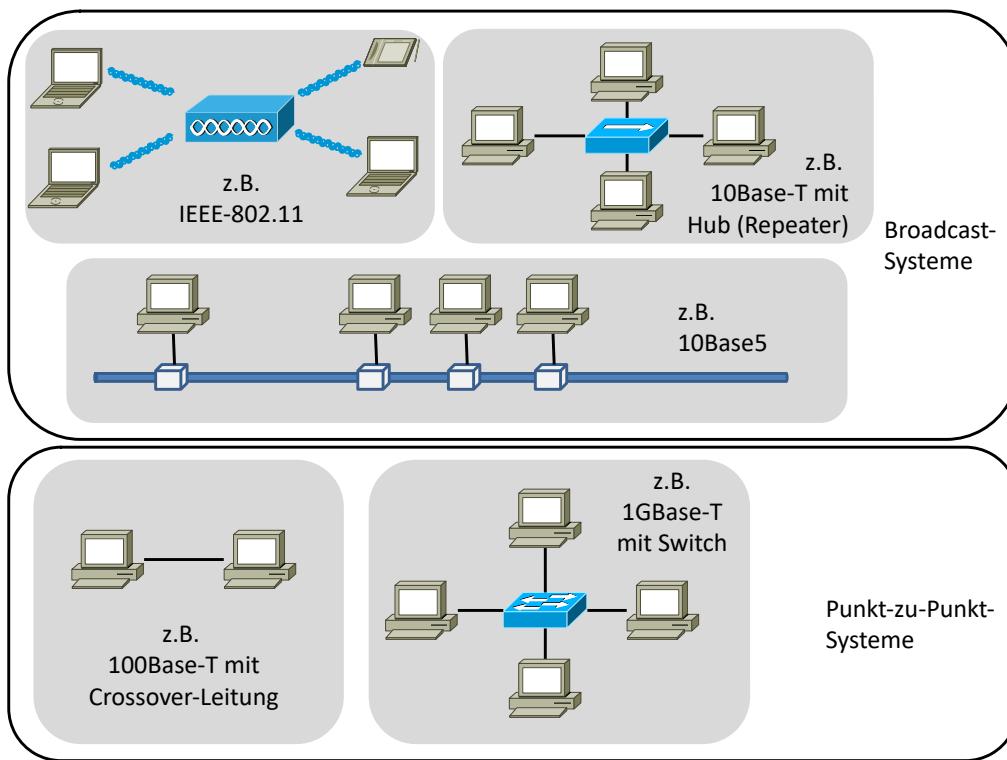


Abbildung 16: Beispiele für Broadcast- und Punkt-zu-Punkt-Netzwerke

2.9.2 - Punkt-zu-Punkt-Netzwerke (Teilstreckennetze)

Die einfachste Verbindung ist die direkte Verbindung zweier Computer miteinander. Sie wird auch **Punkt-zu-Punkt-Netzwerk** genannt.

Unicasts sind einfach zu übertragen. **Multicasts** und **Broadcasts** müssen in den Netzwerk-Geräten speziell behandelt werden damit alle adressierten Empfänger die Daten empfangen.

Netzwerk-Geräte mit Punkt-zu-Punkt-Übertragungskonzept arbeiten nach dem Store-and-Forward-Prinzip. D. h. jedes Netzwerk-Gerät speichert zunächst die Daten und wertet das Zieladressfeld aus um die richtige Weiterleitung aus einer Liste herauszulesen und durchzuführen. Es sind dabei auch mehrere unterschiedliche Dienste möglich. So lässt sich ein Telefondienst und ein Internetdienst, gleichzeitig über die selben Geräte, abwickeln.

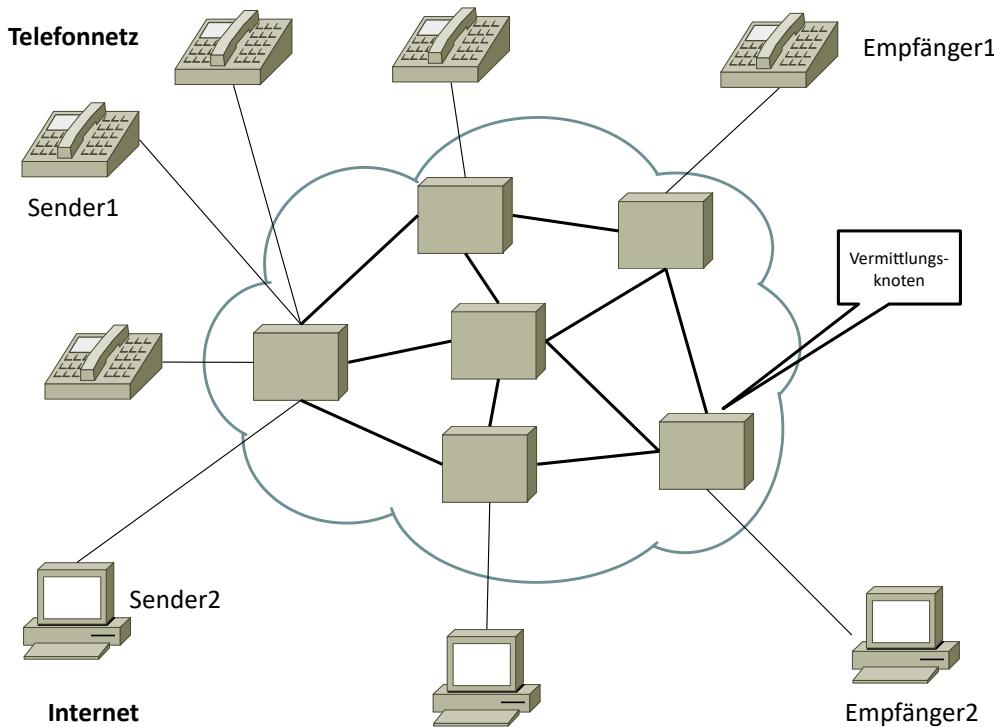


Abbildung 17: Übertragungskonzept von Point-to-Point-Netzen

2.10 - Klassifikation von Rechnernetzwerken

Computernetzwerke können nach unterschiedlichen Gesichtspunkten klassifiziert werden:

- ➊ Betreiber des Netzzugang (öffentlich / privat)
- ➋ Ausdehnung
- ➌ Ziele
- ➍ Verbindungstyp

2.10.1 - Betreiber des Netzzugangs

2.10.1.1 - Öffentlicher Netzzugang

Netzzugänge können wie beim Telefon öffentlich (z. B. von der Telekom) zur Verfügung gestellt werden. Zugang zu diesen Netzen kann jeder nach Bezahlung einer Gebühr bekommen. Bietet der Dienstleister einen Mehrwert, wie z. B. einen Internetzugang an entsteht ein **Value Added Network (VAN)**. Betreiber von Internetzugängen, werden **Internet Service Provider (ISP)** genannt.

2.10.1.2 - Privater Netzzugang

Soll der Netzzugang grundsätzlich nur einer bestimmten Benutzergruppe zur Verfügung gestellt werden spricht man von einem privaten Netzwerk. Dies ist z. B. der Fall bei einem **Local Area Network (LAN)**, in Form eines **Campusnetzwerks** einer Universität, einem **Corporate Network** einer Firma, oder dem **Heimnetzwerk** einer Privatperson (privates LAN).

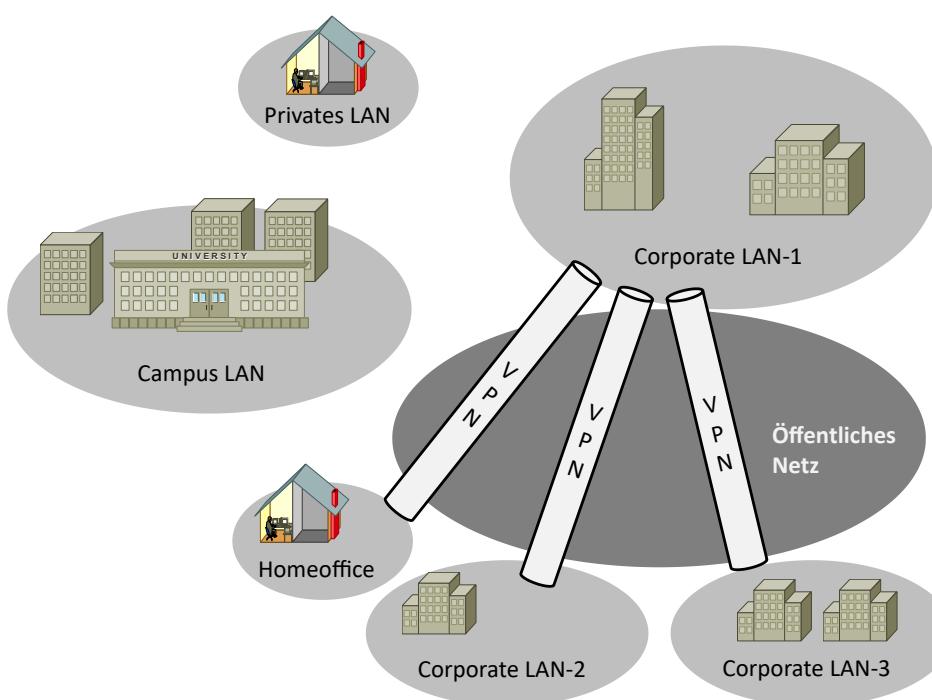


Abbildung 18: Netz-Zugangsarten

Verteilt sich das Corporate Network einer Firma über mehrere Standorte, können die Standorte über ein öffentliches Netzwerk zusammengeschaltet werden. Dabei wird für die Verbindung der Standortnetzwerke ein so genanntes **Virtuelles Privates Netzwerk (VPN)** genutzt. Die Daten werden an der Standortgrenze verschlüsselt und gekapselt, über das öffentliche Netzwerk transportiert und am Zielort wieder entpackt und entschlüsselt. Ein weiteres Beispiel ist ein Mitarbeiter, der im Homeoffice sitzt und über ein VPN mit dem Corporate Network verbunden ist.

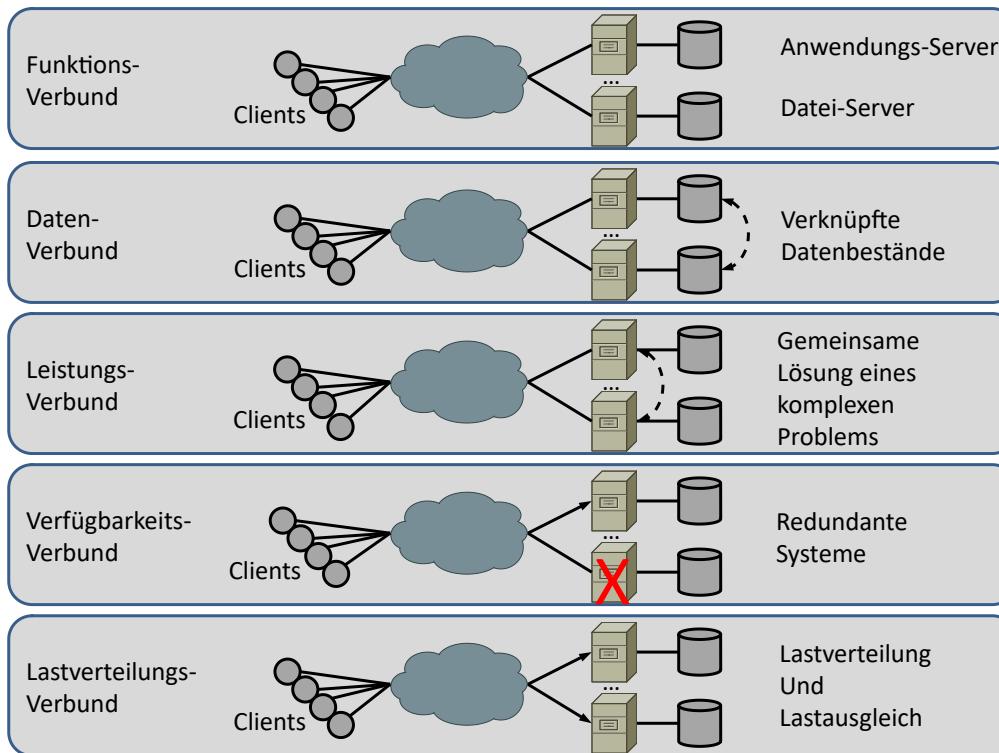
2.10.2 - Ausdehnung eines Netzwerks

Bei der Ausdehnung ist der physikalische Durchmesser und damit auch der Anwendungsfall eines Netzwerks gemeint, der unterschiedliche Größenordnungen annehmen kann.

Kurzbezeichnung	Bezeichnung	Ausdehnung	Anwendung
BAN	Body Area Network	1m	Wearable Computers, BodyNet
PAN	Personal Area Network	10m	Bluetooth
LAN	Local Area Network	10km	LAN / WLAN
SAN	Storage Area Network	10km	RZ und serverorientierte Speichernetzwerke. Optimierte für die Datenspeicherung und Datensicherung. Mit Fiber Channel (FC) Technologie
MAN	Metropolitan Area Network	100km	Ausbreitung über ein Stadtgebiet, wie z. B. WiMAX (IEEE802.16)
WAN	Wide Area Network	Mehrere 1.000km	Öffentliche Netze wie Telefonnetzwerke, GSM, UMTS, LTE
GAN	Global Area Network	Mehrere 10.000km	Erdumspannende Netze, die WANs über Satelliten oder Seekabel miteinander verbinden

2.10.3 - Ziele

Der Betrieb in öffentlichen Einrichtungen und Unternehmen zielt auf die optimale Nutzung von Ressourcen ab. Dabei können Computernetze für die unten genannten Ziele optimiert werden. Mischformen davon sind möglich.



Beim **Funktionsverbund** haben die Server unterschiedliche Funktionen und stellen sich diese gegenseitig zur Verfügung um die Funktionalität eines einzelnen Systems zu erweitern. Dies ist auch die Grundlage einer Client-Server-Architektur. Beispiele hierzu sind AD-Domaincontroller, DNS-Server, DHCP-Server, RADIUS-Server, FileServer, ...

Als Beispiel für einen **Datenverbund** können verteilte Datenbanken oder auch das World Wide Web (WWW) bei dem Dokumente weltweit miteinander verlinkt sind.

Kann die Bearbeitung eines Themas nicht durch einen einzelnen Computer erbracht werden, bietet sich die Verteilung des Problems auf vernetzte Computer in einem **Leistungsverbund** an (Grid-Computing). Voraussetzung ist, dass das Problem in parallele Bearbeitungsstränge zerlegt werden kann. Ein Beispiel hierzu ist die Berechnung der Wettervorhersage.

Zur Erhöhung der Verfügbarkeit einer Anwendung kann diese in weiteren Systemen in einem **Verfügbarkeits-Verbund** vorgehalten werden. Bei Ausfall eines Systems, kann ein anderes System die Anwendung ohne Verlust von Informationen übernehmen. Ein Beispiel hierzu ist das VRRP-Protokoll bei dem ein Router-Ausfall überbrückt werden kann.

Ist das Aufkommen von Anfragen an einen Server zu groß, kann mit weiteren Servern und einer Verteilung der Anfragen reagiert werden. Die **Lastverteilung** wird über spezielle Systeme wie Loadbalancer durchgeführt. Ein Beispiel wäre ein Web-Server eines Versandhauses.

2.10.4 - Verbindungstyp

Als letztes Unterscheidungskriterium für Rechnernetze sollen die Verbindungstypen genannt werden. Dabei wird zunächst in Rundfunksysteme und unterschiedliche Vermittlungssysteme unterschieden. Funknetze wie WLAN nach IEEE-802.11 oder Satellitenfunk basieren auf Funktechnologien. Die Vermittlungssysteme sind an Lichtwellenleiter (LWL) oder Kupferverbindungen gebunden. In Ausnahmefällen können jedoch auch hier z. B. Funkstrecken zur Überbrückung von schwierigem Gelände genutzt werden.

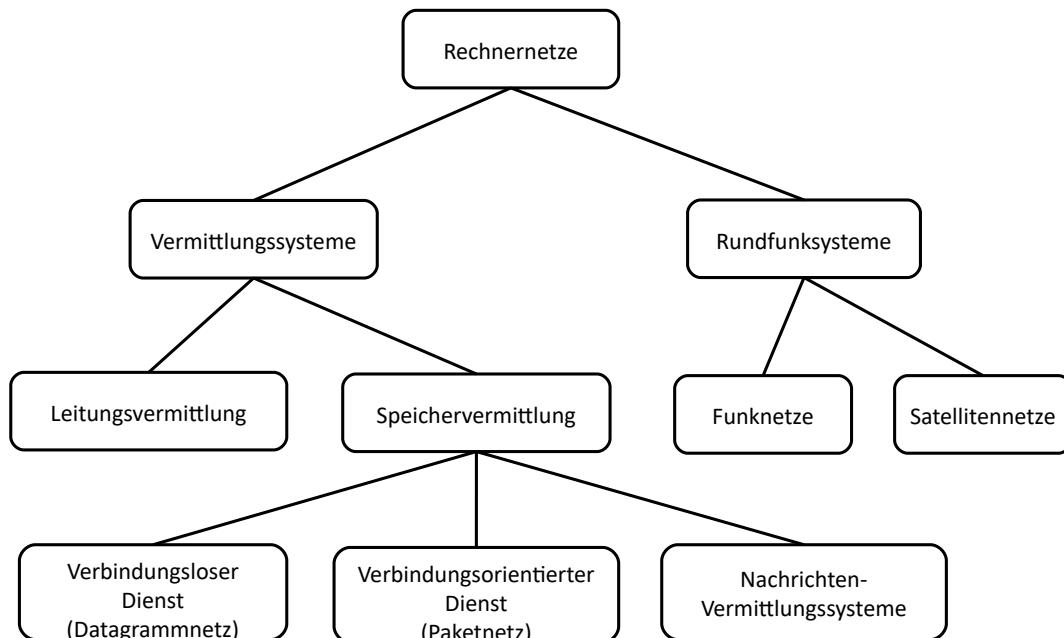


Abbildung 19: Verbindungstypen von Rechnernetzen

2.10.4.1 - Vermittlungssysteme

2.10.4.1.1 - Leitungsvermittlung

Bei der **Leitungsvermittlung** muss vor einem Datenaustausch eine Leitung exklusiv für den Datenaustausch aufgebaut werden. Ein typisches Beispiel ist hierfür das Telefon.

2.10.4.1.2 - Speichervermittlung

Bei der **Speichervermittlung** agieren die Netzwerk-Knoten nach dem Store-and-Forward-Prinzip. Eingehende Daten werden gespeichert, analysiert und dann weiter geleitet. Das bedeutet, dass der verfügbare Speicher und das Speichermanagement neben der Performance eines solchen Knotens, ein wichtiges Entscheidungskriterium bei der Beschaffung ist.

Netztechnik-Grundlagen

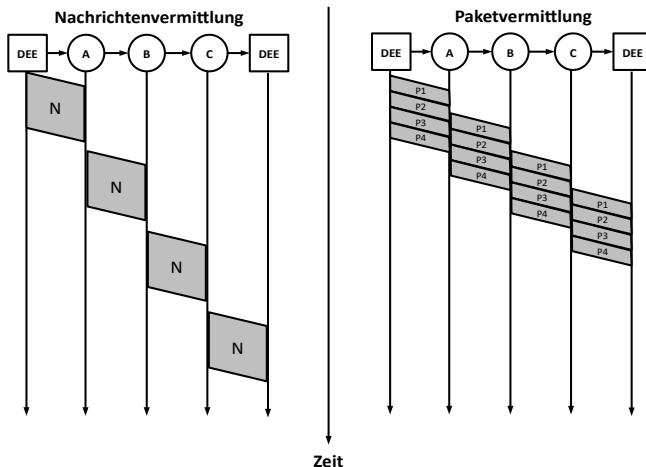


Abbildung 20: Gegenüberstellung: Nachrichtenvermittlung vs. Paketvermittlung

Die **Nachrichtenvermittlung** (engl. message switching) bietet eine absolut sichere Zustellung der Nachrichten. Zeitaspekte sind dabei untergeordnet.

Nachrichten können nicht segmentiert werden und müssen zwischen den einzelnen Netzwerknoten als ganzes übertragen, bevor sie weiter gesendet werden können.

Verbindungslose und verbindungsorientierte Dienste bieten die Möglichkeit der Segmentierung der Information in überschaubare Größen.

Dies führt im Vergleich zur Paketvermittlung zu einer schlechteren Kanalausnutzung.

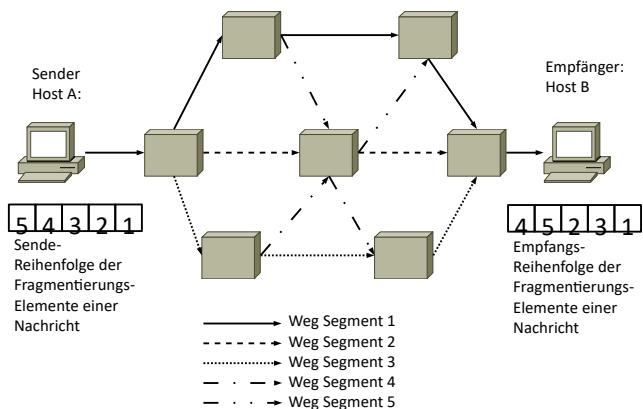


Abbildung 21: Datagramm-Verfahren

Ein **Verbindungsloser Dienst** transportiert **Datagramme** über mehrere Netzwerk-Knoten hinweg zum Ziel. Die zu transportierende Information muss evtl. in kleinere Stücke zerlegt werden. Auf dem Weg zum Ziel können die einzelnen Datagrammteile unterschiedliche Wege nehmen. Das bedeutet, dass am Ziel die Reihenfolge der Datagrammteile nicht mehr dem ursprünglichen Datagramm entspricht. Der Sender sendet die Datagrammteile ohne sich darum zu kümmern, ob es einen Empfänger gibt, oder ob der Empfänger die Daten verstehen oder verarbeiten kann. Das **IP-Protokoll** ist hierfür ein Beispiel.

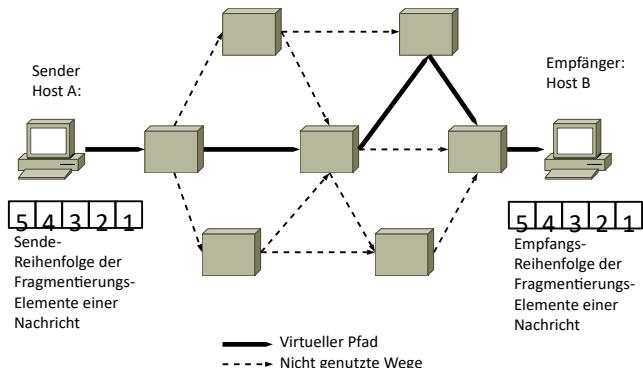


Abbildung 22: Paket-Verfahren

Daten, die ein **Verbindungsorientierter Dienst** transportiert werden **Pakete** genannt.

Vor dem Datenaustausch muss erst eine Verbindung aufgebaut werden.

Die aufgebaute Verbindung wird auch **virtueller Pfad** genannt. Dieser virtuelle Pfad ändert sich während der Übertragung der Daten nicht mehr. Damit ist sichergestellt, dass die Reihenfolge der Pakete beim Sender die gleiche ist, wie beim Empfänger.

Am Ende muss die Verbindung wieder abgebaut werden. Als Beispiel kann hier **MPLS** genannt werden.

2.10.4.2 - Rundfunksysteme

Beschleunigte Elektronen erzeugen elektromagnetische Wellen. Die Anzahl der Schwingungen pro Sekunde wird in Herz (Hz) angegeben und als **Frequenz** (f) bezeichnet.

Die Entfernung zwischen zwei Schwingungsmaxima oder -minima wird als **Wellenlänge** bezeichnet und mit dem griechischen Buchstaben Lambda (λ) angegeben.

Im Vakuum bewegen sich die Wellen mit der maximal möglichen Geschwindigkeit, der **Lichtgeschwindigkeit** (c). In Kupfer (Cu) oder Lichtwellenleitern (LWL) verringert sich die Geschwindigkeit auf $\frac{2}{3}$ der Lichtgeschwindigkeit.

Grundsätzlich gilt im Vakuum:

$$\lambda f = c$$

Da c eine Konstante ist kann λ aus f abgeleitet werden oder umgekehrt. Als Faustregel kann $\lambda f \approx 300$ angegeben werden wenn λ in Metern und f in MHz angegeben wird. Beispiel: 100-Mhz-Wellen sind 3m lang.

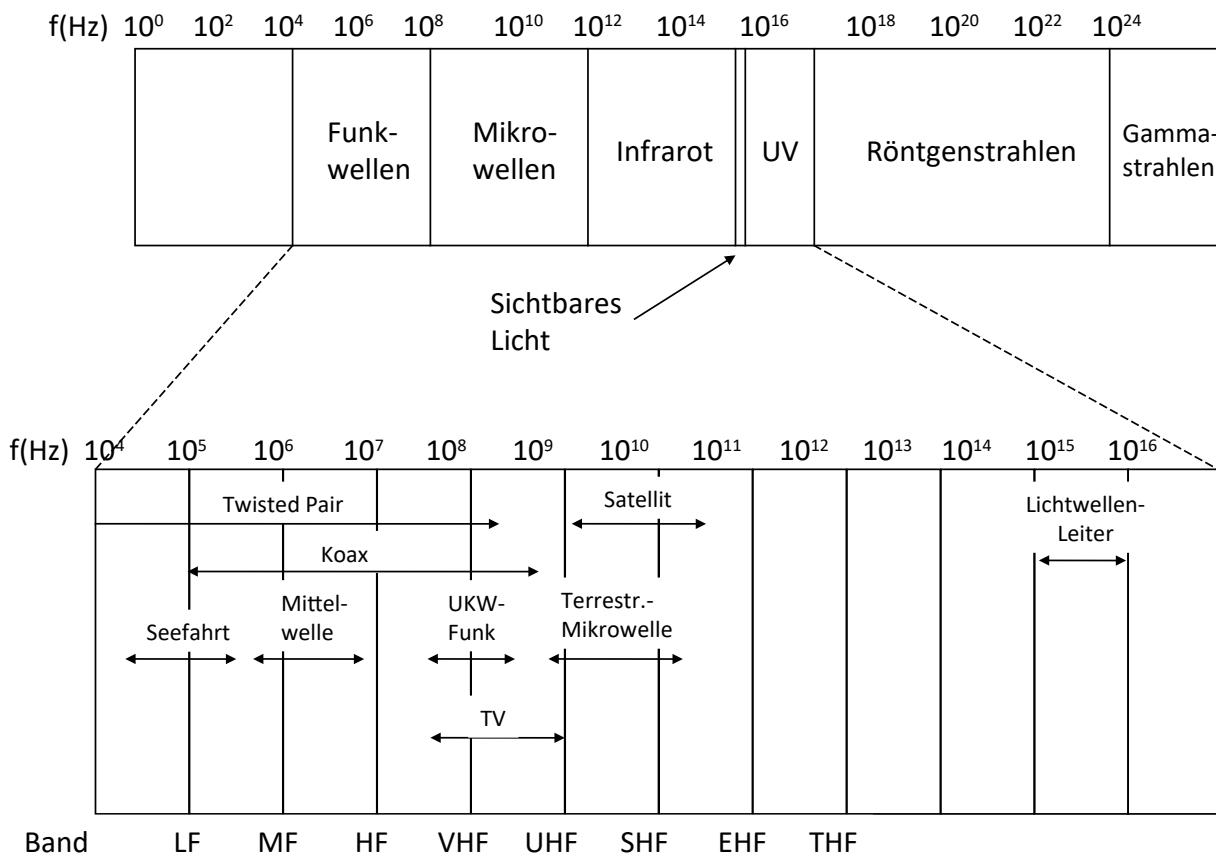


Abbildung 23: Elektromagnetisches Spektrum

Die Bezeichnung der Bänder wurde durch ITU festgelegt und basiert auf den Wellenlängen der Bänder

- LF = Low Frequency (10 – 1 km / 30 – 300 kHz)
- MF = Medium Frequency (1000 – 100 m / 0,3 – 3 MHz)
- HF = High Frequency (100 – 10 m / 3 – 30 MHz)
- VHF = Very High Frequency (10 – 1 m / 20 – 300 MHz)
- UHF = Ultra High Frequency (10 – 1 dm / 0,3 – 3 GHz)
- SHF = Super High Frequency (10 – 1 cm / 3 – 30 GHz)
- EHF = Extremely High Frequency (10 – 1 mm / 30 – 300 GHz)
- THF = Tremendously High Frequency (10 – 1 μm / 0,3 – 3 THz)

2.10.4.2.1 - Radiofunk

Radiowellen haben große Reichweiten und dringen problemlos in Gebäude ein. Sie sind leicht zu erzeugen und haben eine Rundstrahl-Charakteristik.

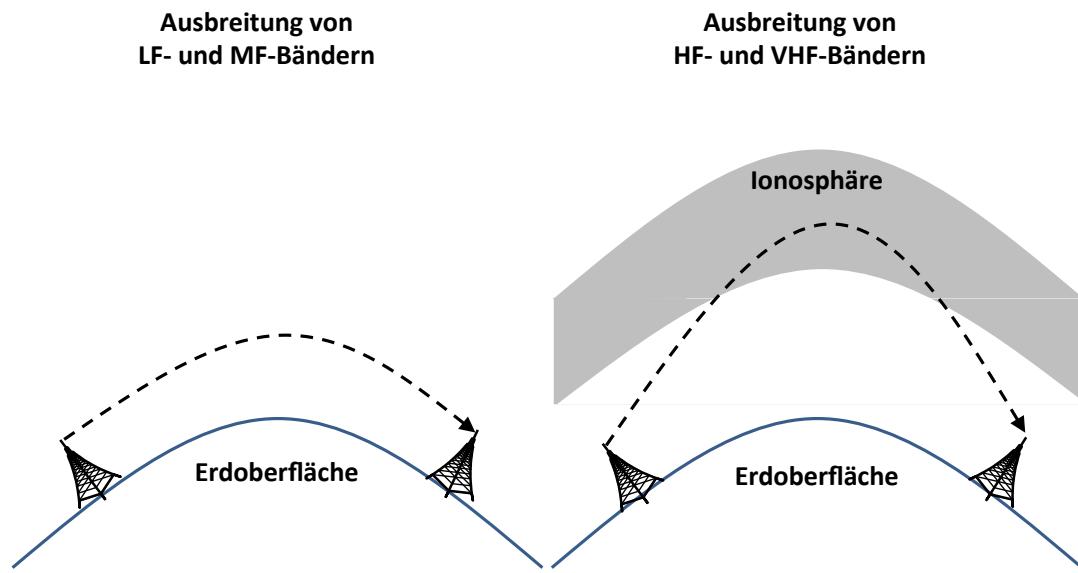


Abbildung 24: Funkwellenausbreitung

Während LF- und MF-Bänder sich entlang der Erdoberfläche ausbreiten werden die HF- und VHF-Bänder an der Ionosphäre reflektiert und haben damit eine noch größere Reichweite. Dies ist der Grund warum z. B. Kurzwellensender über Ländergrenzen hinweg empfangen werden können.

2.10.4.2.2 - Mikrowellen

Vor der Einführung von LWL waren Mikrowellenverbindungen die Grundlage von Ferngesprächen. Heutzutage werden Mikrowellen bei Telefon Handy, TV und WLAN angewendet.

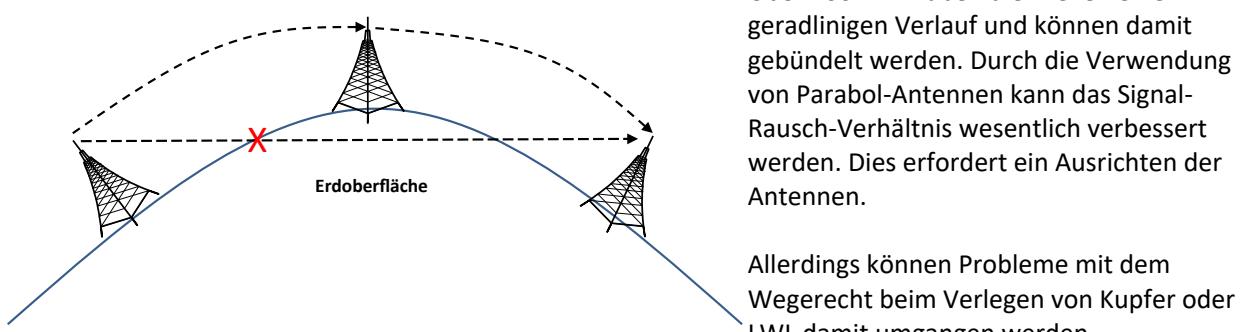


Abbildung 25: Mikrowellenausbreitung

Hindernisse wie Gebäude können von Mikrowellen nicht durchdrungen werden. Da bei großen Strecken die Erde dazwischen kommt sind Repeater erforderlich. Je höher die Sendemasten sind desto weiter können die Repeater voneinander entfernt stehen. Die Entfernung von Repeatern steigt in etwa mit der Quadratwurzel der Antennenhöhe. Bei einem 100 m hohen Sendemast können die Masten ca. 80km weit voneinander entfernt sein.

Durch Brechung an niedrigen atmosphärischen Schichten können Wellen verzögert werden da sie dann einen längeren Weg zurücklegen müssen. Im schlimmsten Fall können dadurch die ungebrochenen Wellen ausgelöscht werden. Diesen Effekt nennt man multipath fading. (dt. Mehrwegeempfang). Die Betreiber halten bis zu 10% der

Frequenzbänder als Ausweichbänder zur Verfügung, um bei gestörten Frequenzen ausweichen zu können.

Zusätzlich kann Wasser in Form von Regen ab 4GHz zu Problemen führen

Im Vergleich zur Verlegung von Kupfer oder LWL, kann der Einsatz von Mikrowellen der günstigere Ansatz sein.

2.10.4.2.3 - Frequenzzuteilung

Frequenzbereiche sind in Zeiten ständiger Bandbreitenerhöhungen ein rares Gut. Frequenzen sind landesrechtlich für fast alle Bereiche (wie Radio, Fernsehen, Handy-Telefonie, Grubenfunk, Polizei, Seefahrt Navigation, Militär, ...) zugeteilt. International regelt die ITU-R die Zuteilung um Geräte zu ermöglichen die weltweit funktionieren.

Für die Zuteilung der Frequenzbänder gibt es 3 unterschiedliche Verfahren.

- ➊ Das älteste Verfahren nennt sich auch Schönheitswettbewerb. Dabei muss jeder Bewerber begründen warum gerade er die öffentlichen Interessen am besten erfüllen kann. Dabei ist Korruption Tür und Tor geöffnet.
- ➋ Daher wurde als nächstes Verfahren das Losverfahren eingeführt. Dabei kann allerdings jeder mitbieten, ohne die Bänder nutzen zu wollen. Die Frequenzbänder kann man dann mit hohem Gewinn weiter verkaufen. Vor allem ist damit auch nicht sichergestellt, dass der beste Bieter zum Zug kommt.
- ➌ Am ehesten kommt man dem öffentlichen Interesse nahe mit dem Versteigerungs-Verfahren. Dabei bietet jeder Bewerber in mehreren Runden. Aus Angst, nicht an den Frequenzbändern teilzuhaben, hatten sich Bieter anfangs während der Versteigerung ständig überboten. Dies führte anfänglich zu unerwarteten Einnahmen der Länder in die Staatskasse und zu einer großen Verschuldung der Bieter-Unternehmen.

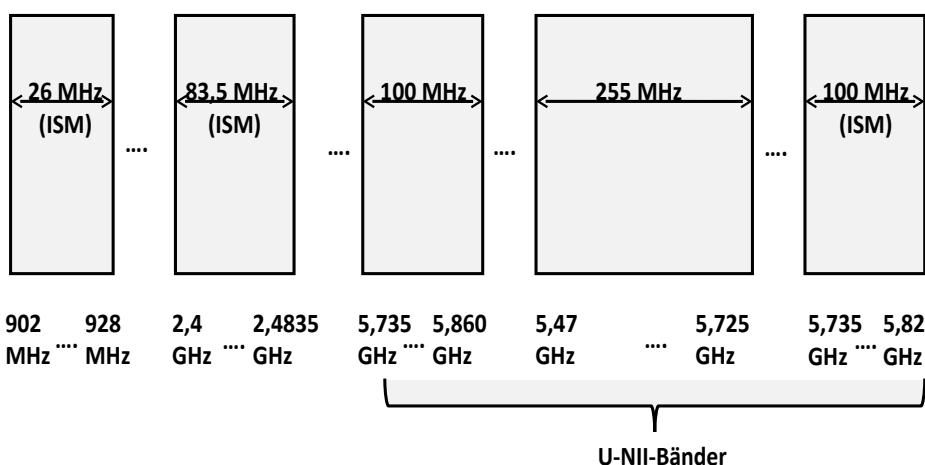
In Deutschland ist für die Versteigerung der Frequenzen die Bundesnetzagentur dafür zuständig.

Bei den letzten Versteigerungen kamen die folgenden Summen zusammen:

- ➊ UMTS August 2000 49Mrd. € für 6 Frequenzbänder
- ➋ WiMax Dezember 2006 56 Mio. € an 5 Bieter
- ➌ LTE April 2010 4,38 Mrd €
- ➍ LTE Juni 2015 Lizenzen an O2, Telekom und Vodafone für 5.081.236.000 €
- ➎ 5G im Juni 2019 nach 497 Bieterrunden wurden insgesamt 270MHz in den Bändern 700, 900, 1500 und 1800MHz an Telefónica, Telekom und Vodafone für 6.549.651.000 € versteigert.

2.10.4.2.4 - ISM-Bänder

Es gibt auch Bänder für die keine Lizenzen erforderlich sind. Das sind die so genannten ISM-Bänder. ISM steht für Industrial, Scientific und Medical, womit die ursprünglichen Anwendungsbereiche genannt sind. Mittlerweile haben sich dort auch WLAN, Bluetooth, Mikrowellenherde, Funkmäuse, Funktastaturen, Bewegungsmelder und andere angesiedelt. Die ISM-Bänder (900 MHz, 2,4 GHz, 5 GHz) dürfen nur mit geringen Sendeleistungen betrieben werden und haben damit nur eine geringe Reichweite. Im 5GHz-Bereich sind auch die so genannten U-NII-Bänder (Unlicenced National Information Infrastructure) angesiedelt.



Da sich mittlerweile viele Anwender in den Bereichen tummeln, müssen ISM-Geräte robust gegen alle in diesem Bereich betriebenen anderen Geräte sein, was nicht immer einfach ist.

Abbildung 26: ISM-Bänder in Deutschland und USA

2.10.4.2.5 - Infrarotübertragung

Infrarotwellen können keine Gegenstände durchdringen. Daher finden sie „nur“ bei Fernbedienungen für TV Stereoanlagen usw. Anwendung.

Allgemein gilt: Je weiter man sich von Langwellen hin zu sichtbaren Lichtwellen bewegt, umso mehr verhalten sich Wellen wie Licht und umso weniger wie Funkwellen.

Dies kann auch zum Vorteil genutzt werden, denn diese Wellen stören Wellen im nächsten Raum nicht. Zur Verbindung von Notebooks untereinander, oder aber auch mit Druckern wurde der IrDA-Standard (Infrared Data Association) entwickelt und teilweise noch eingesetzt.

2.10.4.2.6 - Lichtwellenübertragung

Der ungerichtete optische Richtfunk (free-space-optics) ist seit Jahrhunderten in Benutzung. Moderne Anwendungsfälle basieren auf Laserstrahlen. Da die Verbindungen unidirektional sind muss jeweils ein Laser und ein Fotodetektor vorhanden sein um z. B. eine Verbindung zwischen zwei Gebäuden zu erstellen. Da der Laserstrahl extrem gebündelt und somit ca. 1 mm dünn ist, kommt bei der Ausrichtung des Lasers auf den gegenüberliegenden Stecknadelkopf-großen Fotodetektor eine große Bedeutung zu. Zusätzlich ist der Laserstrahl Einflüssen von Wind, thermischen Strömungen, dichten Nebels und Regen ausgesetzt.

2.10.4.2.7 - Kommunikationssatelliten

Grundsätzlich funktionieren sie wie ein großer Mikrowellenverstärker am Himmel. Mittels mehrerer Transponder können verschiedene Frequenzbereiche abgedeckt werden. Die eingehenden Signale werden verstärkt und auf einer anderen Frequenz zurück auf die Erde gesendet um Interferenzen zu vermeiden. Dieses Verfahren nennt man auch Bent Pipe (dt. Gebogenes Rohr). Die abwärts gerichteten Strahlen können entweder einen großen Teil der Erdoberfläche abdecken, oder einen Bereich von wenigen 100 km.

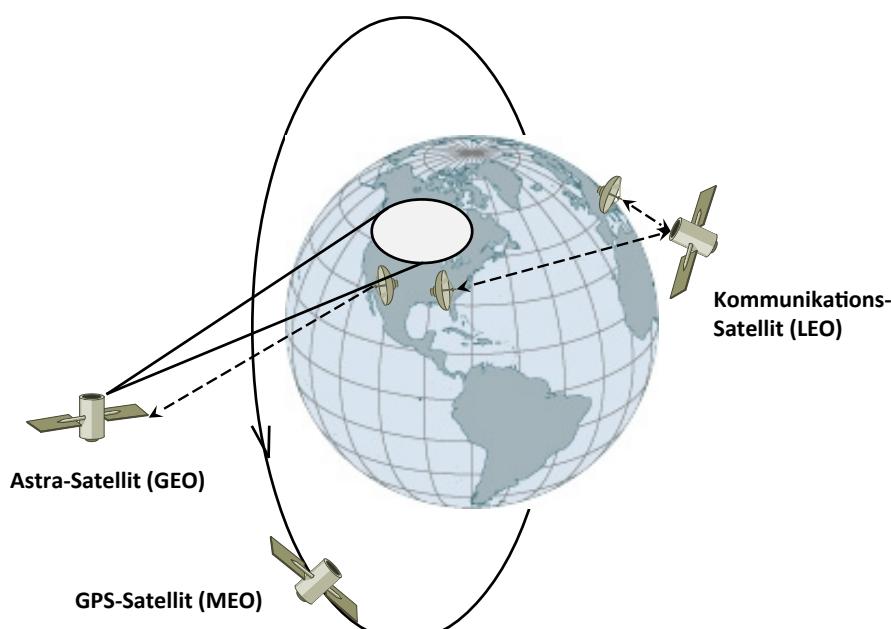


Abbildung 27: Unterscheidung von Anwendungsfällen (LEO / MEO / GEO)

Nach dem Keplerschen Gesetz beträgt die Umlaufzeit eines Satelliten Orbitalradius hoch 3/2. Je nach Höhe der Umlaufbahn (Orbit) werden unterschiedliche Satelliten-Typen unterschieden:

Bezeichnung	Kurzbez.	Höhe	Latenzzeit	Anzahl der benötigten Satelliten für Erdumspannende Abdeckung
Geostationary Earth Orbit	GEO	35.800 km	270 ms	3
Medium Earth Orbit	MEO	6.000 – 20.000 km	35 – 85 ms	10
Low Earth Orbit	LEO	500 – 1.000 km	1 – 7 ms	50

Die beiden Van-Allen-Strahlungsgürtel sind Schichten mit stark geladenen Partikeln, die durch den Erdmagnetismus erzeugt werden. Hier können sich keine Satelliten aufhalten.

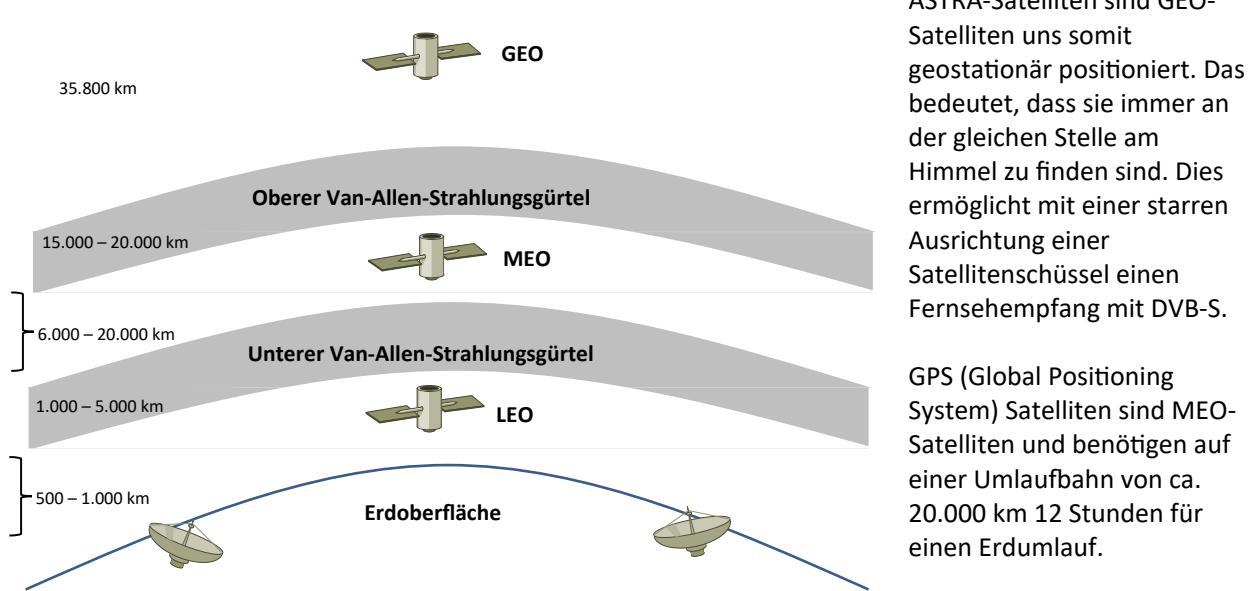


Abbildung 28: Satellitenkommunikation

Nahe der Erdoberfläche beträgt die Umlaufzeit 90 Min. Beispiel: In einer Höhe von 430 km benötigt die ISS ca. 98 Minuten um einmal die Erde zu umkreisen.

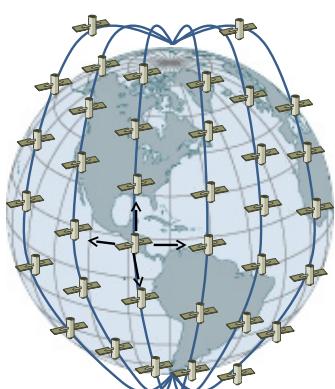


Abbildung 29: IRIDIUM-Satelliten werden.

Als Beispiel für die LEO-Satelliten können die Satelliten des Iridium-Projekts herangezogen werden. 1990 wollte Motorola mit 77 Satelliten einen Kommunikationsservice einrichten. (Element Iridium hat die Nummer 77) Daraus wurden letztendlich 66 Satelliten (Der Name hätte auf Dysprosium geändert werden müssen, was man aber nicht mehr tat). Jeder Satellit hat 4 Nachbarn und sobald ein Satellit aus dem Sichtfeld verschwindet, kann er durch den nächsten ersetzt werden. Die 6 Satelliten-Ketten sind jeweils 32° auseinander. Jeder Satellit hat maximal 48 scharf gebündelte Punktstrahlen mit einer Kapazität von 3840 Kanälen. Die Vermittlung wird über die Satelliten selbst gesteuert was eine aufwändigere Technik der Satelliten erfordert. (Siehe Abbildung 30 auf der linken Seite) Iridium musste 1999 Konkurs anmelden, wurde allerdings 2001 weitergeführt und ist seither gewachsen. Heute können Sprach, Daten, Pager, Fax, und Navigationsdienste über spezielle Handhelds weltweit an jedem Ort (zu Land, Wasser, oder in der Luft) zur Verfügung gestellt werden.

ASTRA-Satelliten sind GEO-Satelliten und somit geostationär positioniert. Das bedeutet, dass sie immer an der gleichen Stelle am Himmel zu finden sind. Dies ermöglicht mit einer starren Ausrichtung einer Satellitenschüssel einen Fernsehempfang mit DVB-S.

GPS (Global Positioning System) Satelliten sind MEO-Satelliten und benötigen auf einer Umlaufbahn von ca. 20.000 km 12 Stunden für einen Erdumlauf.

Netztechnik-Grundlagen

Ein Weiteres Beispiel für LEO-Satelliten sind die 48 Globestar-Satelliten. Diese Arbeiten nach dem Bent-Pipe-Prinzip. (Siehe Abbildung 30 auf der rechten Seite) damit kann die Technik der Satelliten einfacher gehalten werden. Die Vermittlungstechnik wird am Boden abgehandelt wo sie einfacher zu bewerkstelligen ist.

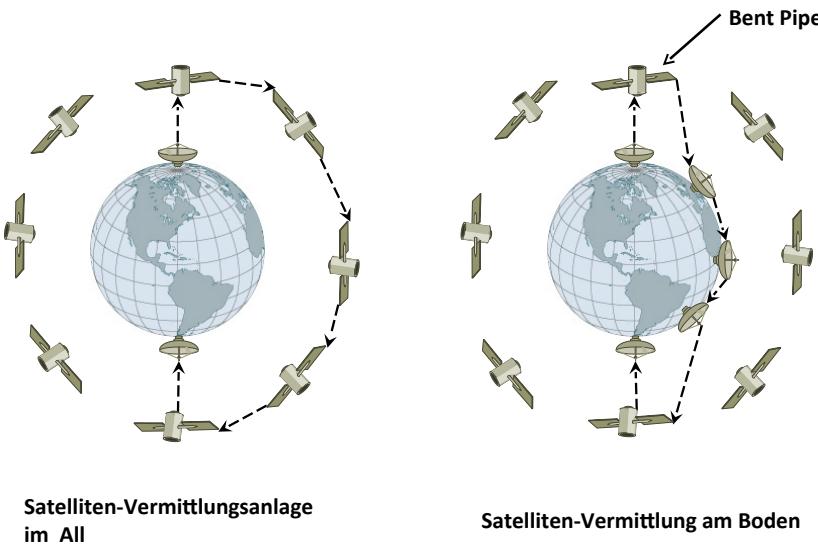


Abbildung 30: Kommunikationsvermittlung bei Satelliten



Train von Starlink-Satelliten

Ein Beispiel für die Satelliten-Vermittlung im All sind die Starlink-Satelliten der Firma SpaceX. Derzeit werden bis zu 60 Satelliten pro Rakete mit mehreren Falcon9-Raketen von SpaceX auf niedrige Umlaufbahnen gebracht. Nach dem Start können sie unter günstigen Bedingungen über mehrere Tage hinweg als sogenannter Train mit bloßem Auge gesichtet werden.

Von dort aus verteilen sie sich über mehrere Wochen hinweg in größerem Abstand auf ihren eigentlichen Orbit.

Pro Orbitalebene sind 66 Satelliten vorgesehen insgesamt sollen am Endausbau 24 Orbitalebenen die Erde umspannen.

Die Kommunikation zwischen den Satelliten erfolgt mittels Laser.

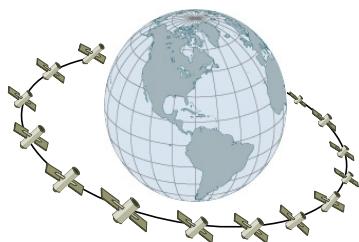


Abbildung 31: Starlink-Orbitalebene

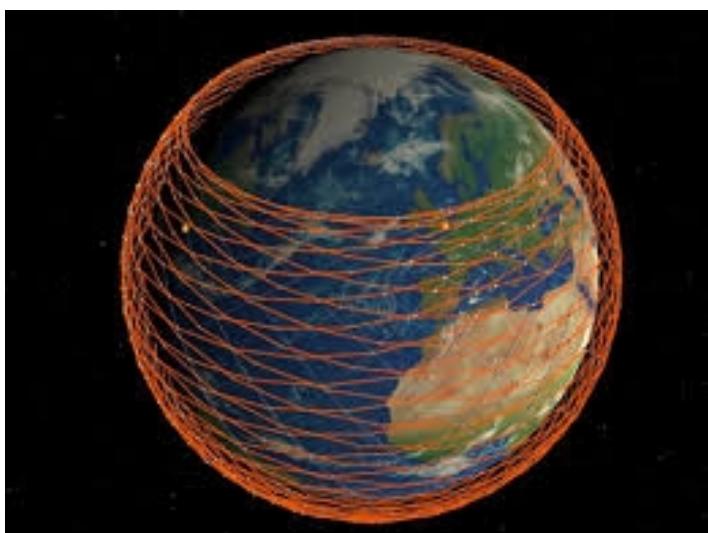


Abbildung 32: Starlink-Abdeckung in erster Stufe.
Quelle: Business Insider

In einer ersten Stufe sollen ca. 1.600 Satelliten in einer Höhe von 550km ausgebracht werden. Dabei sind die Polkappen noch nicht abgedeckt.

In 2 weiteren Stufen werden dann noch Satelliten auf 1100 – 1325km und über den Polen ausgebracht. SpaceX hat die Genehmigung 11.927 Satelliten bis 2027 auszubringen. Dabei werden dann auch die Polkappen abgedeckt.

Weitere 30.000 Satelliten sind für eine Höhe von 330- 580km sind beantragt.

Kritiker bemängeln die Gefahren von Kollisionen und so entstehendem Weltraumschrott und die Lichtverschmutzung am Himmel.

2.10.4.2.7.1 - VSAT

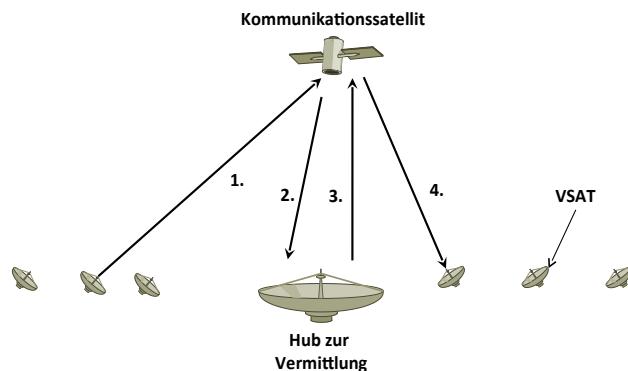


Abbildung 33: VSAT

Eine kostengünstige Entwicklung sind die VSATs (Very Small Aperture Terminal). Diese haben Antennen von 1 m Durchmesser. Da die Vermittlung nicht im Kommunikationssatellit erfolgt, muss die Vermittlung über einen großen Hub organisiert werden. Bei diesem Betriebsmodus hat entweder der Sender oder der Empfänger eine Große Antenne.

2.10.4.2.7.2 - CubeSat

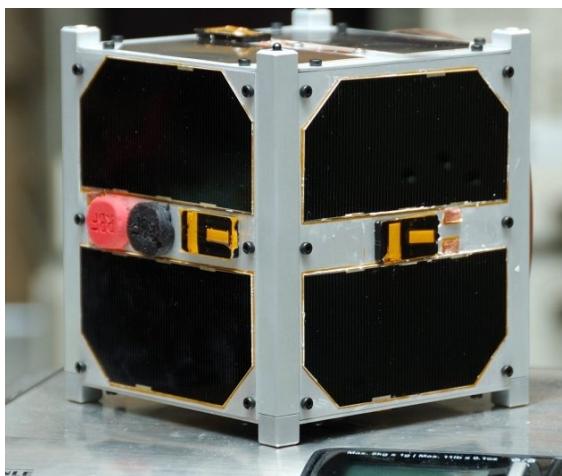


Abbildung 34: Cubesat
Quelle: Wikipedia

CubeSats, auch Nano-Satelliten genannt, sind kleine LEO-Satelliten-Würfel mit wenigen cm Kantenlänge und einem Gewicht von ca. 1 kg. Die Kommunikation mit den Bodenstationen erfolgt über die UHF- und VHF-Bänder. Sie werden zusammen mit einer größeren Nutzlast auf ihren Orbit gebracht und durch die Herstellung in Kleinserien-Produktion können die Kosten pro Satellit drastisch gesenkt werden.

Anwender sind sowohl viele Universitäten als auch ausgefallene Systeme wie z. B. zur Erdbebenvorhersage.

3 - Schichtenmodelle

Das Zerlegen eines Kommunikationssystems kann aufgrund der folgenden Prinzipien erfolgen:

- Da wo ein neuer Abstraktionsgrad benötigt wird soll eine neue Schicht entstehen.
- Jede Schicht soll möglichst eine Funktion abdecken.
- Bei der Funktionsauswahl soll man sich an international geltende Protokolle anlehnen
- Die Grenzen zwischen den Schichten sollen so gewählt werden, dass der Informationsfluss über die Schnittstellen möglichst gering ist.
- Die Anzahl der Schichten sollte so groß sein, dass keine Notwendigkeit dafür besteht verschiedene Funktionen zusammen auf eine Schicht zu packen und so klein dass das Modell nicht unhandlich wird.

3.1 - Ansichten eines Schichtenmodells

- Abstrakte Sicht. Allgemeine Sichtweise mit einer variablen Schichtenanzahl
- Funktionale Sicht. Beschreibt die Aufgaben der verschiedenen Schichten und legt somit eine Schichtenanzahl fest.
- Dienste-Sicht. Definiert die von jeder Schicht erbrachte Dienstleistung

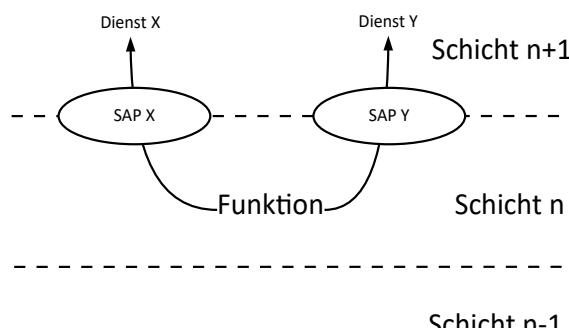


Abbildung 35: Dienstesicht

Das OSI-Referenzmodell geht dabei von verbindungsorientierten Diensten aus. Bei den Diensten werden die Funktionen beschrieben, welche von der Schicht erbracht werden. Die Dienste-Spezifikation enthält das gesamte Dienstleistungsangebot für die nächsthöhere Schicht. Z. B. Für die N-Schicht

- ◆ N-CONNECT (Verbindungsaufbau)
- ◆ N-DATA (Datenaustausch)
- ◆ N-DISCONNECT (Verbindungsabbau)

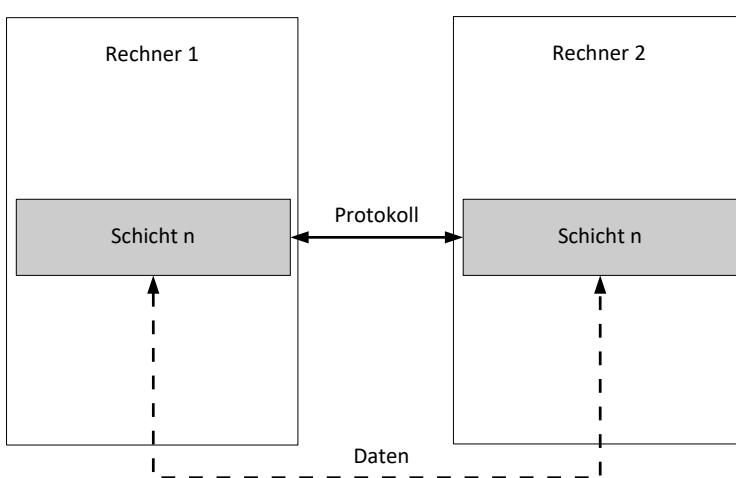


Abbildung 36: Protokollsicht

- Protokollsicht. Beschreibt die Protokolle die zwischen den Kommunikationssystemen der gleichen Schicht ablaufen.

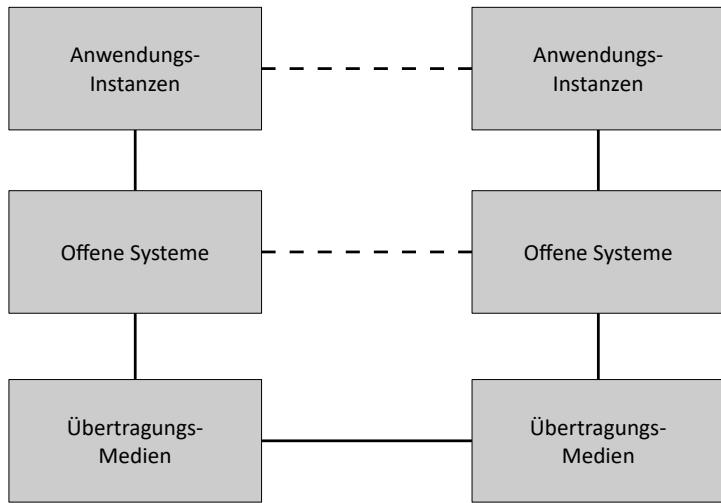
3.2 - Grundelemente einer Kommunikations-Architektur

Abbildung 37: Grundelemente einer Kommunikations-Architektur

3.3 - Protokoll

Durch ein Protokoll können folgende Festlegungen getroffen werden.

- Regeln (Verbindungsaufbau, Datenübertragung, Verbindungsabbau)
- Ablauf (1., 2., 3., ...)
- Kommunikation gleichberechtigter Partner (Peers)

3.4 - Referenzmodelle

Es gibt mittlerweile eine Anzahl verschiedene Referenzmodelle

- ISO-RM
- DARPA, DoD-RM, TCP/IP - RM
- BISDN-RM

3.4.1 - Interaktion zwischen den Schichten

Der Aufbau einer Schicht ist für alle Schichten gleich. (Eine Ausnahme bildet die Schicht 1)

Jede Schicht stellt der übergeordneten (höheren) Schicht einen oder mehrere Dienste zur Verfügung. Auf den Dienst kann über die SAP's (Service Access Point) zugegriffen werden. Damit ist die unterlagerte Schicht der Service Provider. Die überlagerte Schicht ist der Service User. Um der unterlagerten Schicht Steuerinformationen zu übergeben wird die ICI den zu bearbeitenden Daten, der SDU (Service Data Unit) mitgegeben. ICI und SDU bilden zusammen die IDU, die über den SAP, der unterlagerten Schicht übergeben wird.

Damit eine Schicht ihre Aufgabe, zusammen mit dem Schicht-Partner (peer) auf einem anderen Rechner, durchführen kann, muss sie für den Schicht-Partner Informationen zur Verfügung stellen, die sie in einem Header, der PCI (Protocol Control Information), den übergebenen Daten, der SDU (Service Data Unit) voranstellt. PCI und SDU bilden die PDU (Protocol Data Unit), welche zwischen den Instanzen auf der gleichen Ebene ausgetauscht werden. Die Kommunikation zwischen Partner auf der gleichen Ebene wird Protokoll genannt. Die Kommunikation zwischen Partnern auf der gleichen Ebene wird auch „peer-to-peer-communication“ genannt.

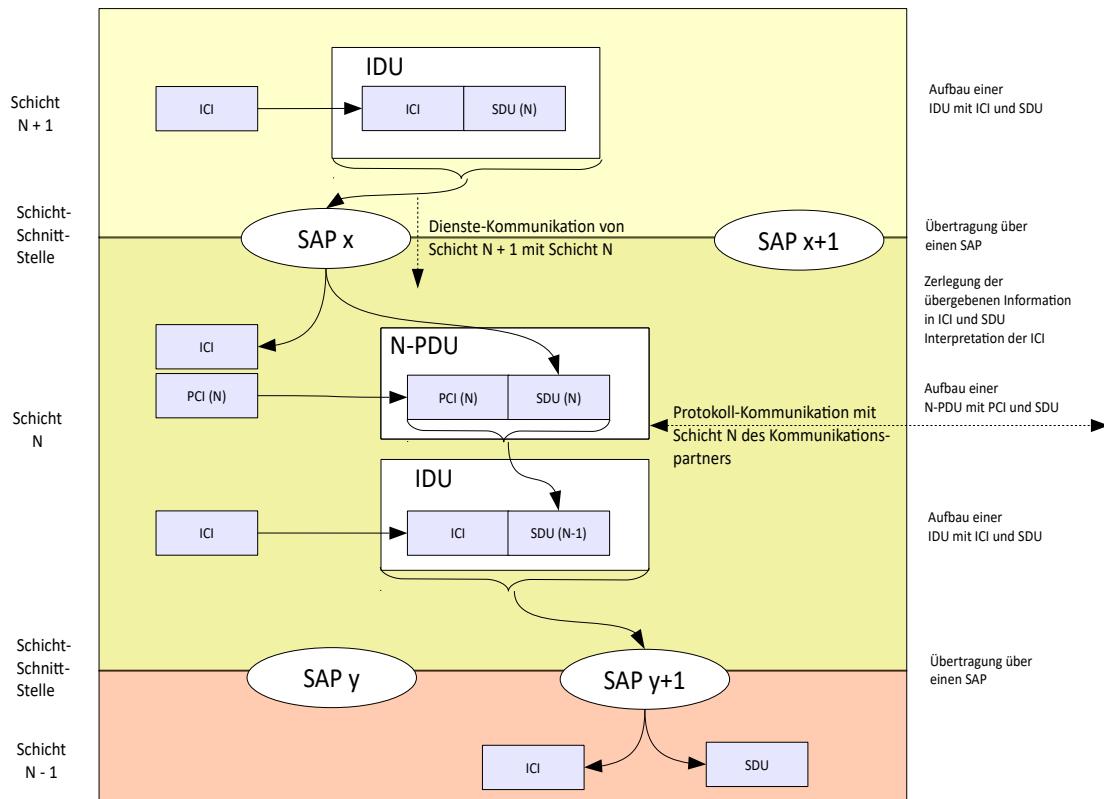


Abbildung 38: Interaktionen zwischen Schichten

Schichtenmodelle

Da in der Literatur die Begriffe, zumindest teilweise auch in Deutsch verwendet werden ist in der folgenden Tabelle eine entsprechende Zuordnung gemacht.

Abkürzung (eng.)	Bedeutung (engl.)	Abkürzung (dt.)	Bedeutung (dt.)
IDU	Interface Data Unit	SDE	Schnittstellen-Daten-Einheit
SDU	Service Data Unit	DDE	Dienst-Daten-Einheit
ICI	Interface Control Information	PSI	Protokoll-Steuer-Information
PDU	Protocol Data Unit	PDE	Protokoll-Daten-Einheit
PCI	Protocol Control Information		
SAP	Service Access Point		

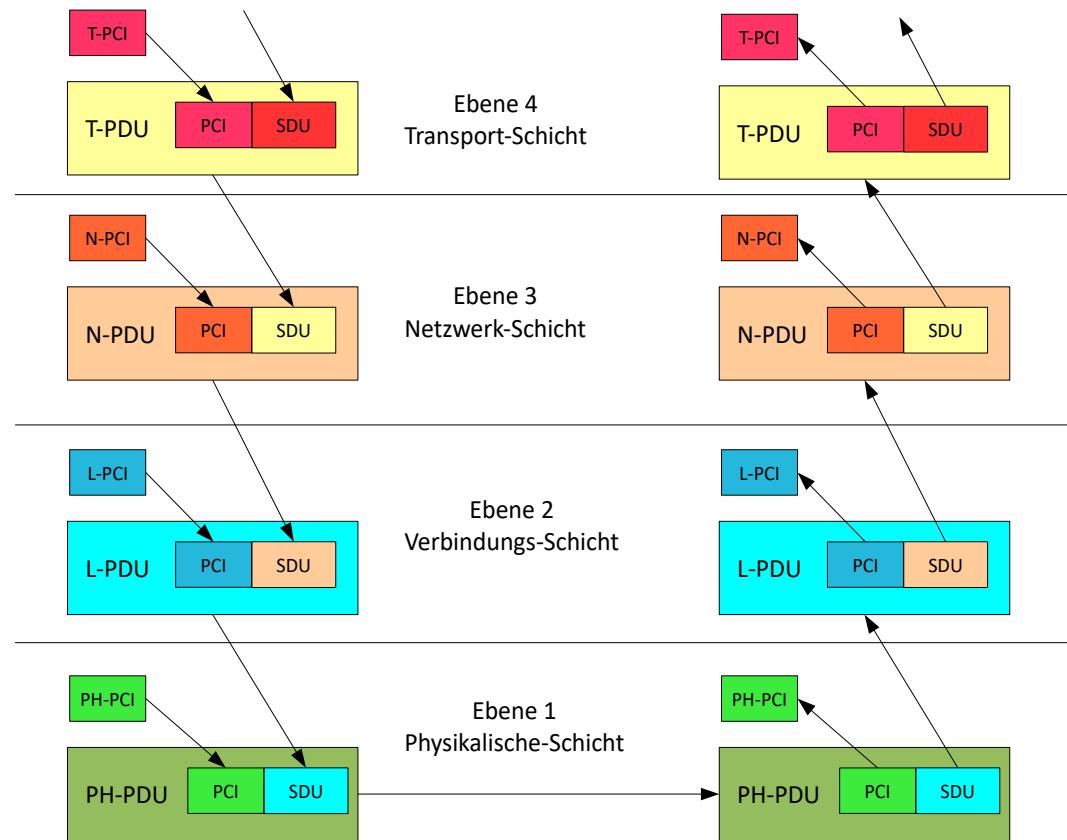


Abbildung 39: Schnittstellen-Übergabe

Die obige Abbildung zeigt, wie die PDU's (beim Schicht-Übergang nach unten) zu SDU's werden. Beim Senden gibt jede Schicht, in der SDU ihrer Partnerschicht Informationen mit, wie sie die SDU weiter bearbeiten soll. Zusammen mit einer PCI wird eine SDU in einer beliebigen Schicht zu einer PDU zusammengeführt.

Beim Übergang nach oben wird eine SDU in einer beliebigen Schicht zu einer PDU. In der Schicht wird die PDU in eine PCI und eine SDU zerlegt. Mit der PCI kann dann die Schicht die SDU bearbeiten und an den in der PCI definierten SAP weitergeben.

3.5 - Bestandteile von Referenzmodellen

In Referenzmodellen gibt es für jede Schicht die folgenden Bestandteile:

- Instanz (Entity)

Dies ist der eigentliche Dienstleistungserbringer einer Schicht. Die Instanz nutzt dabei die Dienste der unterlagerten Schichten, ohne dass deren Funktionsweise nach oben hin relevant ist.

- Service-Provider

Die Instanz der Ebene n ist der Service-Provider für die Ebene n+1.

- Service-User

Die Instanz der Ebene n+1 ist der Service-User der Ebene n.

- SAP

Der Service-Access-Point bildet die Schnittstelle die z. B. die Ebene n+1 verwendet um die Ebene n zu benutzen.

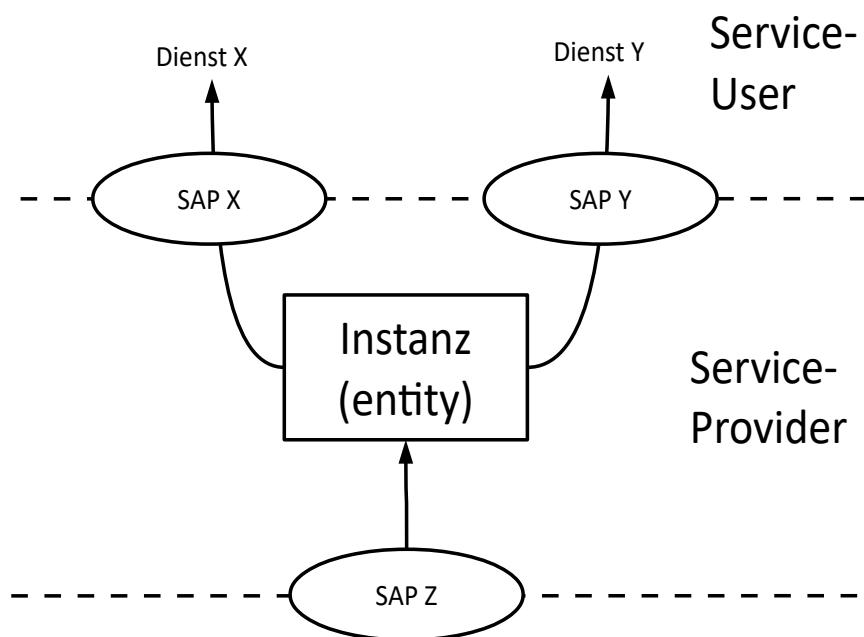


Abbildung 40: Bestandteile von Referenzmodellen

Schichtenmodelle**• Primitive**

Um einen SAP zu nutzen werden so genannte Dienste-Primitive verwendet. Für die unterschiedlichsten Aktivitäten werden grundsätzlich nur diese Primitive angewendet. In der unteren Darstellung sieht man die Nutzung der Primitive in beiden Richtungen. Die Dienste werden nur nach oben hin erbracht.

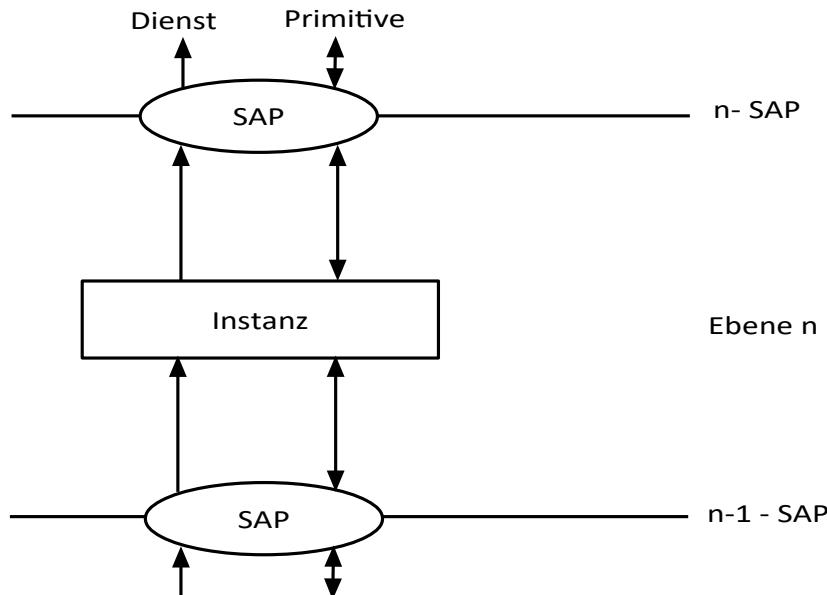


Abbildung 41: Dienste / Primitive

Es sind 4 Primitive definiert, die für alle Dienste Anwendung finden. Hier am Beispiel des Dienstes CONNECT.

◆ N-CONNECT.request

Er entspricht der Anforderung einer Instanz an einen SAP. Es ist die erste Aktion bei der Nutzung eines Dienstes.

◆ N-CONNECT.indication

Die Indication zeigt auf der gegenüberliegenden Protokollseite an, dass eine Anforderung (Response) gestellt wurde.

◆ N-CONNECT.response

Mit dem Response wird auf die Anforderung aktiv reagiert.

◆ N-CONNECT.confirm

Dies ist die Ergebnisanzeige auf den ursprünglichen Request. Darin wird dem Sender des Requests eine Rückmeldung gegeben.

3.5.1 - Primitive bei verbindungsorientierter Kommunikation

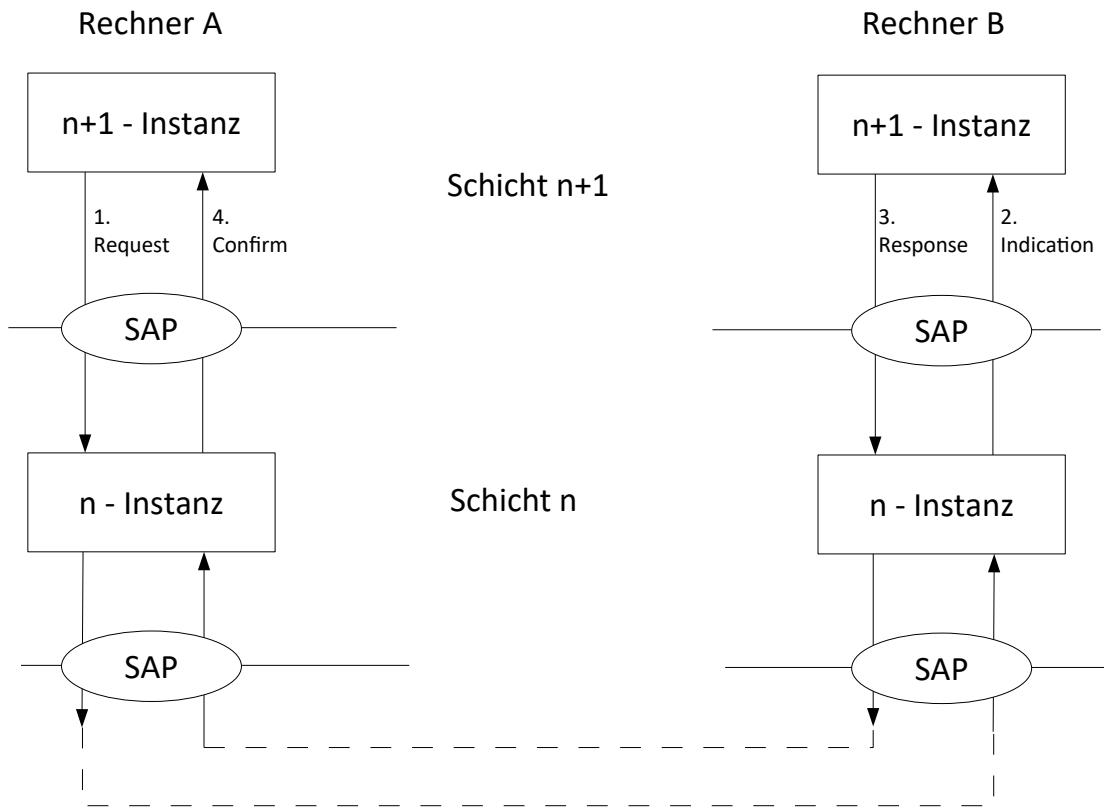


Abbildung 42: Primitive bei verbindungsorientierter Kommunikation

Auf Rechner A will die n+1-Instanz mit der n+1-Instanz auf Rechner B Daten austauschen. Dazu stellt sie, als Service-User eine Anfrage (Request) an die ihr unterlagerte Instanz (n). Dies wird über den SAP der Schicht n abgewickelt.

Als Service-Provider arbeitet die n-Instanz auf dem Rechner A zusammen mit der n-Instanz auf dem Rechner B. Dazu verwenden sie das Protokoll welches auf n-Ebene verwendet wird (n-Protokoll). Mit diesem Protokoll werden n-PDU's ausgetauscht. Nachdem auf Rechner B-Seite die n-Instanz ihre Arbeit verrichtet hat übergibt sie der Schicht n+1 die Anzeige (Indication).

Die Indication wird nun auf Rechner-B-Seite von der n+1-Instanz verarbeitet. Ist die Bearbeitung abgeschlossen, antwortet die n+1-Instanz mit einer Antwort (Response).

Die n-Instanz auf Rechner B übergibt diese Antwort ihrem Partner auf Rechner A an die n-Instanz.

Die n-Instanz auf Rechner A übergibt nun als Service-Provider ihrem Service-User eine Bestätigung (Confirm) über die Durchführung der angeforderten Dienstleistung.

Schichtenmodelle**Zusammenfassung**

Mit dieser Vorgehensweise wird sichergestellt, dass auf eine Anforderung eine Aktion auf der gegenüberliegenden Seite angestoßen wird. Die Gewähr, dass die Aktion auf der gegenüberliegenden Seite erfolgt ist, bekommt der Initiator durch eine Rückmeldung (Confirm). In dieser Rückmeldung erfährt der Initiator ob die Aktion auf der gegenüberliegenden Seite erfolgreich war oder nicht.

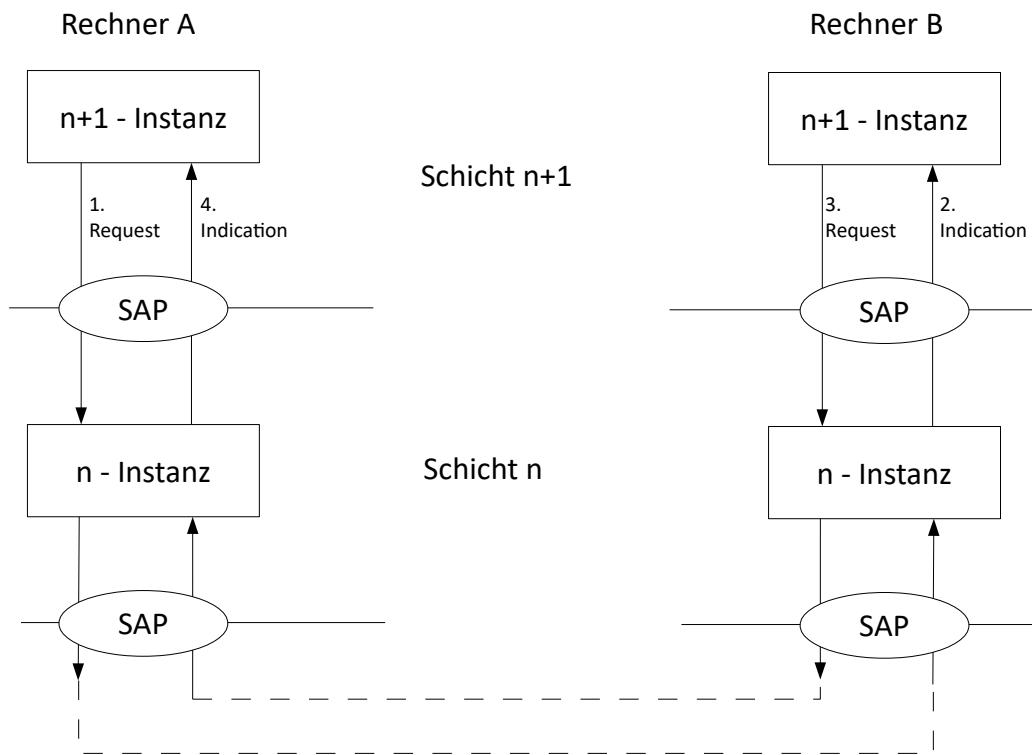
3.5.2 - Primitive bei verbindungsloser Kommunikation

Abbildung 43: Primitive bei verbindungsloser Kommunikation

Bei der verbindungslosen Kommunikation entfallen die Primitive Response und Confirm.

Dadurch haben die $n+1$ -Instanzen keine Möglichkeit zu verfolgen, was aus ihren Anforderungen geworden ist.

Rückmeldungen müssen die überlagerten Schichten selbst durch logische Quittungen, mittels eines neuen Requests, erzeugen.

3.5.3 - Globale und lokale Signifikanz

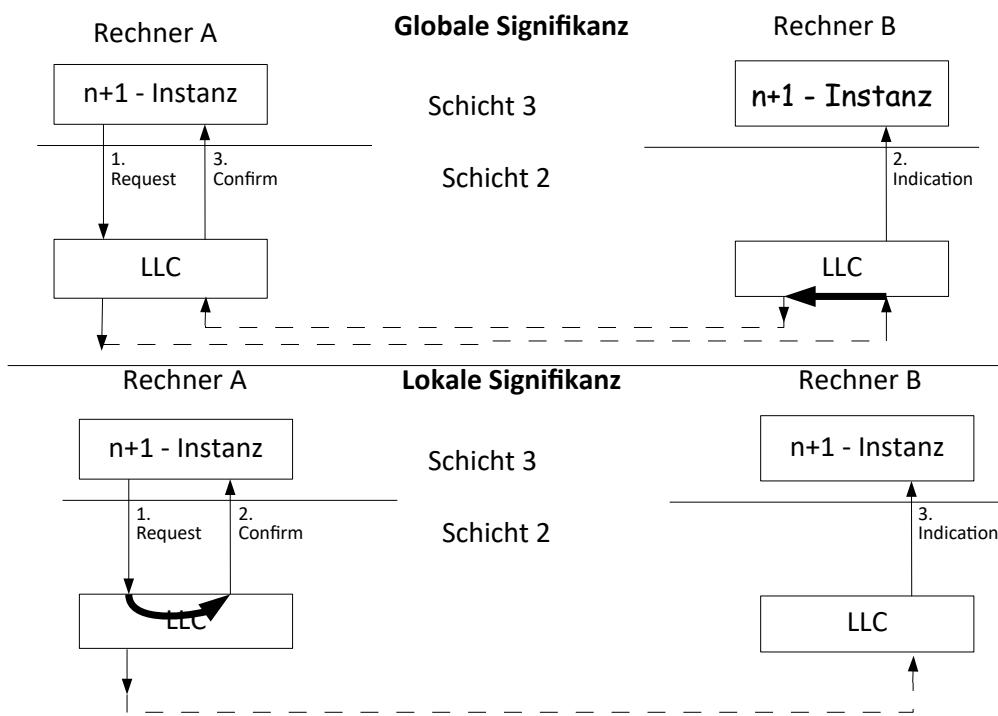


Abbildung 44: Globale und lokale Signifikanz

Bei der verbindungslosen Kommunikation kann eine Rückmeldung trotzdem noch auf zwei unterschiedliche Arten erzeugt werden.

3.5.3.1 - Globale Signifikanz

Hierbei wird die Bearbeitung auf der gegenüberliegenden Seite durchgeführt und nach Abschluss der Bearbeitung die Rückmeldung erzeugt. Dies erzeugt zwar eine Datenübertragung mehr, hat jedoch eine größere Sicherheit da der gesamte Kommunikationsweg außerhalb des Rechners überwacht werden kann.

3.5.3.2 - Lokale Signifikanz

Hierbei wird vom Service-Provider sofort die Rückmeldung erzeugt. Diese Vorgehensweise erspart dem Vorgang eine Datenübertragung und ist somit performanter. Sie ist jedoch nicht in der Lage auf Datenübertragungsfehler außerhalb des Rechners zu reagieren.

3.5.4 - Zusammenfassung

Zwischen gleichberechtigten Kommunikationspartner (Peers) werden Protokolle ausgetauscht bzw. bearbeitet.

Zwischen den Schichten eines Rechners werden Dienstleistungen zur Verfügung gestellt. Dazu nutzen die einzelnen Instanzen die SAP's der unter lagerten Schichten.

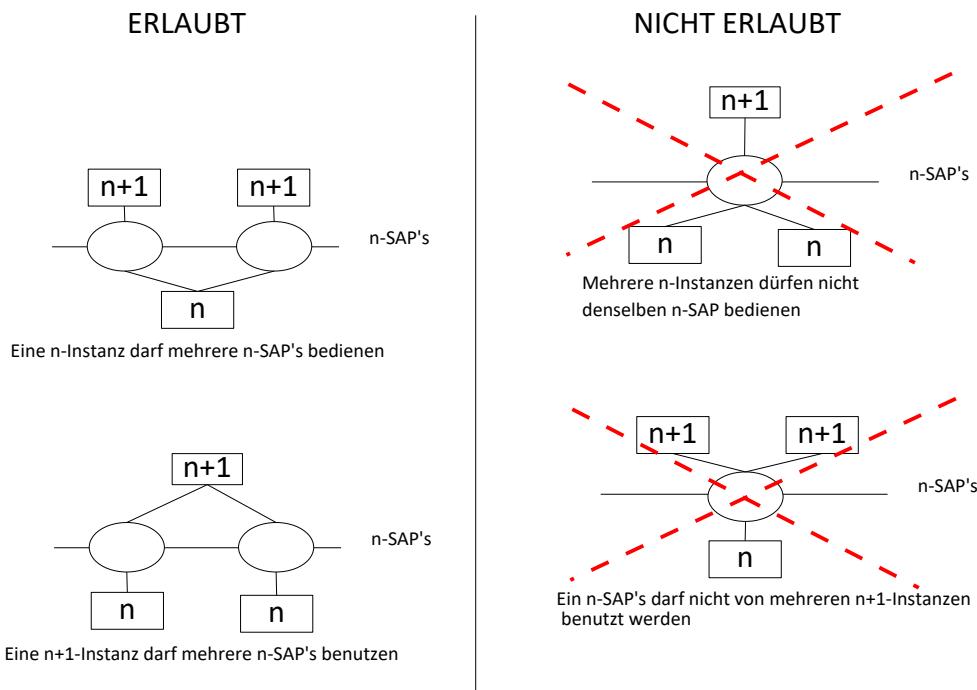


Abbildung 45: SAP-Zugriff erlaubt / nicht erlaubt

4 - OSI-Referenzmodell

4.1 - Einführung

In der unteren Abbildung ist das Open Systems Interconnect Referenz Modell der ISO, im Folgenden OSI-RM genannt, dargestellt. (ISO 7498 und ISO 7498-2) Auf der linken Seite sind die Schichten mit ihren deutschen Bezeichnungen und auf der rechten Seite mit den englischen Begriffen dargestellt. Dazwischen sind die Protokolle und die darin transportierten Daten-Einheiten aufgeführt. Ganz rechts ist die Zugehörigkeit der Schichten auf eine Transport oder Anwendungs-Orientierung zugeordnet. Dies bedeutet, dass die oberen 3 Schichten üblicherweise in den Anwendungen (Applications) realisiert werden. Die unteren 4 Schichten werden dem Transport über das Netzwerk zugeordnet.

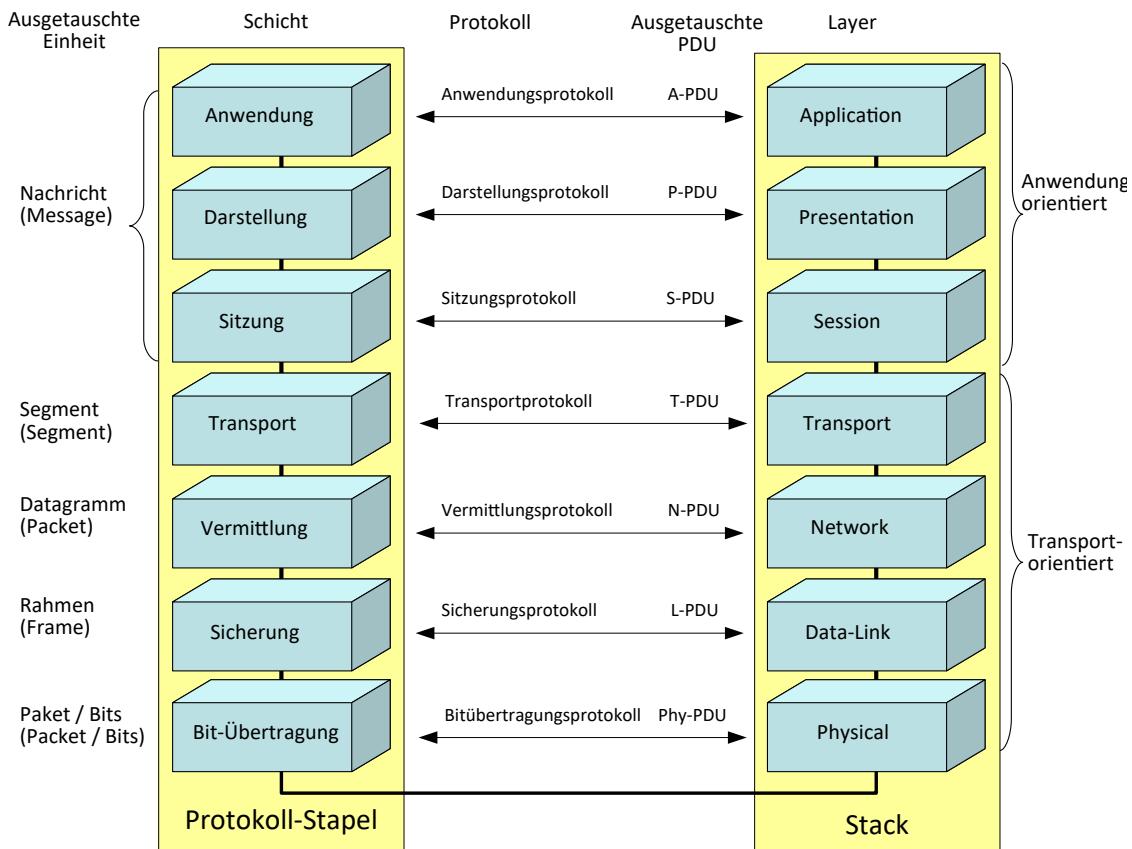


Abbildung 46: ISO-RM-Übersicht

Spaßvögel haben noch eine weitere Schicht definiert. Die 8. Schicht ist der Benutzer der das Gerät am Netzwerk bedient. Von daher kommt in den Helpdesks auch der Hinweis auf ein Layer-8-Problem.

Jedes Endgerät, das über ein Netzwerk kommunizieren will, muss dieses Modell in irgend einer Form realisieren. Jede dieser Schichten ist in einer mehr oder weniger genauen Ausprägung ausgebildet. Es kann auch vorkommen, dass Schichten entfallen, zusammengefasst oder weiter aufgeteilt werden.

Zwischen Endgeräten, die einen Informationsaustausch vornehmen wollen, müssen die gleichen Schichten realisiert sein, denn eigentlich unterhält sich jede Schicht in einem Endgerät mit der gleichen Schicht im gegenüberliegenden Endgerät. Diese Verbindung wird auch Peer to Peer-Verbindung genannt. (deutsch: Verbindung gleichrangiger Partner) Man kann, wie im obigen Bild zu sehen ist, davon ausgehen, dass zwischen den einzelnen Schichten auf gleicher Höhe eine logische Verbindung, ein Protokoll, besteht. Um das Protokoll auszuführen nutzen die Schichten die Dienste der unterlagerten Schichten. Zum Beispiel kommuniziert die Anwendungsschicht auf der einen Seite mit der Anwendungsschicht auf der anderen Seite indem sie die Dienste der Darstellungsschicht unter ihr nutzt.

Die Datenübertragung findet innerhalb eines Rechners in der Vertikalen statt. Der eigentliche Datenaustausch, findet dann auf der Bit-Ebene statt. Also ganz unten!

Im Folgenden werden die Schichten der Reihe nach von unten nach oben genauer erläutert. Verschiedene Eigenschaften einer Schicht, wie z. B. Flusskontrolle, können in anderen Schichten evtl. auch erbracht werden. Wichtig ist bei der Kommunikation zwischen zwei Geräten, dass auf beiden Seiten die gleichen Funktionen von den entsprechenden Partner-Schichten erbracht werden.

4.2 - Bitübertragungs-Schicht (1)

(engl. Physical-Layer)

Hierbei geht es um die physikalische Übertragung von Bits, also Einsen und Nullen. Die Instanzen der Schicht 1 haben keine unterlagerte Schicht mehr denn sie sind direkt über ein physikalisches Medium miteinander verbunden. Die ausgetauschte Einheit ist ein Paket, was zu Irritationen führen kann, denn auf der Ebene 3 werden auch Pakete ausgetauscht.

Mögliche Übertragungsmedien sind:

- Lichtwellenleiter (LWL)
- Kupfer
- Funk

Je nach verwendetem Medium sind die folgenden Funktionen zu realisieren:

- Modulation
- Kodierung
- Takt-Rückgewinnung
- Synchronisation

Auf dieser Ebene findet keine Sicherung der Daten statt. Das bedeutet, dass eventuelle Fehler nicht erkannt werden können. Das muss in höheren Schichten durchgeführt werden.

Die erste Ebene wird oft in zwei Unterebenen aufgeteilt:

- 1b Media-Independent -Interface (AUI bei 10 Mbps, MII bei 100 Mbps, GMII bei 1 Gbps, XGMII bei 10 Gbps)
Hier sind die Anpassungen z. B. an die Datenrate, unabhängig vom Medium, durchzuführen.
- 1a Physical-Media-Dependent (PMD)
Hier sind die vom Medium abhängigen Anpassungen vorzunehmen.

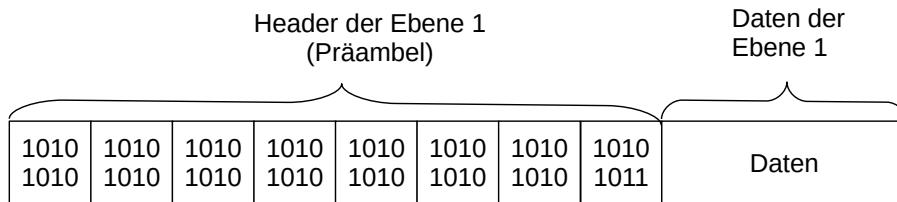


Abbildung 47: Beispiel: Header der Ebene 1 bei Ethernet

4.3 - Sicherungs-Schicht (2)

(engl. Data-Link-Layer)

Diese Schicht dient zum fehlerfreien Datenaustausch zwischen zwei Rechnern. Auf dieser Ebene werden die so genannten Rahmen (engl. Frames) ausgetauscht.

Auf dieser Ebene werden die folgenden Funktionen erbracht:

- ➊ Verbindungsmanagement

- ➌ Steuerung des Medien-Zugriffs. Ist ein Medienzugriffsverfahren erforderlich, wird es z. B. mit CSMA/CD abgehandelt. Vom englischen Begriff „Media Access Control“ (MAC) stammt auch die Bezeichnung MAC-Layer für diese Schicht.
- ➍ Adressierung (über MAC-Adresse oder DSAP (Destination SAP)).

- ➋ Fehlererkennung und eventuelle Korrektur (Durch die Verwendung von Prüfsummen, die an den Rahmen angehängt werden, gibt es leistungsfähige Mechanismen, um Fehler zu erkennen und zu korrigieren)

- ➌ Flusssteuerung (Hierbei wird die bestmögliche Ressourcen-Ausnutzung angestrebt)

Auch diese Ebene wird oft in zwei Unterebenen aufgeteilt:

2b LLC (Logical Link Control) hier können Dienste im Rahmen von IEEE-802.2 bearbeitet werden.
Hier wird die DSAP-Adressierung durchgeführt.

2a MAC-Ebene. Hier wird z. B. die MAC-Adressierung und die Datensicherung abgehandelt.

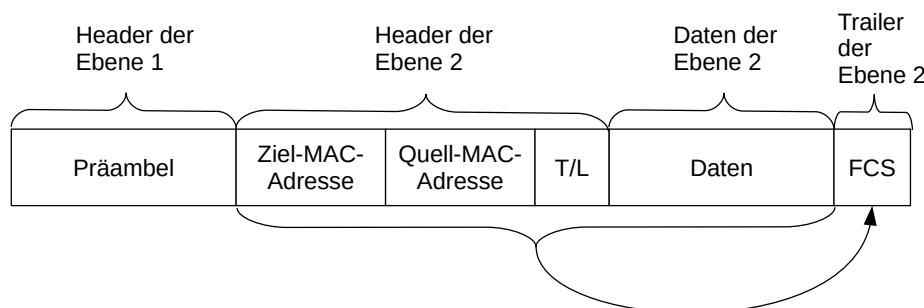


Abbildung 48: Beispiel: Ermittlung der Frame-Check-Sequence bei Ethernet

Zur Bildung der Prüfsumme (Frame-Check-Sequence) wird die Information ab dem Header der Ebene 2 bis zum Ende der Daten herangezogen.

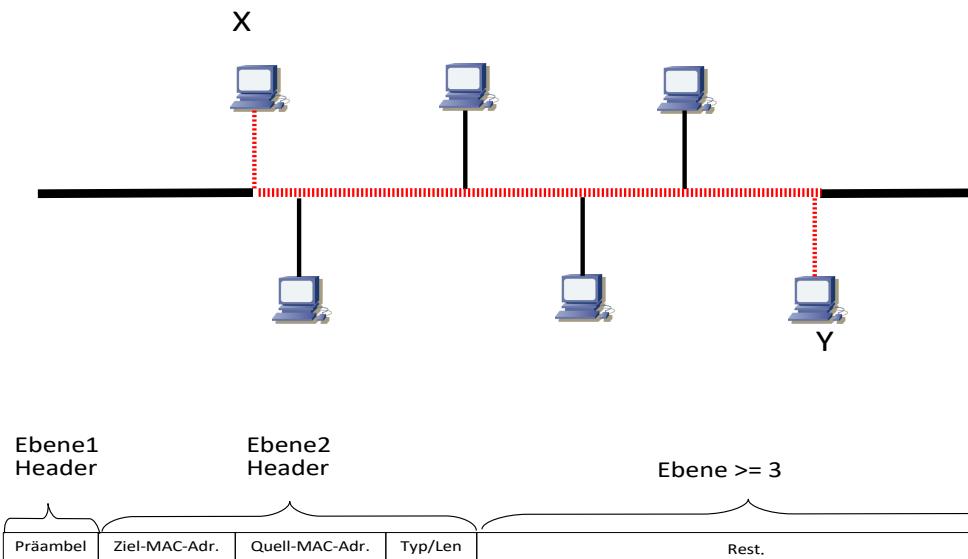


Abbildung 49: Kommunikation auf Ebene2

Damit Geräte z. B. über Ethernet miteinander in einem Netzwerk angesprochen werden können, benötigen die Netzwerk-Interfaces eine Adresse mit der sie eindeutig angesprochen werden können. Dazu wird die MAC-Adresse verwendet. Deshalb hat jede Netzwerk-Schnittstelle eine eigene MAC-Adresse. Für die Bezeichnung MAC-Adresse wird manchmal auch der Begriff Ethernet-Adresse oder Hardware-Adresse verwendet.

Sobald ein Gerät einen Frame über ein Netzwerk übertragen will, muss es die Ziel-MAC-Adresse und die eigene, die Quell-MAC-Adresse, in den MAC-Header eintragen

Die MAC-Adresse des Ziels muss evtl. erst ermittelt werden. Dazu kann z. B. das ARP-Protokoll verwendet werden.

Die eigene MAC-Adresse (also die Sender/Quell-MAC-Adresse) wird vom Hersteller der Netzwerk-Karte fest in einem EPROM (Erasable Programmable Read-Only-Memory) eingebrannt, kann jedoch vom Administrator überschrieben werden.

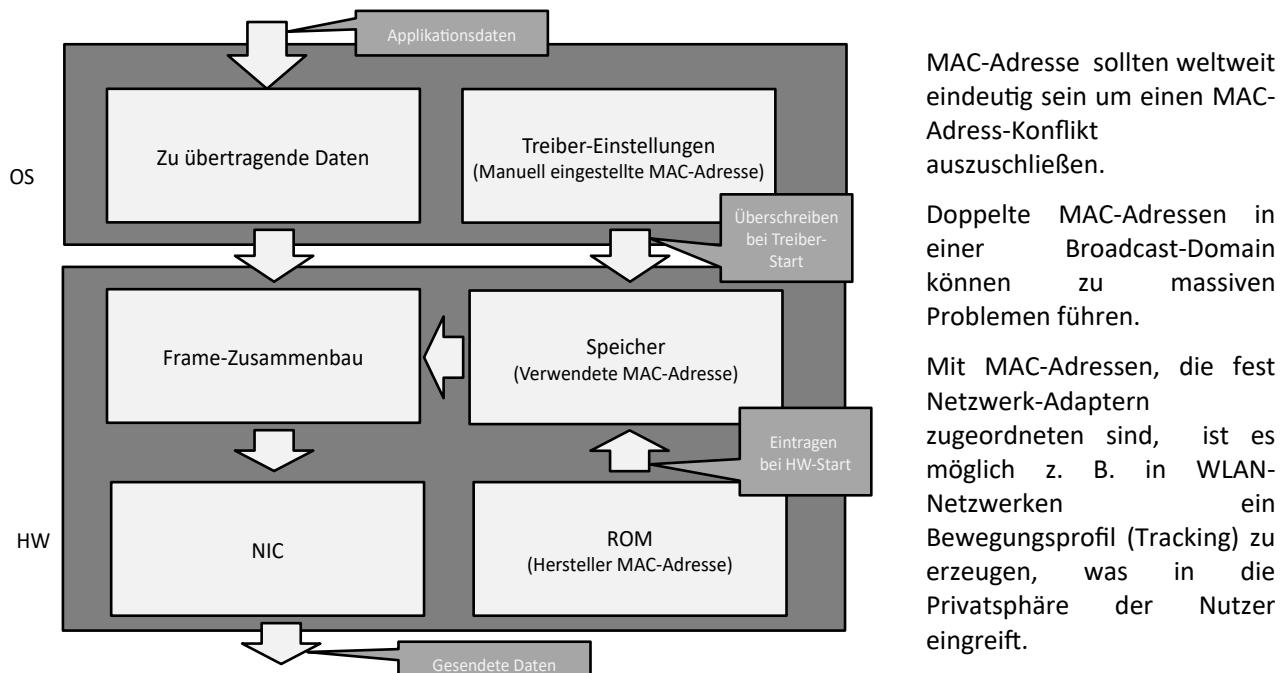


Abbildung 50: MAC-Adress-Zuweisung zum Frame

erfolgen. Solche MAC-Adressen werden z. B. verwendet, solange ein WLAN-Accesspoint mit Probe-Requests

OSI-Referenzmodell

gesucht wird und noch keine Verbindung besteht. Erst wenn der Client sich mit dem AP verbindet wird die Hardware-MAC-Adresse oder die manuell konfigurierte MAC-Adresse verwendet. Diese Funktion existiert ab Windows 10, ab iOS 8 und ab Android 6.

Auf einem Bussystem, wie in Abbildung 49: Kommunikation auf Ebene2, lesen alle an das Netzwerk angeschlossene Geräte alle Frames mit.

Jedes Gerät vergleicht die Ziel-MAC-Adresse mit seiner eigenen MAC-Adresse. Sind die beiden Adressen identisch, wird der Frame weiter verarbeitet.

Entspricht die mitgelesene MAC-Adresse nicht der eigenen MAC-Adresse, werden die Frames nicht weiter verarbeitet und verworfen.

Ausnahmen hiervon sind Multicasts und Broadcasts. Broadcasts werden von allen Geräten weiter verarbeitet. Multicast werden von den Mitgliedern einer bestimmten Gruppe genutzt und deshalb evtl. auch weiter geleitet.

Die Bearbeitung des MAC-Adressen-Vergleichs findet auf der Netzwerk-Karte, also auf der Hardware statt.

Sobald der Frame weiter verarbeitet wird, muss die CPU des Rechners sich damit beschäftigen, da die Ebenen >2 mit Software realisiert werden.

Eine MAC-Adresse besteht bei Ethernet aus 6 Bytes (EUI-48) mit der folgenden Reihenfolge auf der Leitung:

1. Bit I / G - Bit (Individual/Group Bit)

0 = Adressierung einer einzelnen Station (Unicast)

1 = Multicast oder Broadcast

2. Bit G / L - Bit (Global/Local Bit) Universal von IEEE verwaltete Adresse

0 = Die Adresse ist eine von IEEE vergebene Adresse und vom Hersteller eingebrannt.

Sie wird auch Global Administrated Address genannt (GAA)

1 = Die Adresse wurde vom Administrator vergeben.

Sie wird auch Local Administrated Address genannt (GAA)

3. - 24. Bit OUI (Organizationally Unique Identifier) Herstellerkennung (siehe Anhang)

25. - 48 Bit Laufende Nummer, die vom Hersteller vergeben wird.

Beispiele Für MAC-Adressen.

- Broadcast-Adress-Darstellung unter UNIX: FF:FF:FF:FF:FF:FF
- Broadcast-Adress-Darstellung unter Microsoft-Windows : FF-FF-FF-FF-FF-FF
- Unicast-Adress-Darstellung unter Microsoft-Windows: 08-00-27-00-AE-B3
- Broadcast-Adress-Darstellung auf HP-Switch: FFFFFF-FFFFFF

Bevor die MAC-Adresse in den Frame eingebaut wird werden die Bytes gespiegelt. Die Bedeutung wechselt damit Byteweise von MSB zu LSB. Das gleich wird gemacht wen ein Frame von der Leitung übernommen und bearbeitet wird.

Z. B.

0x35	0x7B	0x12	0x00	0x00	0x01
00110101	01111011	00010010	00000000	00000000	00000001

wird zu:

0xAC	0xDE	0x48	0x00	0x00	0x80
10101100	11011110	01001000	00000000	00000000	10000000

Damit kann bereits am ersten Bit erkannt werden, ob es sich um einen Unicast oder Broadcast/Multicast handelt.

IEEE hat für künftige Netze 64-Bit-Adressen unter der Bezeichnung EUI-64 festgelegt.

OSI-Referenzmodell

Da die Hersteller die OUI teuer erwerben müssen, wurden am 1.Januar 2014 weitere Bereiche eingeführt, bei denen es weniger laufenden Nummern gibt die jedoch billiger zu haben sind:

- MA-L = MAC Address Large (entspricht einer EUI48-MAC-Adresse. Der Hersteller hat 2^{24} Bits zur Verfügung)
- MA-M = MAC Address Medium (IEEE legt 28 Bits fest. Der Hersteller hat 2^{24} Bits zur Verfügung)
- MA-S = MAC Address Short (IEEE legt 36 Bits fest. Der Hersteller hat 2^{12} Bits zur Verfügung)

Große Hersteller von Netzwerk-Komponenten kommen mit einer OUI nicht aus. Wer in der MA-L Liste von IEEE nach Cisco sucht, wird Stand 20.12.2021 1097 Einträge von insgesamt 31177 für Cisco finden. Siemens hat 49 und Hewlett Packard hat 254 Einträge.

Da die ersten beiden Bits (I/G und G/L) bereits für andere Zuordnungen vergeben sind stehen den Herstellern tatsächlich nur 22 Bits zur Verfügung.

Damit kann für eine OUI im Rechner an der 2. Stelle nur ein Wert von 4, 8 oder C stehen, wie im folgenden Beispiel zu sehen ist.

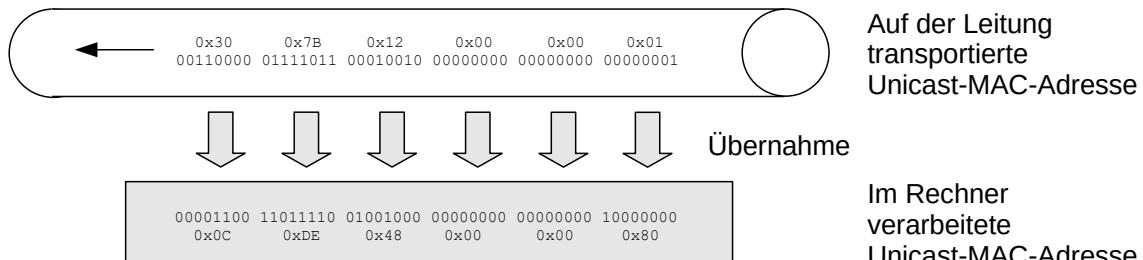


Abbildung 51: Beispiel: Umwandlung von LSB in MSB bei Ethernet

Die Verarbeitung eines Frames hängt davon ab, ob der Frame für das Gerät bestimmt ist. Die folgende Übersicht zeigt die Möglichkeiten auf.

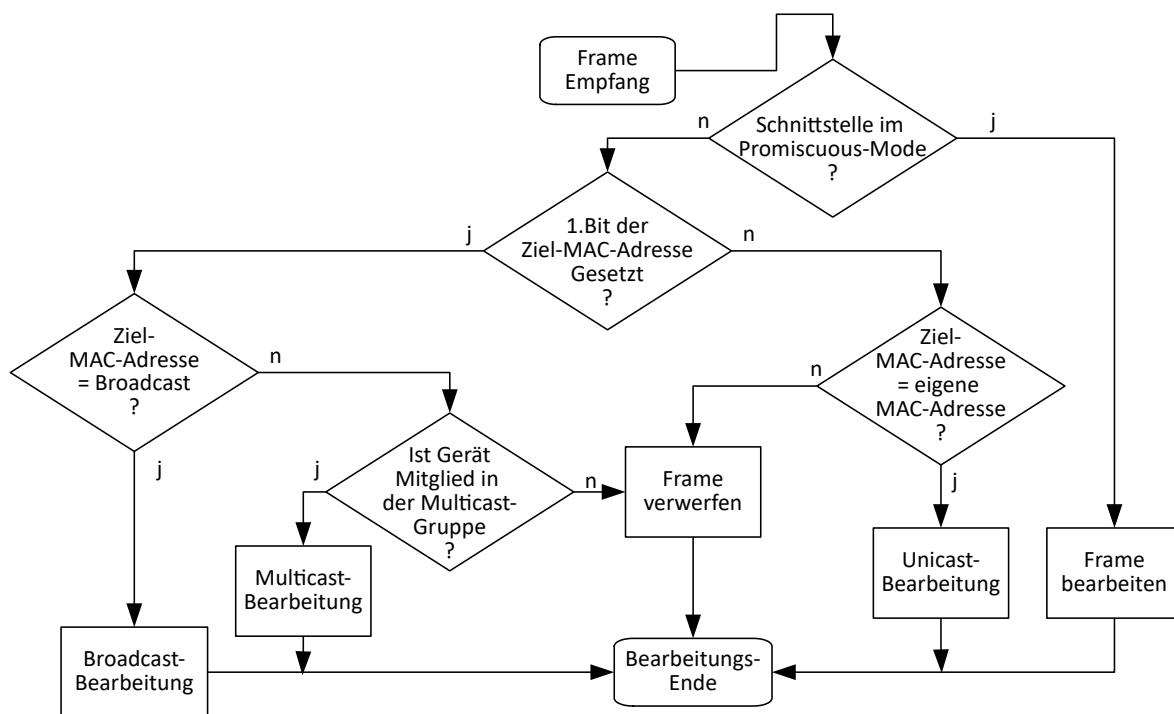


Abbildung 52: Framebearbeitung in Abhängigkeit von der Ziel-MAC-Adresse

Ist die Schnittstelle in den Promiscuous-Mode konfiguriert, dann wird der Frame auf alle Fälle übernommen und weiter bearbeitet.

Ist die Schnittstelle nicht im Promiscuous-Mode, hängt die weitere Bearbeitung vom ersten Bit ab. Broadcast-Adressen werden immer weiter verarbeitet. Multicast-Adressen werden nur bearbeitet, wenn das Gerät in der entsprechenden Multicast-Gruppe ist.

Ist das erste Bit nicht gesetzt, wird die Ziel-MAC-Adresse daraufhin untersucht, ob es die eigene MAC-Adresse ist. Ist das der Fall, wird der Frame weiter verarbeitet. Ansonsten wird der Frame nicht bearbeitet und verworfen.

4.4 - Vermittlungs-Schicht (3)

(engl. Network-Layer)

Diese Schicht dient zur Verbindung von Endsystemen über Transit-Systeme hinweg. Dazu ist eine logische Adressierung einzuführen (z. B. IP-Adressen) um über das lokale Netzwerk hinaus mit Systemen in anderen Netzwerken zu kommunizieren.

Damit Daten über mehrere Netzwerke ausgetauscht werden können ist in den Daten-Headern die Information für die Wegefindung zu hinterlegen. Protokolle mit diesen Informationen werden geroutete Protokolle genannt. Beispiele sind IP und IPX. Damit können die Router welche die Netzwerke miteinander verbinden die Daten zum Ziel transportieren. Um den Routern die Entscheidung für die Wegewahl zu ermöglichen halten sie so genannte Routing-Tabellen. In ihnen sind die Netzwerke mit den möglichen Routen hinterlegt.

Werden die Netzwerke miteinander vermascht, um redundante Wege zu ermöglichen und damit die Ausfallsicherheit zu erhöhen, müssen sich die Router miteinander, über so genannte Routing-Protokolle, unterhalten welche Routen gerade möglich sind. Damit kann die Information für die Wegentscheidung automatisch abgeglichen werden. Beispiele hierfür sind RIP, OSPF, IGRP. Alternativ kann man die Routing-Tabellen auch manuell pflegen. Dann sind die Routen allerdings statisch. Die Router können sich dann nicht mehr automatisch nach dem Ausfall einer Verbindung optimieren.

Da die Router auch Netzwerke mit unterschiedlichen physikalischen Ausprägungen miteinander verbinden kann es vorkommen, dass die Paketgrößen anzupassen sind. Dazu werden die Funktionen:

Fragmentation (deutsch: Zerlegung) und Reassembling (deutsch: wieder zusammen setzen) verwendet.

Auf der Ebene 3 wird nur dafür gesorgt, dass die Pakete an ihr Ziel kommen. Geht ein Paket aus irgend einem Grund verloren, kann aus dieser Schicht heraus nicht darauf reagiert werden. Für Wiederholungen von Paketen ist z. B. die nächste Schicht mit dem TCP zuständig.

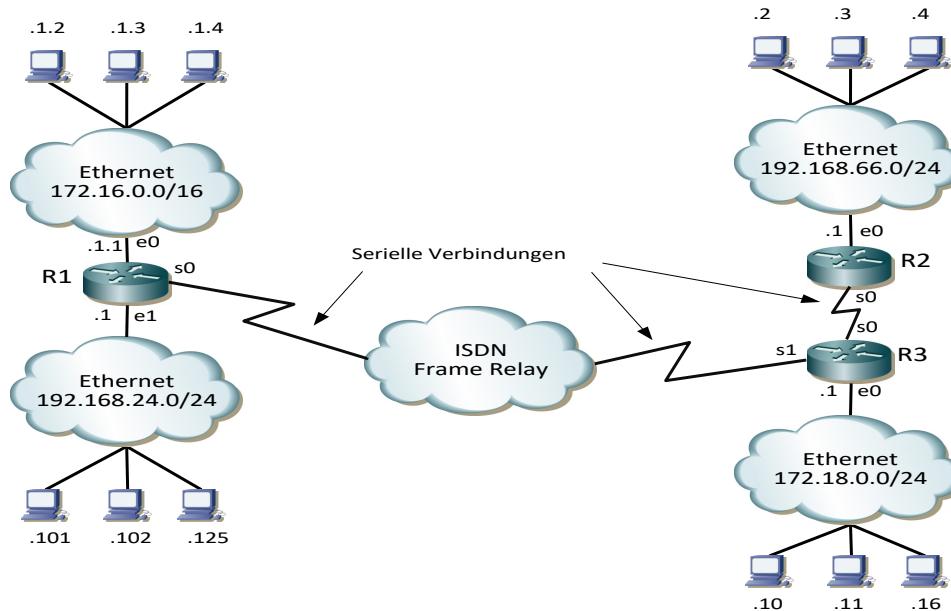


Abbildung 53: Routing

Im obigen Bild sind mehrere verschiedene Netzwerke, die miteinander über das IP-Protokoll kommunizieren, dargestellt. Jedes Gerät hängt an einem IP-Netzwerk mit einer IP-Netzwerk-Adresse (**172.16.0.0/16**) und hat dort eine IP-Host-Adresse (172.16.1.2). Die Router R1 – R3 haben sowohl Ethernet-Schnittstellen (e0 – e1) als auch serielle Schnittstellen (s0 – s1). An den Ethernet-Schnittstellen sind IP-Adressen notwendig. An den seriellen Schnittstellen sind IP-Adressen nicht notwendig jedoch möglich. Damit jeder Router weiß über welche Schnittstelle ein Paket zu transportieren ist, hat er eine so genannte Routing-Tabelle. Angenommen der Rechner rechts unten (IP-Adresse 172.18.0.16) will mit dem Rechner links oben (IP-Adresse 172.16.1.2) kommunizieren, dann sendet er seine Pakete an den Router R3. Im Router R3 befindet sich die folgende Routing-Tabelle in der alle Netzwerke eingetragen sind. Zu jedem Netzwerk ist hinterlegt über welche Router-Schnittstelle das Ziel-Netzwerk zu erreichen ist.

Ziel-Netzwerk	Schnittstelle
192.168.24.0 / 24	s1
192.168.66.0 / 24	s0
172.18.0.0 / 24	e0 (lokal)
172.16.0.0 / 16	s1
0.0.0.0 / 0	s1 (Default Route)

Nachdem der Router R3 das Paket von 172.18.0.16 in Empfang genommen hat, sieht er im Paket-Header nach welche Ziel-IP-Adresse eingetragen wurde. In der obigen vereinfachten Routing-Tabelle findet er in der vorletzten Zeile den richtigen Eintrag (172.16.0.0/16) und sendet deshalb das Paket über seine Schnittstelle s1 an den Router R1.

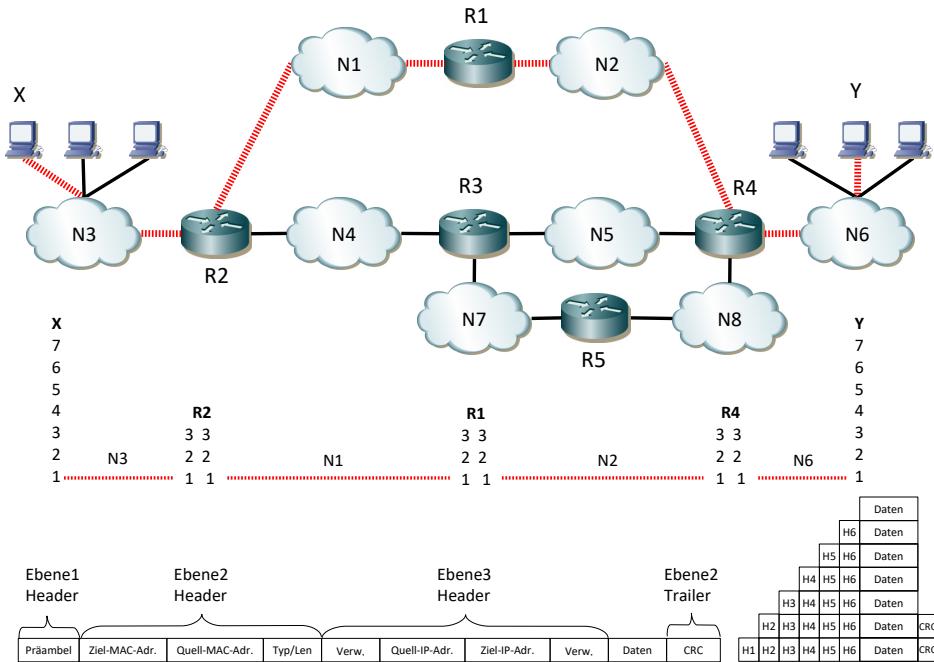


Abbildung 54: Routing über Netzwerk-Grenzen hinweg

In der obigen Abbildung ist dargestellt wie die Datenpakete über die Netzwerke und Router hinweg transportiert werden.

Der Rechner X kommuniziert mit dem Rechner Y. Dabei werden von der Anwendungsebene (7) die Daten mit einem Header für die Ebene 6 versehen und der Ebene 6 übergeben. Die unter lagerten Schichten verfahren genau so und bauen jeweils einen Header dazu. Links unten ist dargestellt wie die Header bis zur 3. Ebene von den Routern interpretiert werden. Dabei sind die Pakete bis auf die Ebene 3 von den auszupacken. Dort sind die IP-Adressen abgelegt. Die IP-Adressen und die Routing-Tabelle werden dann von den Routern für die Wegentscheidung für das Paket herangezogen um die Pakete weiter zu transportieren. Am Ende wird auf dem Ziel-System (Rechner Y) das Paket bis auf die Daten von den einzelnen Schichten ausgepackt.

Je nachdem welche Funktion ein Netzwerk-Gerät hat muss es die Header unterschiedlich tief interpretieren. Router arbeiten auf Ebene 3 und müssen somit die Header bis auf die Ebene 3 bearbeiten.

In der obigen Abbildung ist zu sehen wie die Router aufgrund ihrer Routing-Tabellen ein Paket über ein vermaschtes Netzwerk zum Zielrechner bringen. Stehen einem Router mehrere Wege zum Ziel zur Verfügung, muss er sich für den optimalen Weg entscheiden. Dazu hat er in seine Routing-Tabelle mit der Metrik ein zusätzliches Entscheidungs-Hilfsmittel. Die Metriken sind Kriterien die genutzt werden um einen Weg bei mehreren Wege-Möglichkeiten zu finden. Dazu können folgende Eigenschaften genutzt werden:

- Bandbreite
- Delay (Verzögerung)
- Load (Last)
- Reliability (Zuverlässigkeit)
- Hop-Count (Anzahl der Router bis zum Ziel)

4.5 - Transport-Schicht (4)

(engl. Transport-Layer)

Sie stellt einen transparenten Datenübertragung zwischen Endsystemen zur Verfügung. Dabei sind zwei grundsätzlich unterschiedliche Ausprägungen möglich:

- Verbindungsorientierte-Kommunikation (z. B. TCP)
 - ◆ Dabei ist vor dem eigentlichen Datentransport eine Verbindung zu etablieren.
 - ◆ Erst nach dem Aufbau der Verbindung kann mit dem Datenaustausch begonnen werden.
 - ◆ Nach dem Datenaustausch ist die Verbindung wieder abzubauen.

Für die Umsetzung der Anforderungen werden folgende Mechanismen verwendet:

- Timer
- Wiederholungen
- Flusskontrolle
- Windowing / Stop-and-Wait
- Multiplexing um eine Verbindung mehrfach zu nutzen

- Verbindungslose-Kommunikation (z. B. UDP)
 - ◆ Hierbei werden die Daten in das Netzwerk in Richtung Empfänger gesendet, ohne, dass der Sender weiß, ob der Empfänger empfangsbereit ist. Damit sind die oben aufgeführten Mechanismen, wie Flusskontrolle und Wiederholungen in den überlagerten Schichten zu bearbeiten.

4.6 - Sitzungs-Schicht (5)

(engl. Session-Layer)

Diese Schicht ist die erste anwendungsorientierte Schicht. Deshalb ist die Nutzung dieser Schicht nur mit bestimmten Anwendungen sinnvoll.

Damit ist eine Anwendung strukturierbar. Während des Sitzungsablaufs können Synchronisationspunkte gesetzt werden. Im Fehlerfall kann auf diesen Synchronisationspunkten wieder aufgesetzt werden.

In der Sitzungs-Schicht ist auch die Dialog-Kontrolle untergebracht es gibt hierbei:

- 3 Betriebsarten (Simplex, Half-Duplex, Full-Duplex)
- 3 Phasen (Verbindungsaufbau, Datenübertragung, Verbindungsabbau)

Beispiele für Realisierungen in dieser Schicht sind:

- NFS (Network-File-System unter UNIX)
- XWINDOWS (Fenster-Bearbeitung unter UNIX)

4.7 - Darstellungs-Schicht (6)

(engl. Presentation-Layer)

Unterschiedliche Rechner haben aufgrund unterschiedlicher Betriebssysteme unterschiedliche Darstellungsformen der Daten. Soll eine Applikation auf unterschiedlichen Betriebssystemen ablaufen können, sind Konvertierungen durchzuführen.

Hier werden folgende Umsetzungen abgewickelt:

- Zeichensätze (ASCII, EBCDIC)
- Interpretation von Bytes MSB (Most Significant Bit) / LSB (Least Significant Bit)
- Kompression / Dekompression
- Verschlüsselung / Entschlüsselung

4.8 - Anwendungs-Ebene (7)

(engl. Application-Layer)

Die Anwendung ist die Schnittstelle zwischen dem Anwender und der Rechner-Kommunikation. Beispiel hierfür sind:

- | | |
|--------|------------------------------------|
| ● FTP | File Transfer Protocol |
| ● SMTP | Simple Mail Transfer Protocol |
| ● SNMP | Simple Network Management Protocol |
| ● DNS | Domain Name Service |

5 - Abtastung

5.1 - Klassifizierung von Signalen

Signale können sowohl von ihrem Wert und vom zeitlichen Verlauf her sowohl kontinuierlich als auch diskret auftreten.

So nimmt ein Mikrofon ein Signal auf und gibt es als analoges (zeit- und wert-kontinuierliches) Signal weiter.

In einem Rechner können digital nur zeit-diskrete (also abgetastete) und wert-diskrete (also quantisierte) Signale verarbeitet werden. Dazu werden die zeit- und wert-kontinuierlichen Signale von einem A/D-Wandler (Analog/Digital-Wandler) zu zeit- und wert-diskreten Signalen umgewandelt. [HELÖ-NATE-2000][BOS-EIDN-2012]

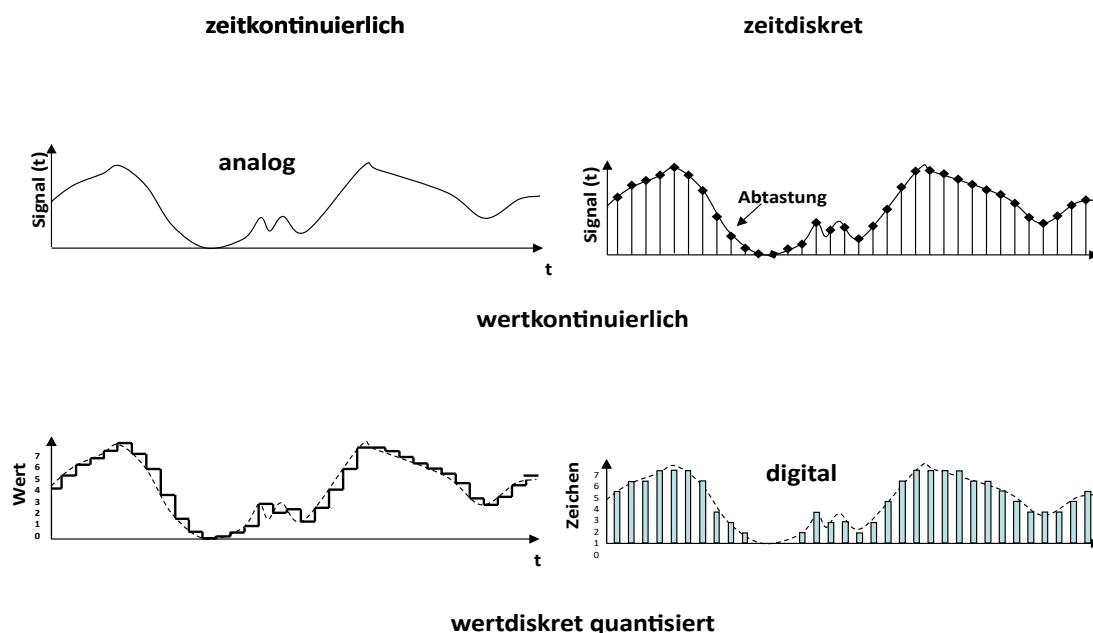


Abbildung 55: Klassifizierung von Signalen

5.2 - Abgetastete Signale

Analoge Signale sind fortlaufend in der Zeit und im Wert. Digitale Signale sind quantifiziert mit 2^n -Werten. Für jede **Abtastung** können n -Bits verwendet werden. Hier ergibt sich die Granularität, also der kleinste Abstand zwischen zwei möglichen Messwerten. Je mehr Bits verwendet werden, desto „feiner“ kann gemessen werden.

Bei der Abtastung der Signale muss in diskreten, äquidistanten Intervallen (t_s) abgetastet werden. Hier erhebt sich die Frage: „Wie oft muss innerhalb eines bestimmten Zeitraums abgetastet werden?“.

Die Grenze (Frequenz) mit der mindestens abgetastet werden muss, wird auch **Nyquist-Kriterium**, **Nyquist-Grenze** oder **Nyquist-Frequenz** genannt. Sie ergibt sich als die halbe **Abtastfrequenz** eines zeit-diskreten Signals.

$$f_{Nyquist} = \frac{1}{2} f_{Abtast} \quad (1)$$

Daraus ergibt sich das so genannte **Abtasttheorem**:

Wenn alle Anteile in einem Signal f_{Signal} kleinere Frequenzen als die Nyquist-Frequenz f_{Nyquist} haben, kann das Signal beliebig genau rekonstruiert werden.

Ein Signal, das keine Frequenzen größer B (f_{max}) enthält, kann man aus seinen Abtastwerten wiedergewinnen, wenn diese mit der Abtastfrequenz (f_{Abtast}) abgetastet werden.

$$f_{\text{Signal}} < f_{\text{Nyquist}} \quad (2)$$

Damit muss die Abtastfrequenz (f_{Abtast}) doppelt so groß sein wie die höchste Frequenz im abzutastenden Signal (f_{Signal}). Wird dies nicht eingehalten, entstehen nichtlineare Verzerrungen (**Aliasing-Effekt**).

$$f_{\text{Abtast}} > 2f_{\text{Signal}} \quad (3)$$

Daraus ergibt sich das Abtastintervall (T_{Abtast}).

$$T_{\text{Abtast}} < \frac{1}{2}B \quad (4)$$

Wird also mit mindestens der doppelten Frequenz als dem abzutastenden Signal abgetastet, kann das Signal jederzeit rekonstruiert werden.

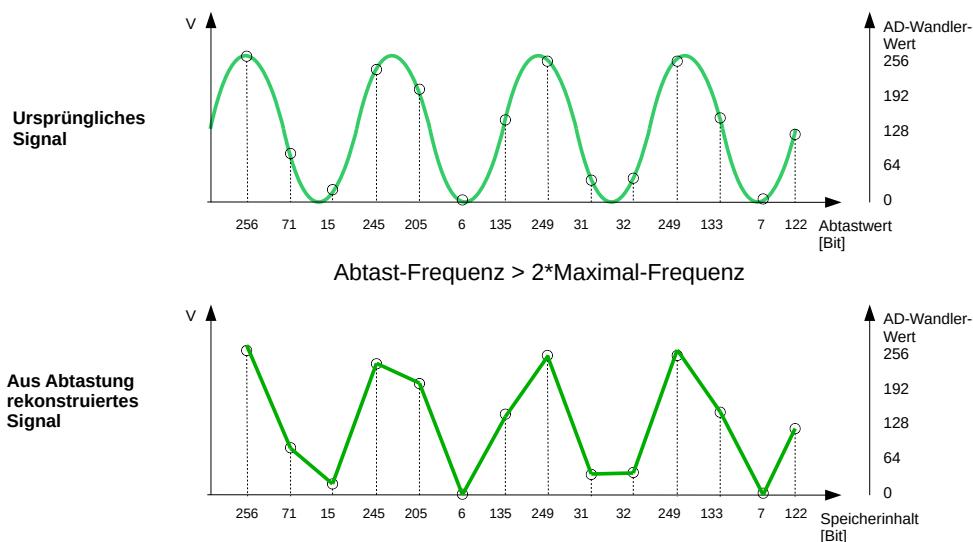


Abbildung 56: Abtastung mit $f_A > 2B$

Abtastung

Wird ein Sinus-Signal mit genau der doppelten Frequenz abgetastet und fällt die Abtastung zeitlich mit dem Nulldurchgang zusammen, kann das ursprüngliche Signal nicht wieder hergestellt werden.
Nur unter der Prämisse, dass es sich um ein Sinussignal handelt, bei dem die Nulldurchgänge erfasst wurden, kann das ursprüngliche Signal wieder hergestellt werden.

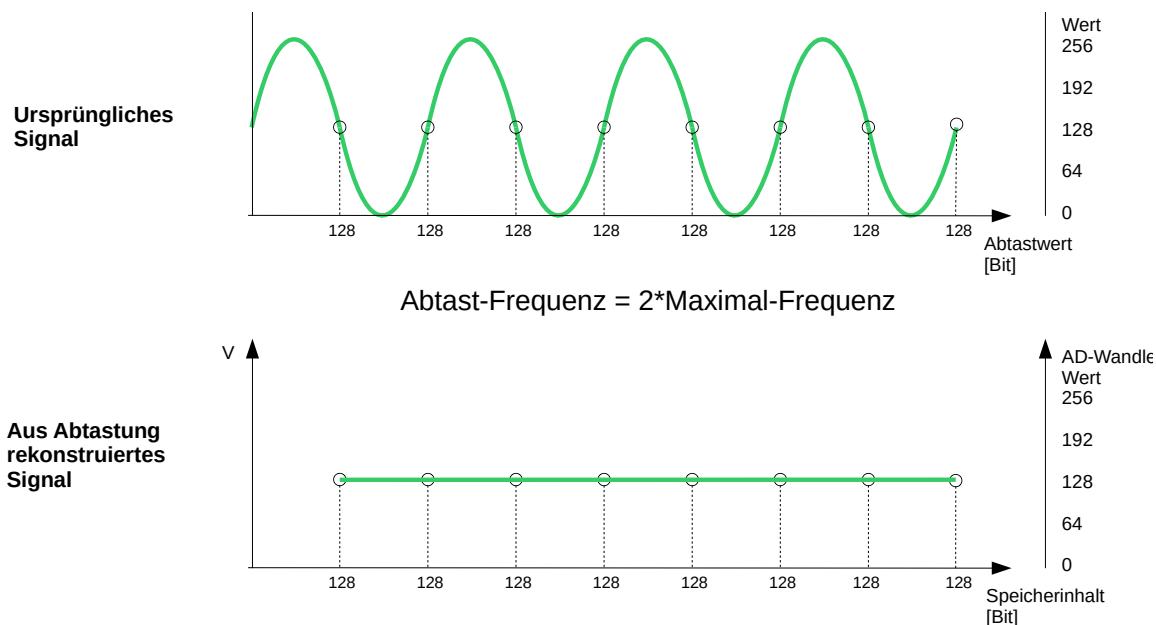


Abbildung 57: $f_A = 2B$

Ist die Abtastfrequenz kleiner als die doppelte abzutastende Frequenz kann das Original-Signal nicht wieder hergestellt werden.

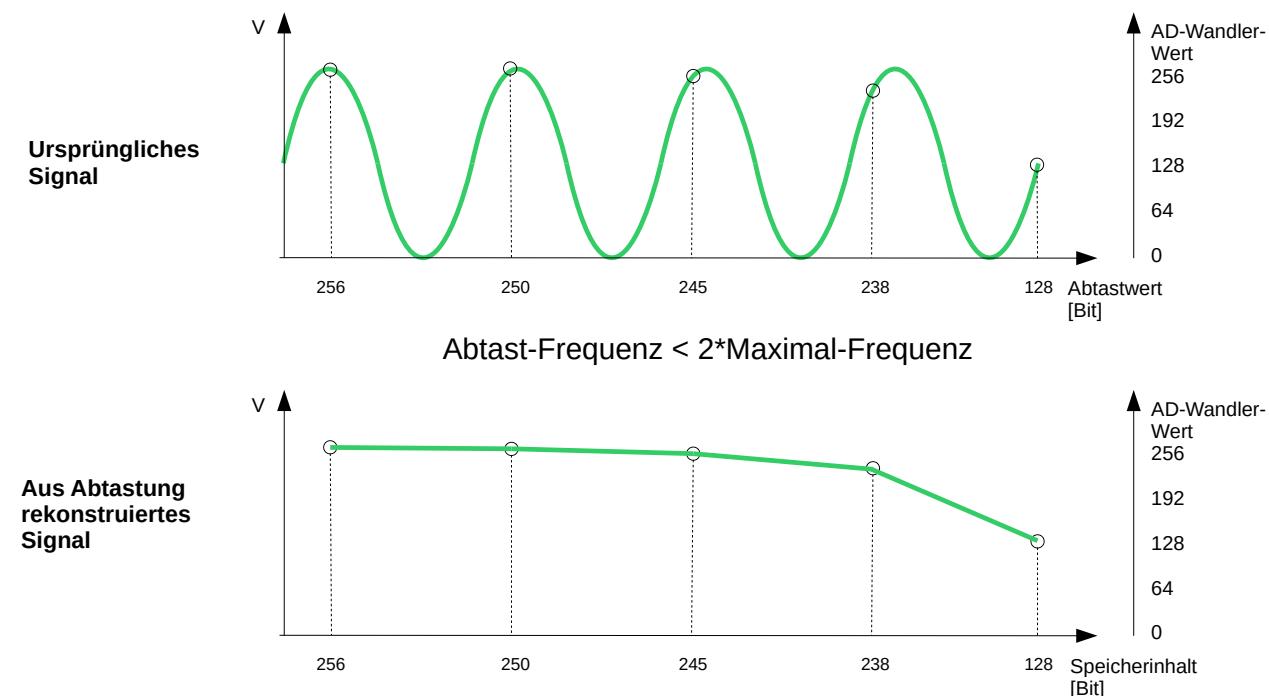


Abbildung 58: $f_A < 2B$

5.3 - Begriffe der Abtastung

Am Beispiel eines zeit-kontinuierlichen Signals sollen die Begriffe der Abtastung erläutert werden.

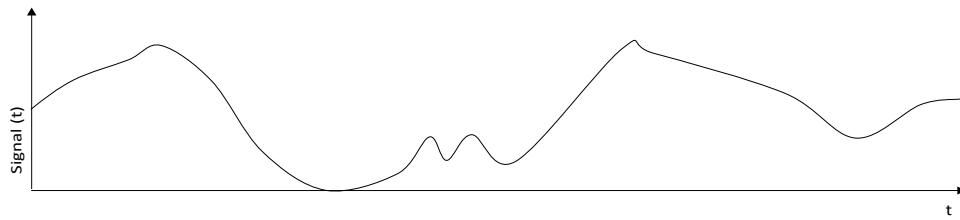


Abbildung 59: Zeit-kontinuierliches Signal

Das Signal soll innerhalb einer Sekunde 5 Mal abgetastet werden.

Damit wird das zeit-kontinuierliche Signal in festen (diskreten) Zeitabständen, also mit dem Abtastintervall (T) 1/5 Sec abgetastet.

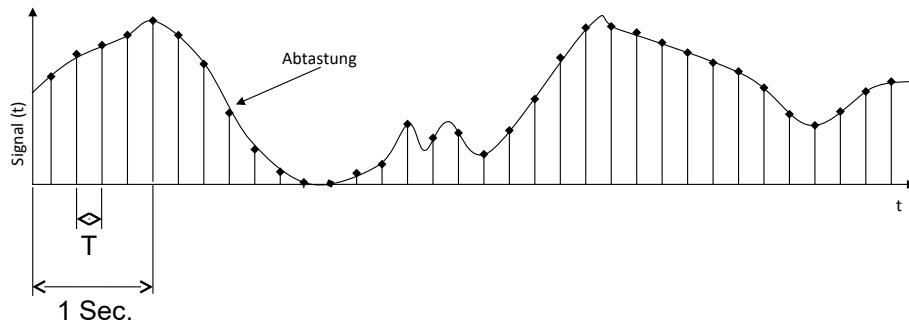


Abbildung 60: Abtastintervall

In Abbildung 60 wird bei jeder Abtastung ein zeit-diskreter, wert-kontinuierlicher Wert ermittelt.

In einem realen A/D-Wandler (Analog/Digital-Wandler) wird allerdings ein wert-diskreter Wert ermittelt werden. In Abbildung 61 wird der ermittelte Wert einem Zeichen zugeordnet. Da Werte von 0 bis 7 möglich sind, sind pro Zeichen 3 Bit erforderlich.

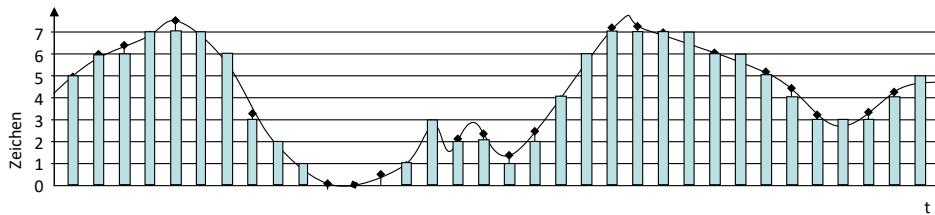


Abbildung 61: Zeit- und wert-diskrete Abtastung

Abtastung

Bei der Abtastung kann der genaue Wert aufgrund des begrenzten Wertebereichs nicht exakt abgetastet werden. Die Differenz zwischen Originalsignal und Abtastwert/Symbol wird **Quantisierungsrauschen** genannt.

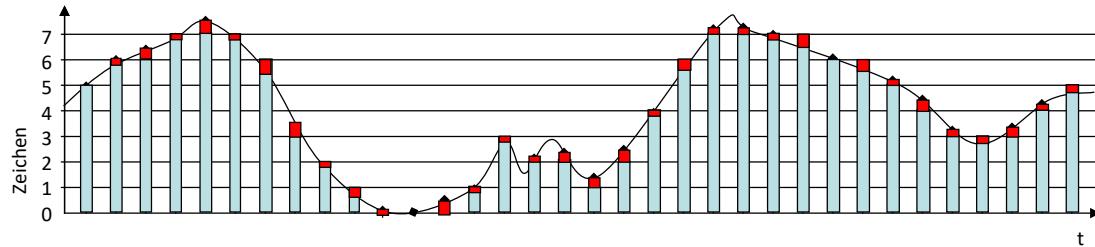


Abbildung 62: Quantisierungsrauschen

Um das Quantisierungsrauschen zu reduzieren, muss die Anzahl der Abtastwerte erhöht werden. Damit erhöht sich der Zeichenvorrat und folglich die Anzahl der Bits, die pro Symbol zu übertragen werden muss.

Bei einer Abtastung von 5 Symbolen pro Sekunde entsteht eine Symbolrate von 5 **Baud** (Bd).

Ein **Schritt** ist die kleinste systemtechnisch realisierbare Zeiteinheit und entspricht dem **Abtastintervall** (T).

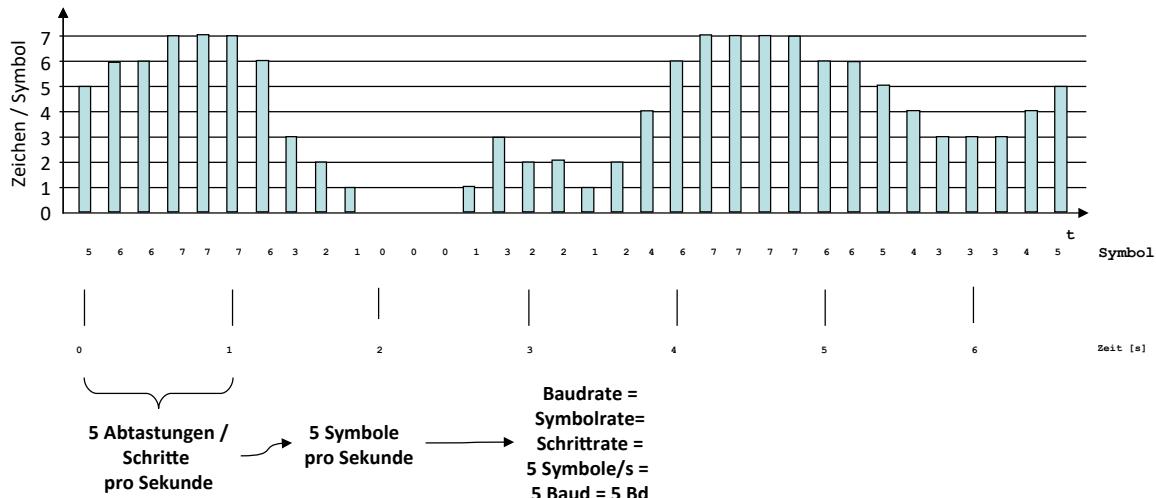


Abbildung 63: Baudrate / Symbolrate / Schritt

Die Übertragungsgeschwindigkeit / Bitübertragungsrate / Bitrate ergibt sich aus der Anzahl der Zeichen pro Sekunde multipliziert mit der Bits pro Zeichen Im Beispiel 5 Zeichen/s * 3Bit/Zeichen = 15 Bit/s.

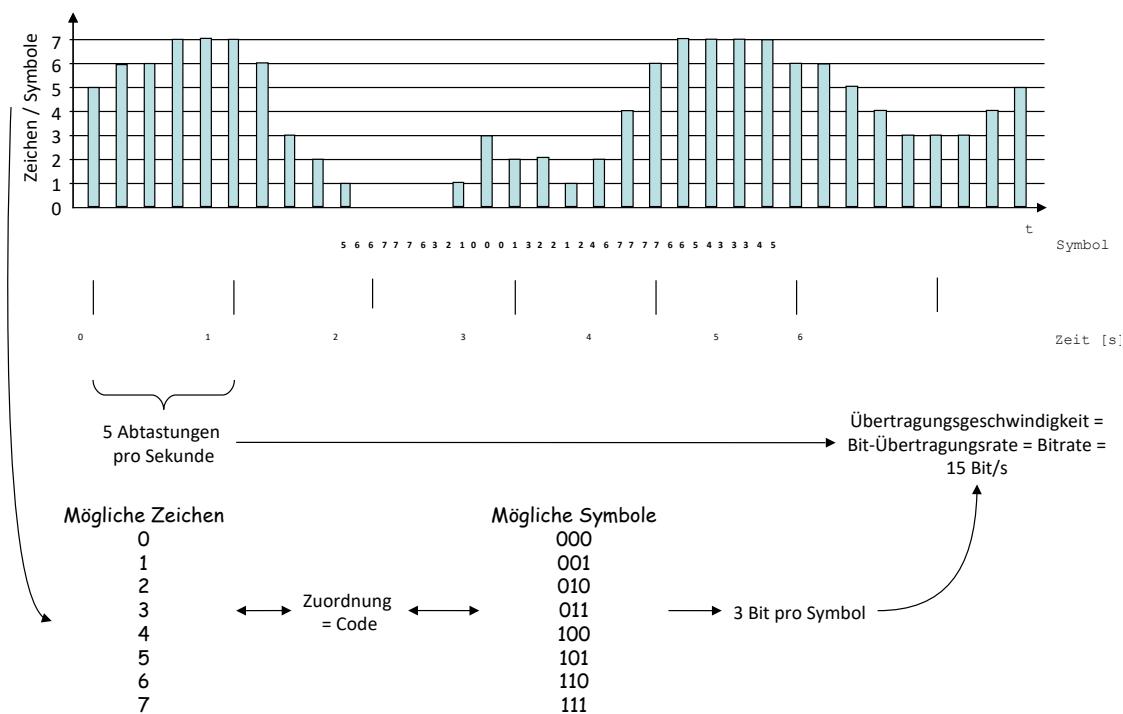


Abbildung 64: Übertragungsgeschwindigkeit

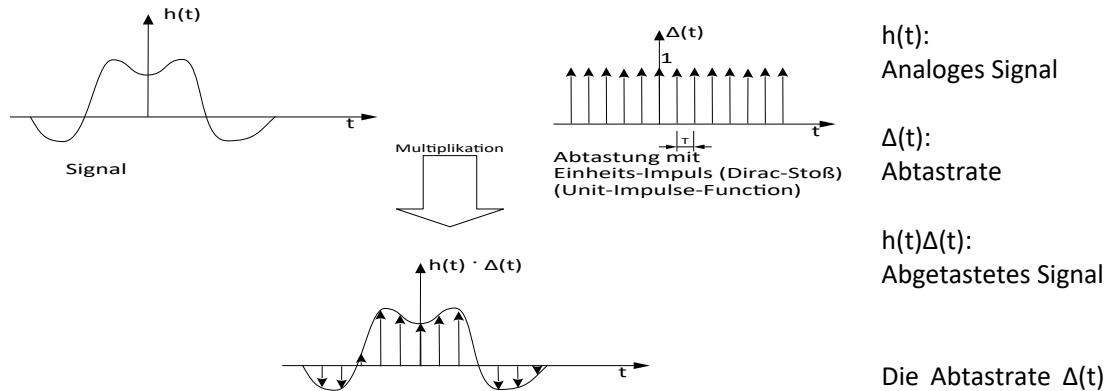
Achtung:

Baudrate = Bitrate gilt nur wenn pro Schritt ein Symbol mit nur einem Bit gesendet wird!

5.4 - Aliasing-Effekt

5.4.1 - Beispiel einer richtigen Abtastung

Im folgenden ist eine Abtastung einer ausreichenden Abtastfrequenz dargestellt.



Die Abtastrate $\Delta(t)$ ist klein genug um den Kurvenverlauf hinreichend genau zu erfassen.

Abbildung 65: Aliasing1-Zeitbereich

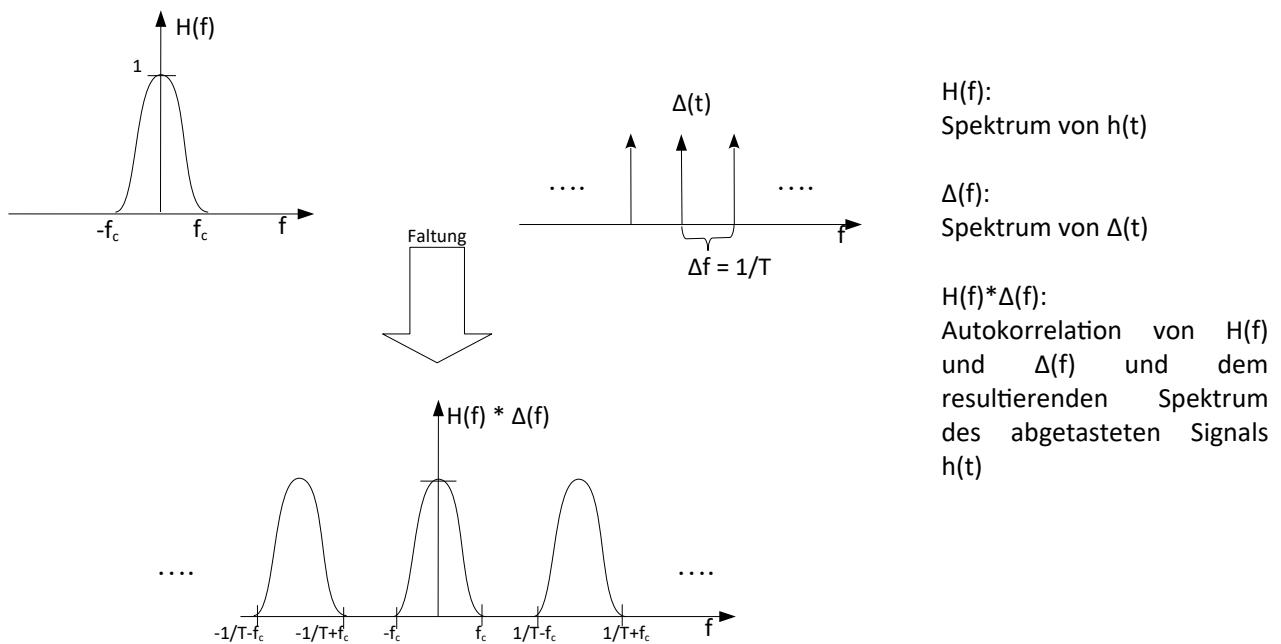


Abbildung 66: Aliasing1 - Frequenzbereich

Durch die Faltung überlagern sich der Dirac-Impuls und das Spektrum des Signals. Einer Vergrößerung des Abtastintervalls ΔT entspricht eine Verringerung des Abstandes Δf des Dirac-Impulses im Frequenzbereich.

Um sicherzustellen, dass im resultierenden Spektrum [Abbildung: 66] die Signale sich nicht überschneiden muss das Abtastintervall mindestens der doppelten abzutastenden Frequenz entsprechen. Daher kommt auch die Aussage für das **Nyquist-Kriterium (1)**.

Im obigen Bild ist im resultierenden **Spektrum** der Abstand zwischen den Frequenzen groß genug um sie sauber voneinander unterscheiden zu können. Damit ist die Abtastfrequenz ausreichend.

5.4.2 - Beispiel einer falschen Abtastung

Nun folgt eine Abtastung bei der die Abtastfrequenz nicht ausreichend ist.

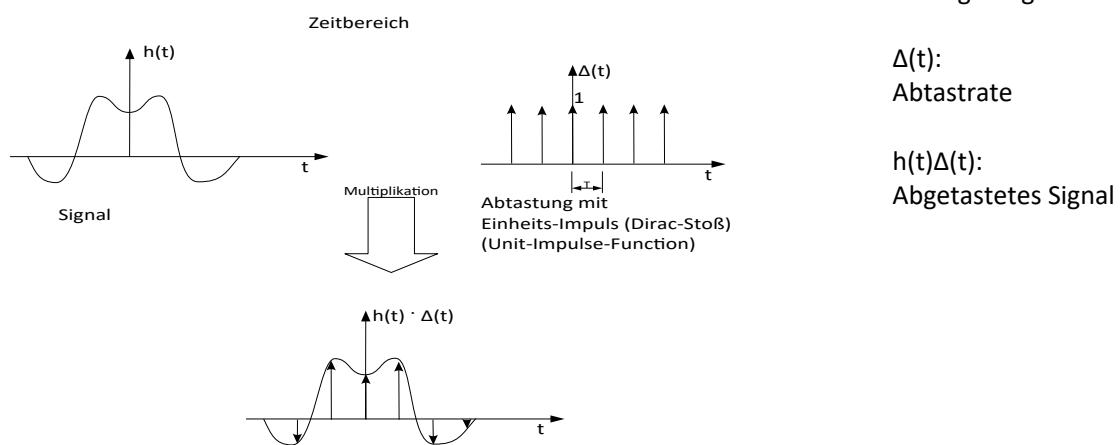


Abbildung 67: Aliasing2 Zeitbereich

Die Abtastrate $\Delta(t)$ ist hier zu groß. Dadurch schieben sich die Spektren der Dirac-Impulse im Frequenzbereich zusammen und die Kurvenverläufe überlagern sich. Beim Empfänger können die einzelnen Spektren nicht mehr sauber voneinander getrennt werden.

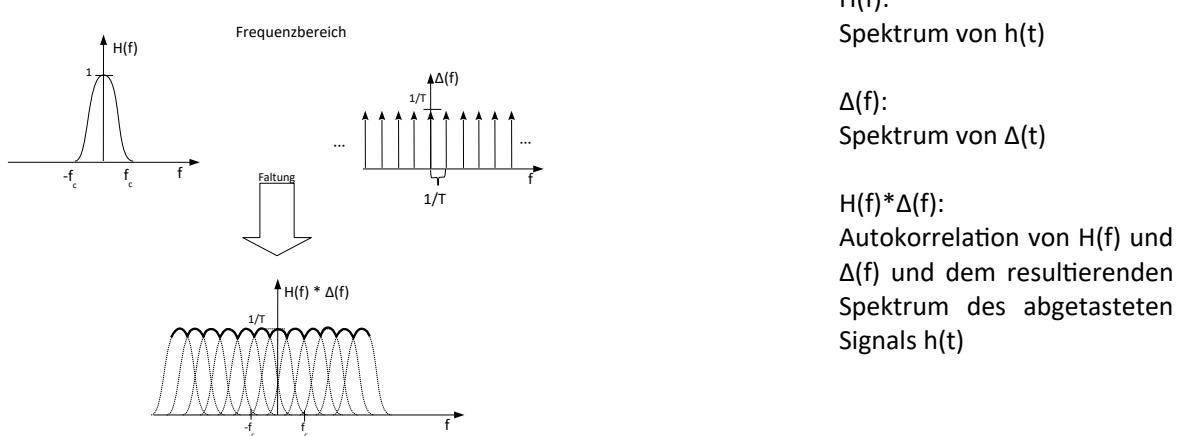


Abbildung 68: Aliasing2 - Frequenzbereich

Im resultierenden Ergebnis sind die einzelnen Spektren nicht mehr sauber voneinander trennbar da eine Überlappung auftritt.

Aliasing bedeutet also, dass der ursprüngliche Kurvenverlauf nicht mehr naturgetreu nachgebildet werden kann. Dies ist z. B. bei Bildschirmanzeigen der Fall wenn aus einer geraden diagonalen Linie eine Treppe wird oder wenn bei einem Western-Film die Räder einer Postkutsche anfangen, sich rückwärts zu drehen.

5.5 - Darstellung eines Signals

Sinus-Signale können sowohl als Kurvenverlauf als auch im Zeigerdiagramm dargestellt werden.

Die Darstellung kann auch im Zeitbereich sowie im Frequenzbereich erfolgen.

$$s(t) = A \sin(\omega t + \Phi) \quad (5)$$

Dabei gilt:

- A = Amplitude
- $\omega = 2\pi f$ = Kreisfrequenz
- Φ = Phasenlage
- f = Frequenz in Hz
- T = Periodendauer in s
($f = 1/T$)

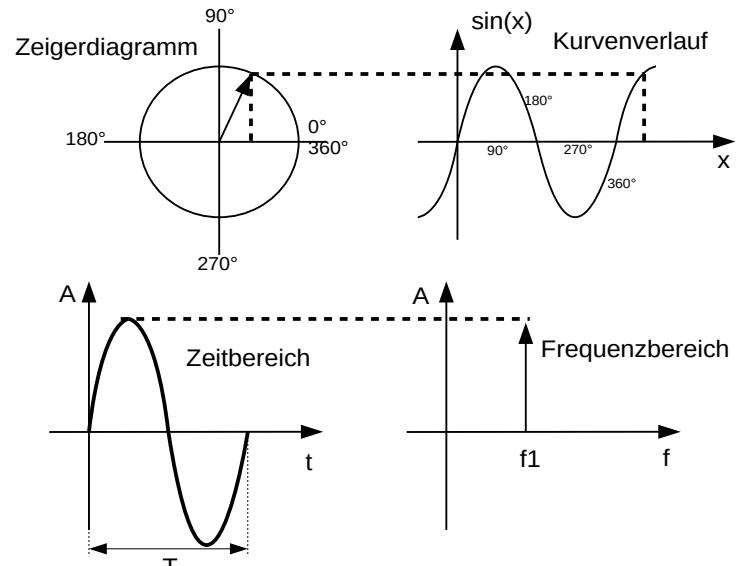


Abbildung 69: Darstellungsmöglichkeiten von Sinus-Signalen

5.6 - Fourier-Transformation eines periodischen Signals

Jean-Baptiste Fourier bewies im frühen 19. Jahrhundert, dass jede periodisches Signal $s(t)$ als unendliche Summe von Sinus und Cosinus-Funktionen gebildet werden kann. Ein so genannte Fourier-Reihe kann folgendermaßen gebildet werden.

$$s(t) = a_0 + a_1 \cos(\omega t) + b_1 \sin(\omega t) + a_2 \cos(\omega t) + b_2 \sin(\omega t) + a_3 \cos(\omega t) + b_3 \sin(\omega t) + \dots \quad (6)$$

Fourier-Reihe:

$$s(t) = a_0 + \sum_{n=1}^{\infty} a_n \cos(n \omega t) + \sum_{n=1}^{\infty} b_n \sin(n \omega t) \quad (7)$$

Die so genannten Fourier-Koeffizienten lauten:

$$a_0 = \frac{1}{T} \int_0^T s(t) dt \quad (8)$$

$$a_n = \frac{2}{T} \int_0^T s(t) \cos n \omega t dt \quad (9)$$

$$b_n = \frac{2}{T} \int_0^T s(t) \sin n \omega t dt \quad (10)$$

Die Amplitude lässt sich mit der folgenden Formel ermitteln:

$$c_n = \sqrt{a_n^2 + b_n^2} \quad (11)$$

Beispiel:

Gegeben sei ein Rechtecksignal mit der Periodendauer 2π . In der folgenden Abbildung ist oben das Original-Signal auf der linken Seite im Zeitbereich zu sehen.

Auf der rechten Seite ist das gleiche Signal im Frequenz-Bereich zu sehen. Hier müssten eigentlich unendlich viele Oberwellen dargestellt sein. Der Einfachheit halber wurden nur die ersten 5 Überlagerungen dargestellt.

Eine grobe Annäherung an das Signal kann schon mit der Überlagerung der beiden Sinussignale $s_1(t)$ und $s_2(t)$ zum Signal $s_{12}(t)$ erreicht werden.

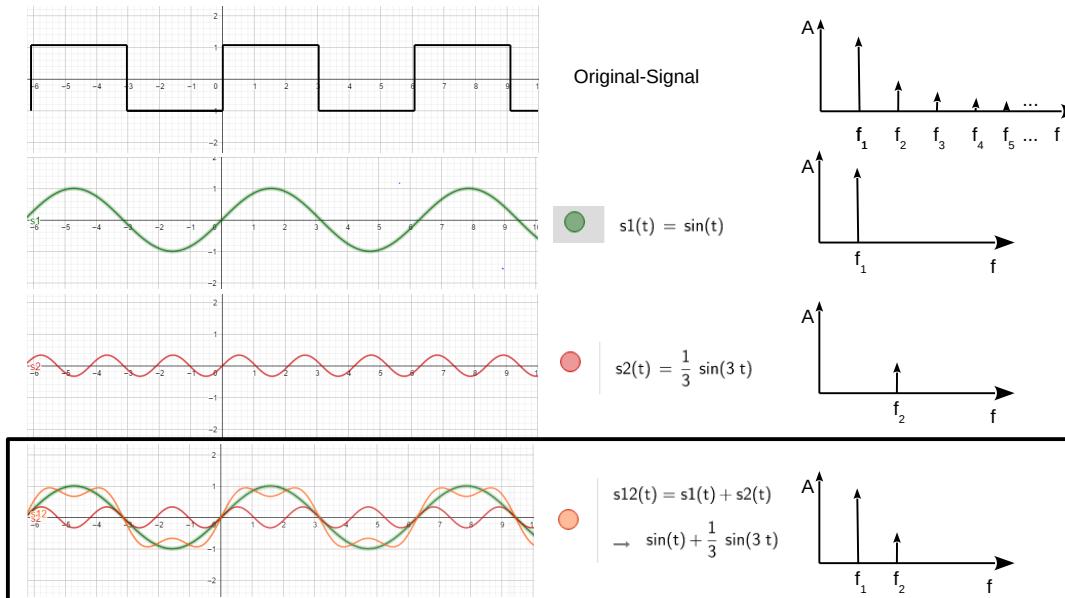


Abbildung 70: Fourier-Synthese (Teil-1)

Eine weitere Verbesserung kann mit dem Hinzufügen der Signale $s_3(t)$ und $s_4(t)$ erreicht werden. Dies kann immer weiter so fortgesetzt werden, bis schließlich das Originalsignal mit einer unendlichen Anzahl von Überlagerungen synthetisiert wurde.

Abtastung

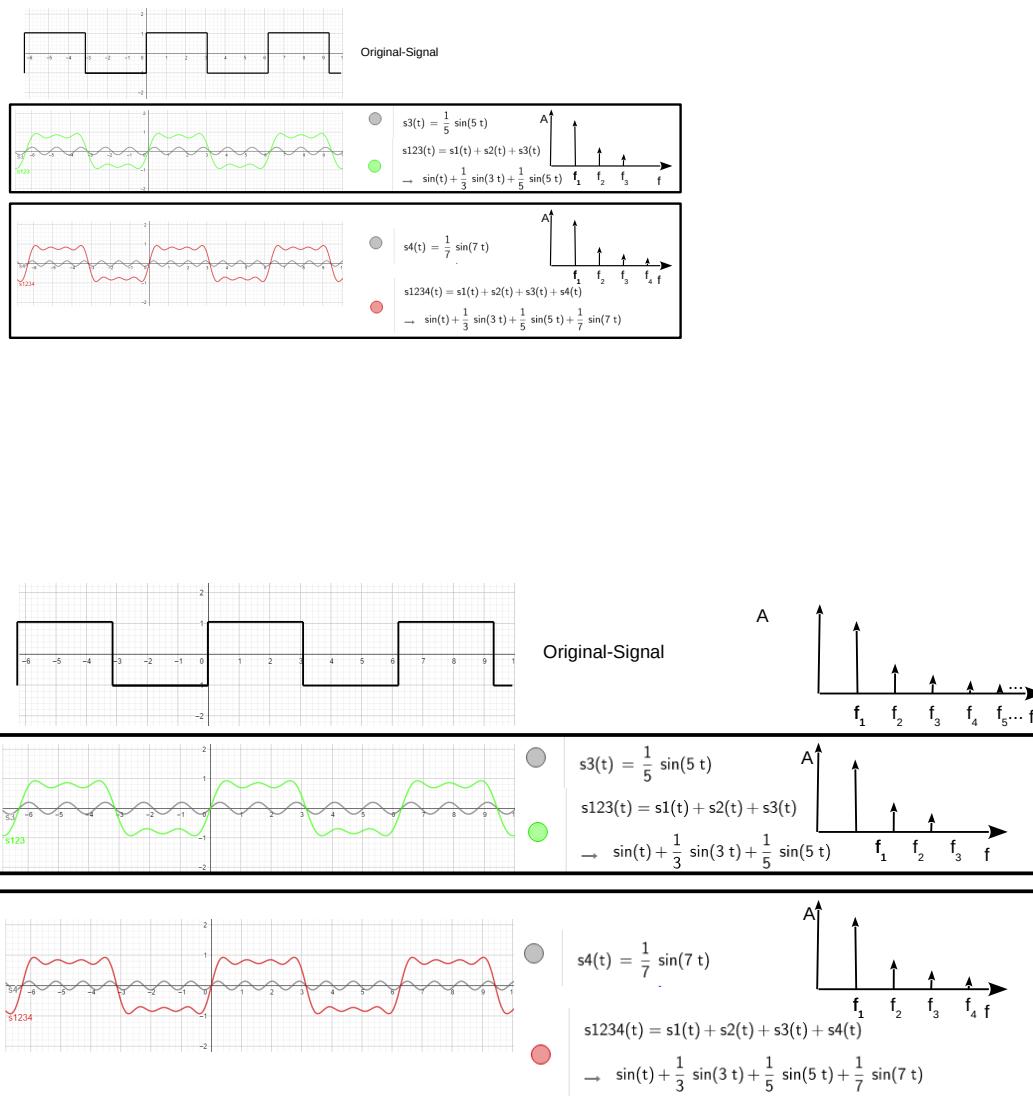


Abbildung 71: Fourier-Synthese (Teil-2)

Die Spannende Frage ist, wann ist das Signal ausreichend genug zusammengesetzt, um ohne Informationsverlust beim Empfänger zusammengesetzt zu werden.

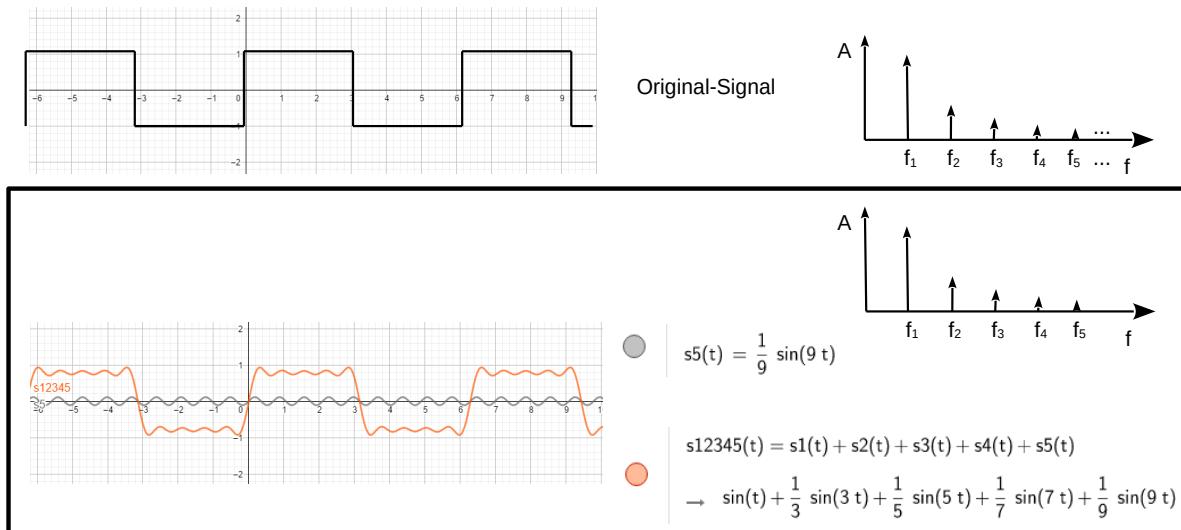


Abbildung 72: Fourier-Synthese (Teil-3)

Je naturgetreuer der periodische Impuls dargestellt werden soll, desto mehr Oberwellen sind erforderlich. Damit vergrößert sich zwangsläufig auch die notwendige Bandbreite! Somit ist die Definitionen für die Bandbreite: Bandbreite ist die Differenz zwischen maximaler und minimaler Fourier-Frequenz.

Ab einer Grenzfrequenz f_g werden Signale stark abgeschwächt und in ihrer Phasenlage beeinflusst.

Für die Bandbreite einer Leitung kann angegeben werden:

Unter der Bandbreite B einer Leitung versteht man den Frequenzbereich bei dem mit dieser Leitung noch keine Verzerrungen auftreten.

6 - Digitale Datenübertragung

6.1 - Einleitung

Bei analogen Signalen können kleinste Störungen zu einer verfälschten Information beim Empfänger führen.

Eine Fehlererkennung und eine Fehlerkorrektur ist allerdings nur bei einer digitalen Verarbeitung möglich denn es ist einfacher die Erkennung von „Nullen und Einsen“ durchzuführen als eine Vielzahl von analogen Werten.

Die Vorteile der digitalen Datenübertragung sind:

- Datenkompression durch Quellencodierung
- Fehlererkennung und Fehlerbehebung durch Kanalcodierung
- Verschlüsselung zur Erhöhung der Vertraulichkeit, Authentizität
- Übertragung mehrerer Verbindungen über einen Kanal durch Multiplexing
- Vermittlung von Informationen über mehrere Netzwerke hinweg

Im folgenden Kapitel werden die Grundbegriffe dazu erklärt.

6.2 - Maximale Kanalkapazität (C_N)

Zuerst ist zu klären, welche Datenmenge über einen Kanal innerhalb einer bestimmten Zeit gesendet werden kann. Dazu betrachten wir die maximale Datenübertragungsrate eines störungsfreien Kanals. Dieses Maximum ist nur ein theoretischer Wert, da bei jeder Übertragung von Daten über einen Kanal Störungen auftreten und damit nicht das Maximum übertragbar ist.

Die maximale Datenübertragungsrate C_N bei einem störungsfreien Kanal mit der Bandbreite (B) ist gegeben durch:

$$C_N = 2B \quad (12)$$

Die Bandbreite B wird in Hz = 1/Sekunde angegeben.

C_N wird in Symbolen / Sekunde = Baud angegebenen.

Dies ergibt sich aus dem Abtasttheorem. (siehe hierzu auch das Kapitel Abtastung)

Bei einem binären Symbolalphabet, wenn also pro Symbol 2 unterschiedliche Zeichen übertragen werden können, ist die Bitrate in bit / s = bps (bits per second) = der Symbolrate in Baud.

Natürlich kommt es darauf an wie groß das Symbolalphabet ist. Bei L unterschiedlichen Symbolen lassen sich $Id(L)$ Bits pro Symbol darstellen:

$$C_N = 2B Id(L) \quad (13)$$

Beispiel:

Bei einer Bandbreite von 500 Hz können maximal 1000 Baud übertragen werden. Bestehen die Symbole aus 0 und 1, also zwei unterschiedlichen Bit, erreicht man eine Datenrate von 1000 bit/s, denn $Id(2) = 1$.

Bestehen die Symbole aus dem deutschen Alphabet (A – Z) hat man 26 unterschiedliche Zeichen. $Id(26) = 4,70044$. Damit würde sich die Datenrate um den Faktor 4,70044 auf 4700,44 bit/s = 4,7 kbit/s erhöhen.

6.3 - Kanalkapazität (C)

Leider gibt es keinen Übertragungskanal der störungsfrei ist. Claude E. Shannon zeigte 1948, dass das Signal-zu-Rausch-Verhältnis (SNR = Signal to Noise Ratio) sich hier auswirkt. Das SNR wird in dB angegeben. Dabei kommt das Verhältnis von Signalleistung (P_s) zu Rauschleistung (P_N , N = Noise) zum tragen. Da Spannungen einfacher zu messen sind, kann das SNR auch mittels der effektiven Spannungen ermittelt werden.

$$SNR = 10 \cdot \lg\left(\frac{P_s}{P_N}\right) = 20 \lg\left(\frac{U_{effS}}{U_{effN}}\right) \quad (14)$$

Damit ergibt sich für die Kanalkapazität aus dem Shannon-Hartley-Gesetz:

$$C = B \cdot I_d\left(1 + \frac{S}{N}\right) = B \cdot I_d\left(1 + \frac{P_s}{P_N}\right) \approx \frac{B}{3} \cdot 20 \cdot \lg\left(\frac{U_s}{U_N}\right) \quad (15)$$

Voraussetzung hierbei ist, dass das Rauschen ein weißes Rauschen ist. Dann spricht man von einem AWGN-Kanal (mit additivem weißen gaußschen Rauschen (Noise))

Nimmt man die Übertragungszeit (T) hinzu, kommt man auf die Informationsmenge (I) die über einen Kanal in einer bestimmten Zeit übertragen werden kann

$$I = T \cdot B \cdot I_d\left(1 + \frac{P_s}{P_N}\right) \approx T \cdot \left(\frac{B}{3}\right) \cdot 20 \cdot \lg\left(\frac{U_s}{U_N}\right) \quad (16)$$

Das Signal zu Rausch Verhältnis wird oft auch als Dynamic (D) bezeichnet. Damit vereinfacht sich die Formel zu:

$$I = T \cdot B \cdot D \quad (17)$$

Im normalen Leben sind alle technischen Signale mit einem unerwünschten Rauschen kombiniert. Oft ist es nicht erforderlich ein Signal mit maximaler Auflösung zu quantifizieren.

Beispiel:

Ein Signal mit 10V und 1V Rauschen in der Amplitude bedeutet, dass 10 unterschiedliche Abtastwerte erkannt werden können.

Durch jedes zusätzliche Bit bei der Quantisierung wird die Amplitude des Rauschens mit dem Wert 2 dividiert. Dadurch profitiert der Dynamic-Anteil um 6 dB denn $20 \lg(2) = 6,0206$.

Bei der Sprachübertragung gilt ein Signal zu Rausch-Verhältnis von 48 dB als ausreichend. Dies ist der Grund dafür, dass 8 Bit bei der Sprach-Quantifizierung verwendet werden.

Eine erfolgreiche Übertragung hängt nur vom Signal-zu-Rausch-Verhältnis ab. Nicht von der absoluten Signalstärke.

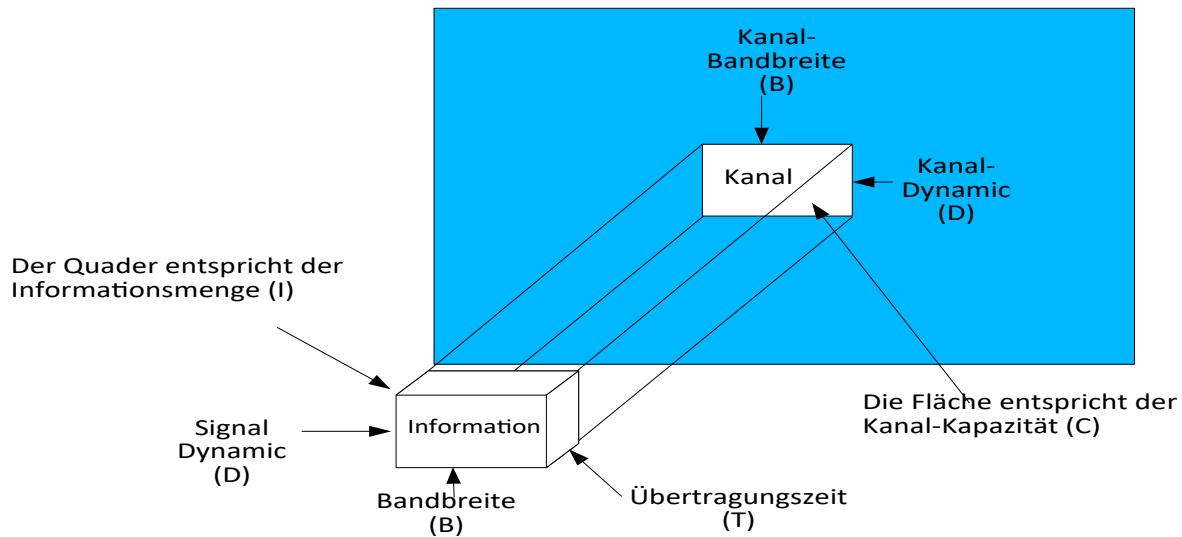
Um die Datenübertragung möglichst optimal zu gestalten, muss an der Empfängerseite das Signal vom Rauschen möglichst gut zu unterscheiden sein.

Um einen optimalen Kanal zu erhalten, können die Parameter geändert werden. Die Parameter sind jedoch voneinander abhängig. Z. B eine Erhöhung der Übertragungszeit bei gleich bleibender Bandbreite und Informationsmenge wird eine Verminderung des dynamischen Anteils (mehr Rauschen) mit sich bringen. Deshalb ist dann mit einer größeren Signalleistung gegen zu steuern.

6.4 - Message Cube

Shannon's Beschreibung der Informationsmenge (I) kann auch als 3-dimensionaler Quader beschrieben werden.

Abbildung 73: Message-Cube



Das Quader-Volumen beschreibt die Informationsmenge (I) mit den Kanten T , B und D .

Die Fläche mit den Seiten Bandbreite (B) und Dynamic (D) entspricht der Kanalkapazität (C).

6.5 - Multiplex-Verfahren

Moderne Systeme sind in der Lage für mehrere unabhängige Signale einen Kanal zu verwenden. Das hierbei verwendete Verfahren wird Multiplexing genannt. Dazu werden die drei Kanten des Message-Cubes verwendet. Je nachdem welche Seite verwendet wird, wird sie in Teile (Bereiche) zerlegt, um sie unterschiedlichen Verbindungen zuzuordnen.

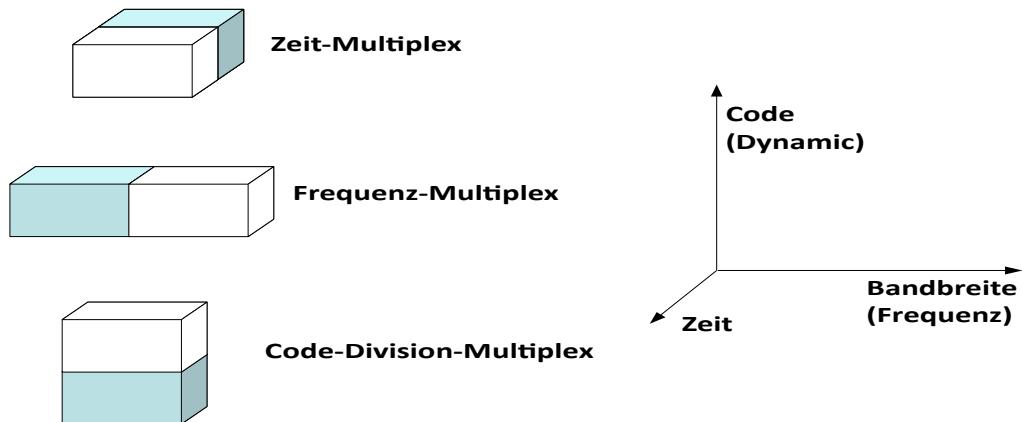


Abbildung 74: Multiplex-Verfahren

6.5.1 - Zeit-Multiplex

Hierbei wird jedem Teilnehmer ein Zeitschlitz (Slot) zugewiesen. In diesem Zeitschlitz werden die digitalisierten Sprach-Informationen übertragen. Für diese Art der Datenübertragung sind Puffer notwendig, in denen die Informationen für die Zeitschlüsse gesammelt und wieder abgegeben werden können.

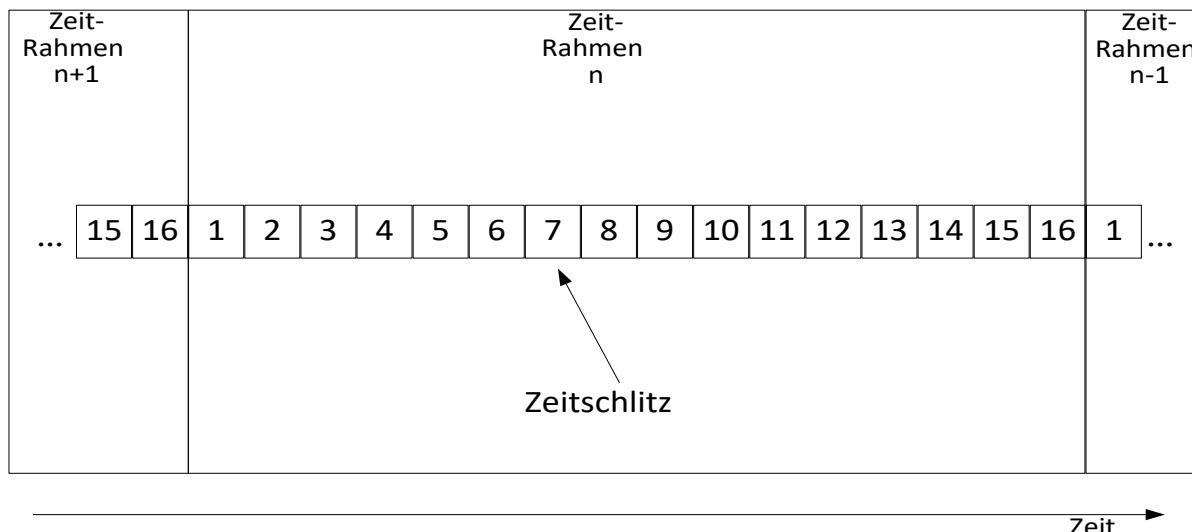


Abbildung 75: Zeitmultiplex

6.5.2 - Frequenz-Multiplex

Durch entsprechende Schaltkreise (Filter) ist es möglich die Richtungen zu extrahieren. Dann werden die Richtungen auf unterschiedliche Frequenzen moduliert.

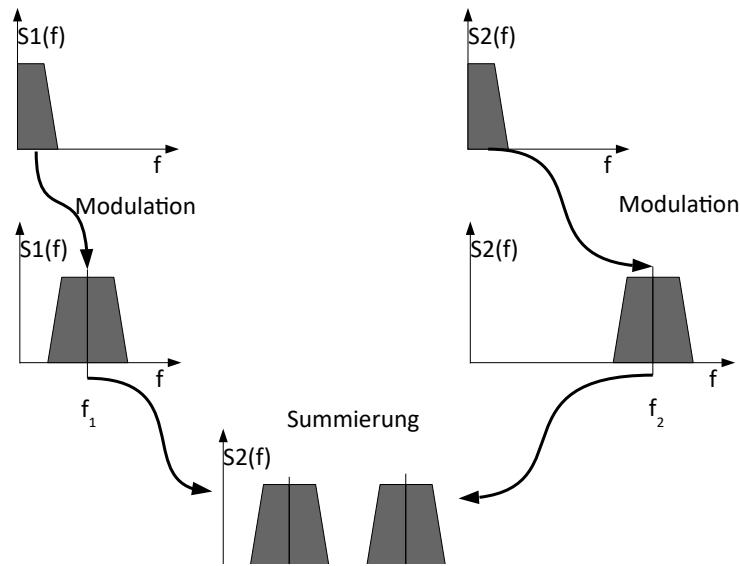


Abbildung 76: Frequenzmultiplex

6.6 - Modem

Neben der Übertragung von Sprache über analoge Systeme kann durch spezielle Geräte (Modems) auch digitale Information übertragen werden. Der Begriff Modem ist ein Kunstwort aus den Begriffen Modulation und Demodulation.

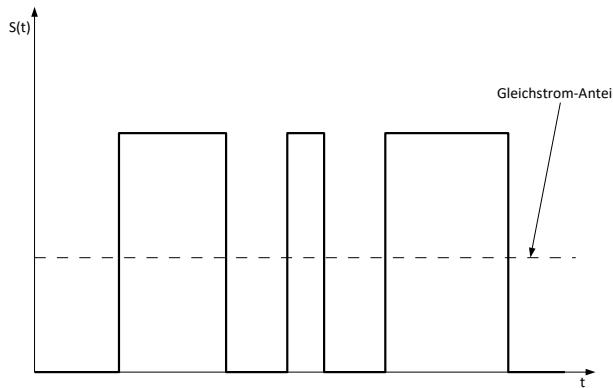


Abbildung 77: Gleichstrom-Anteil

Die Bandbreite von Telefonverbindungen beträgt 3100Hz (300Hz – 3400Hz). Leider kann auf einem solchen Kanal keine digitale Datenübertragung erfolgen, da digitale Signale einen Gleichstrom-Anteil beinhalten können. Dieser Gleichstrom-Anteil kann nicht ohne zusätzliche Maßnahmen übertragen werden.

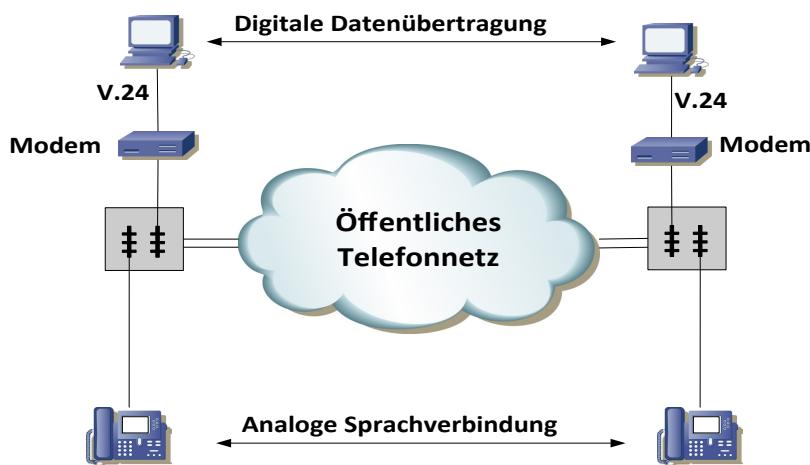


Abbildung 78: Übertragung über das öffentliche Telefonnetz

6.6.1 - Modem-Standards nach ITU-T

Modemtyp	Datenrate	Modulation / Übertragung	Netzwerk / Leitung	Hilfskanal
Betriebsart	in Bit / s			
V.21 asynchron synchron	bis 300	FSK Duplex	Telefon-Wählnetz 2-Draht	-
V.22 asynchron synchron	300 600 1200	2-, 4DPSK duplex	Telefon-Wählnetz / Mietleitung 2-Draht	-
V.22bis asynchron	2400	4-QAM duplex	Telefon-Wählnetz 2-Draht	75 Bit/s
V.23 asynchron synchron	600 1200	FSK halbduplex	Telefon-Leitung 2-Draht	75 bit/s
V.26 synchron	2400	4-DPSK halbduplex	Mietleitung 4-Draht	75 bit/s
V.26bis synchron	1200 2400	2-, 4-PSK halbduplex	Telefon-Wählnetz 2-Draht	75 Bit/s
V.27 synchron	4800	8-PSK duplex	Mietleitung 2-Draht (halbduplex) 4-Draht (vollduplex)	75 Bit/s
V.29 synchron	9600	4- / 16QAM duplex	Mietleitung 4-Draht	-
V.32 asynchron synchron	9600	4-QAM duplex	Telefon-Wählnetz 2-Draht Echokompensation	75 Bit/s
V.32bis	4800 9600 14400	128-QAM duplex	Telefon-Wählnetz 2-Draht	
V.34 asynchron synchron	28800	256-QAM 4-dim TCM duplex	Telefon-Wählnetz 2-Draht	-
V.34bis asynchron synchron	33600	256-QAM 4-dim TCM duplex	Telefon-Wählnetz 2-Draht Schnittstelle V.11	-
V.90 asynchron	56000 downstream 33600 upstream	PCM downstream 256-QAM 4-dim TCM upstream	Telefon-Wählnetz 2-Draht	-
V.92 asynchron	56000 downstream 48000 upstream	PCM downstream ? upstream	Telefon-Wählnetz 2-Draht	-

6.6.2 - 2-Draht und 4-Draht Verbindungen

Die meisten Verbindungen sind duplex Verbindungen. Dies bedeutet, dass zu einem beliebigen Zeitpunkt ein Datenaustausch in beiden Richtungen möglich ist.

Angenommen zwei Partner (A und B) wollen miteinander kommunizieren dann kann man für jede Richtung ein Leitungspaar verwenden.

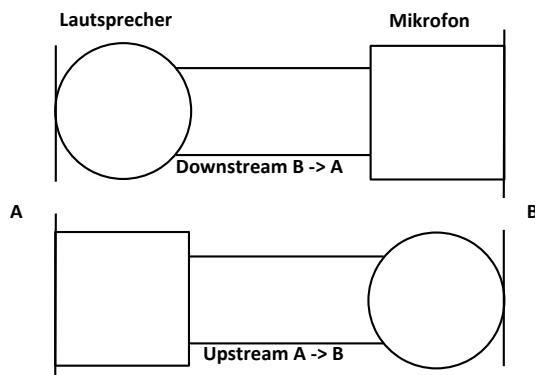
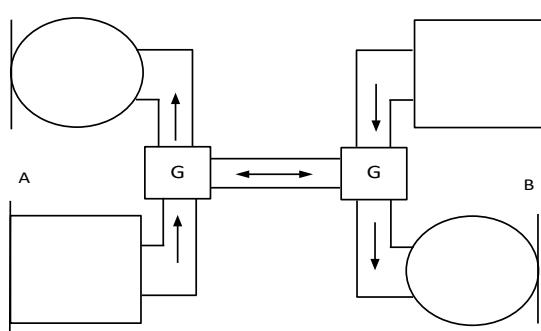


Abbildung 79: 4-Draht-Verbindung

Diese Verbindung benötigt 4 Drähte. Diese Verkabelung ist teuer. Allerdings ist eine Kommunikation in beiden Richtungen gleichzeitig möglich.

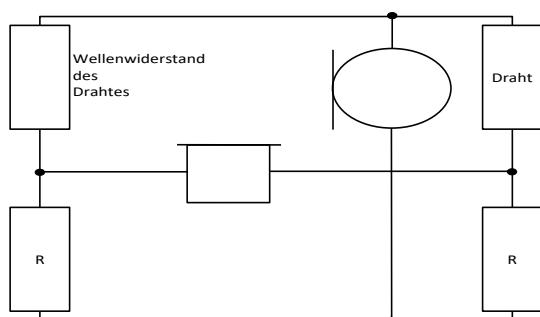
Die Telekommunikationsunternehmen haben diese aufwändigen Installationen schon immer gescheut und sind über technische Möglichkeiten auf eine Halbierung der notwendigen Drähte-Anzahl gekommen.

6.6.3 - Schaltungstechnisch



Mit einem Gabelschaltung kann die Auf trennung der 2-Draht-Verbindung in einen Mikrofonzweig und einen Lautsprecherzweig vorgenommen werden.

Abbildung 80: Gabelumschalter



Mit einer ideal abgeglichenen Brückenschaltung können beide Richtungen getrennt werden.

Wichtig ist hierbei auch, dass die eigene Stimme nur auf der gegenüberliegenden Seite und nicht auf dem eigenen Lautsprecher zu hören ist.

Abbildung 81: Brückenschaltung

6.7 - Digitale Übertragung im Basisband

6.7.1 - Synchrone Übertragung

Bisher wurde erkannt, dass jede Information digital übertragen werden kann. Im Folgenden sollen die hierbei entstehenden Probleme und deren Lösungen abgehandelt werden. Wo ist der Beginn eines Oktetts (8 Bits)? Wie kann das MSB (Most Significant Bit) gefunden werden?

6.7.2 - Taktimpuls

Zuerst ist der Takt zurück zu gewinnen. Bei z. B. 10Base T wird kein gesondertes Taktsignal übertragen. Es gibt nur einen unendlichen Strom von Pulsen ohne Beginn und ohne Ende.

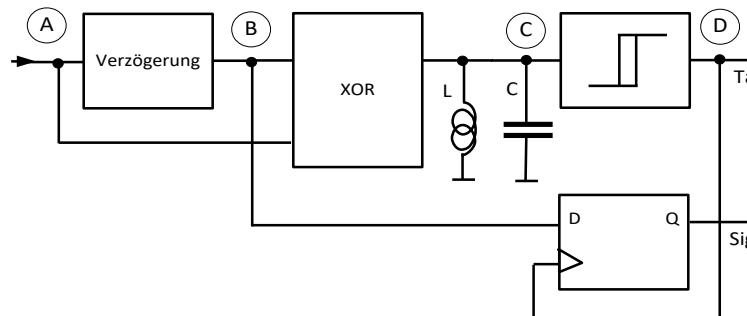


Abbildung 82: Takt-Rückgewinnung-1

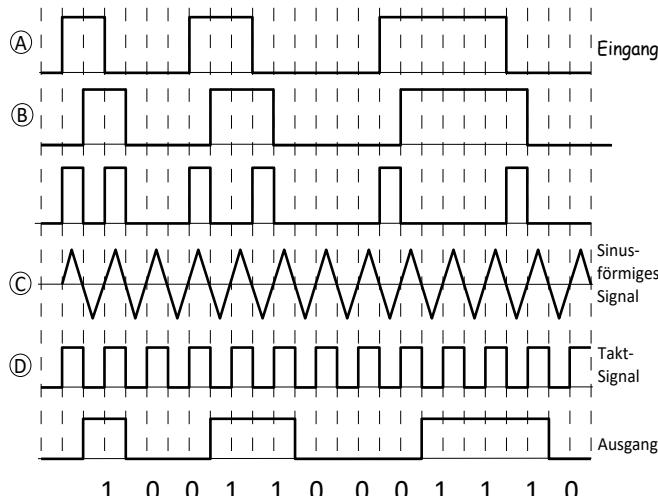


Abbildung 83: Takt-Rückgewinnung-2

Bei der hier gezeigten Takt-Rückgewinnung ist es eine Voraussetzung, dass keine langen Folgen von Nullen oder Einsen übertragen werden.

Deshalb gibt es Wirecodes die eine lange Folge mit gleichartigen Bits ausschließen.

6.7.3 - Scrambling und Descrambling

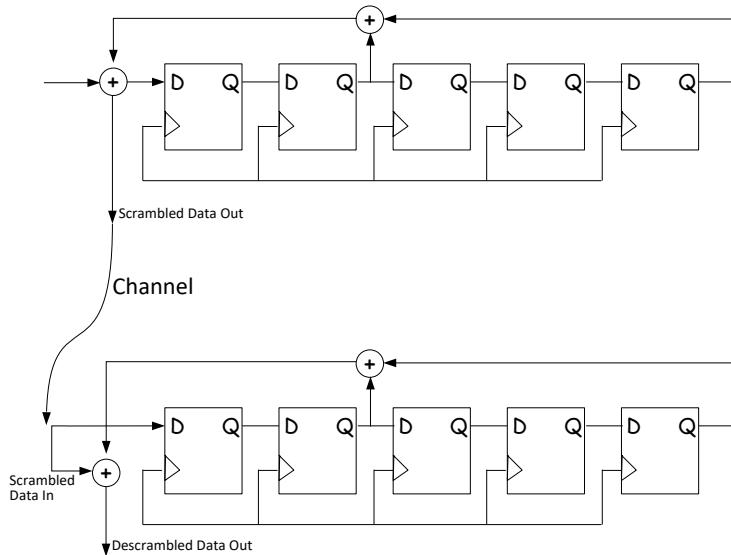


Abbildung 84: Scrambling - Descrambling

Im vorigen Kapitel wurde die Takt-Rückgewinnung erklärt und es ist klar geworden, dass eine lange Folge von Nullen oder Einsen die Takt-Rückgewinnung erschwert. Deshalb gibt es Mechanismen die sicher stellen, dass lange Folgen von Nullen oder Einsen unterbrochen werden. Mit dem Scrambling (deutsch: vermischen) wird sichergestellt, dass lange Folgen gleicher Bits nicht übertragen werden.

6.7.4 - Synchronisation

Ist am Ausgang erkannt wie der Bitstrom aus Einsen und Nullen aussieht, kann man sich daran machen den Anfang eines Rahmens (engl. Frames) zu suchen. Dazu werden die Daten im Eingangspuffer mit 8 Decodern, die jeweils um ein Bit versetzt zugreifen, gleichzeitig untersucht.

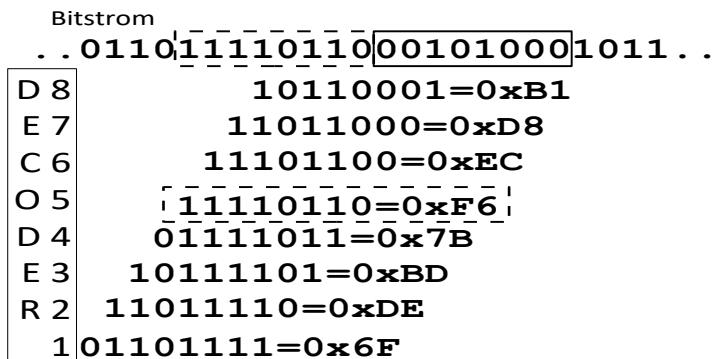


Abbildung 85: Rahmen-Ausrichtung

In der oberen Abbildung wird nach dem Bitmuster 1110110, 001010001 gesucht. Der Decoder 5 hat die Bitfolge gefunden.

Digitale Datenübertragung

Bei Ethernet in der Version 2 werden auf der Schicht 1 im ISO/OSI-RM 7 Bytes verwendet, um eine gesicherte Takt-Rückgewinnung zu erzeugen und die Rahmen-Ausrichtung zu vereinfachen.

Die Präambel-Bytes haben alle die Bitfolge 10101010. Das letzte Byte der Präambel der so genannte Start Frame Delimiter (SFD) (deutsch: Start-Rahmen-Begrenzer) hat die Bitfolge 10101011.

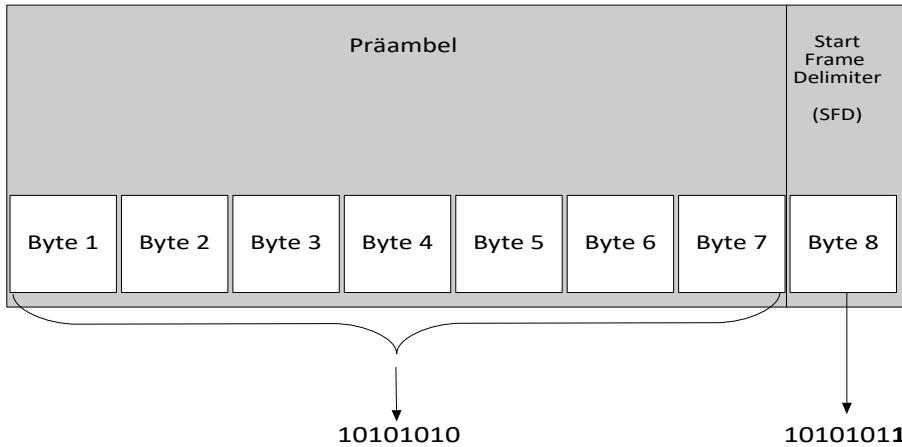


Abbildung 86: Präambel

Alle nach dem SFD folgenden Bytes gehören zum relevanten Teil des Rahmens.

6.8 - Asynchrone Datenübertragung

Wird für langsame Verbindungen, bei denen keine Takt-Rückgewinnung erforderlich ist, verwendet. Der Empfänger kennt die Taktrate und kann mit speziellen Start und Stopp-Bits die Grenzen jedes Wortes (Bytes) erkennen. Mit der Startbit-Erkennung wird der interne Zeittakt zurückgesetzt.

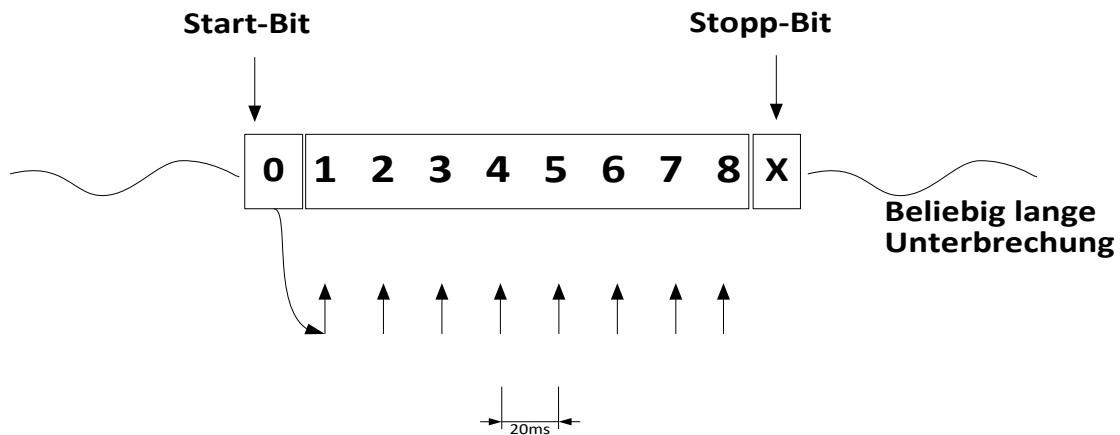


Abbildung 87: Asynchrone Datenübertragung

Asynchrone Datenübertragung wie bei der seriellen Schnittstelle V.24 / RS232 am PC. Für die Konfiguration einer seriellen Schnittstelle ist oft 8N1 angegeben, was 8Datenbits, keine Paritätsbits und 1 Stopp-Bit als Einstellung für die Schnittstelle beschreibt.

6.9 - Grundbegriffe

6.9.1 - Alphabet

Satz von definierten Symboltypen. Zahl 0-9 Buchstaben a-z, A-Z. Das italienische, deutsche oder englische Alphabet hat 26 Symbole. (A-Z) Das schwedische Alphabet hat 29 Symbole (A-Z, Å, Ä, Ö). Das Russische Alphabet hat 33 Symbole.

Die Ausgabe einer Informationsquelle kann als unendliche Reihe von Symbolen betrachtet werden. Jedes Zeichen (Symbol) hat eine bestimmte Wahrscheinlichkeit. In jeder Sprache ist die Wahrscheinlichkeit für das Auftreten eines Zeichen unterschiedlich.

Buchstabe	Häufigkeitsverteilung im deutschen Alphabet in %	Häufigkeitsverteilung im englischen Alphabet in %	Buchstabe	Häufigkeitsverteilung im deutschen Alphabet in %	Häufigkeitsverteilung im englischen Alphabet in %
a	6,51	8,2	n	9,78	6,7
b	1,89	1,5	o	2,51	7,5
c	3,06	2,8	p	0,79	1,9
d	5,08	4,3	q	0,02	0,1
e	17,4	12,7	r	7	6
f	1,66	2,2	s	7,27	6,3
g	3,01	2	t	6,15	9,1
h	4,76	6,1	u	4,35	2,8
i	7,55	7	v	0,67	1
j	0,27	0,2	w	1,89	2,4
k	1,21	0,8	x	0,03	0,2
l	3,44	4	y	0,04	2
m	2,53	2,4	z	1,13	0,1

6.9.2 - Anforderungen an eine Datenübertragung

Die wichtigsten Anforderungen an eine Datenübertragung sehen folgendermaßen aus:

Eigenschaft	Anforderung
Qualität	Wenige Fehler
Zuverlässigkeit	24h * 7 Tage * 52 Wochen
Geschwindigkeit	Möglichst schnell
Kapazität	Möglichst viel Daten gleichzeitig
Integrität, Sicherheit	Möglichst sicher vor Mitlesen, Verändern, Wiederholen, ..
Kosten	Die Kosten sind möglichst niedrig zu halten

Alle Anforderungen können nicht gleichzeitig erfüllt werden. Deshalb ist für unterschiedliche Anwendungen ein anderes Konzept (ein anderer Optimierungsschwerpunkt) zu wählen.

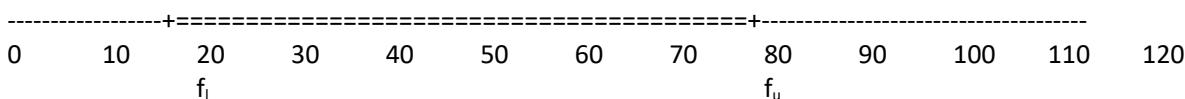
- Bilddaten -> Qualität hoch Kosten hoch
- Sprachdaten -> Kosten niedrig

6.9.3 - Bandbreite

Für die Bandbreite gibt es unterschiedliche Betrachtungsweisen, die den selben Namen verwenden. Aus funktechnischer Sicht ist die Bandbreite (engl. Bandwidth) eine Ausschnitt aus einem Frequenzband, in dem eine minimale Dämpfung auftritt.

Das Frequenzband wird durch eine untere Frequenz (lower -> f_l) und eine obere Frequenz (upper -> f_u) begrenzt.

Beispiel:



$$B = f_u - f_l = 80 \text{ kHz} - 20 \text{ kHz} = 60 \text{ kHz}$$

Aus IT-technischer Sicht ist die Bandbreite ein Synonym für die maximal mögliche Datenübertragungsrate eines Kanals.

6.9.4 - Baud-Rate

Anzahl der pro Sekunde durchgeführten Abtastungen in Symbols/s oder Msym/s.

6.9.5 - Bit

Abkürzung für „Binary Digit“. Klein geschrieben ist es eine Einheit wie m oder °C. Groß geschrieben wird immer ein bestimmtes Zeichen 0 oder 1 angewendet.

6.9.6 - Bit-Übertragungsrate

Die Bit-Übertragungsrate ist die über den Kanal gesendete Menge an Information und entspricht der Anzahl der Zeichen pro Sekunde mal der Anzahl der Bits pro Zeichen. Wird in Bits pro Sekunde (bps) angegeben.

6.9.7 - Byte

Gruppe von 8 Bit. Wird auch als Oktett bezeichnet.

6.9.8 - Code

Zuordnung zwischen Zeichen und Symbolen.

6.9.9 - Entscheidungsinhalt

Wenn n die Anzahl von Symbolen eines Alphabets beschreibt, ergibt $Id(n)$ den Entscheidungsinhalt. In Bit / Symbol.

$$H_0 = Id(n) = \frac{\log(n)}{\log(2)} \quad (18)$$

Beispiel: Unser Alphabet mit 26 Buchstaben hat einen Entscheidungsinhalt von
 $H_0 = Id(26) = 4,7004$ Bit/Symbol.

6.9.10 - Information

In der Informationstheorie bedeutet der Begriff Information, die von einem Sender zu einem Empfänger übermittelt wird, dass es sich dabei um etwas Neues / dem Empfänger bisher unbekanntes handelt.

6.9.11 - Informationsgehalt

Der Informationsgehalt , also der informative Wert eines Symbols x_i , ist umso größer, je seltener es auftritt. Somit hat eine Nachricht den Informationsgehalt = 0 wenn die Wahrscheinlichkeit des Eintretens = 1 ist. Die Wahrscheinlichkeit des Auftretens von diesem Symbol ist $P(x_i)$. Der Informationsgehalt (I_x) in bit/Symbol eines unabhängigen Symbols x_i ist:

$$I_x = Id\left(\frac{1}{P(x_i)}\right) \quad (19)$$

Beispiel aus unserem Alphabet unter der Annahme, dass alle Wahrscheinlichkeiten gleich verteilt sind.:

$$I_x = Id\left(\frac{1}{\frac{1}{26}}\right) = \frac{\log(26)}{\log(2)} = 4,7004 \text{ Bit / Symbol}$$

6.9.12 - Durchschnittlicher mittlerer Informationsgehalt (Entropie)

Der durchschnittliche Informationsgehalt wird in der Literatur oft auch Shannonsche mittlere Unsicherheit oder auch Entropie genannt. Die Entropie ist eine Ableitung aus dem zweiten Satz der Thermodynamik. Daraus lassen sich folgende Erkenntnisse ableiten:

- ➊ Wärmeenergie wandert immer von warm nach kalt.
- ➋ Es gibt keine periodisch arbeitende Maschine, die mechanische Arbeit allein durch Abkühlung eines Energiespeichers erzeugt.
- ➌ Alle Zustandsänderungen in einem abgeschlossenen System verlaufen so, dass die Entropie zunimmt.
 $\Delta S > 0$ bedeutet, dass alle Zustandsänderungen die Unordnung in einem abgeschlossenen System erhöhen.

Je größer die Ordnung eines Systems ist, desto geringer ist die Entropie. Um die Entropie zu verringern ist Energie erforderlich um z. B. Dinge zu sortieren und in eine „Ordnung“ zu bringen. Das Maximum der Entropie erhält man, wenn das Auftreten jedes Symbols die gleiche Wahrscheinlichkeit hat.

$$\overline{I}_x = H = \sum_{i=1}^n P(x_i) Id\left(\frac{1}{P(x_i)}\right) \quad (20)$$

Digitale Datenübertragung

Beispiel[HELÖ-NATE-2000]:

Eine Person X zieht aus einer Lostrommel Kugeln welche schwarz, weiß oder rot sein können und teilt die gezogene Farbe einer Person Y mit. Dabei erzeugt sie die Nachrichten „Schwarz“, „Weiß“ oder „Rot“. Der Empfänger kennt die Wahrscheinlichkeiten, mit denen die Farben in der Lostrommel auftreten.

- Wahrscheinlichkeit für das Auftreten von Weiß = $P_w = 70\%$
- Wahrscheinlichkeit für das Auftreten von Schwarz = $P_s = 20\%$
- Wahrscheinlichkeit für das Auftreten von Rot = $P_r = 10\%$

Es ist offensichtlich, dass die Nachricht Rot am seltensten auftritt. Damit hat sie den größten Informationsgehalt. Wären alle Kugeln weiß, wäre die Wahrscheinlichkeit P_w der Nachricht „Weiß“ = 1. Damit hätte die Nachricht „Weiß“ keinen Informationsgehalt. Damit lassen sich zwei Erkenntnisse festhalten:

- Der Informationsgehalt I_x einer Nachricht ist umso größer, je kleiner die Wahrscheinlichkeit ihres Auftretens also die Größe des „Überraschung“ ist.
- Eine Nachricht mit der Wahrscheinlichkeit $P_x = 1$ hat den Informationsgehalt $I_x = 0$

X	P_x	I_x	H
Weiß	$P_w = 0,7$	0,514 bit	1,156 bit
Schwarz	$P_s = 0,2$	2,321 bit	
Rot	$P_r = 0,1$	3,321 bit	

Im obigen Beispiel wird die Entropie $H = 1,156$ bit/Symbol

$$H = 0,7 * \text{Id}(1/0,7) + 0,2 * \text{Id}(1/0,2) + 0,1 * \text{Id}(1/0,1)$$

$$H = 0,7 * 0,514 + 0,2 * 2,321 + 0,1 * 3,321$$

$$H = 0,36 + 0,464 + 0,3321 = 1,156$$

Der Maximalwert der Entropie ergibt sich immer für die Gleichverteilung aller Symbole. $P_w = P_s = P_r = 1/3$. Er wird **Entscheidungsgehalt** H_0 genannt und wir mit dem Wert $H_0 = 1,584$ bit/Symbol.

$$H = 3 * (0,333 * \text{Id}(1/0,333))$$

$$H = 3 * (0,333 * 1,586) = 1,584$$

6.9.13 - Redundanz und Relevanz (Zugehörigkeit)

Jede Abweichung von der Gleichverteilung der Wahrscheinlichkeiten der Symbole führt zu einer Verringerung des mittleren Informationsgehalts der Nachricht. Diese Verringerung der Entropie nennt man Redundanz (R).

$$R = H_0 - H \quad (21)$$

Im obigen Beispiel wird $R = H_0 - H = 1,584 - 1,156 = 0,42$ bit/Symbol

Manchmal wird in der Literatur noch die relative Redundanz (r) angegebenen.

$$r = \frac{H_0 - H}{H_0} \quad (22)$$

Die relative Redundanz ergibt sich zu $r = (H_0 - H) / H_0 = (1,584 - 1,156) / 1,156 = 0,27$

Eine Nachricht kann mit 2 Parametern beschrieben werden:

- Redundanz (Mehrfaches Auftreten der Information)
- Relevanz (Wichtiger Teil der Information)

Weiteres Beispiel[HELÖ-NATE-2000]I:

Die Bandbreite von 3100 Hz ist relevant für die Übertragung der menschlichen Sprache. Mit Rücksicht auf statistische Abhängigkeiten der Zeichen / Buchstaben in der menschlichen Sprache verringert sich die Entropie auf etwa 1 bit / Symbol.

Mit dem deutschen Alphabet und den obigen Werten ergibt sich für die Redundanz:

$$R = 4,7 - 1 = 3,7 \text{ Bit /Symbol}$$

Daraus folgt:

78,7 % der Sprache sind redundant.

6.9.14 - Nachrichten-Ebene

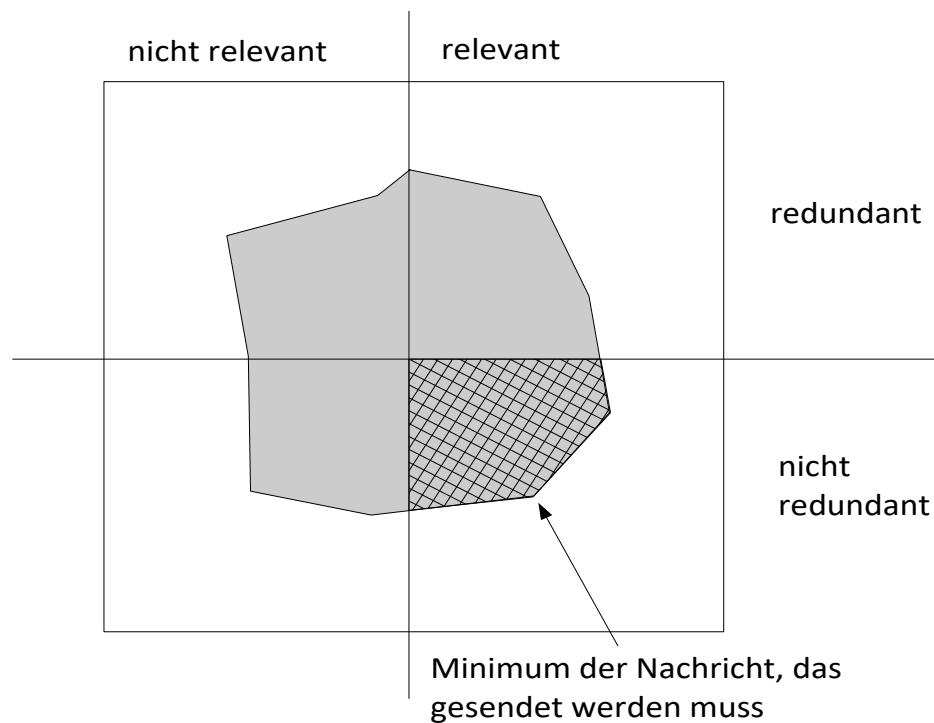


Abbildung 88: Nachrichten-Ebene

Der Teil einer Nachricht welcher redundant ist, ist bereits bekannt oder die Nachricht enthält die Information doppelt.

Redundanz wird einer Nachricht hinzugefügt um Fehler zu erkennen und zu beheben.

6.9.15 - Informationsquelle

Teil eines Systems, das Nachrichten erzeugt. Eine Quelle hat ein Alphabet, welches eine endliche Anzahl von Symbolen hat.

6.9.16 - Kanal

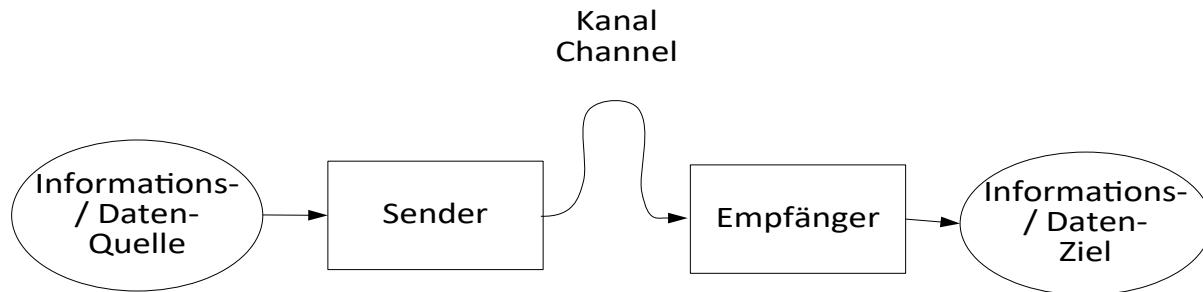


Abbildung 89: Kanal

Die von einer Datenquelle erzeugten Informationen werden über einen Kanal von einem Sender zu einem Empfänger übertragen, der die Informationen an das Datenziel, die so genannte Datensenke, übergibt.

6.9.17 - Nachricht

(engl. Message)

Eine Nachricht ist ein Satz von Zeichen oder Stati, die für die Datenübertragung genutzt werden können.

6.9.18 - Schritt

Ein Schritt ist die kleinste systemtechnisch realisierbare Zeiteinheit, in der eine gewisse Anzahl von Bits übertragen werden.

6.9.19 - Schrittgeschwindigkeit

Anzahl der Schritte pro Zeiteinheit. Die Einheit ist Baud. Nur wenn genau ein bit pro Schritt übertragen wird, gilt:
 $1 \text{ baud} = 1 \text{ bit/s}$

Werden bei einer Abtastung 2 Bits abgetastet gilt:

$1 \text{ baud} = 2 \text{ bit/s}$

Die Anzahl der Bits pro Sekunde auf dem Kanal wird durch das Modulationsverfahren festgelegt.

6.9.20 - Signal

Ein Signal (lat. signalis) ist dazu bestimmt ein Zeichen (lat. signum) zu geben. Besitzt ein Signal eine Bedeutung kann es zur Übertragung einer Nachricht genutzt werden. Wird ein Signal zur Auswertung von Information genutzt, wird es Nutzsignal genannt. Behindert ein Signal die Informationsübertragung wird es Störsignal genannt.

6.9.21 - Symbol

Ein Symbol ist ein Element um einen Teil einer Meldung zu transportieren. Ein Symbol ist notwendigerweise mindestens ein Bit. Es kann auch aus mehreren Bits bestehen. So können z. B. 4 Symbole (00, 01, 10, 11) 4 verschiedene Phasen beschreiben.

6.9.22 - Zeichen

(engl. Character)

Ein Zeichen ist ein Signal mit einer festgelegten Bedeutung. Jede Abtastung sendet eine Information also ein Zeichen. Das Zeichen besteht also aus mindestens einem Bit. Werden bei einer Abtastung mehrere Bits abgetastet, dann enthält ein Zeichen genau die Anzahl an Bits die bei einer Abtastung entstehen.

6.10 - Codierung

Mit Codierung wird der Übergang einer Signaldarstellung in eine andere Signaldarstellung bezeichnet.

- ➊ Beim Source-Coding werden Codes erzeugt die möglichst wenige Daten erzeugen, die über die Leitung zu transportieren sind.
- ➋ Beim Channel-Coding werden Fehler-Erkennungs und -Behebungsmethoden implementiert. Dazu sind wiederum redundante Informationen in den Datenstrom einzufügen.
- ➌ Beim Wire-Coding wird ein optimaler Code ausgewählt um eine möglichst störungsfreie Datenübertragung auf der Leitung zu gewährleisten.

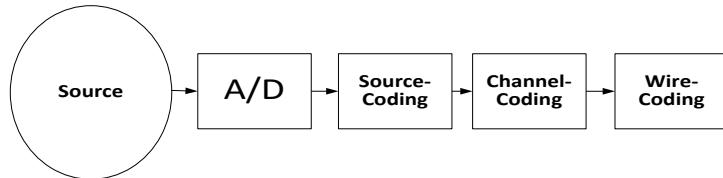


Abbildung 90: Kodierungsarten

6.10.1 - Source-Coding

6.10.1.1 - Einleitung

Dient zur Reduzierung der zu transportierenden Datenmenge. Eine Reduzierung von Speicherplatz ist eng verbunden mit weniger zu übertragenden Daten. Schließlich ist Source-Codierung eine Kostenfrage. Andererseits ist die Codierung ein komplexes, aufwändiges Verfahren, was einen erheblichen technischen Aufwand bedeutet.

Beispiel:

Eine Datenquelle kennt 4 Symbole (A, B, C und D)

Die Wahrscheinlichkeit des Auftretens der Symbole ist:

$$P(A) = 0,5$$

$$P(B) = 0,25$$

$$P(C) = 0,125$$

$$P(D) = 0,125$$

Aus der Formel (20) ergibt sich die Entropie $H = 1,75$ bit/Symbol

$$H = 0,5 * \text{Id}(1/0,5) + 0,25 * \text{Id}(1/0,25) + 0,125 * \text{Id}(1/0,125) + 0,125 * \text{Id}(1/0,125)$$

$$H = 0,5 * 1 + 0,25 * 2 + 0,125 * 3 + 0,125 * 3 = 1,75$$

Eine zu übertragende Nachricht sieht folgendermaßen aus:

```

..0      1      2
..123456789012345678901234..
..AACACABABBABADAACBDAABD..
  
```

Eine zuerst vorgenommene Codierung könnte so aussehen:

$$A = 00$$

$$B = 01$$

$$C = 10$$

$$D = 11$$

Die obige Nachricht mit 24 Symbolen ergibt einen Informationsinhalt von $24 * 1,75 = 42$ Bits. Mit dem obigen Code erhält man jedoch $2 * 24 = 48$ Bits. Dies bedeutet, dass 6 Bits redundant sind.

Digitale Datenübertragung

Ein besseres Ergebnis bringt eine weitere Codierung:

$$\begin{aligned} A &= 1 \\ B &= 01 \\ C &= 001 \\ D &= 000 \end{aligned}$$

Damit werden 42 Bits benötigt. Dies entspricht dem Informationsgehalt. Damit ist die Redundanz eliminiert.

Fano Bedingung:

Wenn kein Codewort existiert, das der Anfang eines anderen Codewortes ist, dann ist jeder Satz von Codewörtern korrekt.

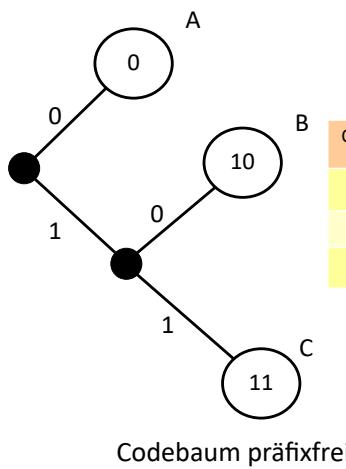
Beweisen kann man das mit der **Kraft-Millan-Ungleichung**.

Ein D-närer Präfixfreier Code mit den Codewortlängen ($w_1, w_2, w_3, \dots, w_L$) existiert genau dann, wenn gilt:

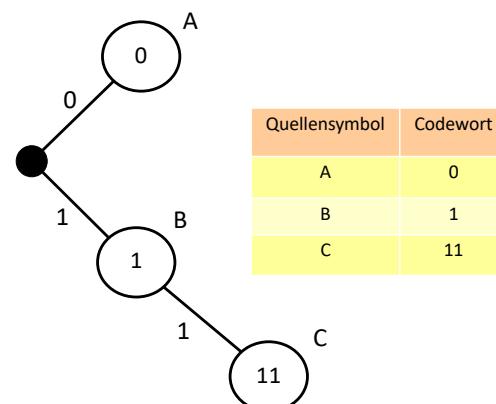
$$\sum_{i=1}^L D^{-w_i} \leq 1 \quad (23)$$

Beispiel:

Gegeben sei ein Code mit 3 Codewörtern mit variabler Länge. Beim Präfixfreien Codewort links, entsprechen alle Codewörter einem Endknoten. Beim nicht Präfixfreien Codewort rechts, kann man sehen, dass nicht alle Codewörter einem Endknoten entsprechen.



Quellsymbol	Codewort
A	0
B	10
C	11



Quellsymbol	Codewort
A	0
B	1
C	11

Abbildung 91: Codebaum einer präfixfreien und einer nicht präfixfreien Codierung

Wird auf die Codes die Kraft-Millan-Ungleichung angewandt, kann man sehen, dass im Fall des präfixfreien Codes mit den Längen für A=1, B=2 und C=2 :

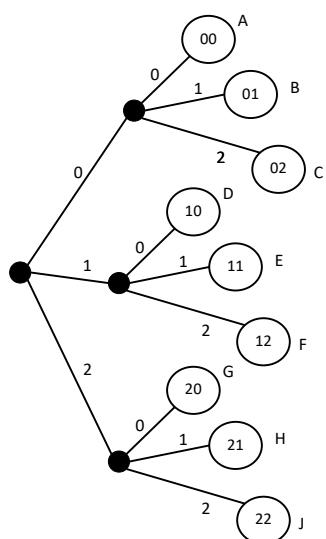
$$2^{-1} + 2^{-2} + 2^{-2} = 0,5 + 0,25 + 0,25 = 1 \leq 1$$

erfüllt ist.

Im Fall des nicht präfixfreien Codes mit den Längen für A=1, B=1 und C=2

$$2^{-1} + 2^{-1} + 2^{-2} = 0,5 + 0,5 + 0,25 = 1,25 \leq 1$$

nicht erfüllt ist.



Quellensymbol	Codewort
A	00
B	01
C	02
D	10
E	11
F	12
G	20
H	21
J	22

Es ist auch vorstellbar, dass es nicht nur Codes mit einer binären Codierung gibt. Im folgenden Beispiel ist ein ternärer Code realisiert.

Es ist leicht zu erkennen, dass dieser Code präfixfrei ist.

Auch hier ist die Kraft-Millan-Ungleichung erfüllt.

$$9 * 3^2 = 9 * 0,1111.. = 1 \leq 1$$

Wie schon oben zu sehen war, ergibt sich bei einem präfixfreien Code der Wert = 1 wenn der Codebaum vollständig genutzt ist.

Hinweis:

Wenn alle Symbole die gleiche Häufigkeit haben, ist keine Reduzierung der Redundanz möglich.

In einem deutschen oder englischen Text ist der Buchstabe „e“ häufiger als der Buchstabe „q“. Damit sollte der Buchstabe „e“ einen kürzeren Code als der Buchstabe „q“ haben. Dieses Prinzip hat im Morse-Code dazu geführt, dass der Buchstabe „e“ mit einem Punkt „.“ und der Buchstabe „q“ mit „---.“ codiert wird.

Symbol	Code	Symbol	Code	Symbol	Code	Symbol	Code
a	-.	w	--		-..	8	----
b	-...	x	-..-	m	--	9	----
c	-.-.	y	-.--	n	-.	0	-----
d	-..	z	--..	o	---	Punkt	.-.-.
e	.	1	----	p	.--.	Komma	--..--
f	..-	2	...--	q	--.-	Fragezeichen	..--..
g	--.	3-	r	-.	Doppelpunkt	-----
h	4	s	...	Semikolon	-.-.-
i	..	5	t	-	Trennung	-...-
j	---	6	-....	u	..-	Bruchstrich	-..-
k	-.-	7	-----	v	...-	Anführungszeichen	.-.-.

6.10.1.2 - Huffmann-Codierung

Der Huffmann-Code erfüllt die Fano-Bedingung und wird bei Kodierungsalgorithmen wie JPEG verwendet.

Um einen Text zu codieren sind folgende Schritte zu durchlaufen:

1.

Die Symbole einer gegebenen Quelle (z. B. ASCII-Text) werden nach der Häufigkeit ihres Auftretens in einer Tabelle angeordnet.

2.

Die Symbole mit der niedrigsten Häufigkeit werden mit 0 und 1 codiert und in der Tabelle gekennzeichnet.

3.

Die beiden Symbole werden zu einem neuen Symbol zusammengefasst und die Wahrscheinlichkeit ihres Auftretens wird addiert. Da die beiden Symbole zusammengefasst wurden, ist die Tabelle um eine Zeile kürzer. Die Wahrscheinlichkeiten werden in der Tabelle berücksichtigt indem sie addiert werden. Die Schritte 2 und 3 werden so lange wiederholt, bis nur noch eine Zeile übrig ist.

4.

Man nimmt die letzte Tabelle und geht die Tabellen rückwärts bis zur ersten Tabelle durch und druckt den Code-Baum aus. Mit jeder Tabelle bekommt man eine Code-Entscheidung und zwei Zweige des Code Baumes. Man liest jetzt den Code-Baum vom Start bis zu jedem Knoten und erhält den Code für jedes Symbol.

6.10.1.3 - Beispiel für eine Huffmann-Codierung in Tabellenbearbeitung

Es gibt 10 Symbole (x_1, x_2, \dots, x_{10}) mit den folgenden Wahrscheinlichkeiten (P) ihres Auftretens

Symbol :

x_1	0,25
x_2	0,15
x_3	0,2
x_4	0,2
x_5	0,05
x_6	0,07
x_7	0,025
x_8	0,02
x_9	0,025
x_{10}	0,01

Im ersten Schritt sind die Symbole und ihre Wahrscheinlichkeit in eine Tabelle ein zu sortieren.

Pos	Tabelle 1	Tabelle 2	Tabelle 3	Tabelle 4	Tabelle 5
1	X1 = 0,25	X1 = 0,25	X1 = 0,25	X1 = 0,25	X1 = 0,25
2	X3 = 0,2	X3 = 0,2	X3 = 0,2	X3 = 0,2	X3 = 0,2
3	X4 = 0,2	X4 = 0,2	X4 = 0,2	X4 = 0,2	X4 = 0,2
4	X2 = 0,15	X2 = 0,15	X2 = 0,15	X2 = 0,15	X2 = 0,15
5	X6 = 0,07	X6 = 0,07	X6 = 0,07	X7X9X8X10 = 0,08	X6X5 = 0,12 -> 0
6	X5 = 0,05	X5 = 0,05	X5 = 0,05	X6 = 0,07 -> 0	X7X9X8X10 = 0,08 → 1
7	X7 = 0,025	X8X10 = 0,03	X7X9 = 0,05 -> 0	X5 = 0,05 → 1	
8	X9 = 0,025	X7 = 0,025 -> 0	X8X10 = 0,03 -> 1		
9	X8 = 0,02 -> 0	X9 = 0,025 → 1			
10	X10 = 0,01 → 1				

In der Tabelle 1 werden im nächsten Schritt die Positionen 9 (X8) und 10 (X10) mit 0 und 1 codiert. Die Wahrscheinlichkeiten werden addiert ($0,01 + 0,02 = 0,03$). Das neu entstandene Element x8X10 wird aufgrund seiner neuen Wahrscheinlichkeit an der Position 7 in der Tabelle 2 einsortiert. x7 und x9 sind um eine Position nach unten gerutscht.

In der Tabelle 2 wird, wie in Tabelle 1, die beiden letzten Positionen mit 0 und 1 codiert sowie die Wahrscheinlichkeiten addiert. Das Ergebnis (X7X9) wird wiederum aufgrund seiner Wahrscheinlichkeit auf die Position 7 in der Tabelle 3 einsortiert.

Pos	Tabelle 6	Tabelle 7	Tabelle 8	Tabelle 9
1	X1 = 0,25	X6X5X7X9X8X10X2 = 0,35	X3X4 = 0,4	X6X5X7X9X8X10X2X1 = 0,6 -> 0
2	X3 = 0,2	X1 = 0,25	X6X5X7X9X8X10X2 = 0,35 -> 0	X3X4 = 0,4 → 1
3	X4 = 0,2	X3 = 0,2 -> 0	X1 = 0,25 -> 1	
4	X6X5X7X9X8X10 = 0,2 -> 0	X4 = 0,2 -> 1		
5	X2 = 0,15 → 1			

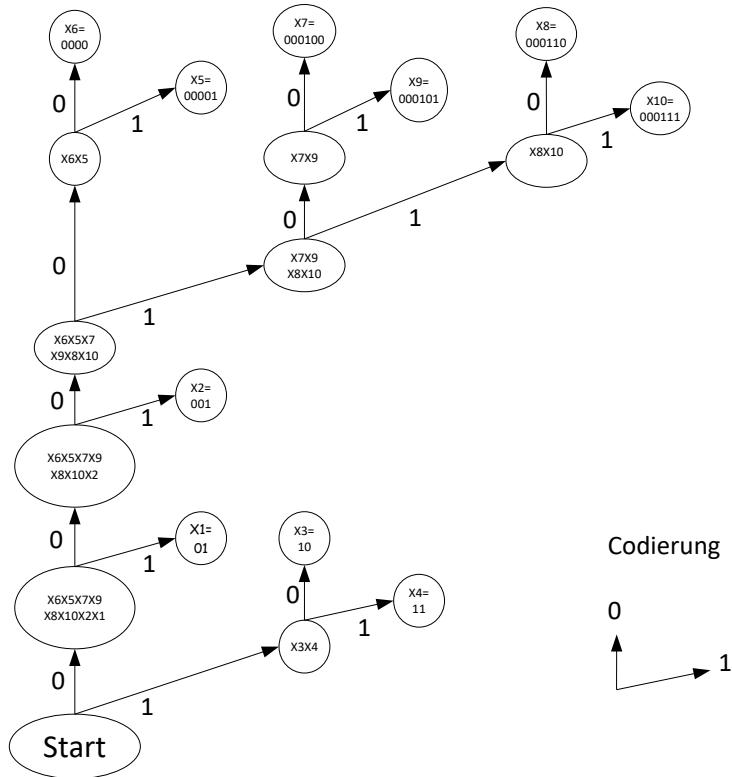


Abbildung 92: Huffmann-Codierung

Jetzt lässt sich der Code-Baum erstellen. Bei jeder 0 wird der Stamm verlängert. Bei jeder 1 wird ein Ast angehängt.

Für jedes Zeichen kann nun der Code ermittelt werden indem vom Start aus die Einsen und Nullen aneinander gehängt werden.

So hat z. B. X2 den Code 001 und x10 den Code 000111.

6.10.1.4 - Beispiel für eine Huffmann-Codierung in graphischer Bearbeitung

Anhand eines Textbeispiels und einer graphischen Lösung soll hier nochmals die Huffman-Codierung gezeigt werden. Der Text lautet „DIGITAL COMMUNICATION“. Dabei ist folgendes zu beachten. Der Text ist genau 21 Buchstaben lang, denn das Blanc in der Mitte ist mit zu zählen!

123456789012345678901

DIGITAL COMMUNICATION

Nun wird für jeden Buchstaben die Anzahl des Auftretens ermittelt und neben die Buchstaben an der linken Seite eines Blattes geschrieben. Zur Überprüfung muss die Summe aller Anzahlen den Wert 21 ergeben.

Nun werden die Buchstaben nochmals unten auf das Blatt geschrieben. Dabei werden die Buchstaben nach der Anzahl ihres Auftretens sortiert.

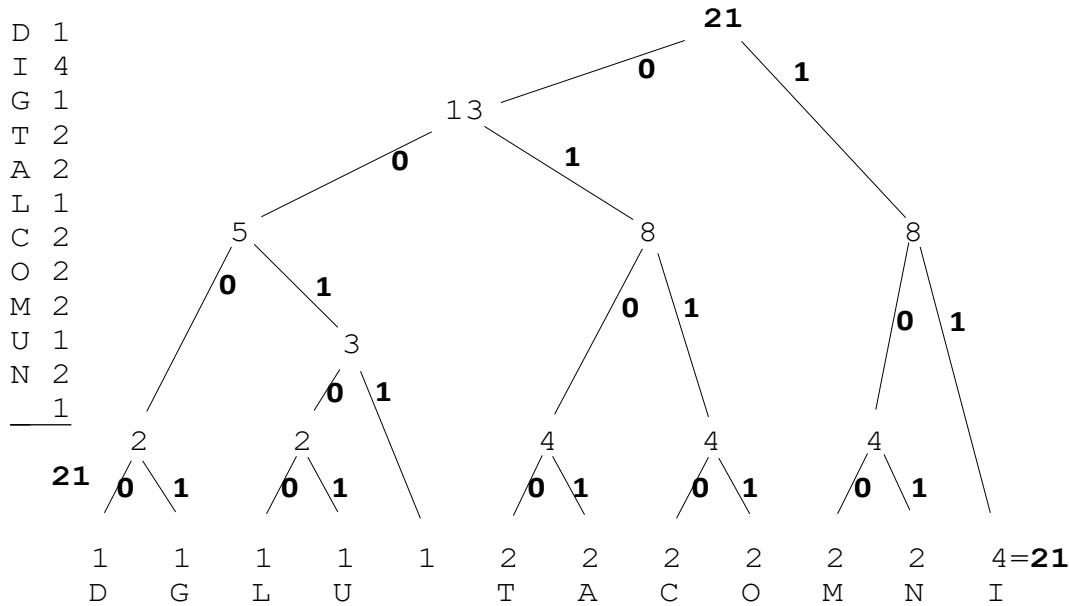


Abbildung 93: Huffmann-Codierung (Graphisch)

Geht man davon aus, dass die 12 unterschiedlichen Buchstaben mit einem Code übertragen werden, der für jeden Buchstaben gleich lang ist, dann wäre für jeden Buchstaben 4 Bits zu codieren. Dies würde zu einer codierten Länge von 84 Bits führen.

Über die Buchstaben werden die Anzahlen des Auftretens im Text geschrieben. Nun werden die jeweils kleinsten Zahlen addiert. Sie bilden die Äste die aus einem neuen Knoten nach unten erwachsen. Die Summe wird in dem neuen Knoten platziert. Dies wird so lange fortgesetzt bis nur noch eine Zahl übrig bleibt. Wenn alles richtig gelaufen ist kommt (natürlich) wieder die Zahl 21 heraus.

Am Ende werden die Äste nach Links mit einer 0 beschriftet und die Äste nach Rechts mit einer 1.

Jetzt kann für jeden Buchstaben der Code abgelesen werden. Dabei geht man von oben den Baum entlang bis zum entsprechenden Buchstaben nach unten. Z. B. D=0000, U=00101.

Der komplette codierte Text sieht dann folgendermaßen aus:

```
D | I | G | I | T | A | L | _ | C | O | M | M | U | N | I | C | A | T | I | O | N |
0000|11|0001|11|0100|0101|00100|0011|0110|0111|100|100|00101|101|11|0110|0101|0100|11|0111|101|
```

Wer sich die Mühe macht und die Bits nachzählt kommt auf den Wert 74. Dies ist eine Reduzierung der zu übertragenden Information um 10 Bits.

Bei der Übertragung von Daten mit Huffmann-Codierung ist normalerweise die Code-Tabelle mit zu übertragen. Damit auf beiden Seiten gleich codiert wird.

Die Kompressionsrate ist stark von der Wahrscheinlichkeitsverteilung der zu codierenden Symbole abhangig. Wird bei der Ubertragung nur ein Bit verfalscht, ist der gesamte folgende Text nicht mehr decodierbar!

6.10.2 - Channel-Coding

Im letzten Kapitel wurden Redundanzen so weit als möglich reduziert. Damit wurde die zu übertragenden Datenmenge auf ein Minimum reduziert. Leider haben diese Maßnahmen jedoch dazu geführt, dass Fehler in der Übertragungsstrecke unter Umständen den gesamten restlichen Datenaustausch zerstören. Fehler können bei der Übertragung immer auftreten. Rauschen oder sonstige Störungen können nie ganz ausgeschlossen werden. Der Empfänger ist dann nicht mehr in der Lage aus dem empfangenen Signal das gesendete Symbol korrekt zu decodieren. Fehler können als einzelne Bit-Fehler (Bit-Error) auftreten oder in Gruppen angehäuft (Burst-Error) auftreten.

Mit Channel-Coding-Algorithmen wird die zu übertragende Information gegen mögliche Fehlereinflüsse geschützt.

Grundsätzlich kann man den Fehlern mit zwei unterschiedlichen Strategien begegnen:

- Fehlererkennung und Wiederholung der Datenübertragung. (automatic repeat)
- Fehlerkorrektur (FEC = Forward Error Correction)

6.10.2.1 - Fehlererkennung

Bei der Fehlererkennung wird zusätzliche also redundante Information in die Datenübertragung integriert. Die eigentliche Fehlerbehebung wird durch das Anfordern einer Wiederholung der Datenübertragung angestoßen.

6.10.2.1.1 - Fehlererkennung durch Paritätsbits

Die Parität einer Bitkette (Wort) der Länge n ist die Anzahl der Einsen in diesem Wort.

Ein Code, dessen Worte alle eine gerade Anzahl von Einsen aufweist, besitzt eine gerade Parität. Bei einer ungeraden Parität ist die Anzahl immer ungerade.

Aus einem Code mit Wörtern der Länge $n-1$ entsteht durch Anhängen eines Paritätsbits ein Code mit gerader bzw. ungerader Parität.

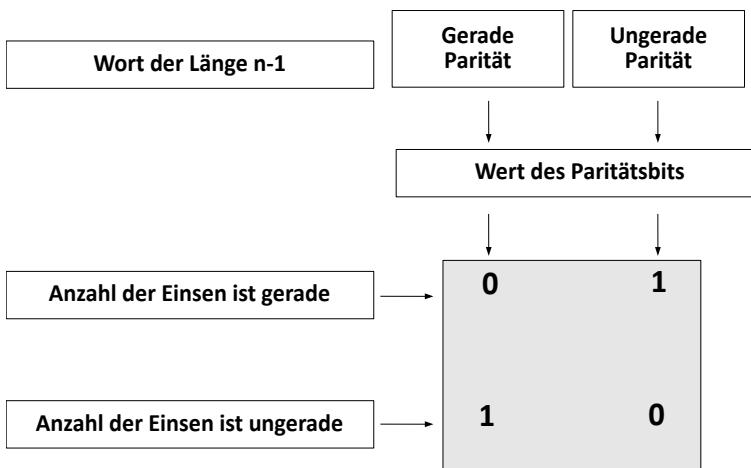


Abbildung 94: Ermittlung des Paritätsbits

In der folgenden Tabelle ist zu erkennen wie das Anhängen des Paritätsbits für gerade und ungerade Paritätsbits durchgeführt wird:

- Bei geraden Parität ist so aufzufüllen, dass immer eine gerade Anzahl von Einsen entsteht.
- Bei der ungeraden Parität ist so aufzufüllen, dass immer eine ungerade Anzahl von Einsen entsteht.

Code ohne Parität		Code mit Parität	
Hexadezimal-Darstellung	Binär-Darstellung	Gerade Parität	Ungerade Parität
0	0000	00000	00001
1	0001	00011	00010
2	0010	00101	00100
3	0011	00110	00111
4	0100	01001	01000
5	0101	01010	01011
6	0110	01100	01101
7	0111	01111	01110
8	1000	10001	10000
9	1001	10010	10011
A	1010	10100	10101
B	1011	10111	10110
C	1100	11000	11001
D	1101	11011	11010
E	1110	11101	11100
F	1111	11110	11111

6.10.2.1.2 - Hamming-Distanz

Die Distanz zweier Codewörter ist die Anzahl der Bits in denen sich die beiden Codewörter unterscheiden.

So haben die Codewörter 0000 und 1111 die Distanz 4. Die Codewörter 0000 und 0001 haben die Distanz 1.

Die Hamming-Distanz ist der minimale Abstand aller möglichen Codewörter eines Codes.

Allgemein gilt:

Die Fehlererkennungs- und -korrektureigenschaften eines Codes hängen von seinem Hamming Abstand ab.

Zum Auffinden von d Fehlern benötigt man einen Hamming-Abstand von $d + 1$.

Zur Korrektur von d Fehlern braucht man einen Hamming-Abstand von $2d + 1$.

Digitale Datenübertragung

Die Benutzung einer Untermenge der Codeworte ist die grundlegende Idee der Kanal-Codierung
das Auftreten eines Bitfehlers führt dazu, dass ein gültiges Codewort in ein ungültiges Codewort geändert wird.

Beispiel:

Wird ein 2 Bit-Binärcode um ein Prüfbit erweitert, entsteht folgende Zuordnung:

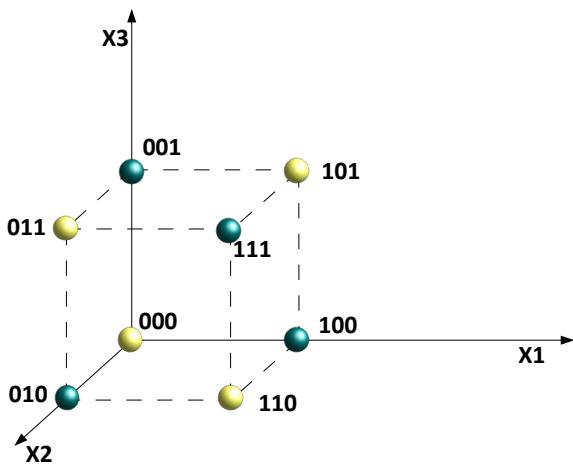
2 Bit-Binärcode + Parity-Bit -> 3 Bit-Binärcode

00	0	000	\	
01	1	011		gültige Codes
10	1	101		
11	0	110	/	

001	\	
010		ungültige Codes
100		
111	/	

Wird ein gültiger Code wie z. B. 000 übertragen kann durch einen Bitfehler 001 auf der Empfängerseite ankommen.
001 ist ein ungültiger Code. Somit ist erkannt, dass ein Fehler bei der Datenübertragung aufgetreten ist. Leider kann jetzt nicht auch noch die Fehlerkorrektur stattfinden. Denn aus dem Code 001 könnte 000 oder 011 oder 101 als gültiger Code möglich sein. In diesem Beispiel ist also nur eine Fehlererkennung möglich. Für eine evtl. gewünschte Fehlerkorrektur müssten weitere Bits eingefügt werden.

Man kann jedes Codewort an eine Ecke eines Würfels legen. Bei 3 Bit lässt sich jedes Codewort als Punkt in einem 3dimensionalen Raum interpretieren.



Auf der linken Seite (1.) werden alle Codeworte einem Wert mit 3 Bits zugewiesen. Damit sind 8 Codeworte möglich.

Reduziert man die Anzahl der gültigen Codeworte auf die Hälfte (4 gültige Codeworte) hat jedes Codewort einen ungültigen Codewort als Nachbar. Auf jeder Fläche des Würfels hat ein gültiges Codewort den nächsten gültigen Nachbarn auf der Flächen-Diagonalen der Seite. Hier lassen sich Fehler nur erkennen. Eine Fehlerkorrektur ist nicht möglich.

Abbildung 95: Code-Würfel

Bei einer weiteren Reduzierung auf 2 gültige Codeworte (3.) kann nicht nur ein Fehler erkannt sondern auch noch korrigiert werden. Hier liegen die gültigen Codeworte auf der Raum-Diagonalen.

6.10.2.2 - Zweidimensionale Parität

Die Paritätsbits können auf einzelne Codewörter oder auf Blöcke von Codewörtern angewendet werden. Allerdings ist bei der Verwendung von Paritätsbits die Wahrscheinlichkeit, dass Bitfehler unerkannt bleiben zu hoch. Deshalb wird die Paritätsprüfung dann mehrfach oder zweidimensional angewendet. Dazu werden die zu schützenden Codewörter in einer Matrix angeordnet. In jeder Zeile der Matrix wird ein Paritätsbit (Querparitätsbits) angehängt. Danach wird unter jeden Block noch eine Zeile mit Längsparitätsbits angehängt. Hier wird für jede Spalte das Paritätsbit erzeugt.

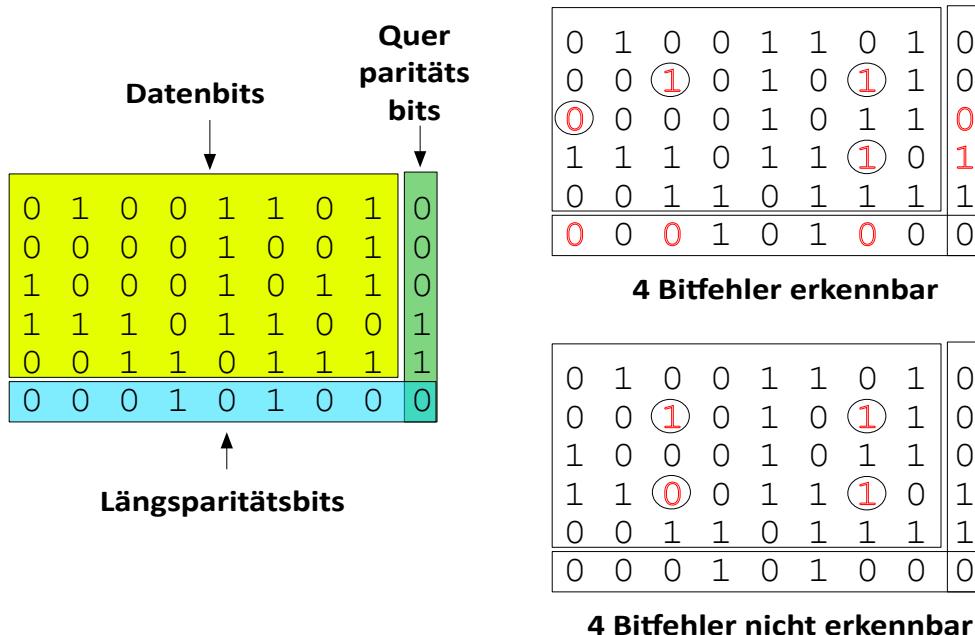


Abbildung 96: Fehlererkennung mit Paritätsbits bei zweidimensionaler Parität

Mit dieser zweidimensionalen Parität können alle 2- und 3-Bit-Fehler erkannt werden. Bei den 4-Bit Fehlern sind nicht alle Bitfehler erkennbar. Dies ist dann der Fall, wenn sich die Fehler sowohl in den Zeilen als auch in den Spalten gegenseitig ausgleichen. Dann kann durch ein Paritätsbit nicht mehr erkannt werden, dass sich, in den zu überwachenden Daten, ein Doppelfehler eingeschlichen hat.

6.10.2.3 - Echo

Bei dieser Methode werden die empfangenen Daten zum Sender wieder zurückgesandt. Dort werden sie analysiert und auf Fehler hin untersucht. Im Fehlerfall werden die Daten nochmals gesendet. Diese Vorgehensweise wird in Terminals eingesetzt.

6.10.2.4 - CRC (Cyclic Redundancy Check)

Diese Vorgehensweise ist etwas komplizierter, wird aber häufig angewendet.

Es werden so genannte zyklische Blockcodes verwendet. Ein systematischer Blockcode (Nutz- und Prüfbits sind in zwei Blöcken angeordnet) wird als zyklisch bezeichnet, wenn die zyklische Vertauschung der Bits eines Codewortes wieder ein gültiges Codewort ergibt. Die zyklischen Codes lassen sich auf einfache Weise mit rückgekoppelten Schieberegistern erzeugen und prüfen.

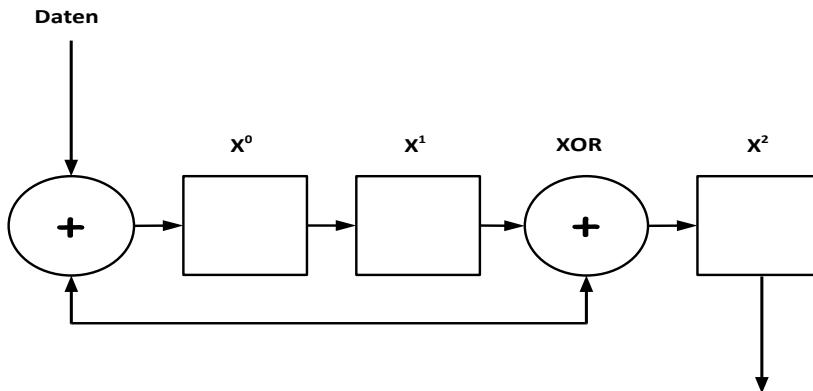


Abbildung 97: CRC-Berechnung

Die redundante Information wird als Block-Prüffolge (FCS, Frame Check Sequence) berechnet und an die Nutzdaten angehängt. Dazu werden die Bits der Nutzinformation als Koeffizienten eines Polynoms aufgefasst. Dieses Polynom wird durch ein festgelegtes Generatorpolynom dividiert. Der Rest bildet die Blockprüfsumme. Sender und Empfänger berechnen die Prüfsumme auf die gleiche Weise. Stellt der Empfänger zwischen seiner berechneten Prüfsumme und der angehängten Prüfsumme einen Unterschied fest weiß er, dass die Übertragung fehlerhaft war.

Ablauf:

Die n Nutzdaten-Bits werden folgendermaßen interpretiert.

$$U(x) = u_{n-1}x^{n-1} + u_{n-2}x^{n-2} + \dots + u_1x + u_0$$

Das Generatorpolynom ist vom Grad k . Es gilt $g_k = g_0 \neq 0$.

$$G(x) = g_kx^k + g_{k-1}x^{k-1} + \dots + g_1x + g_0$$

An die Nutzinformation werden k Nullbits angehängt. k ist der Grad des Generatorpolynoms. Dies entspricht dem Polynom $x^k U(x)$.

$x^k U(x)$ wird unter Verwendung von Modulo-2-Arithmetik durch $G(x)$ dividiert. Dabei entsteht ein Restpolynom $R(x)$ das höchstens vom Grad $k - 1$ ist.

Bei der Modulo-2-Arithmetik sind die Operationen Addition, Subtraktion und Exklusiv-Oder identisch.

Die Koeffizienten von $R(x)$ werden in das CRC-Feld eingetragen. Damit erhält man die Nutzinformation mit dem angehängten CRC-Feld das Polynom $B(x) = (x) - R(x)$. Dieses Polynom ist durch $G(x)$ ohne Rest teilbar.

Der Empfänger teilt das empfangene Polynom durch $G(x)$.

Bei einer fehlerfreien Übertragung ergibt $B(x) / G(x)$ den Wert 0.

Ein CRC-Verfahren mit einem 16-Bit-CRC-Feld kann alle Burst-Fehler mit 16 oder weniger Bit Länge erkennen.

Es werden 99,997% aller längeren Burst-Fehler erkannt.

Bei einem 32-Bit-CRC-Feld sind die entsprechenden Werte 32 Bit und 99,99999995%.

6.10.2.4.1 - Beispiel für eine CRC-Bearbeitung

Wir haben eine 8-Bit-Nachricht M. Ihr Wert sei 10011010. Das entspricht folgendem Polynom.

$$M(x) = 1 \cdot x^7 + 0 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 0 \cdot x^0 = x^7 + x^4 + x^3 + x^1$$

Das Generatorpolynom G sei vom Grad 3.

$$G(x) = x^3 + x^2 + x^0 \text{ In diesem Beispiel sei } G(x) = 1101.$$

Zuerst wird M(x) mit x^3 multipliziert, denn das Generatorpolynom ist vom Grad 3. Dies entspricht einer Verschiebung um 3 Stellen nach links. Damit wird aus 10011010 der Wert 10011010000.

Danach wird M(x) mit G(x) einer XOR-Operation unterzogen.

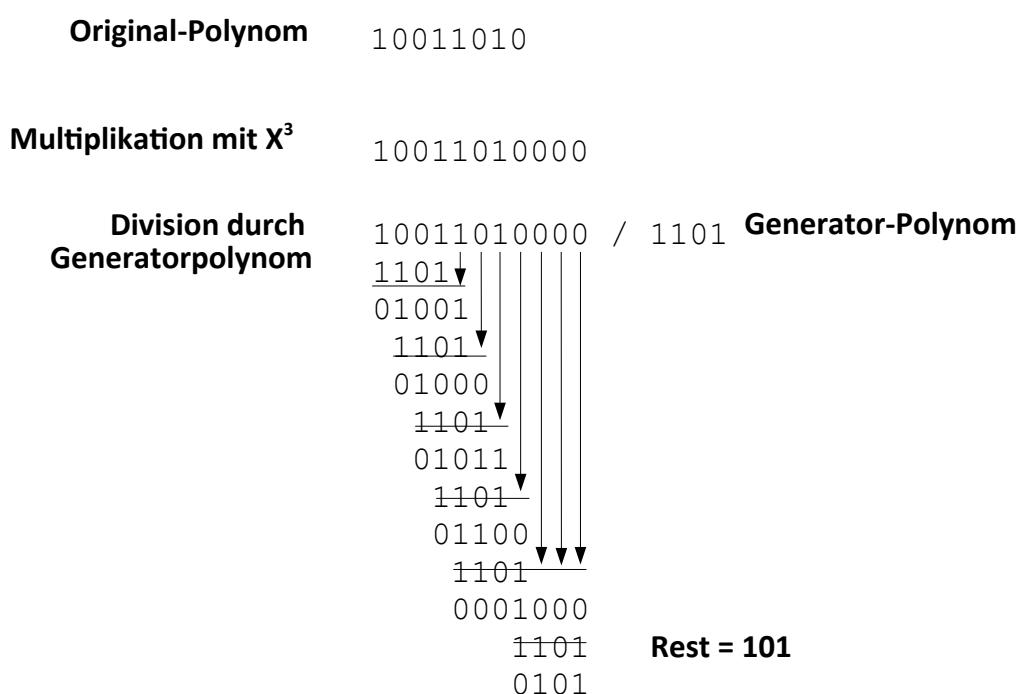


Abbildung 98: CRC-Berechnungsbeispiel

Damit ergibt sich für den Rest der Wert 101. Dieser Rest wird mit $M(x) \cdot x^3$ XOR-verknüpft. Das Ergebnis lautet 10011010101. Dieser Wert wird als N(x) gesendet.

Digitale Datenübertragung

Auf der Empfängerseite wird $N(x)$ einer Division mit dem selben Generatorpolynom unterzogen. Das heißt, $N(x)$ wird durch $G(x)$ dividiert. Entsteht hierbei der Rest = 0 kann davon ausgegangen werden, dass keine Fehler bei der Datenübertragung aufgetreten sind.

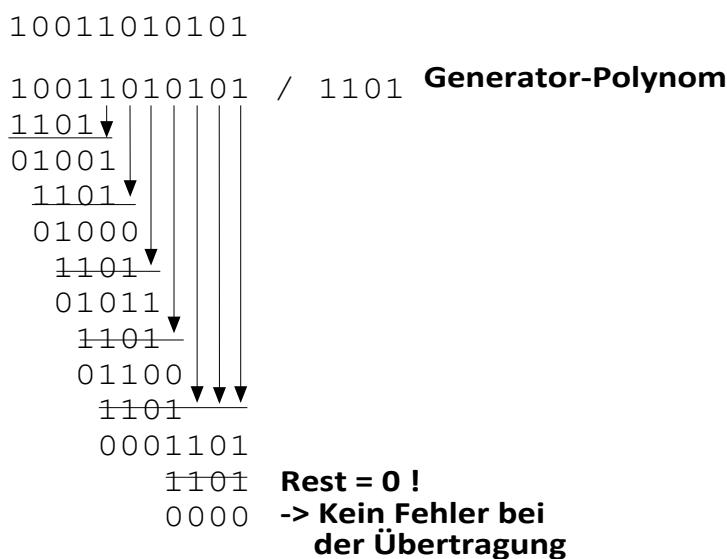
Übertragenes-Polynom**Division durch Generatorpolynom**

Abbildung 99: CRC-Bearbeitung auf der Empfängerseite

Übliche CRC-Generatorpolynome sind:

Tabelle 1: CRC-Verfahren (Quelle: Wikipedia)

CRC	Verwendung	$C(x)$	MHD	Länge
CRC-4	CCITT	$x^4 + x + 1$	3	15
CRC-5	USB	$x^5 + x^2 + 1$	3	31
	Bluetooth	$x^5 + x^4 + x^2 + 1$		15
CRC-7	SD/MMC	$x^7 + x^3 + 1$	3	127
CRC-8	Dallas / Masim 1-Wire-Bus	$x^8 + x^2 + x^1 + 1$	4	127
CRC-8	ITU-T	$x^8 + x^2 + x^1 + 1$	4	127
CRC-8	AES / EBU	$x^8 + x^4 + x^3 + x^2 + 1$	4	255
CRC-10		$x^{10} + x^9 + x^5 + x^4 + x + 1$		
CRC-12		$x^{12} + x^{11} + x^3 + x^2 + 1$		
CAN-CRC	CAN-Bus	$x^{15} + x^{14} + x^{10} + x^8 + x^7 + x^4 + x^3 + 1$	6	127
CRC-16 IBM		$x^{16} + x^{15} + x^2 + 1$	4	32767
CRC-16 CCITT	XMODEM	$x^{16} + x^{12} + x^5 + 1$	4	32767

CRC	Verwendung	C(x)	MHD	Länge
CRC-32	Ethernet	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$	3	$2^{32} - 1$
CRC-64 ISO3309		$x^{64} + x^4 + x^3 + x + 1$		

In Tabelle 1: CRC-Verfahren (Quelle: Wikipedia) bedeutet MHD die Minimale Hamming Distanz.

6.10.3 - Wire-Codes

(deutsch: Leitungscodes)

Hier geht es um die physikalische Darstellung von codierten Symbolen auf:

- ## Kupferleitungen

Auf einer Kupferleitung können Nutzdaten durch Spannungsschwankungen übertragen werden.

- LWL

Bei Lichtwellenleitern (LWL) kommen Lichtimpulse zu Einsatz.

- Funk

Bei Funk werden Elektromagnetische Wellen übertragen.

6.10.3.1 - Grundvoraussetzungen

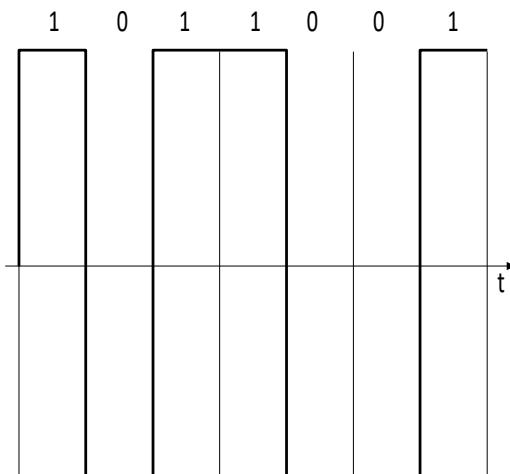
Möglichst kein Gleichstromanteil denn dadurch muss mehr Leistung übertragen werden. Dies führt z. B. zu einer Erwärmung von Kupferleitungen.

Eine einfache Takt-Rückgewinnung sollte möglich sein.

Es sollte eine hohe Effizienz und Stabilität erreicht werden.

Es sind unterschiedliche Codierungsverfahren im Gebrauch:

- Zweistufige (Bi-Phase) Leitungscodierungen können durch zwei Spannungen erzeugt werden.



Der Vorteil hierbei ist eine einfache Takt-Rückgewinnung

Abbildung 100: Zweistufige Leitungskodierung

- #### Dreistufige Leitungscodierung

Diese auch ternäre Codes genannten Wire-Codes haben 3 unterschiedliche Pegel. Z. B. MLT3. Dazu werden 3 unterschiedliche Spannungen verwendet. +1, -1 und 0 Volt.

- #### Vierstufige Leitungscodierung

Quaternäre Leitungscodes

- ## Fünfstufige Leitungscodes

Quinäre Leitungscodes

Mehrwertige Leitungscodes werden da eingesetzt wo die Fundamentalfrequenz auf den Leitung reduziert werden soll. Dafür sind dann auf der Empfängerseite hochwertige Empfänger-Bausteine notwendig, denn diese Codes sind störanfälliger.

6.10.3.2 - NRZ (Non Return to Zero)

NRZ-Verfahren arbeiten nach dem Prinzip der differentiellen Codierung. D. h. nicht der Spannungspegel ist ausschlaggebend, sondern der Pegelwechsel.

Die NRZ-Codierung hat einen hohen Gleichspannungsanteil. Im Extremfall $\pm \infty$. Diese Codierung wird bei Magnetaufzeichnungsverfahren verwendet. Es besteht keine Möglichkeit zur Takt-Rückgewinnung.

6.10.3.2.1 - NRZ-L

Wechsel von -Pegel auf +Pegel bedeutet 1.

Wechsel von +Pegel auf -Pegel bedeutet 0.

6.10.3.2.2 - NRZ-M

Wechsel des Pegel bedeutet 1.

Kein Pegelwechsel bedeutet 0.

6.10.3.2.3 - NRZ-S

Wechsel des Pegel bedeutet 0.

Kein Pegelwechsel bedeutet 1.

6.10.3.2.4 - RZ (Return to Zero)

Unipolar

Bei jeder 1 wird einen halben Takt lang ein +Pegel angelegt.

Bei 0 bleibt der Pegel auf 0.

Bipolar

Bei jeder 1 wird einen halben Takt lang ein +Pegel angelegt.

Bei jeder 0 wird einen halben Takt lang ein -Pegel angelegt.

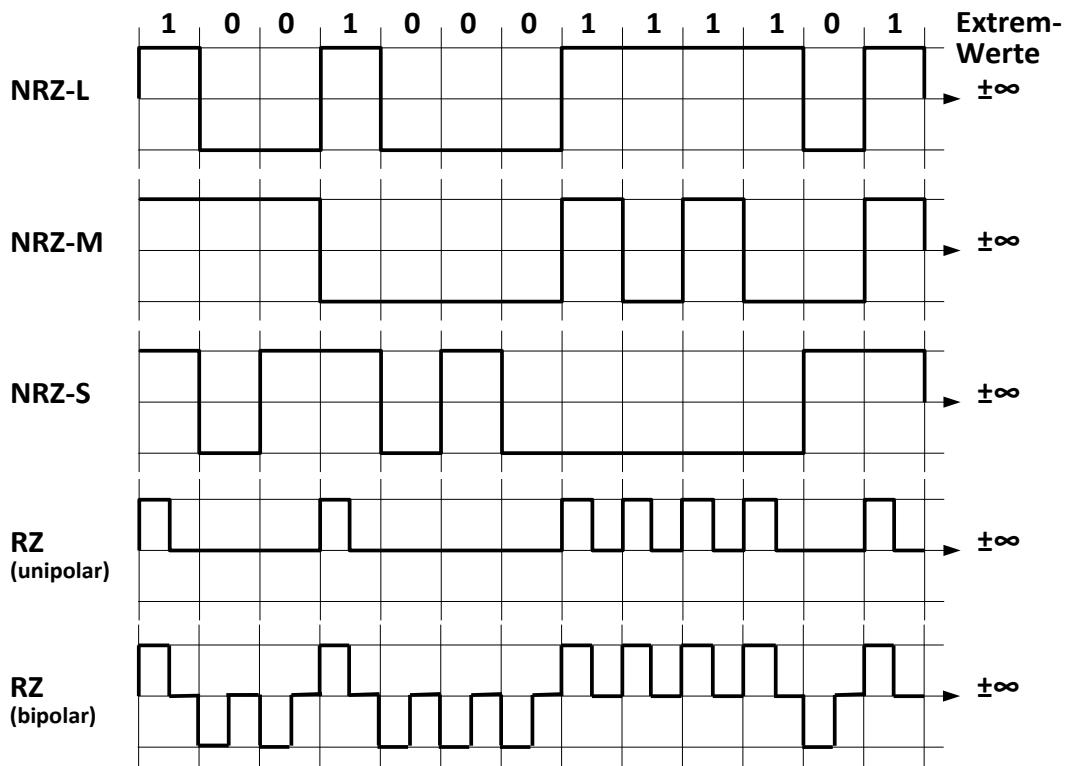


Abbildung 101: NRZ-Wire-Codes

6.10.3.3 - Biphase-Codierung

Bei der Biphasen-Codierung liegen folgende Prinzipien zugrunde:

- Bei jedem Bit-Intervall findet ein Übergang statt. Dadurch ist eine Taktrückgewinnung einfach möglich.
 - Einfachere Fehlererkennung. Das Ausbleiben eines Übergangs kann für die Fehlererkennung genutzt werden.
 - Kein Gleichstrom-Anteil.

6.10.3.3.1 - Biphase-L (Level)

Eine 0 wird durch eine, in der Mitte des Intervalls fallende, Flanke dargestellt.

Eine 1 wird durch eine, in der Mitte des Intervalls steigende, Flanke dargestellt.

6.10.3.3.2 - Biphase-M (Mark)

Eine 1 wird durch eine Flanke in der Mitte des Intervalls gekennzeichnet.

Eine 0 wird durch das Fehlen einer Flanke in der Mitte des Intervalls gekennzeichnet.

6.10.3.3.3 - Biphase-S (Space)

Eine 0 wird durch eine Flanke in der Mitte des Intervalls gekennzeichnet.

Eine 1 wird durch das Fehlen einer Flanke in der Mitte des Intervalls gekennzeichnet.

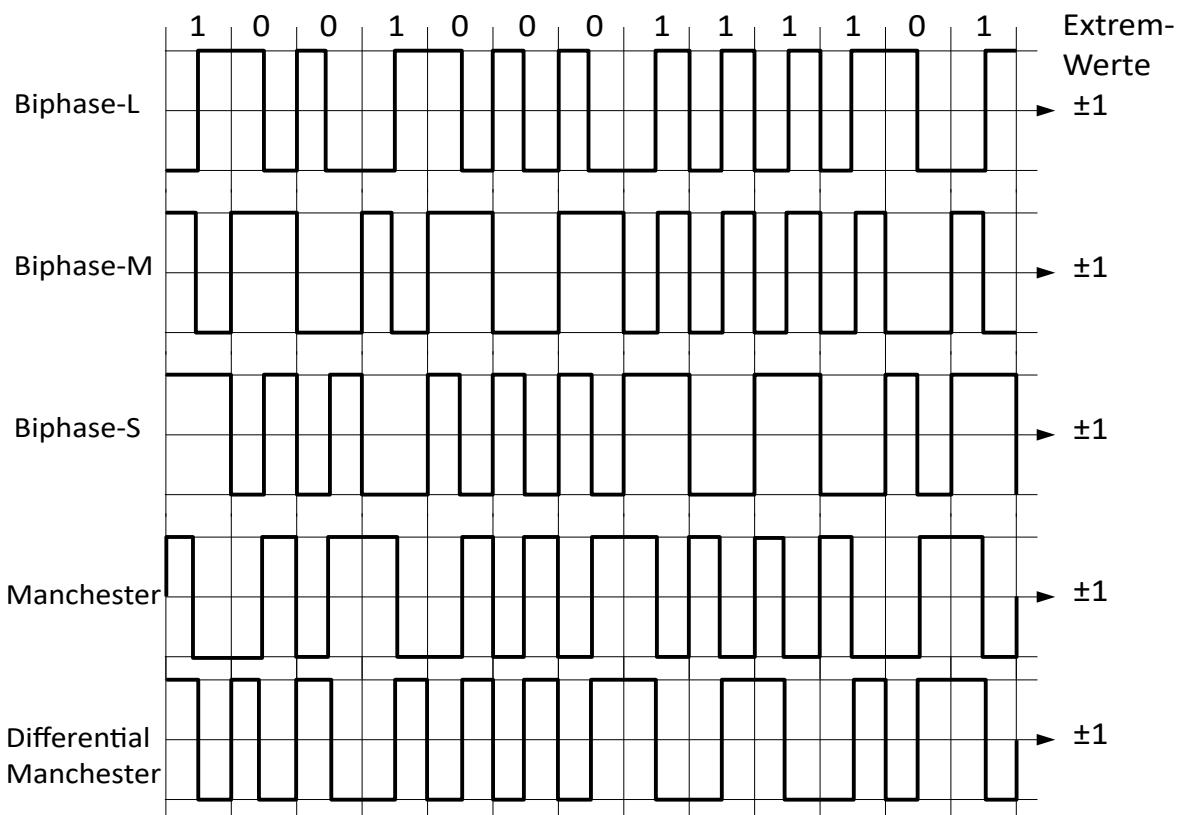


Abbildung 102: Biphase und Manchester-Codierung

6.10.3.3.4 - Manchester

Eine 1 wird durch eine hohe Spannung in der ersten Intervall-Hälfte dargestellt. Eine 0 wird durch eine hohe Spannung in der zweiten Intervall-Hälfte dargestellt.

6.10.3.3.5 - Differential Manchester

Eine 1 wird dadurch angezeigt dass am Intervall-Anfang keine Änderung statt findet. Eine 0 wird dadurch angezeigt dass am Intervall-Anfang eine Änderung statt findet.

6.10.3.4 - Ternary-Wire-Codes

Diese Codes haben 3 Pegelwerte (+1, -1 und 0).

6.10.3.4.1 - AMI-NRZ

Bei jeder 1 wird ein Impuls während des gesamten Intervalls im Wechsel mit + und – übertragen.

Bei 0 bleibt der Pegel auf 0.

6.10.3.4.2 - AMI-RZ

Bei jeder 1 wird ein Impuls während eines halben Intervalls im Wechsel mit + und – übertragen.

Bei 0 bleibt der Pegel auf 0.

6.10.3.4.3 - HDB3

Entspricht einer 1 einem AMI-NRZ

Bei einer 0 wird bei 4 Nullen in Folge der letzte Impuls wiederholt. Dies entspricht einer Codeverletzung.

6.10.3.4.4 - MLT3 (Multiple Level 3)

Hierbei wird zuerst eine Umkodierung von 2 auf 3 Pegel vorgenommen. Damit werden 3 anstelle von 2 Spannungspegeln ausgenutzt.

Dadurch reduziert sich bei FDDI die Fundamentalfrequenz von 62,5 MHz auf 31.25 MHz. Somit sind Leitungslängen bis zu 100 m möglich.

Bei jeder 1 wird ein Pegelwechsel von 0,+1,0,-1 vorgenommen. Bei einer 0 bleibt der Pegel erhalten. Damit ist bei langen 0-Folgen keine Taktrückgewinnung möglich! Deshalb muss bei 100BASE-TX , also Fastethernet auf Twisted-Pair-Leitungen, vorher erst eine 4B/5B-Codierung erfolgen.

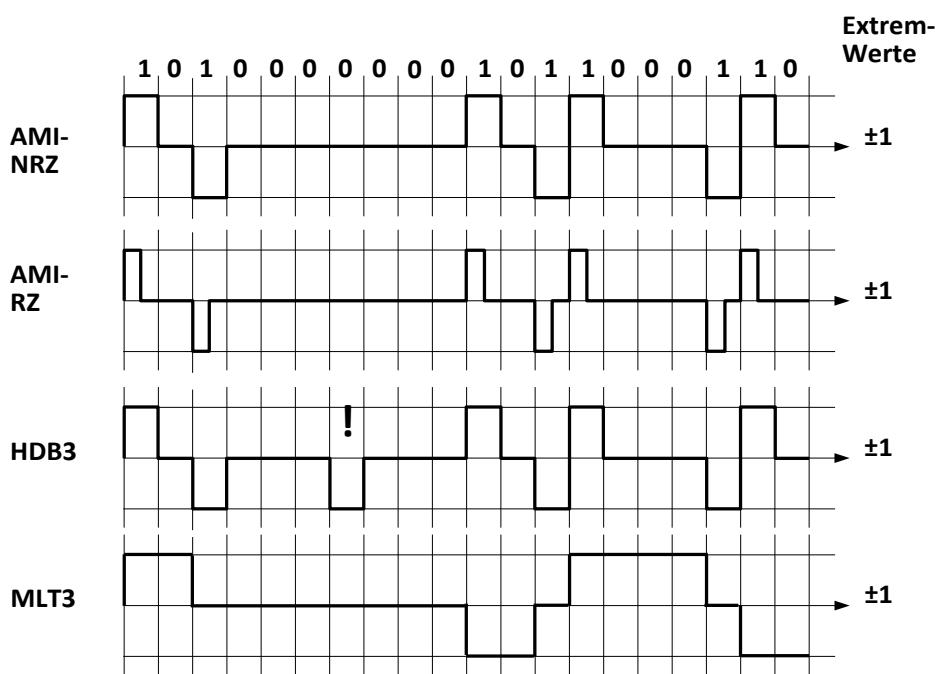


Abbildung 103: Ternary-Wire-Codes

6.10.4 - Bitfehlerrate

(engl. Bit Error Rate)

$$BER = \frac{\text{Anzahl der Bitfehler}}{\text{Anzahl aller übertragenen Bits}}$$

Ein ideales Signal sieht folgendermaßen aus:

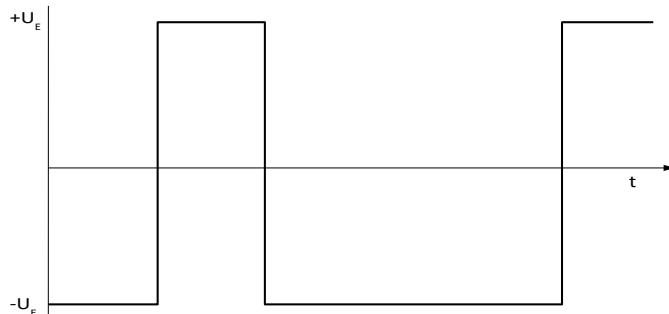


Abbildung 104: Ideales Signal

Durch Störungen wie z. B. Rauschen wird die Wahrscheinlichkeit, dass das Signal so aussieht folgendermaßen aussehen.

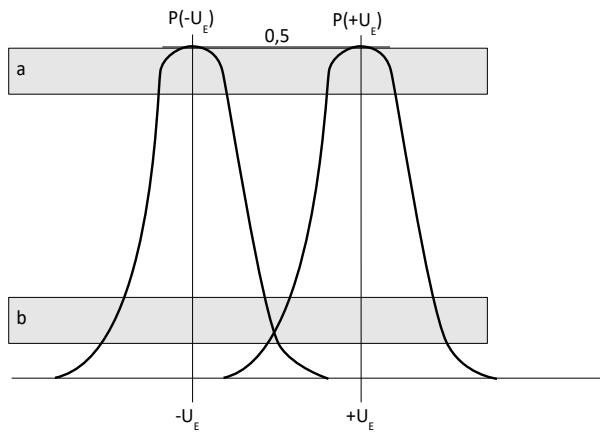


Abbildung 105: Wahrscheinlichkeitsverteilung eines Signals

- Lichtbögen durch vorbeifahrende Züge
- Defekte Leitungen

a

Für ein rauschbehaftetes Signal ist es wahrscheinlich in der engen Umgebung von $+U_E$ oder $-U_E$ zu messen.

b

Es ist sehr selten ein Signal zu messen das weit vom Wert $+U_E$ oder $-U_E$ entfernt ist.

Bei einem Schwellwert von 0 kann ein Wert $+U_E$ nicht von einem Wert $-U_E$ unterschieden werden. Dies ist der Bereich für Bitfehler.

Weitere Gründe sind :

- Ein-/Ausschalten von Geräten (Spannungsspitzen)
- Übersprechen zwischen Adernpaaren
- Reflexionen bei schlecht abgeschlossenen Leitungen

Wenn ein Bitfehler auftritt, ist es wahrscheinlich, dass ein weiterer Bitfehler auftritt. Bitfehler haben ein Burst-Verhalten. Dies bedeutet, dass sie gehäuft auftreten.

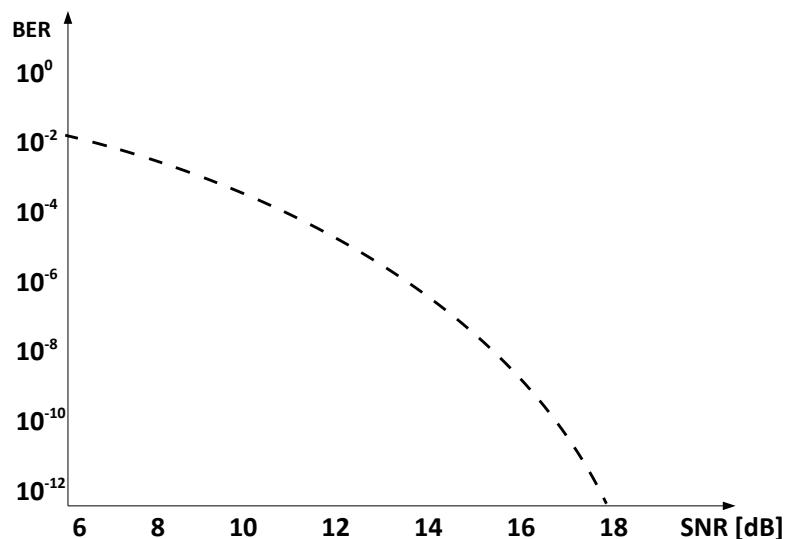


Abbildung 106: Zusammenhang zwischen BER und SNR

Je größer das SNR (Signal to Noise Ratio), desto weniger Bit-Fehler treten auf.

6.10.5 - Augenmuster

Die Qualität einer Übertragung kann auch mit den Augenmustern dargestellt werden.

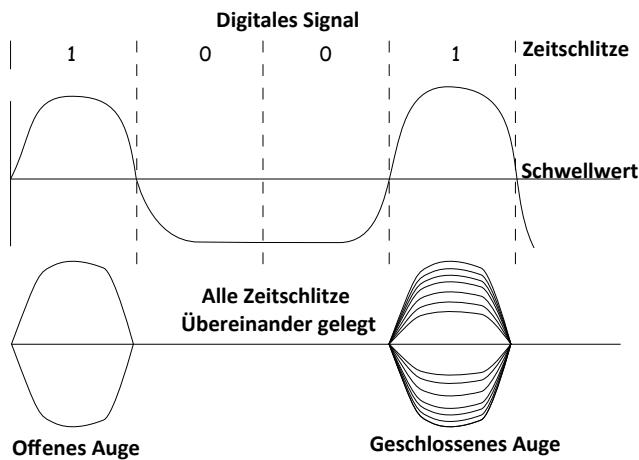


Abbildung 107: Augenmuster

Werden die Zeitschlitze übereinandergelegt erhält man das typische Augenmuster.

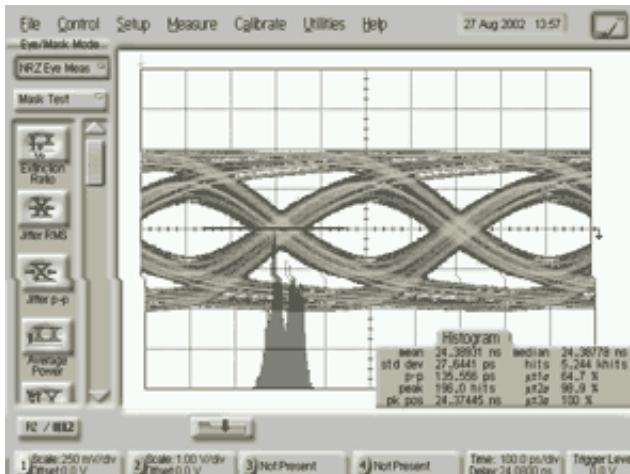


Abbildung 108: Geschlossenes Auge bei einer zweistufigen Leitungscodierung

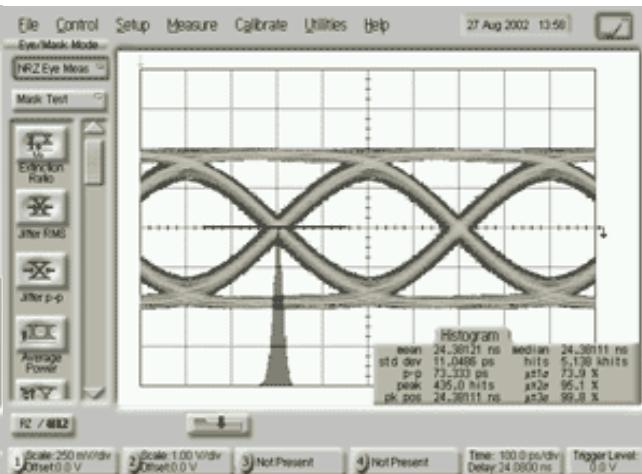


Abbildung 109: Offenes Auge bei einer zweistufigen Leitungscodierung

7 - Modulation

Bei der Übertragung von Daten über Lichtwellenleiter oder Kupfer kann das Signal direkt im Basisband übertragen werden. Soll allerdings ein Signal über einen Funkkanal übertragen werden, muss es zuerst in ein höheres Frequenzband verschoben werden. Das ist notwendig, da sonst z. B. die Antennen unhandliche Größen annehmen würden. [HELÖ-NATE-2000][BOS-EIDN-2012]

Der Zusammenhang zwischen Frequenz und Wellenlänge, die für die Antennenbauform und damit deren Größe verantwortlich ist lautet:

$$\lambda = \frac{c}{f} \quad (24)$$

Wobei die c mit 299.792.458 die Lichtgeschwindigkeit in Meter pro Sekunde angegeben wird. F ist die Frequenz in Hz (1/s) und λ die Wellenlänge, welche in m angegeben wird.

7.1 - Einleitung

Bei der **Modulation** wird ein **Trägersignal** durch das Signal der Signalquelle in einem oder mehreren Parametern verändert. Das Ergebnis ist ein Signal, das über Funk einfach übertragen werden kann.

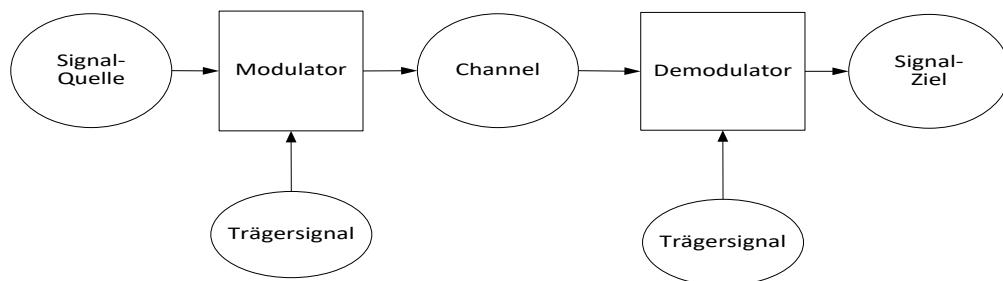


Abbildung 110: Modulation - Demodulation

Auf der Empfängerseite kann das Original-Signal durch eine **Demodulation** wieder gewonnen werden. Die Demodulation wird dadurch bewerkstelligt, indem mit dem gleichen Trägersignal nochmals moduliert wird.

Da die Übertragung oft in beiden Richtungen laufen soll, gibt es Geräte in denen sowohl ein Modulator als auch ein Demodulator enthalten sind. Diese Geräte werden Modem genannt.

Als Trägersignal werden Sinusschwingungen (Sinusträger) oder Pulsträger verwendet. Das Trägersignal $s(t)$ hat folgende Zusammensetzung:

$$s(t) = a(t) \cos(2\pi f(t) + \varphi(t)) = a(t) \cos(\omega(t) + \varphi(t)) \quad (25)$$

Bei der Modulation werden die folgenden Teile beeinflusst:

a ist die Amplitude des Trägers.

f ist die Frequenz des Trägers. Wobei $2\pi f$ der Kreisfrequenz ω des Trägers entspricht.

φ ist die Phase des Trägers.

Die harmonische Schwingung lässt sich gleichwertig auch als komplexe Schwingung über die Eulersche Identität angeben.

$$s(t) = a(t) \cdot e^{j\omega t} \quad (26)$$

Die Formel kann man in einen Realteil $s_R(t)$ und einen Imaginärteil $s_I(t)$ zerlegen.

$$s_R(t) = \Re \{ a \cdot e^{j\omega t} \} = \frac{1}{2} (a \cdot e^{j\omega t} + a \cdot e^{-j\omega t}) \quad (27)$$

$$s_I(t) = \Im \{ a \cdot e^{j\omega t} \} = \frac{1}{2j} (a \cdot e^{j\omega t} - a \cdot e^{-j\omega t}) \quad (28)$$

Die geklammerten Ausdrücke stellen die Schwingung als eine Summe einer positiven und einer negativen Frequenz dar. Im Zeigerdiagramm ist das grafisch durch zwei gegenläufige Zeiger darstellbar. Die beiden Anteile zeigen sich nach einer Modulation durch ein oberes und ein unteres Seitenband.

Modulationsverfahren

Je nachdem welcher Teil des Trägersignals beeinflusst wird unterscheidet man die Modulationsverfahren. Bei analogen zu übertragenden Signalen wird das Trägersignal kontinuierlich geändert. Dabei werden die folgenden Parameter des Trägersignals beeinflusst:

• Amplitude

Eine Beeinflussung der Amplitude wird **Amplitudenmodulation** genannt.

• Frequenz

Wird die Frequenz durch das zu übertragende Signal beeinflusst, spricht man von **Frequenzmodulation**.

• Phase

Eine Veränderung der Phase des Trägersignals wird **Phasenmodulation** genannt.

Bei digitalen zu übertragenden Signalen wird das Trägersignal abrupt geändert. Deshalb spricht man hier auch von einer **Umtastung**. Hierbei gibt es die folgenden Verfahren:

• Amplitude

Eine Beeinflussung der Amplitude wird **Amplitudenumtastung** (engl. **Amplitude Shift Keying = ASK**) genannt.

• Frequenz

Wird die Frequenz durch das zu übertragende Signal beeinflusst, spricht man von **Frequenzumtastung** (engl. **Frequency Shift Keying = FSK**).

• Phase

Eine Veränderung der Phase des Träger-Signals wird **Phasenumtastung** (engl. **Phase Shift Keying = PSK**) genannt.

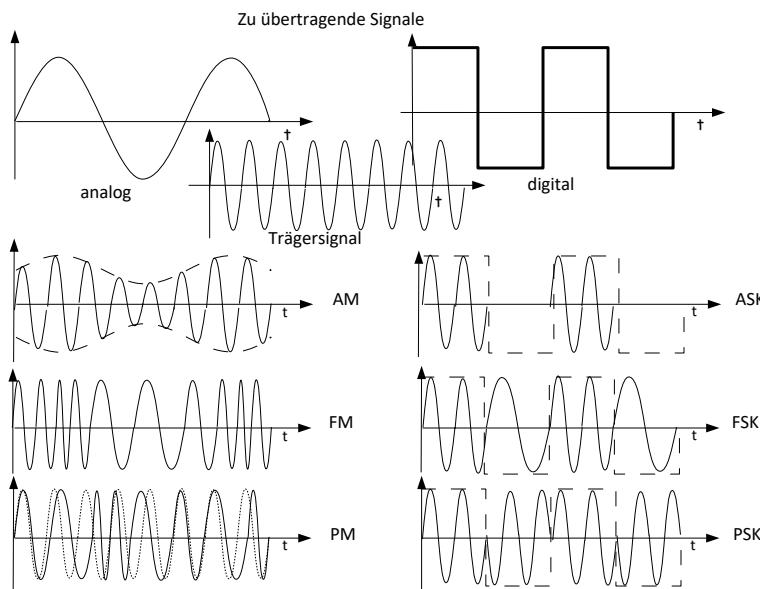


Abbildung 111: Modulationsarten

7.2 - Lineare Modulation

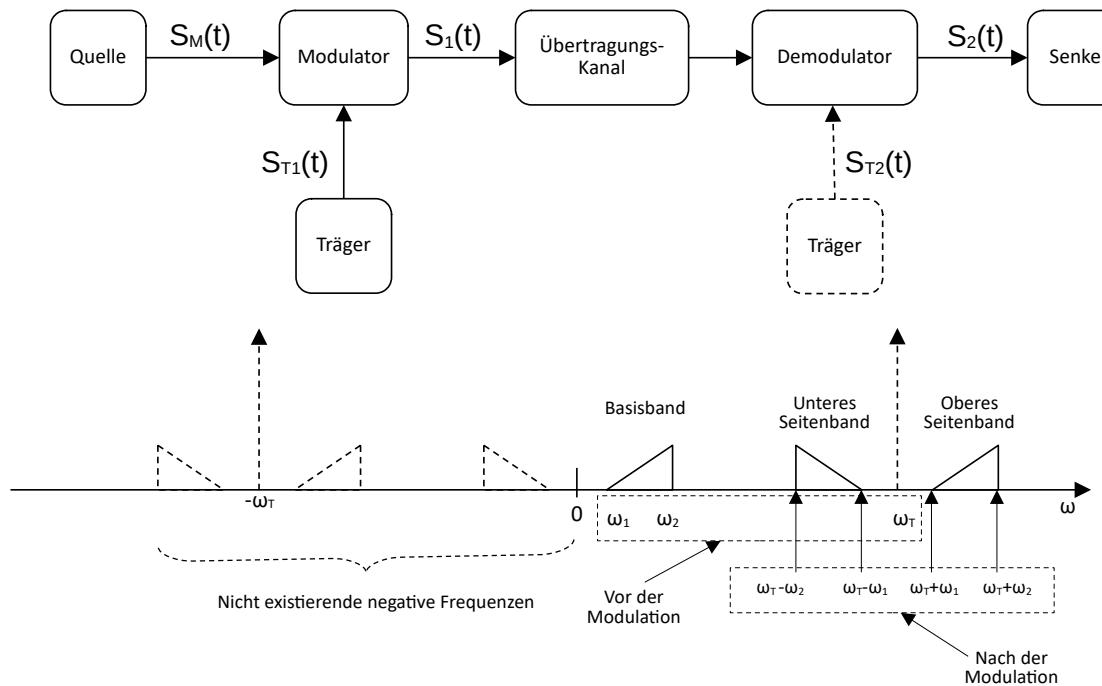


Abbildung 112: Signale der Modulation

In der Abbildung 112 ist oben das von der Quelle erzeugte modulierende Signal $S_M(t)$ zu sehen. Es wird Basisband-Signal genannt. In ihm ist die zu übertragende Information enthalten. Das modulierte Trägersignal $S_T(t)$ ist ein Sinus- oder Pulsträger. Bei den Sinusträgern können die Amplitude die Frequenz oder die Phase moduliert werden. Bei den Pulsträgern können die Amplitude, die Frequenz, die Phase, oder die Pulsweite(Dauer) moduliert werden.

Unten ist der Frequenzbereich zu sehen. Ausgehend von der Frequenz $\omega = 0$, sind auf der rechten Seite vor der Modulation nur die beiden Signale (Basisband (ω_1 bis ω_2) und Trägersignal (ω_T)) vorhanden. Nach der Modulation gibt es zusätzlich die beiden Seitenbänder (unteres ($\omega_T - \omega_2$ bis $\omega_T - \omega_1$) und oberes ($\omega_T + \omega_1$ bis $\omega_T + \omega_2$)). Seitenband). Zu mathematischen Zwecken wurden noch die negativen Frequenzen eingeführt. Da sie oft in der Literatur auftreten wurden sie hier der Vollständigkeit halber gestrichelt dargestellt. In der Realität existieren sie jedoch nicht und werden ab hier auch nicht weiter verwendet.

Im vorliegenden Abschnitt soll der folgende Sinusträger verwendet werden.

$$s_T(t) = \hat{S}_T \cos(\omega_T t + \varphi_T) \quad (29)$$

Das erzeugte Ausgangssignal $s_1(t)$ einer Multiplizierschaltung ist linear abhängig von $S_M(t)$.

$$s_1(t) = k_1 \cdot S_M(t) \cdot \hat{S}_T \cos(\omega_T t + \varphi_T) \quad (30)$$

Das modulierende Signal lässt sich folgendermaßen beschreiben:

$$s_M(t) = \hat{s}_M(t) \cos(\omega_M t + \varphi_M) \quad (31)$$

Enthält $S_M(t)$ mehrere Frequenzen, kann man den Übertragungssatz anwenden um $S_1(t)$ zu erzeugen.

$$\cos \alpha \cdot \cos \beta = \frac{1}{2} [\cos(\alpha + \beta) + \cos(\alpha - \beta)] \quad (32)$$

Damit erhält man das Modulationsprodukt

$$s_1(t) = \frac{1}{2} k_1 \cdot \hat{S}_M \cdot \hat{S}_T \cdot \cos(\omega_T + \omega_M) + (\varphi_T + \varphi_M) + \frac{1}{2} k_1 \cdot \hat{S}_M \cdot \hat{S}_T \cdot \cos(\omega_T - \omega_M) + (\varphi_T - \varphi_M) \quad (33)$$

Unter der Prämisse, dass man sich nur für das Modulationsprodukt in der Frequenzebene interessiert, kann man $\varphi_T = \varphi_M = 0$ setzen.

Vereinfacht man noch

$$\hat{S}_1 = \frac{1}{2} k_1 \cdot \hat{S}_M \cdot \hat{S}_T \quad (34)$$

erhält das Modulationsprodukt folgendes Aussehen

$$S_1(t) = \hat{S}_1 \cdot \cos(\omega_T + \omega_M) + \hat{S}_1 \cdot \cos(\omega_T - \omega_M) \quad (35)$$

Die Kreisfrequenz ω_M steht stellvertretend für die Kreisfrequenzen eines von ω_1 bis ω_2 begrenzten Basisbandes. Entsprechend Gleichung (35) erzeugt die Kreisfrequenz ω_M des Basisbandes eine obere Seitenbandfrequenz ($\omega_T + \omega_M$) und eine untere Seitenbandfrequenz ($\omega_T - \omega_M$). Jedes der beiden Seitenbänder hängt linear mit dem Basisband zusammen. Zusammen mit den nicht existierenden negativen Frequenzen kann man erkennen, dass sich eine lineare Modulation als einfache Anwendung des Frequenz-Verschiebungssatzes anwenden lässt.

Man kann auch erkennen, dass die von ω_2 herrührende untere Seitenbandlinie eine kleinere Frequenz hat als die von ω_1 herrührende. Um dies zu dokumentieren verwendet man für die Darstellung der Bänder Dreiecke. Dies hat nichts mit den Amplituden zu tun!

Auf der Empfängerseite erfolgt die Demodulation durch eine weitere Modulation mit einem Träger der selben Frequenz und Phase, wie auf der Senderseite. Die Demodulation mit Hilfe des frequenz- und phasenrichtigen Trägers nennt man kohärente Modulation oder Synchronmodulation. Wird der Träger nicht mitübertragen, lässt er sich aus den beiden Seitenbändern erzeugen.

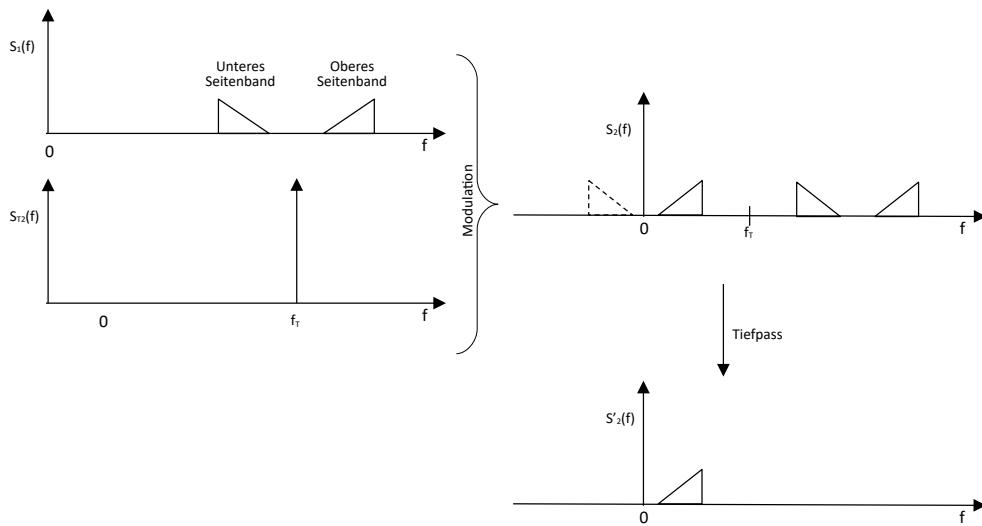


Abbildung 113: Demodulation

Daraus resultiert eine weitere Frequenzverschiebung und das ursprüngliche Basisband kann durch einen Tiefpassfilter ausgefiltert werden.

Da die bei den Seitenbändern die gleiche Information beinhalten kann durch Ausfiltern eines Seitenbandes Bandbreite und somit auch Übertragungsenergie eingespart werden. Dann wird von einer Single-Side-Band-Modulation (SSB) gesprochen.

7.3 - Analoge Modulationsverfahren

7.3.1 - Amplitudenmodulation (AM)

Die Amplitudenmodulation (AM) ist ein lineares Modulationsverfahren.

Der Träger S_c kann folgendermaßen beschrieben werden:

$$S_c(t) = (a_0 \cdot \cos(2\pi f_0 t + \phi_0)) \quad (36)$$

Wobei a_0 eine konstante Amplitude ist. Ist $a_1 > 0$ ergibt sich das amplitudenmodulierte Signal dann aus:

$$S_{AM}(t) = (a_0 + a_1 \cdot x(t) \cdot \cos(2\pi f_0 t + \phi_0)) \quad (37)$$

Der Modulationsgrad m ist definiert als:

$$m = \frac{a_1}{a_0} \quad (38)$$

7.3.1.1 - Modulationsindex

Um die optimalen Spannungen (Maximale Spannung = V_{max} und minimale Spannung = V_{min}) bei der Amplitudenmodulation zu verwenden wird der Modulationsindex herangezogen.

Zur Berechnung des Modulationsindex m wird folgende Formel verwendet:

$$m = \frac{(V_{max} - V_{min})}{(V_{max} + V_{min})} \quad (39)$$

7.3.1.2 - 50%-Modulation

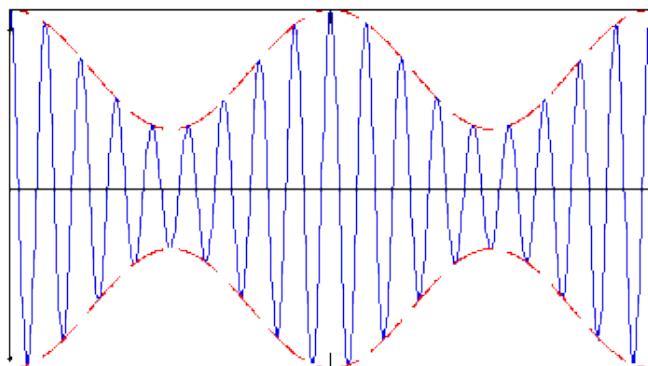


Abbildung 114: 50%-Modulation

Bei einer 50% Modulation ($m = 0,5$) sind beispielsweise folgende Spannungen möglich:

$$m = (3 - 1) / 3 + 1 = 0,5$$

Das AM-modulierte Signal enthält hierbei die beiden Seitenträger und den unmodulierten Träger. Dies wird als Zweiseitenband-AM mit Träger bezeichnet.

7.3.1.3 - 100%-Modulation

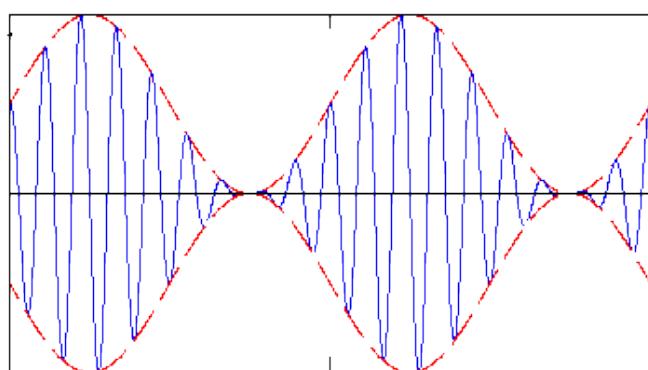


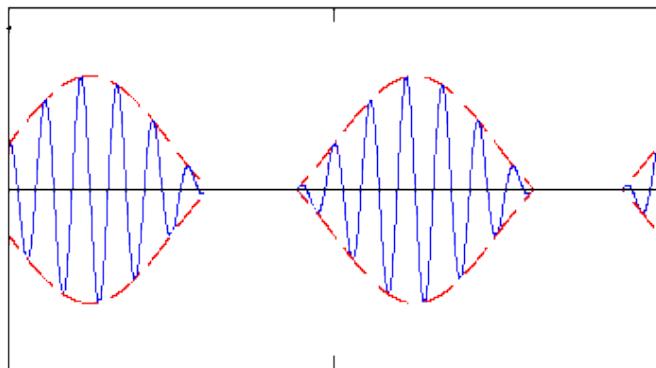
Abbildung 115: 100%-Modulation

Die optimalen Ergebnisse werden bei einer 100 prozentigen Modulation ($m = 1$) erzielt.

$$M = (2 - 0) / 2 + 0 = 1$$

Bei dieser Modulation verschwindet der unmodulierte Träger. Dies wird als Zweiseitenband-AM ohne Träger bezeichnet.

7.3.1.4 - Übermodulation



Bei einer Übermodulation ($m > 1$) treten Verluste auf.

$$M = (2,5 - 0,5) / 2,5 + 0,5 = 1,5$$

Abbildung 116: Übermodulation

7.3.2 - Frequenzmodulation (FM)

Die Frequenzmodulation gehört zu den Winkelmodulationsverfahren. Bei Winkelmodulationsverfahren wird generell nur die Phase verändert. Allerdings ändert die FM die Momentanfrequenz proportional zum Quellsignal wohingegen die Phasenmodulation (PM) den Phasenverlauf proportional zum Quellsignal ändert.

Die Momentankreisfrequenz $\omega(t) = 2\pi f(t)$ der Trägerschwingung wird mit dem Quellsignal $x(t)$ beeinflusst.

$$\omega(t) = \omega_0 + \Delta\Omega \cdot x(t) \quad (40)$$

Der Kreisfrequenzhub $\Delta\Omega = 2\pi\Delta F$. Wobei ΔF die maximale Abweichung der Momentanfrequenz von der Frequenz des unmodulierten Trägers ist.

Das FM-Signal kann vereinfacht folgendermaßen beschrieben werden.

$$S_{FM}(t) = a_0 \cdot \cos(\Phi(t) + \varphi_0) \quad (41)$$

Dabei ist $\Phi(t)$ die Momentanphase. Die Momentankreisfrequenz ist die Ableitung der Momentanphase:

$$\omega(t) = \frac{d\Phi(t)}{dt} \quad (42)$$

Damit gilt für die Momentanphase:

$$\Phi(t) = \omega_0 t + \Delta\Omega \cdot \int_0^t x(\tau) d\tau + \Phi_0 \quad (43)$$

Φ_0 ist der Anfangswert der Momentanphase zum Zeitpunkt $t = 0$. Fasst man Φ_0 und φ_0 in Φ_0 zusammen, so erhält man das FM-modulierte Sendesignal.

$$S_{FM}(t) = a_0 \cdot \cos(\omega_0 t + \Delta\Omega \cdot \int_0^t x(\tau) d\tau + \Phi_0) \quad (44)$$

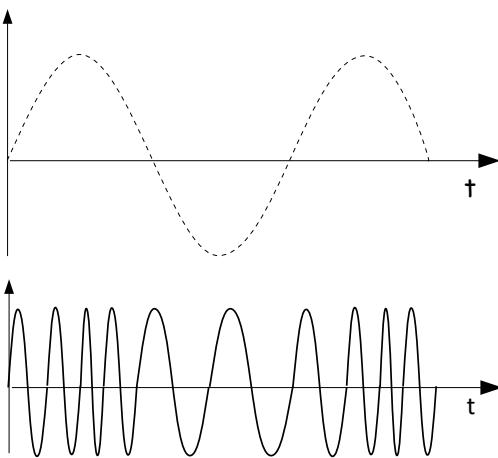
Modulation

Abbildung 117: Frequenzmodulation (FM)

In Abbildung 117 ist das Quellsignal gestrichelt dargestellt. Das modulierte Sendesignal ist darunter zu sehen. Bei der digitalen FM werden zur Übertragung von 0 und 1 zwei unterschiedliche Frequenzen f_1 und f_2 verwendet. Die Frequenz einer zu übertragenden Rechteck-Kurve/Welle wird FSK-Rate genannt und ist mehrere hundert Male langsamer als f_1/f_2 . Das Optimum für die Wahl des Abstandes von f_1 zu f_2 kann bezogen auf die Übertragungsdauer eines Bits T_b folgendermaßen definiert werden.

$$\Delta f = f_1 - f_2 = \frac{1,43}{T_b} \quad (45)$$

$$f_1 = a \cos(\omega - \Delta\omega)t$$

$$f_2 = a \cos(\omega + \Delta\omega)t$$

7.4 - Binäre Modulationsverfahren.

Wie bereits bei den Modulationsverfahren beschrieben wird die Modulation - da nur Einsen oder Nullen übertragen werden - auch Umtastung (eng. shift keying) genannt. Wird nur ein Bit übertragen, muss das übertragene Signal nur 2 Zustände ($x_0(t)$ und $x_1(t)$) annehmen. In den folgenden Beispielen soll immer die gleiche Folge an Informationsbits ((101100011101) übertragen werden.

7.4.1 - Unipolare Modulation

Bei der unipolaren Modulation gilt $x_0(t) = 0$ und $x_1(t) = x(t)$. Dabei entsteht entweder kein Signal ($x_0(t) = 0$), oder nur ein Signal mit einem Realteil ohne einen Imaginäranteil ($x_1(t) = x(t)$).

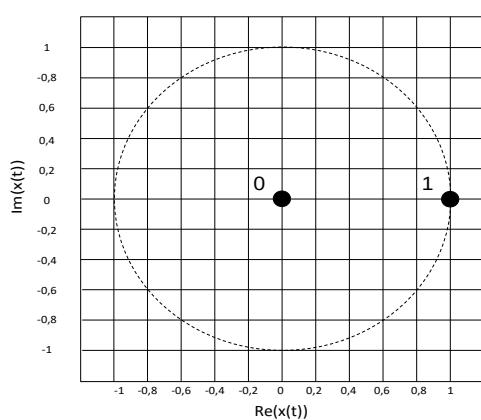


Abbildung 118: Komplexe Ebene bei der unipolaren Übertragung

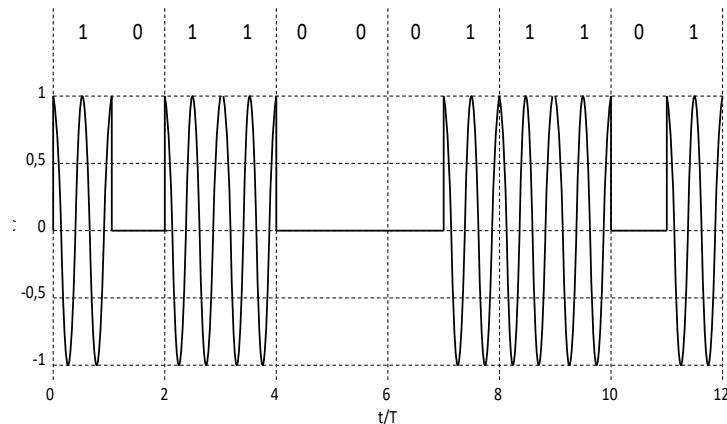


Abbildung 119: Signalverlauf der unipolaren Übertragung

Wie beim Signalverlauf zu sehen ist wird bei jedem Signal nur ein Bit übertragen. Das Ausbleiben eines Signals bedeutet eine Null. Das Übertragen eines cosinus-Signals bedeutet eine Eins.

Hierbei wird sichtbar, dass es beim Senden langer Nullfolgen problematisch wird, den Takt auf der Empfängerseite zurückzugewinnen.

7.4.2 - Bipolare Modulation

Bei der bipolaren Modulation gilt $x_0(t) = x(t)$ und $x_1(t) = -x(t)$. Dabei entsteht entweder das Signal $x(t) = 0$, oder nur das Signal $-x(t) = 1$. Beide Signale haben nur einen Realteil ohne einen Imaginäranteil.

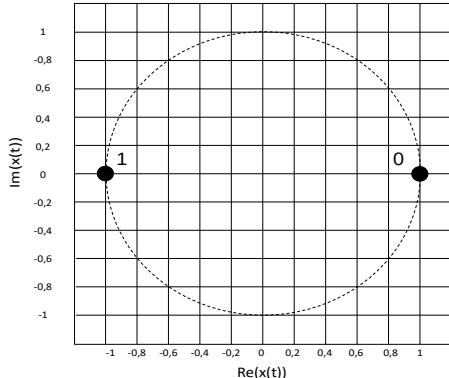


Abbildung 120: Komplexe Ebene bei der bipolaren Übertragung (BPSK)

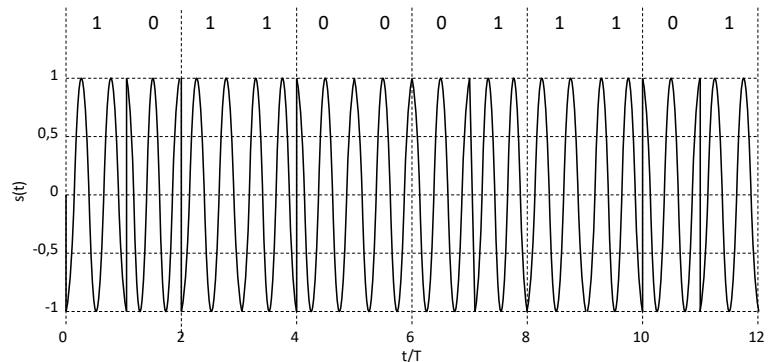


Abbildung 121: Signalverlauf der bipolaren (BPSK) Übertragung

In den obigen Darstellungen wird eine Binary Phase Shift Keying-Modulation (BPSK) gezeigt. Die Amplitude und die Frequenz bleiben gleich nur die Phase ändert sich.

Eine Null wird mit einem Cosinus-Signal übertragen. Eine Eins wird mit einem negierten Cosinus-Signal übertragen. Der Wechsel von einer Null zu einer Eins, und umgekehrt, bedeutet somit einen Phasensprung von 180° .

Auch hier wird mit jedem Signal nur ein Bit übertragen. Lange Folgen von Nullen oder Einsen sind hier jedoch kein Problem mehr.

Der größere Abstand der beiden Signale führt zu einem größeren Fehlerabstand, was die Übertragung weniger anfällig auf Störeinflüsse macht.

7.4.3 - Orthogonale Modulation

Bei der orthogonalen Modulation besteht gilt $\langle s_0(t), s_1(t) \rangle = 0$. Die Null hat nur einen Imaginärteil und die Eins hat nur einen Realteil. Zwischen den beiden Signalen besteht eine Phasenverschiebung von $\pi/2$. Damit stehen die Signale orthogonal aufeinander.[BOS-EIDN-2012]

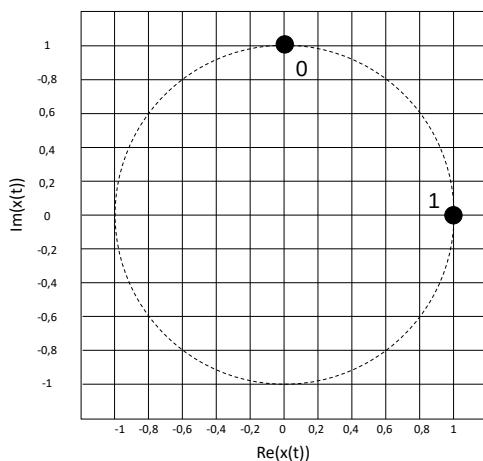


Abbildung 122: Komplexe Ebene bei der orthogonalen Übertragung

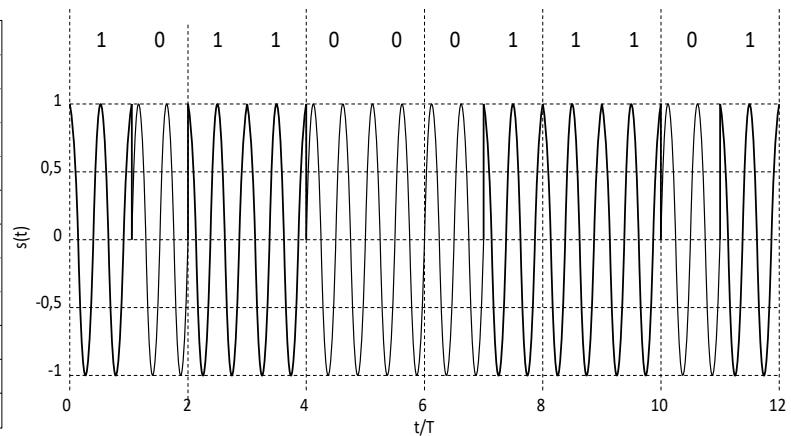


Abbildung 123: Signalverlauf einer orthogonalen Übertragung

Im Beispiel ist $x_1(t) = \text{rect}(t/T)$. $x_0(t) = \text{rect}(t/T) \cdot e^{+j\pi/2}$ ist ein komplexwertiges Signal. Das Signal für S_0

$$S_0(t) = \Re \{ x_0(t) \cdot e^{j2\pi f_0 t} \} = \Re \{ \text{rect}\left(\frac{t}{T}\right) \cdot e^{j(2\pi f_0 t + \pi/2)} \} = \text{rect}\left(\frac{t}{T}\right) \cdot \cos\left(2\pi f_0 t + \frac{\pi}{2}\right) \quad (46)$$

Ist damit orthogonal zum Signal S_1

$$S_1(t) = \Re \{ x_1(t) \cdot e^{j2\pi f_0 t} \} = \Re \{ \text{rect}\left(\frac{t}{T}\right) \cdot e^{j2\pi f_0 t} \} = \text{rect}\left(\frac{t}{T}\right) \cdot \cos(2\pi f_0 t) \quad (47)$$

7.5 - Mehrwertige digitale Modulationsverfahren

Mehrwertig bedeutet, dass ein bestimmtes Signal $s_i(t)$ aus M Signalen ausgewählt werden kann was $\log_2(M)$ Bits entspricht. Deshalb wird in der Regel $M = 2^m$ gewählt. Damit entspricht ein Signal m -bit. Die Zuordnung der Bits zu den Signalen wird **Labeling** genannt.

Bei der Verwendung von 2^m Signalen erhöht sich die binäre Datenübertragungsrate um den Faktor m gegenüber einer binären Datenübertragungsrate.

Die Euklidische Distanz δ zwischen zwei Signalen im Signalraum kann dazu herangezogen werden um ein Modulationsverfahren zu charakterisieren. Sie kann für zwei Signale $x_i(t)$ und $x_j(t)$ nach der folgenden Formel ermittelt werden.

$$\delta = \sqrt{(\Re\{x_i(t)\} - \Re\{x_j(t)\})^2 + (\Im\{x_i(t)\} - \Im\{x_j(t)\})^2} \quad (48)$$

Eine größere Euklidische Distanz führt zu einer geringeren Symbolfehlerwahrscheinlichkeiten. Deshalb hat das Binary Phase Shift Keying (BPSK) Modulationsverfahren die größte Euklidische Distanz.

7.5.1 - Mehrwertige Amplitude Shift Keying (ASK)

Werden 2 Bits für die Übertragung mit einem Signal verwendet sind $2^2 = 4$ unterschiedliche Signale erforderlich. Das Labeling wurde so gewählt, dass sich benachbarte Signale nur in einem Bit unterscheiden. [BOS-EIDN-2012]

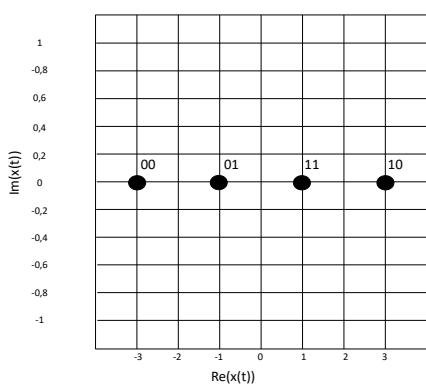


Abbildung 124: Komplexe Ebene bei der Übertragung von 4-ASK

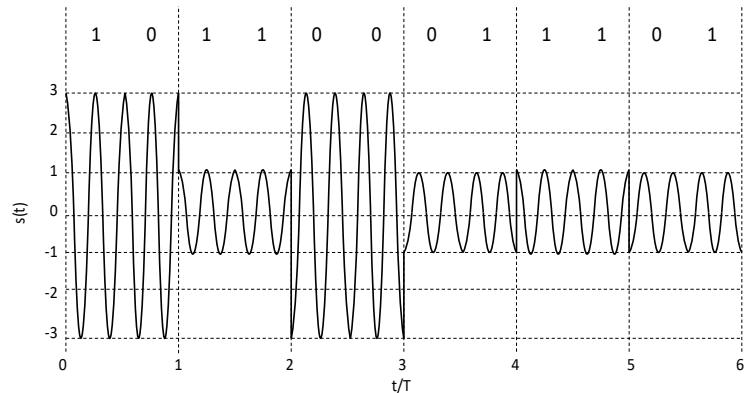


Abbildung 125: Signalverlauf einer 4-ASK-Übertragung

In der komplexen Ebene können die beiden Symbole 00 und 01 auch als um 180 Grad phasenverschobene Versionen von 10 und 11 verstanden werden (was einer Kombination von Amplituden und Phasenmodulation entspricht).

Bei der 4-ASK ist die Euklidische Distanz $\delta = 2$ zwischen zwei benachbarten Signalen. Z. B.

$$\delta = \sqrt{(\Re\{3\} - \Re\{1\})^2 + (\Im\{0\} - \Im\{0\})^2} = 2 \quad (49)$$

In Abbildung 125 ist zu erkennen, dass die Signale eine unterschiedliche Amplitude und damit auch unterschiedliche Energie haben, was eigentlich zu vermeiden ist, da manche Anwendungen damit Probleme haben. Unter der Voraussetzung, dass alle Signale gleich-wahrscheinlich auftreten, kann die mittlere Energie folgendermaßen berechnet werden:

$$E[x_i^2] = \frac{1}{4}((-3)^2 + (-1)^2 + 1^2 + 3^2) = \frac{20}{4} = 5 \quad (50)$$

7.5.2 - Mehrwertige Frequency Shift Keying (FSK)

Die zu übertragende Information wird in unterschiedlichen Frequenzen codiert. Dafür werden 2^m unterschiedliche Frequenzen benötigt um die Signale zu übertragen. Im folgenden Beispiel werden $2^2 = 4$ Signale für die Übertragung von jeweils 2 Bit übertragen.

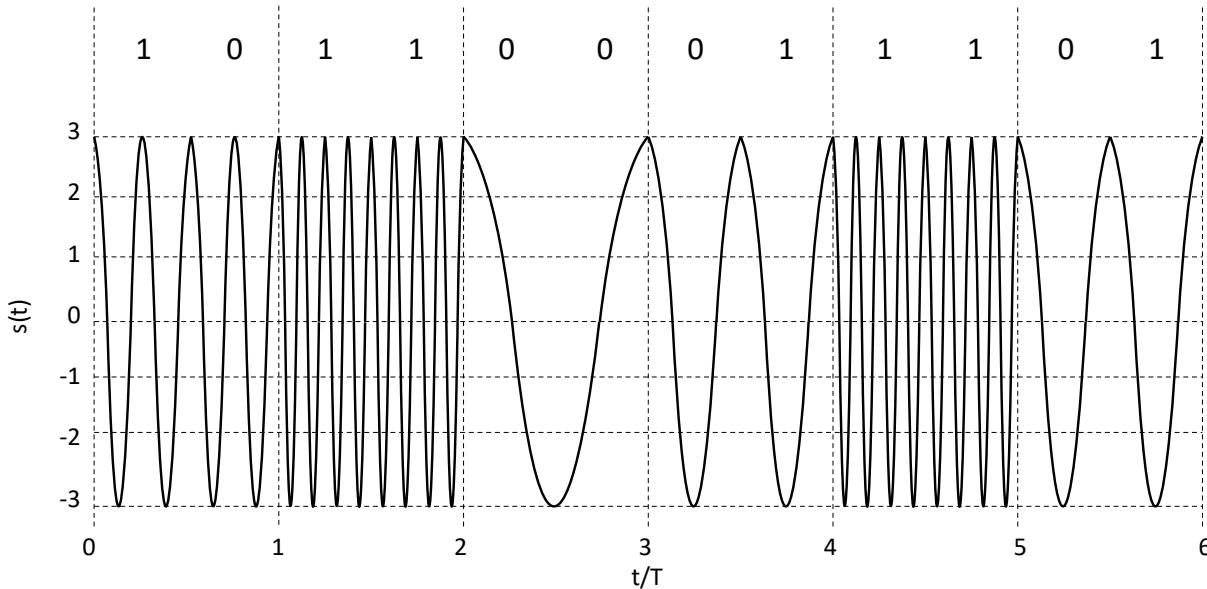


Abbildung 126: Signalverlauf einer 4FSK-Übertragung

Eine Darstellung in der komplexen Ebene macht hier keinen Sinn, da nur ein Punkt dargestellt werden würde. Es gibt keine Änderung in der Amplitude und der Phase.

7.5.3 - Mehrwertige Phase Shift Keying (PSK)

Die zu übertragende Information wird in unterschiedlichen Phasen codiert. Dies hat den Vorteil, dass alle Signale die gleiche Energie haben. Damit ändert sich am Sender die abgestrahlte Energie für unterschiedliche Symbole nicht.

Die minimale Euklidische Distanz ist $\delta = \sqrt{2}$. Dreht man die Konstellation wie in Abbildung 127 um $\pi/4$ nach rechts, dann liegt Das Signal 00 auf den Koordinaten (1,0) und das Signal 01 auf den Koordinaten (0,1). Damit ergibt sich die Distanz zu $\delta = \sqrt{1+1} = \sqrt{2}$.

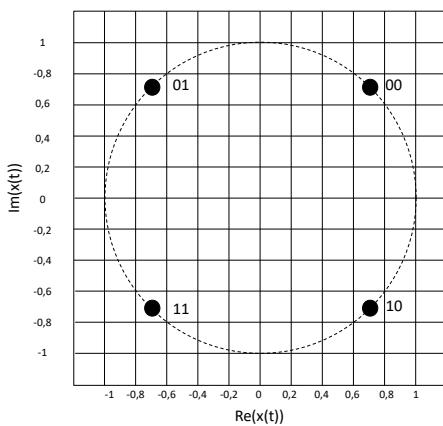


Abbildung 127: Komplexe Ebene bei der Übertragung von QPSK

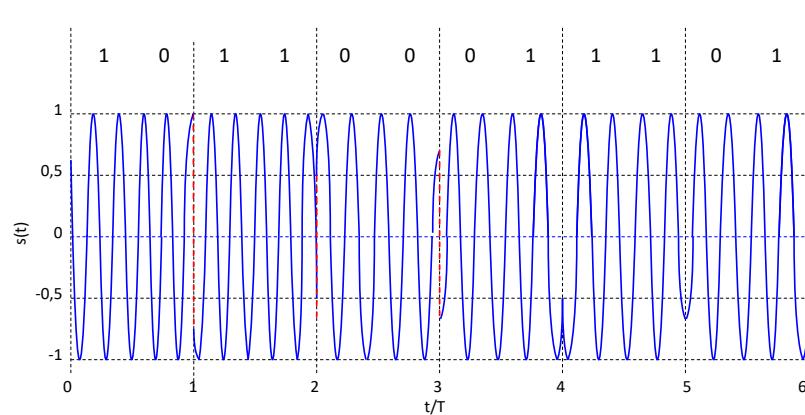


Abbildung 128: Signalverlauf einer QPSK-Übertragung

QPSK kann als zweidimensionale BPSK aufgefasst werden. Mögliche Phasenänderungen sind somit:

Single Bit $0^\circ, 180^\circ$

Dibit $0^\circ, 90^\circ, 180^\circ, 270^\circ$

Tribit $0^\circ, 45^\circ, 90^\circ, 135^\circ, 180^\circ, 225^\circ, 270^\circ, 315^\circ$

16-QAM $15^\circ, 45^\circ, 75^\circ, 105^\circ, 135^\circ, 165^\circ, 195^\circ, 225^\circ, 255^\circ, 285^\circ, 315^\circ, 345^\circ$

7.6 - Quadrature Phase Shift Keying (QPSK, 4PSK)

Wählt man die mögliche Phasenverschiebung mit 90° können 2 Bit pro Symbol übertragen werden. Bei dieser Modulationsart bleibt die Amplitude konstant.

Da die Information in der Phasenverschiebung hinterlegt ist und nicht in der Amplitude, ist diese Modulationsart gegen Rauschen unempfindlich.

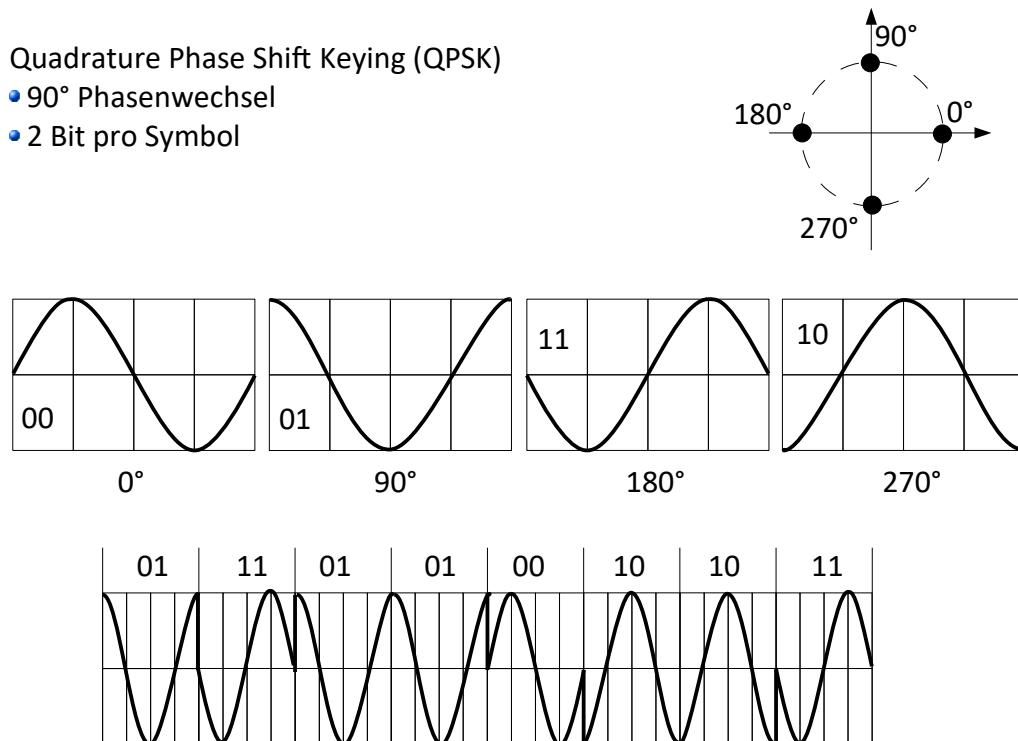


Abbildung 129: QPSK

Man kann diesen Faden jetzt weiter spinnen und die Abstände immer feiner granulieren. Bei jeder Halbierung kann ein Bit mehr pro Symbol übertragen werden.

Dadurch sind jeweils ein Bit mehr pro übertragenem Symbol möglich. Kombiniert man die PSK noch mit unterschiedlichen Amplituden kommt man zur Quadrature Amplitude Modulation (QAM). Hier werden 3 unterschiedliche Radien (Amplituden) und damit unterschiedliche Energien, sowie 12 Phasenwinkel verwendet.

Modulation

Im Signalraum kann man die QAM als zweidimensionale ASK auffassen. In Abbildung 130 ist zu sehen, dass eine vervierfachte 4-ASK 16 Signalpunkte hat was zur Bezeichnung 16-QAM frt. Wie bei ASK ist die minimale Euklidische Distanz $\delta = 2$. Bei gleich wahrscheinlichen Signale ist die mittlere Energie 6.

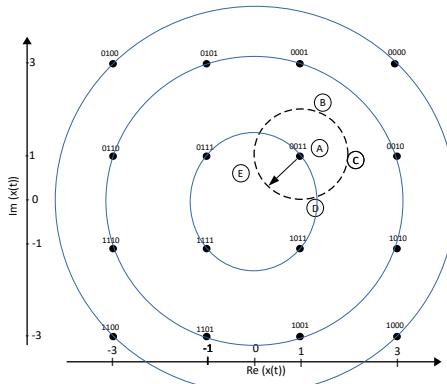


Abbildung 130: Komplexe Ebene bei der Übertragung von 16QAM

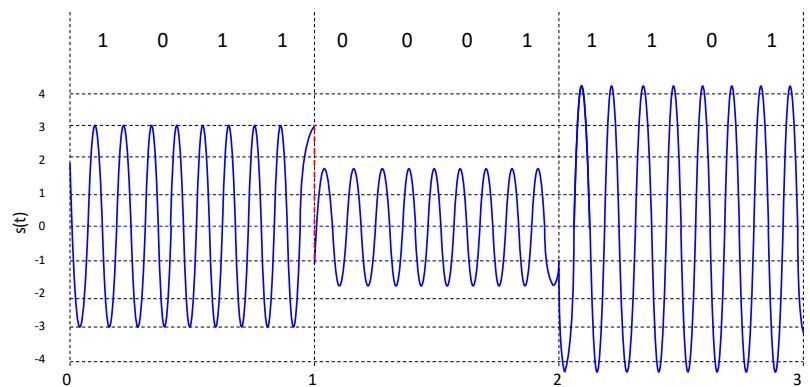


Abbildung 131: Signalverlauf einer 16QAM-Übertragung

Jeder Signalpunkt ist mit 4 Bit gelabelt, weshalb für die Übertragung der verwendeten Bitfolge nur drei Symbole erforderlich sind.

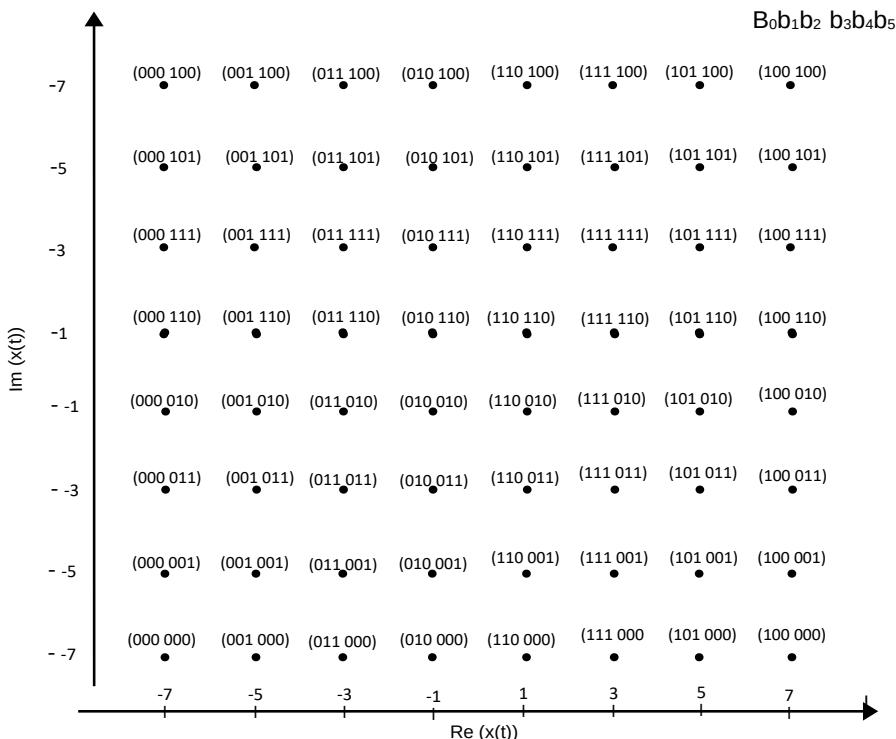


Abbildung 132: 64-QAM

Das Spiel lässt sich immer weiter treiben. In Abbildung 132 ist eine 64-QAM dargestellt. Damit lassen sich 6 Bit übertragen.

Mittlerweile gibt es das 4096-QAM-Modulationsverfahren. Damit lassen sich mit einem Symbol alle 12 Bits der verwendeten Bitfolge übertragen.

7.7 - Pulsmodulation

Bei der Pulsmodulation wird als Träger keine Sinuswelle sondern eine Pulsfolge verwendet.

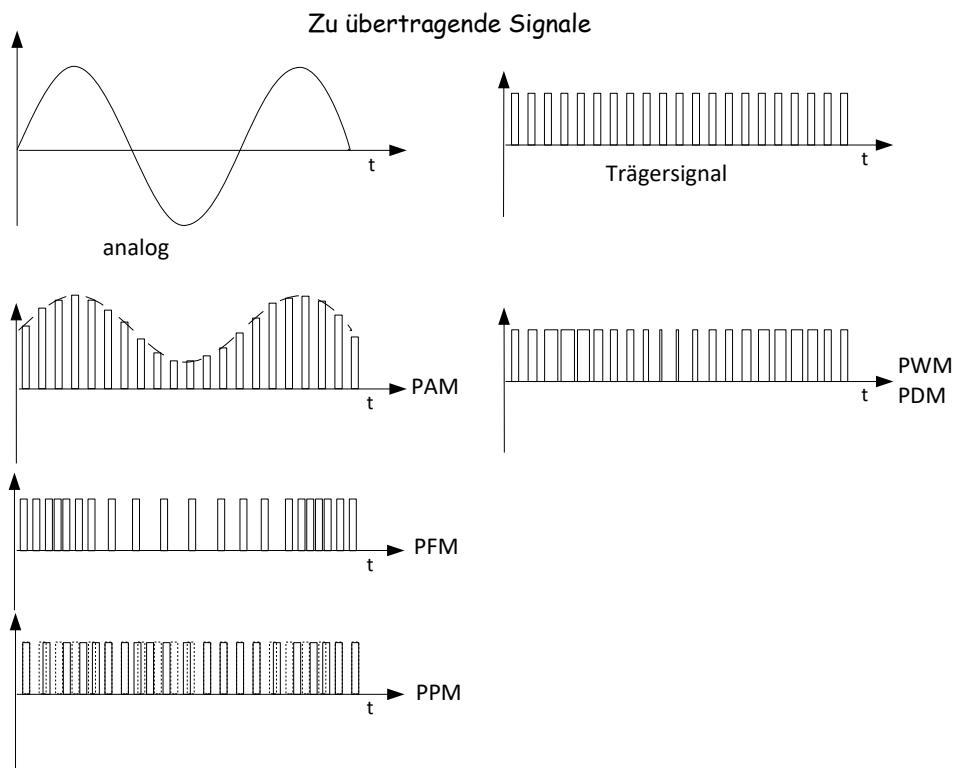


Abbildung 133: Pulsmodulation

7.7.1 - Pulsamplitudenmodulation (PAM)

Hierbei wird die Amplitude der Pulsfolge moduliert.

7.7.2 - Pulsfrequenzmodulation (PFM)

Hierbei wird die Frequenz der Pulsfolge moduliert.

7.7.3 - Pulsphasenmodulation (PPM)

Hierbei wird die Phase der Pulse moduliert.

7.7.4 - Pulsweitenmodulation (PWM) Pulsdauermodulation (PDM)

Hierbei wird die Dauer / Weite der Pulse durch die Modulation beeinflusst.

7.7.5 - Spektrum der Pulsmodulation

Auch bei der Pulsmodulation entstehen im Frequenzbereich Seitenbänder

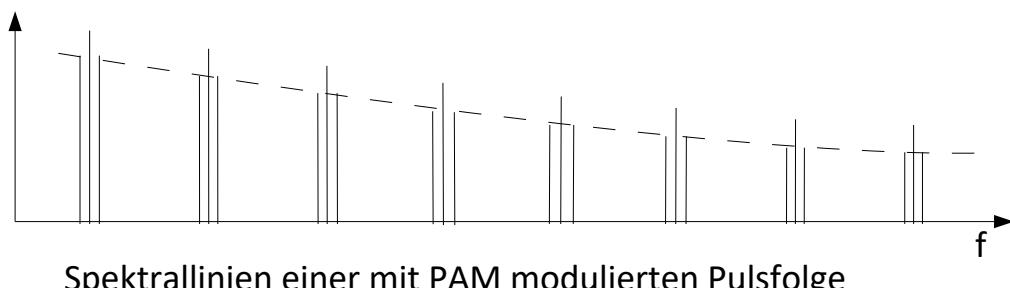
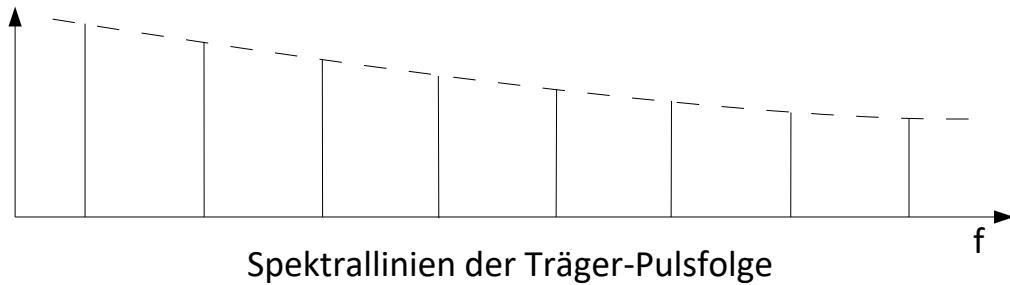


Abbildung 134: Spektrallinien bei PAM

Ein pulsmoduliertes Signal trägt die Information mehrfach (bei PAM doppelt). Dies bedeutet eine hohe Redundanz was auch zu einer höheren erforderlichen Bandbreite führt.

Werden die Impulse kurz genug gemacht, können die Zwischenräume zwischen den Pulsen für die Einfügung weiterer pulsmodulierter Signale verwendet werden. Dies entspricht einem Zeitmultiplex-Verfahren.

7.8 - Direkte Kodierung der Abtastwerte

Hierbei wird das Ergebnis der Quantisierung bei der Abtastung für die Modulation verwendet. Das Verfahren wird PCM (Pulse Code Modulation) genannt.

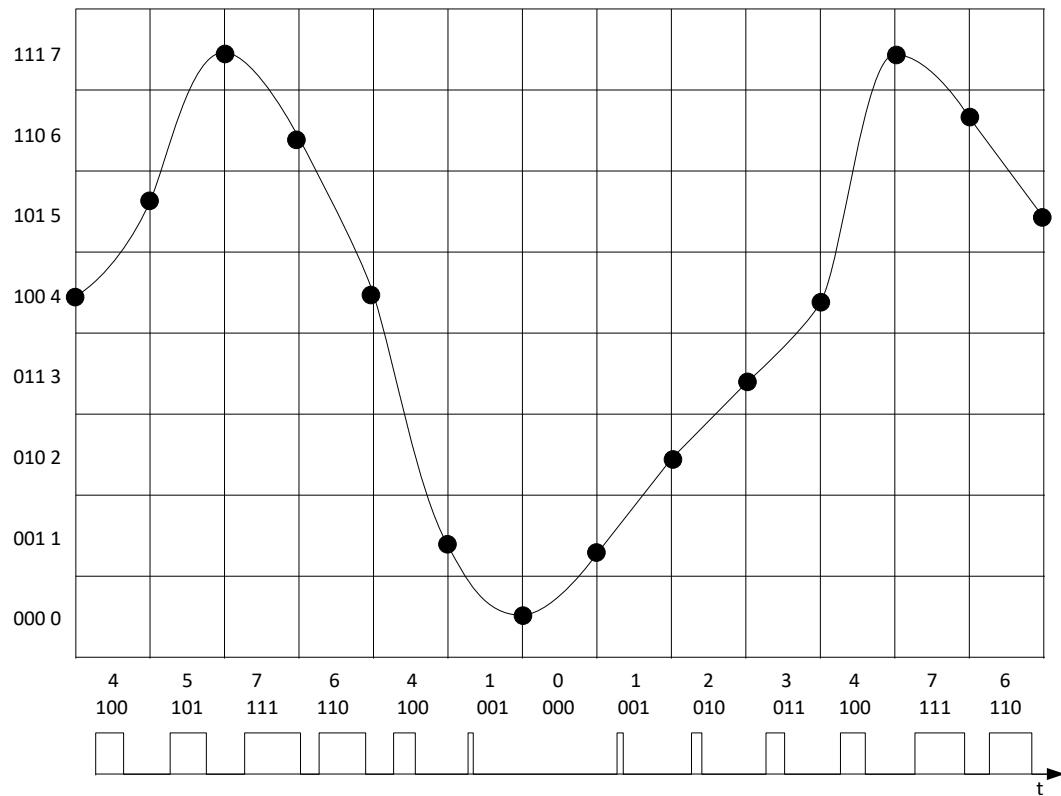


Abbildung 135: PCM

In der obigen Abbildung ist der Kurvenverlauf in der PCM moduliert. Der resultierende Wire-Code ist ein NRZ-Code.

7.9 - Deltamodulation (DM) / Differenz Puls Code Modulation (DPCM)

Bei der Deltamodulation wird so moduliert, dass immer nur der Wert 0 oder 1 zu übertragen ist. Dabei wird ausgehend von der vorangegangenen Abtastung ein Vorhersagewert ermittelt. Der Vorhersagewert ist 1 wenn der tatsächliche Abtastwert über dem vorhergesagten Wert liegt. Der Vorhersagewert ist 0, wenn der tatsächliche Abtastwert unter dem vorhergesagten Wert liegt.

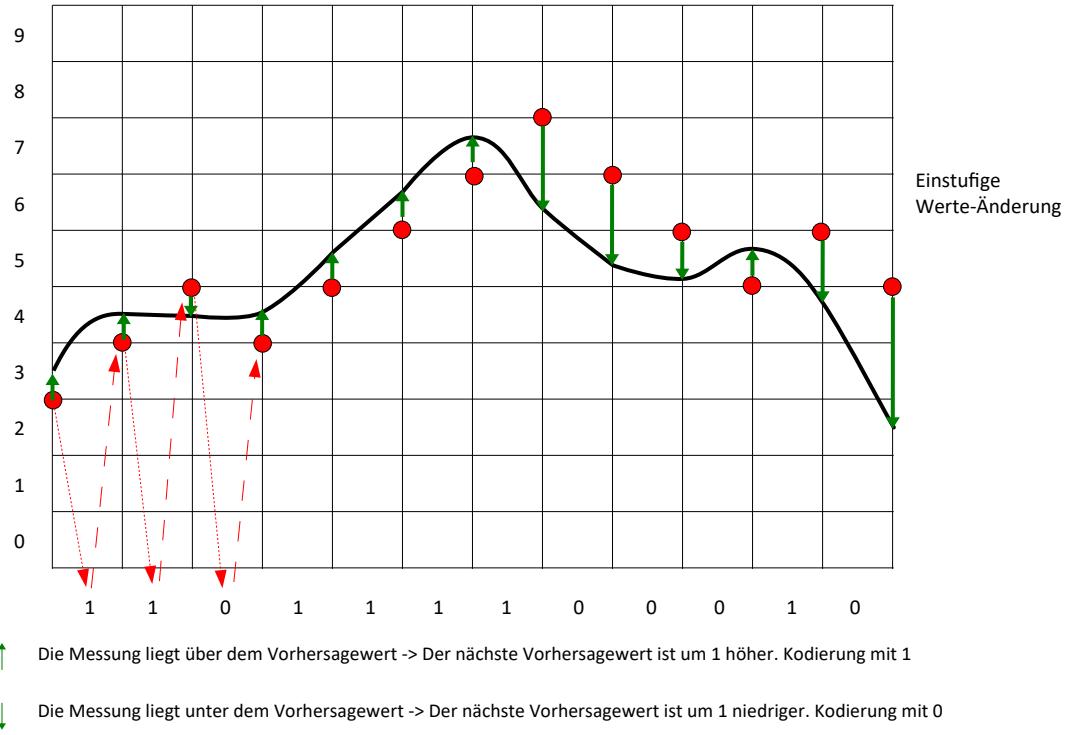


Abbildung 136: Differenz-Modulation

Die Differenz zwischen Signal und Vorhersagewert wird binär codiert und übertragen.

Bei großen Signalsprüngen ist dieses Verfahren zu ungenau! Abhilfe bringt hier die „Adaptive Deltamodulation ADM“. Dabei wird jeder n-te gleich lautende Wert nicht mit 1 sondern um den doppelten Wert geändert.

Ein Nachteil dieses Verfahrens ist, dass es schlecht einer Gleichspannung folgen kann. Ein Kompromiss ist hier die Differenz-Pulsecode-Modulation. Hierbei wird die einstufige Werte-Ermittlung durch eine mehrstufige Quantisierung ersetzt. Eingesetzt wird dieses Verfahren bei der Übertragung von Fernsehbildern.

7.10 - Zusammenfassung

Sinusträger	analog	Amplitudenmodulation	AM
		Einseitenbandmodulation	EM / SSB
		Frequenzmodulation	FM
		Phasenmodulation	PM
	digital	Amplitudenumtastung	ASK
		Frequenzumtastung	FSK
		Phasenumtastung	PSK
Pulsträger	uncodiert	Pulsamplitudenmodulation	PAM
		Pulsfrequenzmodulation	PFM
		Pulsphasenmodulation	PPM
		Pulsdauermodulation	PDM / PWM
	codiert	Pulscodemodulation	PCM
	Bezug auf die Vorgeschichte	Deltamodulation	DM / ADM

8 - Leitungstheorie

8.1 - Unterschied zwischen Leitung und Kabel

Kabel werden in der Erde oder im Meer verlegt. Dies erfordert besondere Schutzmaßnahmen die bei Leitungen nicht erforderlich sind. Somit sind Kabel besonders geschützte Leitungen.

8.2 - Stromkreis

Eine Leitung ermöglicht es, den Verbraucher vom Energieerzeuger räumlich getrennt zu platzieren.

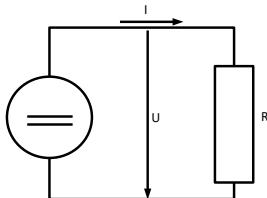
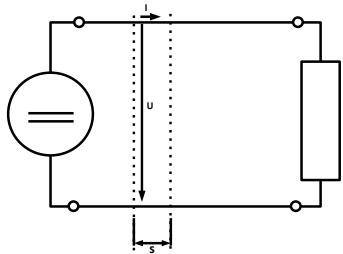


Abbildung 137: Stromkreis

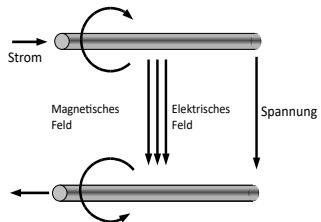


Um die Auswirkungen der eingeführten Leitung auf den Stromkreis zu ermitteln wird ein Stück der Länge s aus der Leitung herausgegriffen.

Ist der Abschnitt kurz genug, ist die Spannung am Anfang genauso groß wie am Ende. Ebenso haben die Ströme am Anfang und am Ende den gleichen Wert.

Abbildung 138: Ausschnitt aus Stromkreis

Werden Wechselspannungen angelegt, können die folgenden Effekte nachgewiesen werden:



- ➊ Der Strom durch einen Leiter erzeugt ein Magnetfeld um den Leiter.
- ➋ Die Spannung zwischen den Leitern erzeugt ein elektrisches Feld

Abbildung 139: Magnetisches und elektrisches Feld

8.3 - Ersatzschaltbild

Für ein Ersatzschaltbild ergeben sich damit folgende Komponenten

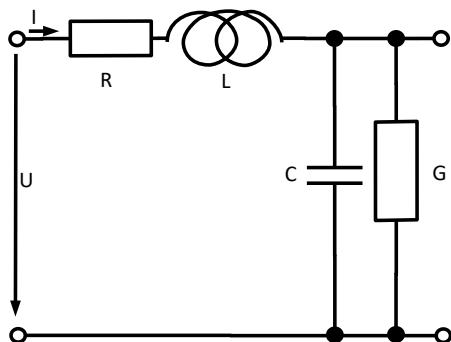


Abbildung 140: Leitungs-Ersatzschaltbild

- R = Widerstand Der Leiter ist normalerweise keine Supraleitung und hat somit einen Widerstand.
- G = Ableitung Die Isolation zwischen den Leitern hat zwar einen hohen Widerstandswert, sie ist jedoch nicht unendlich groß.
- L = Induktivität Ein stromdurchflossener Leiter erzeugt ein Magnetfeld.
- C = Kapazität Das elektrische Feld zwischen zwei Leitern wirkt wie ein Kondensator.

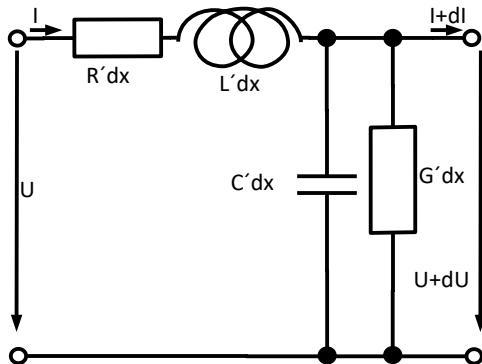
Bezieht man die Einheiten auf eine Leitung der Länge s bekommt man die so genannten Leitungsbeläge.

- $R' = R_s / s$ = Widerstandsbelag = Widerstand pro Länge
- $G' = G_s / s$ = Ableitungsbelag = Ableitung pro Länge
- $L' = L_s / s$ = Induktivitätsbelag = Induktivität pro Länge
- $C' = C_s / s$ = Kapazitätsbelag = Kapazität pro Länge

Eine Leitung ist homogen wenn alle Beläge längs der Leitung bezüglich der Zeit konstant sind. (Nicht bezogen auf die Frequenz!)

8.4 - Wellenwiderstand

Betrachtet man beim Ersatzschaltbild einen Leitungsabschnitt der Länge dx bekommt das Ersatzschaltbild folgendes Aussehen



Hierbei unterscheiden sich die Spannung und der Strom zwischen Anfang und Ende der Leitung

Es gibt einen Spannungsabfall am komplexen Längswiderstand ($R' + j\omega L'$)s und einen Strom durch den komplexen Querleitwert ($G' + j\omega C'$)s

Abbildung 141: Ermittlung des Wellenwiderstandes

Daraus ergeben sich für die Spannung und den Strom folgende Formeln:

$$U = I(R' + j\omega L')dx + U + dU \quad (51)$$

$$I = (U + dU)(G' + j\omega C')dx + I + dI \quad (52)$$

Bzw.

$$\frac{dU}{dx} = -I(R' + j\omega L') \quad (53)$$

$$\frac{dI}{dx} = -U(G' + j\omega C') \quad (54)$$

Wird (1) nach x differenziert und dI/dx aus (2) eingesetzt erhält man eine Differenzialgleichung 2. Ordnung

$$\frac{d^2U}{dx^2} = (R' + j\omega L') \cdot (G' + j\omega C') \cdot U \quad (55)$$

Lösen kann man diese Gleichung durch Integrieren mit dem folgenden Ansatz

$$U = a \cdot e^{yx} \quad (56)$$

Durch Einsetzen von (4) in (3) erhält man die Ausbreitungskonstante y :

$$y^2 = (R' + j\omega L') \cdot (G' + j\omega C') \quad (57)$$

bzw.

$$y = \pm \sqrt{(R' + j\omega L') \cdot (G' + j\omega C')} \quad (58)$$

Daraus folgen zwei Lösungen für die Abhängigkeit der Spannung mit dem Abstand x vom Leitungsanfang

$$U = a_1 e^{-yx} + a_2 e^{yx} \quad (59)$$

Die Stromstärke kann mit

$$I = -\frac{1}{R' j\omega C'} \cdot \frac{dU}{dx} \quad (60)$$

unter Berücksichtigung von (5) unter Beachtung des Abstandes x vom Leitungsanfang ermittelt werden

$$I = a \frac{1}{Zw} \cdot e^{-yx} - a \frac{2}{Zw} \cdot e^{yx} \quad (61)$$

Leitungstheorie

Daraus lässt sich der Wellenwiderstand Z_w beschreiben, der einem Signal entgegenwirkt.

$$Z_w = \sqrt{\frac{R + j\omega L}{G + j\omega C}} \quad (62)$$

Die komplexe Ausbreitungskonstante γ kann in einen Real- und einen Imaginärteil zerlegt werden.

$$\gamma = \alpha + j\beta \quad (63)$$

Dann wird aus (5)

$$U = a_1 e^{-\gamma \cdot x} + a_2 \cdot e^{\gamma \cdot x} = a_1 \cdot e^{-\alpha x} \cdot e^{-j\beta x} + a_2 \cdot e^{\alpha x} \cdot e^{j\beta x} \quad (64)$$

Der Begriff Welle wird deutlich, wenn man U aus (5) und I aus (6) mit dem Drehfaktor $e^{j\omega t}$ multipliziert.

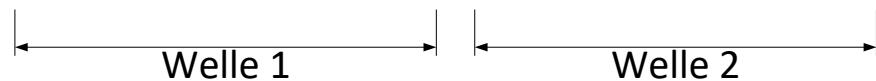
$$U \cdot e^{j\omega t} = a_1 \cdot e^{-\alpha x} \cdot e^{j(\omega t - \beta x)} + a_2 \cdot e^{\alpha x} \cdot e^{j(\omega t + \beta x)} \quad (65)$$

$$I \cdot e^{j\omega t} = \frac{a_1}{Z_w} \cdot e^{-\alpha x} \cdot e^{j(\omega t - \beta x)} + \frac{a_2}{Z_w} \cdot e^{\alpha x} \cdot e^{j(\omega t + \beta x)} \quad (66)$$

Damit gibt es nicht nur eine Abhängigkeit von der Zeit t sondern auch vom Ort x bezogen auf den Leitungsanfang.

Sieht man sich (7) an, kann man sehen, dass sich die Spannung aus 2 überlagerten Wellen ergibt.

$$U \cdot e^{j\omega t} = a_1 \cdot e^{-\alpha x} \cdot e^{j(\omega t - \beta x)} + a_2 \cdot e^{\alpha x} \cdot e^{j(\omega t + \beta x)}$$



Hauptwelle (Welle 1) Ausbreitung in positiver Richtung mit exponentiell abnehmender Amplitude

Reflektierte Welle (Welle 2) Ausbreitung in negativer Richtung mit ebenfalls exponentiell abnehmender Amplitude

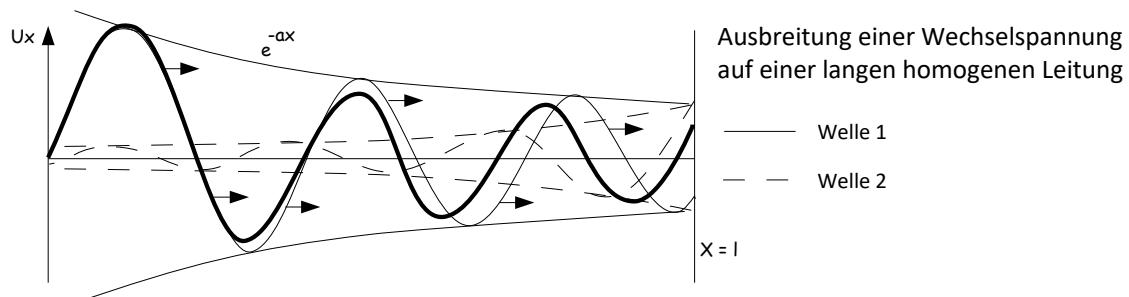
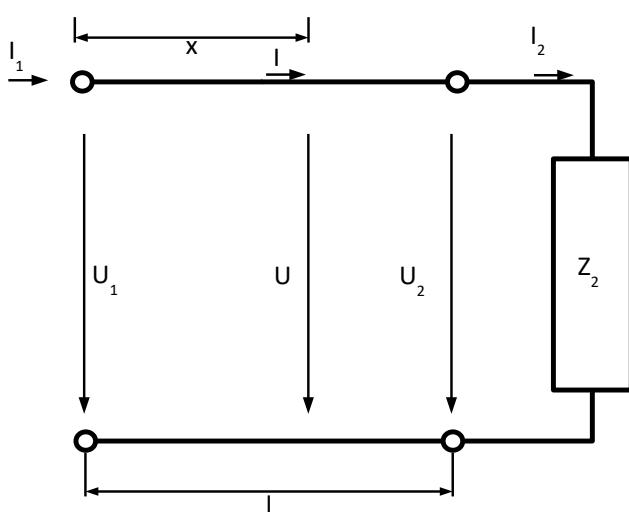


Abbildung 142: Wellenausbreitung

8.5 - Reflexion



Das Entstehen einer reflektierten Welle erklärt sich daraus, dass der am Ende der Leitung angeschlossene Abschlusswiderstand dort ein bestimmtes Verhältnis von Spannung und Strom erzwingt.

Zur Beantwortung der Frage, wie reflektierte Wellen entstehen, kann (5) und (6) in seine Bestandteile, Haupt- und Reflektierte Welle, zerlegt werden.

Abbildung 143: Reflexion

Hauptwelle

$$U_H(x) = U_{H0} e^{-\gamma \cdot x} \quad (67)$$

$$I_H(x) = \frac{U_{H0}}{Z_W} e^{-\gamma \cdot x} \quad (68)$$

Reflektierte Welle

$$U_R(x) = U_{R0} e^{-\gamma \cdot x} \quad (69)$$

$$I_R(x) = \frac{U_{R0}}{Z_W} e^{-\gamma \cdot x} \quad (70)$$

Somit erhält man für das Ende der Leitung ($x = l$)

$$U_2 = I_2 \cdot Z_2 = U_H(l) + U_R(l) \quad (71)$$

$$\frac{I_2}{I} = \frac{\frac{U_H(l)}{Z_w} - \frac{U_R(l)}{Z_w}}{1} \quad (72)$$

$$\frac{U_R(l)}{U(l)} = \frac{\frac{U_H(l)}{Z_w} - \frac{U_R(l)}{Z_w}}{\frac{U_H(l)}{Z_w} + \frac{U_R(l)}{Z_w}} \cdot \frac{Z_w}{2} \quad (73)$$

Nach U_R aufgelöst

$$\frac{U_R(l)}{U(l)} = \frac{Z_w - Z_H}{Z_w + Z_H} = r \quad (74)$$

Damit wird der Reflexionsfaktor r

$$r = \frac{Z_w - Z_H}{Z_w + Z_H} \quad (75)$$

Hier lassen sich drei wichtige Sonderfälle feststellen:

1. Anpassung bei $Z_2 = Z_w$
Hier **verschwindet** die Welle
2. Kurzschluss bei $Z_2 = 0$
Hier wird die Welle mit **umgekehrter** Polarität reflektiert $U_R = -U_H$
3. Leerlauf bei $Z_2 = \infty$
Hier wird die Welle mit der **selben** Polarität reflektiert $U_R = U_H$

8.6 - Ausbreitungsgeschwindigkeit

Bei hohen Frequenzen ($f > 1\text{MHz}$) und kurzen Leitungen können Widerstände und Ableitwerte vernachlässigt werden. Somit werden $R' = 0$ und $G' = 0$.

Die Ausbreitungskonstante γ ergibt sich zu:

$$\gamma = \alpha + j\beta = \sqrt{(R' + j\omega L')(G' + j\omega C')} \quad (76)$$

Hierbei ist α die Dämpfungskonstante und β die Phasenkonstante.

Durch $R' = 0$ und $G' = 0$ entsteht.

$$\gamma = \alpha + j\beta = \sqrt{j\omega L' j\omega C'} \approx j\omega \sqrt{L' C'} \quad (77)$$

Die Phasenkonstante β ergibt sich mit

$$\beta = \omega \sqrt{L' C'} \quad (78)$$

Die Ausbreitungsgeschwindigkeit v ist:

$$v = \frac{\omega}{\beta} = \frac{1}{\sqrt{L' C'}} \quad (79)$$

Damit kann die Laufzeit $T_D = l/v = \beta l/\omega$ mit:

$$T_D = \sqrt{L' C'} \cdot l \quad (80)$$

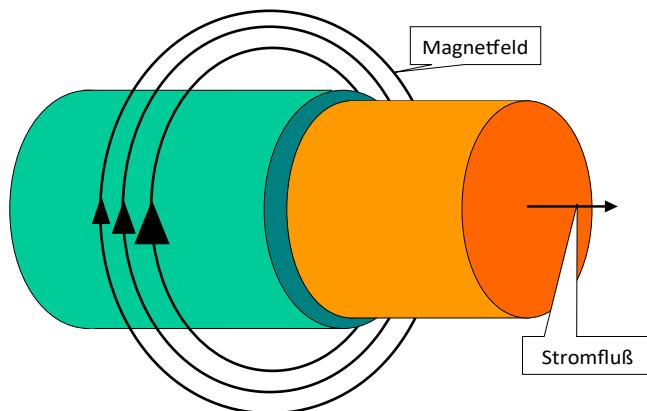
errechnet werden.

Die Ausbreitungsgeschwindigkeit einer Welle im Leiter beträgt ca. 2/3 der Lichtgeschwindigkeit c im Vakuum.

$c = 299792 \text{ km/s}$

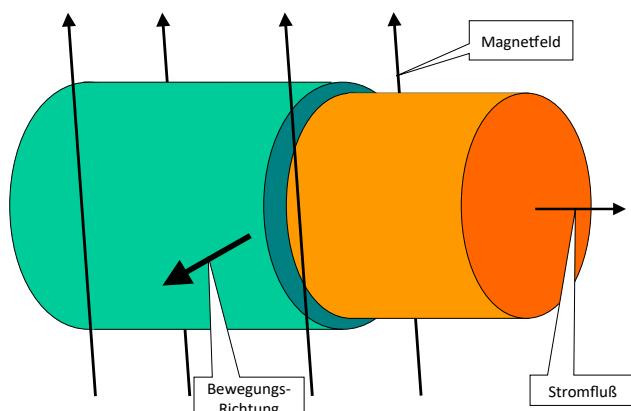
9 - Leitungsmessungen

Um all die möglichen Messwerte der Verkabelungstechnik zu verstehen, sind einige Grundlagen zu klären. Vor allem die Zusammenhänge zwischen stromdurchflossenen Leitern und Magnetismus, sind für viele Kennwerte zuständig.



Ein stromdurchflossener Leiter erzeugt um sich herum, auf seiner gesamten Länge, ein Magnetfeld. In der linken Abbildung ist dargestellt, wie das Magnetfeld um einen Leiter herum aufgebaut wird.

Abbildung 144: Magnetfeld um Leiter



Die nächste Abbildung zeigt, den umgekehrten Vorgang. Ein Leiter, der durch ein Magnetfeld bewegt wird, induziert eine Spannung. Diese Spannung, hat einen Strom im Leiter zur Folge.

Wird an einen Leiter eine Wechselspannung angelegt, resultiert daraus ebenso ein wechselndes Magnetfeld. Ein ständig auf und abgebautes Magnetfeld, kann die Bewegung des Leiters ersetzen.

Das von einem Strom durchflossenen Leiter erzeugte Magnetfeld, beeinflusst somit durch die Induktion wiederum anderer, in der Nähe liegende, Leiter.

Dieser Effekt wird in einem Transformator für die Umsetzung von Spannungen ausgenutzt. Bei den Leitungen hat dieser Effekt einen störenden Einfluss.

Abbildung 145: Induktion

Grundsätzlich bestehen bei den Twisted-Pair-Kabeln Unterschiede im Dämpfungsverhalten und im Nah-Nebensprechen (NEXT; engl. Near End Crosstalk) sowie im Störabstand (engl. SNR (Signal to Noise Ratio))

9.1 - Link-Definitionen

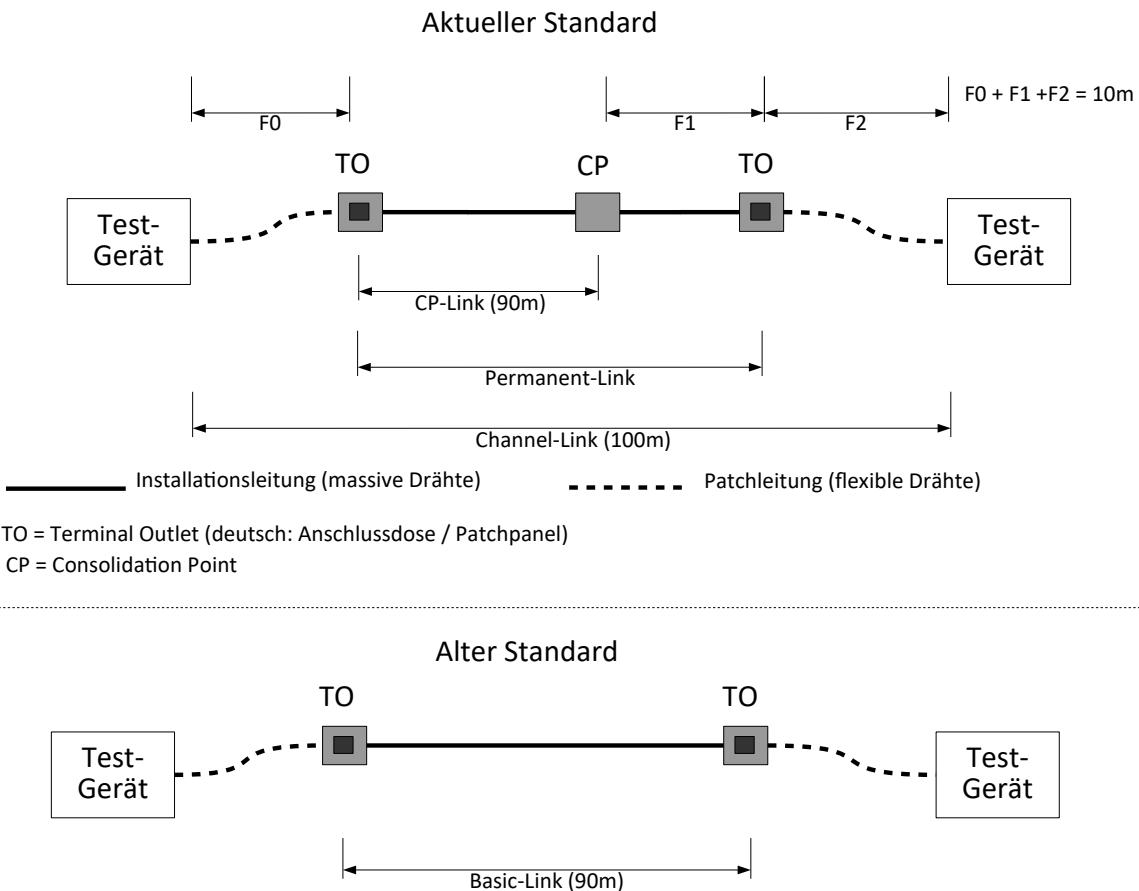


Abbildung 146: Link-Definitionen

Um ein Verkabelungssystem auszumessen, muss zuvor bestimmt werden, welche Teile in die Messung eingehen sollen.

Je nach dem ob der Permanent- oder der Channel-Link gemessen werden soll, ist an den Testgeräten ein kalibriertes Patchkabel im Messadapter integriert oder nicht.

Wird der Permanent-Link gemessen wird ein Messadapter mit kalibrierter Messleitung bis zur Dose verwendet.

9.2 - Messungen bei Twisted Pair-Leitungen

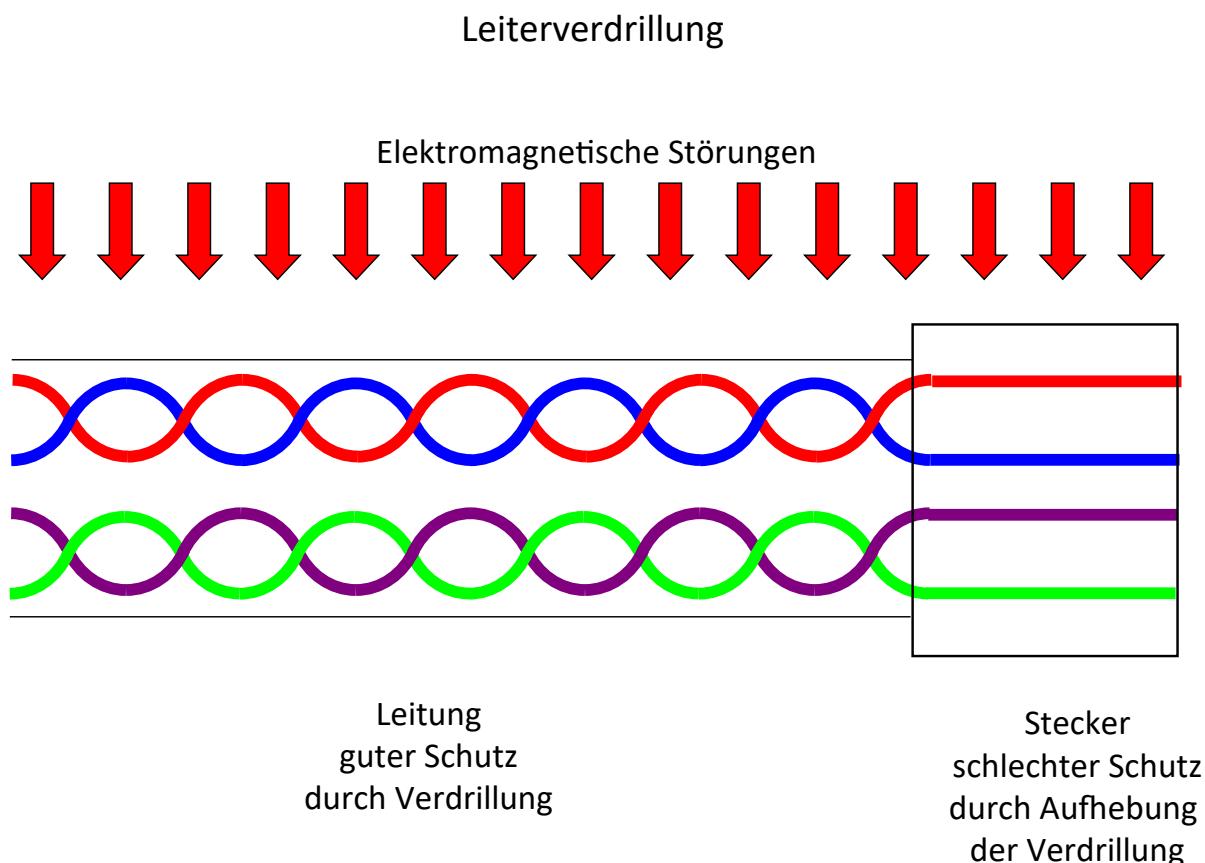


Abbildung 147: Wirkprinzip der Twisted-Pair-Leitungen

Induzierte Störungen heben sich im Verlauf einer Verdrillung auf da sie von zwei Seiten auf die Leiter einwirken. Solange die Leitung verdrillt entstehen kaum Störungen. Nur da, wo die Verdrillung aufgehoben ist, also am Stecker, werden Spannungen (also Störungen) induziert.

9.3 - NEXT, FEXT

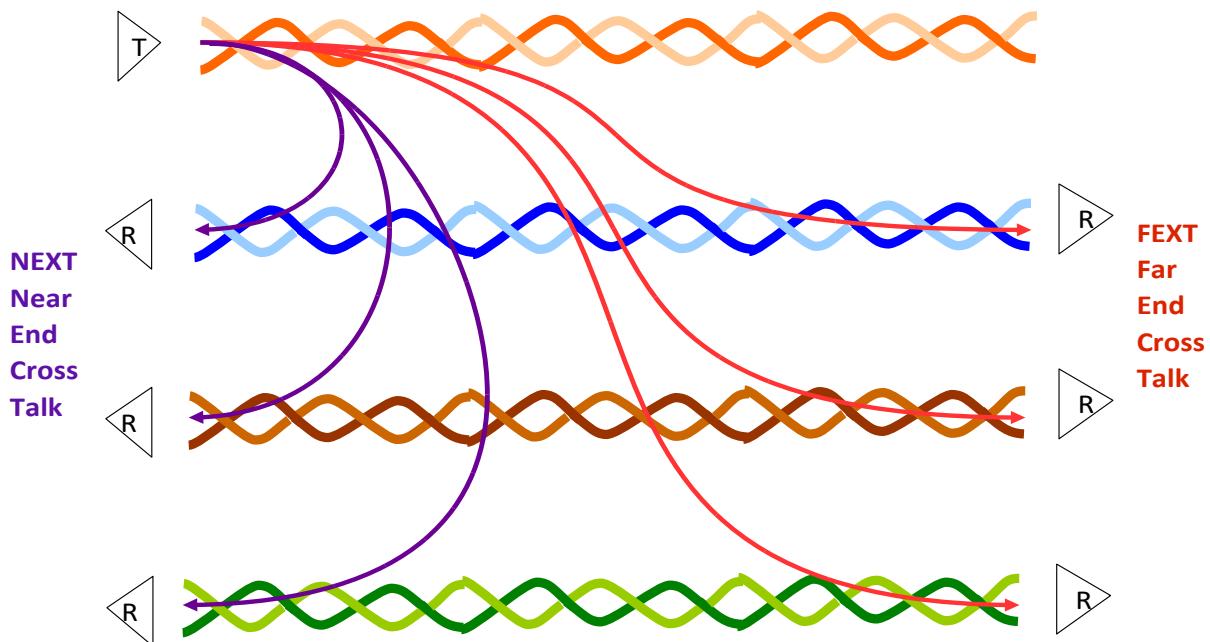


Abbildung 148: NEXT / FEXT

In der obigen Abbildung wird die Bedeutung der Störungssignale NEXT und FEXT erläutert. Auf der linken Seite, ist die nahe gelegene Mess- und Signal-Seite. Auf der rechten Seite, ist die entfernt gelegene Mess-Seite. Die Enden der entfernten Paare werden mit dem Wellenwiderstand abgeschlossen.

Das auf der linken, nahen Seite erzeugte Störsignal heißt auf der linken Seite Nah-Nebensprechen (engl: NEXT (Near End Crosstalk)).

Das an der rechten, fernen Seite gemessene Störsignal, heißt Fern-Nebensprechen (engl: FEXT (Far End Crosstalk)).

NEXT und FEXT wird als Verhältnis von Originalsignal und induziertem Störsignal in Dezibel (db) angegeben. Je größer der Wert in dB, desto besser ist die Leitung. Bei einer Kabellänge von 100 Metern sollte der Wert für das Nah-Nebensprechen bei mindestens -32dB liegen.

Jeweils -6dB entspricht einer Verdopplung der Signal-Abschwächung.

$$NEXT = 20 \cdot \log UT / UR \quad (81)$$

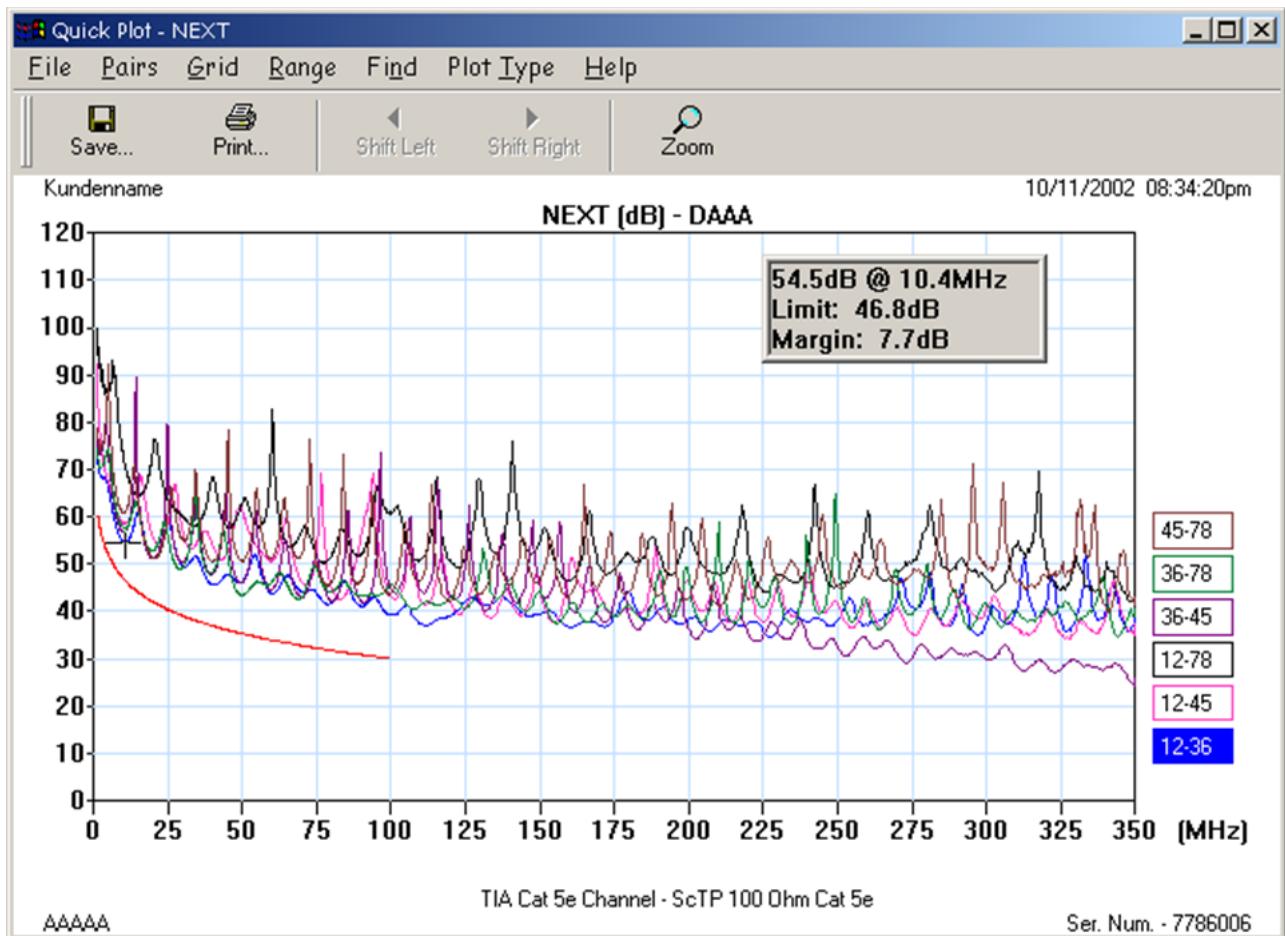


Abbildung 149: NEXT-Messung

Bei der NEXT- und FEXT-Messung werden die 4 Adernpaare gegeneinander verglichen. Die Adernpaare werden so nummeriert, wie sie bei einem RJ-45 Stecker aufgelegt werden.

Adernpaare:

- 1-2
- 3-6
- 4-5
- 7-8

Dies bedeutet, dass 6 Messungen notwendig sind:

- 1,2 – 3,6
- 1,2 – 4,5
- 1,2 – 7,8
- 3,6 – 4,5
- 3,6 - 7,8
- 4,5 – 7,8

Leitungsmessungen

In der obigen Abbildung sind die 6 Messverläufe über der Grenzwertlinie dargestellt. Liegen die Verläufe über der Grenzwertlinie, sind die Messwerte „ok“. Lägen sie darunter, würde für diese Messung ein „FAULT“ ausgegeben werden. Da ein CAT5e-Channel nur bis 100MHz definiert ist, hört die Grenzwertlinie bei 100MHz auf. Je größer der db-Wert, desto größer ist der Unterschied zwischen dem gesendeten Nutzsignal und dem empfangenen Störsignal.

9.4 - SNR

(deutsch: Störabstand)

Der Störabstand (SNR; engl Signal to noise ratio; deutsch: Signal zu Rauschen Verhältnis) ist der Abstand des Signal-Spannungspegels im Verhältnis zum Störsignalpegel. SNR berücksichtigt alle Störungen, sowohl durch Übersprechen erzeugten Störungen, als auch die, die von außen auf eine Leitung einwirken.

Vom Störabstand hängt die Empfindlichkeit des Empfängers ab. Damit lässt sich die Qualität eines Übertragungskanals beschreiben. Daraus resultiert auch die Reichweite und die Fehlerrate der Datenübertragung. Der SNR-Wert ist von der Frequenz abhängig.

$$SNR(f) = NEXT(f) - a_{ges}(f) \quad (82)$$

SNR kann durch Messung ermittelt werden:

$$SNR [dB] = 10 \log(P_T / P_{Rausch}) \quad (83)$$

oder

$$SNR [dB] = 20 \log(U_T / U_{Rausch}) \quad (84)$$

9.5 - BER Bit Error Rate

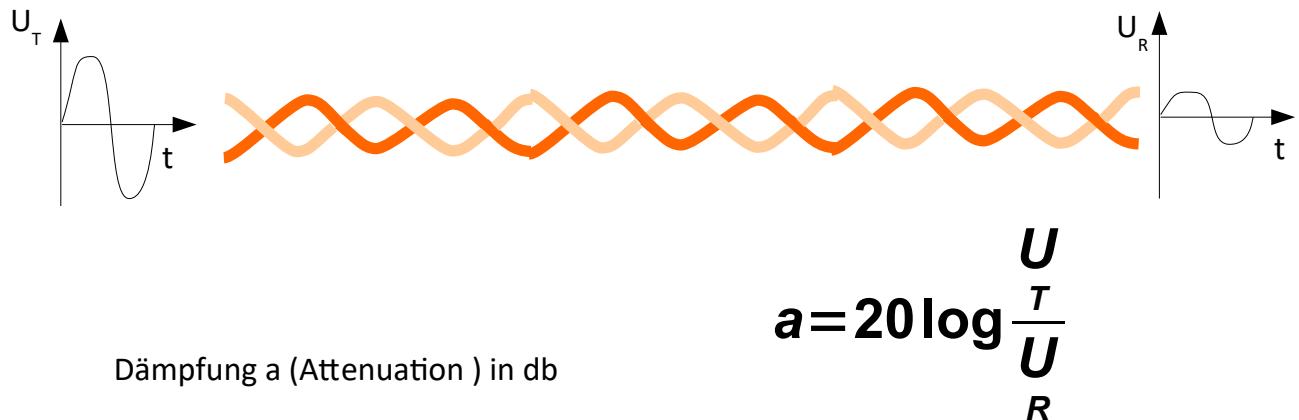
(deutsch Bitfehlerrate)

Dabei werden die Anzahl der richtig übertragenen Bits, mit der Anzahl der fehlerhaft übertragenen Bits verglichen. Die BER ist bei der Übertragung von Daten direkt vom SNR abhängig. Je größer das SNR ist, desto kleiner ist die BER.

9.6 - Dämpfung

Die Signal-Dämpfung (a, vom englischen attenuation) nimmt mit zunehmender Frequenz des übertragenen Signals zu. Neuere Standards verwenden den Begriff Einfügedämpfung (engl. Insertion Loss).

Bei der Messung wird die Signalamplitude an der Eingangsseite mit der Signalamplitude an der Ausgangsseite verglichen. Die Darstellung erfolgt in db.



Verhältnis U_R / U_T	Dezibel
1	0
$1 / 2$	-6
$1 / 4$	-12
$1 / 5$	-14
$1 / 10$	-20
$1 / 20$	-26

Verwendet wird der absolute Betrag

Abbildung 150: Dämpfung / attenuation

Die Messung wird für jedes Paar getrennt durchgeführt. Damit erhält man für den Messvorgang 4 Messverläufe.

Leistungsmessungen

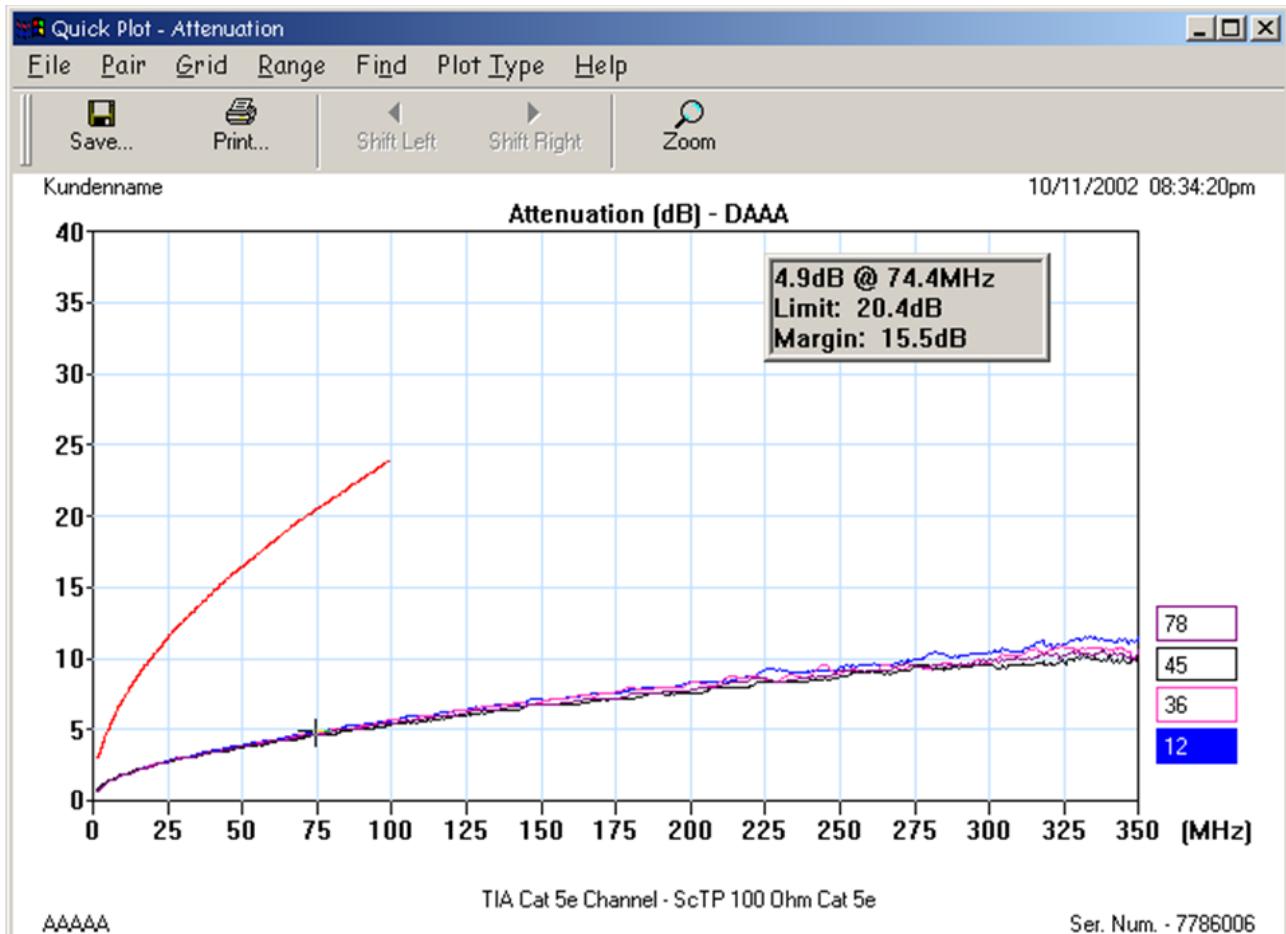


Abbildung 151: Dämpfungsmessung

Die obere kurze Linie bedeutet den Grenzwert, den die Messverläufe nicht überschreiten dürfen. Da ein CAT5e-Channel nur bis 100MHz definiert ist, hört die Grenzwertlinie bei 100MHz auf.

Je kleiner der Dämpfungswert in db, desto besser , da große Werte einen großen Verlust des Signals auf der Leitung bedeuten.

Hier liegt auch der Grund für die Begrenzung einer Twisted-Pair-Leitung auf maximal 100m.

Wird anstelle des Spannungspegels die Leistung als zu vergleichende Messgröße verwendet, ergibt sich folgende Formel:

$$a[\text{dB}] = 10 * \log P_T / P_R \quad (85)$$

In der folgenden Abbildung ist dies dargestellt. D. h. je größer die Frequenz auf der Leitung ist, desto kürzer ist die mögliche Leitungslänge! Bei einer Länge des Kabels von 100 Metern sollte eine Signal-Dämpfung von 22 db nicht überschritten werden.

Um dem Verbraucher Qualitätsunterschiede bzw. Einsatzgebiete von verdrillten Kupferkabeln an die Hand zu geben, wurden Kategorien für Kabel definiert. Siehe auch Leitungsklassen.

9.7 - ACR

Das Verhältnis von Dämpfung und Nah-Nebensprechen wird als ACR (attenuation to crosstalk Ratio; deutsch: Dämpfungs-zu-Nebensprechen Verhältnis) bezeichnet und gibt einen sehr guten Wert für die Leitungsqualität.

Im Gegensatz zum SNR berücksichtigt das ACR die Störungen, die innerhalb derselben Leitung durch Übersprechen der anderen Adernpaare entstehen.

Das ACR wird nicht gemessen, sondern aus der NEXT- und Dämpfungsmessung berechnet. Das ACR wird wie die Dämpfung und das Nebensprechen in db angegeben und folgendermaßen berechnet:

$$ACR[db] = NEXT[db] - a[db] \quad (86)$$

Als Verhältnis (ohne db):

$$ACR = NEXT/a \quad (87)$$

Der ACR-Wert darf nicht mit dem SNR verwechselt werden.

In der folgenden Abbildung ist zu erkennen, dass sowohl die Dämpfungs- als auch die NEXT-Werte mit zunehmender Frequenz schlechter werden. D. h. je größer die Frequenz auf der Leitung ist, desto kürzer ist die mögliche Leitungslänge!

Um dem Verbraucher Qualitätsunterschiede bzw. Einsatzgebiete von verdrillten Kupferkabeln an die Hand zu geben, wurden Kategorien für Kabel definiert. Siehe auch Leitungsklassen. Für die einzelnen Kategorien sind in der folgenden Abbildung die Grenzwert-Verläufe dargestellt. Je nach Kategorie enden die Grenzwerte bei der Grenzfrequenz für welche die Kategorie ausgelegt ist.

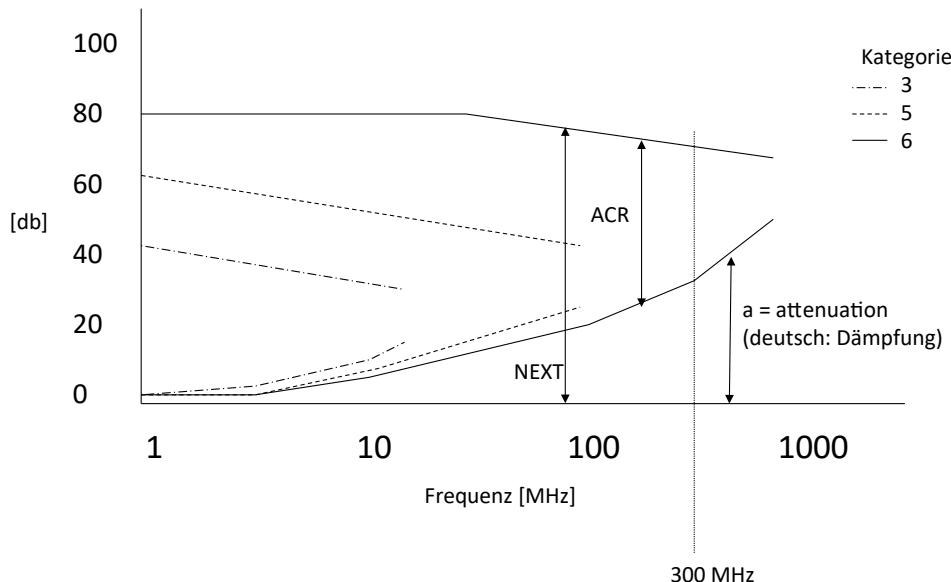


Abbildung 152: a, NEXT, ACR

In der obigen Abbildung kann man erkennen, dass ein möglichst großer ACR-Wert anzustreben ist.

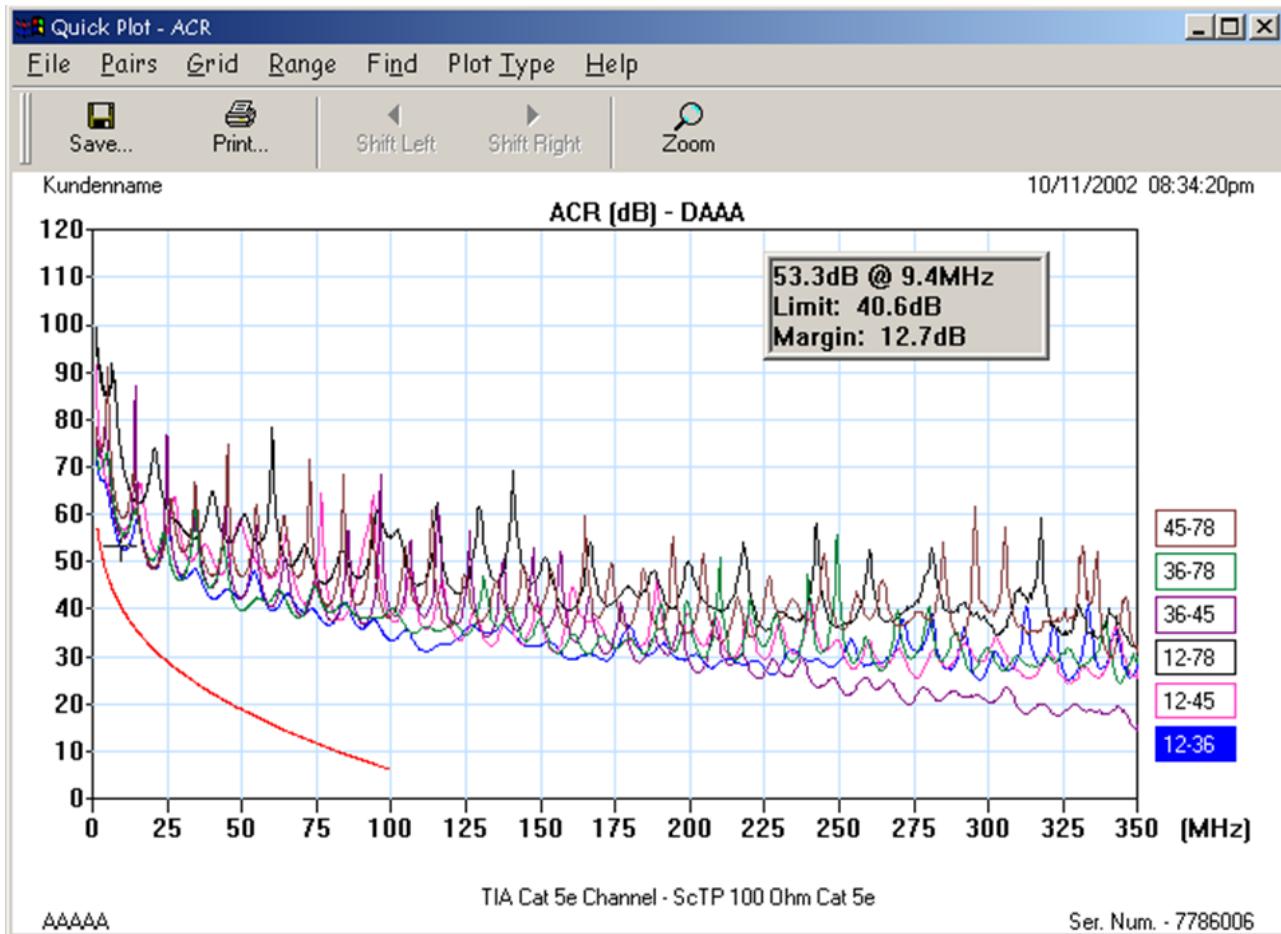
Leistungsmessungen

Abbildung 153: ACR-Messung

Da bei der ACR-Ermittlung die NEXT Messungen mit berechnet werden, sind hier wiederum 6 Messverläufe zu sehen. Die kurze, untere Kurve (bis 100MHz) stellt den Grenzwert dar, der von allen Verläufen zu überbieten ist.

9.8 - PSNEXT (Power Sum NEXT), PSFEXT (Power Sum FEXT)

Hierbei geht es nicht um Messungen sondern, wie beim ACR, um Berechnungen. Es werden die Summen aller NEXT / FEXT-Leistungsmessungen, die auf einen Leiter einwirken, addiert.

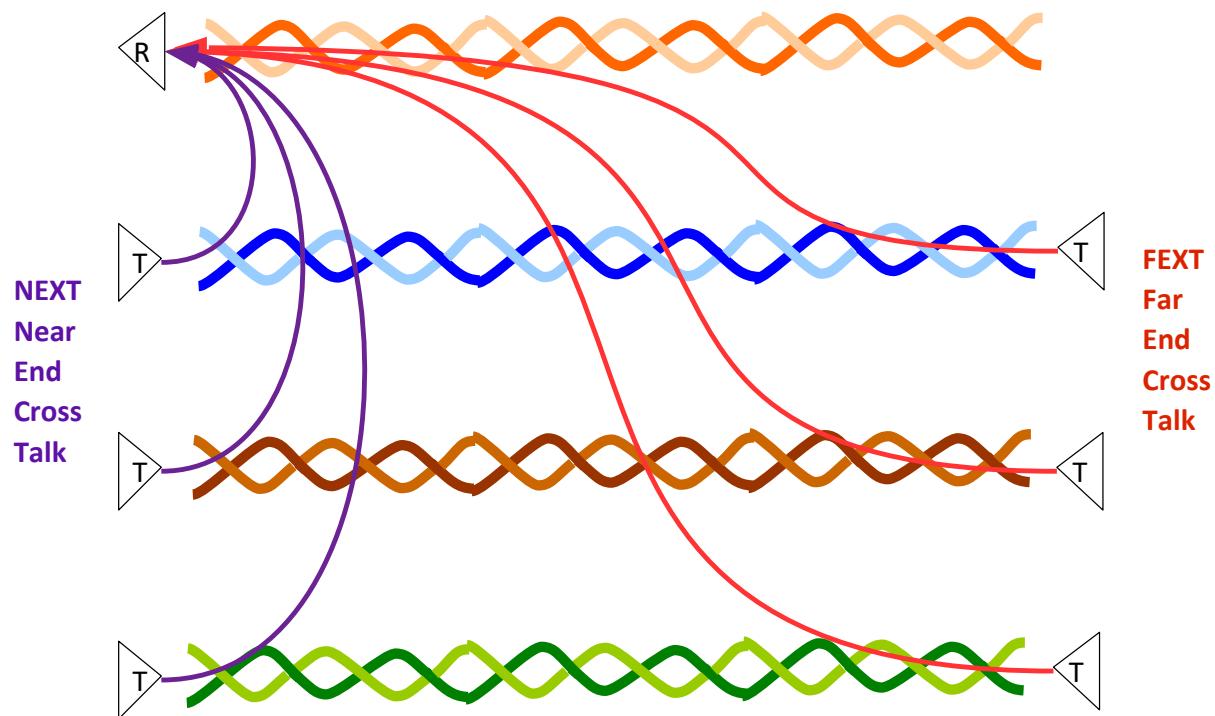


Abbildung 154: PSNEXT / PSFEXT

9.9 - PSACR (Power Sum ACR)

Dies ist keine Messung, sondern eine Addition der 4 möglichen ACR-Werte einer 4-Paarigen Leitung. Wie bei den ACR-Werten ist ein möglichst großer PSACR-Wert anzustreben.

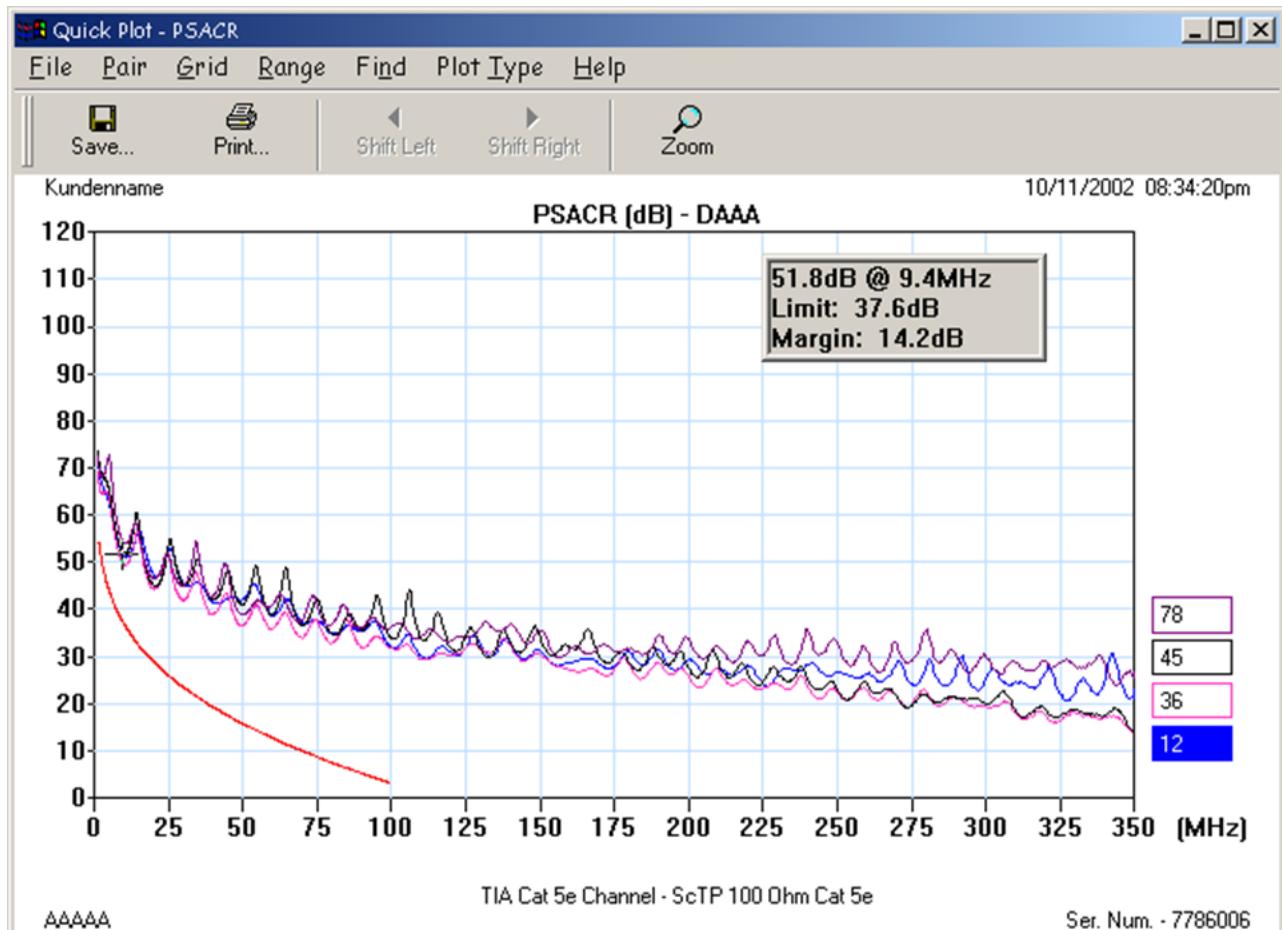


Abbildung 155: PSACR-Messung

9.10 - ELFEXT (Equalized Level FEXT)

(deutsch: Niveaugleiches Fern-Nebensprechen))

Hierbei wird das Verhältnis des übersprechenden Ausgangssignals zu eigentlichen Ausgangssignal ermittelt. Bei diesem Test wird für jedes Paar das Verhältnis zwischen FEXT und Dämpfung ermittelt.

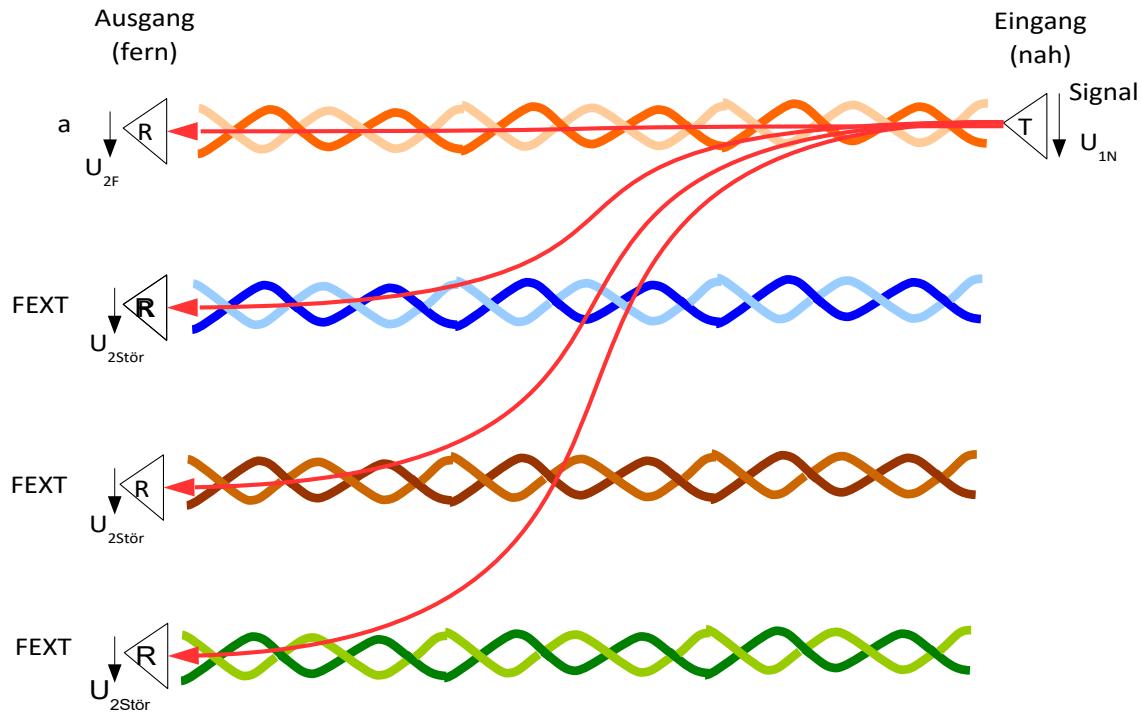


Abbildung 156: ELFEXT

Dazu wird am fernen Ende ein Signal auf ein Adernpaar gelegt. Am gleichen Adernpaar wird am anderen Ende der Dämpfungswert ermittelt. Der FEXT-Wert wird danach bei allen anderen Adernpaaren ermittelt.

Danach wird die Differenz zwischen den gemessenen FEXT-Werten (möglichst großer dB-Wert) und den Dämpfungsmessungen (möglichst kleiner dB-Wert) errechnet. Dabei gilt:

$$\text{ELFEXT [db]} = \text{FEXT [db]} - a [\text{db}] \text{ oder } \text{ELFEXT [db]} = |20 * \log(U_{2\text{Stör}} / U_{2F})| \quad (88)$$

Dies bedeutet, dass ein möglichst großer Wert anzustreben ist. Da sowohl die Dämpfung als auch das Nebensprechen von der gleichen Leitungslänge beeinflusst werden ist der Wert von der Leitungslänge unabhängig. Da diese Berechnung, wie bei der ACR-Berechnung vorgenommen wird kann beim ELFEXT auch von einem Far End-ACR gesprochen werden.

ELFEXT ist nicht wichtig für 10BaseT oder 10BaseTX, da hierbei nur jeweils ein Paar für den Datentransport in eine Richtung notwendig ist. Hier sind die ACR-Werte wichtig. Z. B. bei 1000Base-T werden allerdings die Signale auf allen 4 Adernpaaren transportiert. Dies führt dazu, dass entweder eine niedrigere Frequenz auf den Adernpaaren ausreicht (und alte Technik weiterhin verwendet werden kann) oder höhere Datenraten übertragen werden können.

9.11 - PSELFEXT (Power Sum ELFEXT)

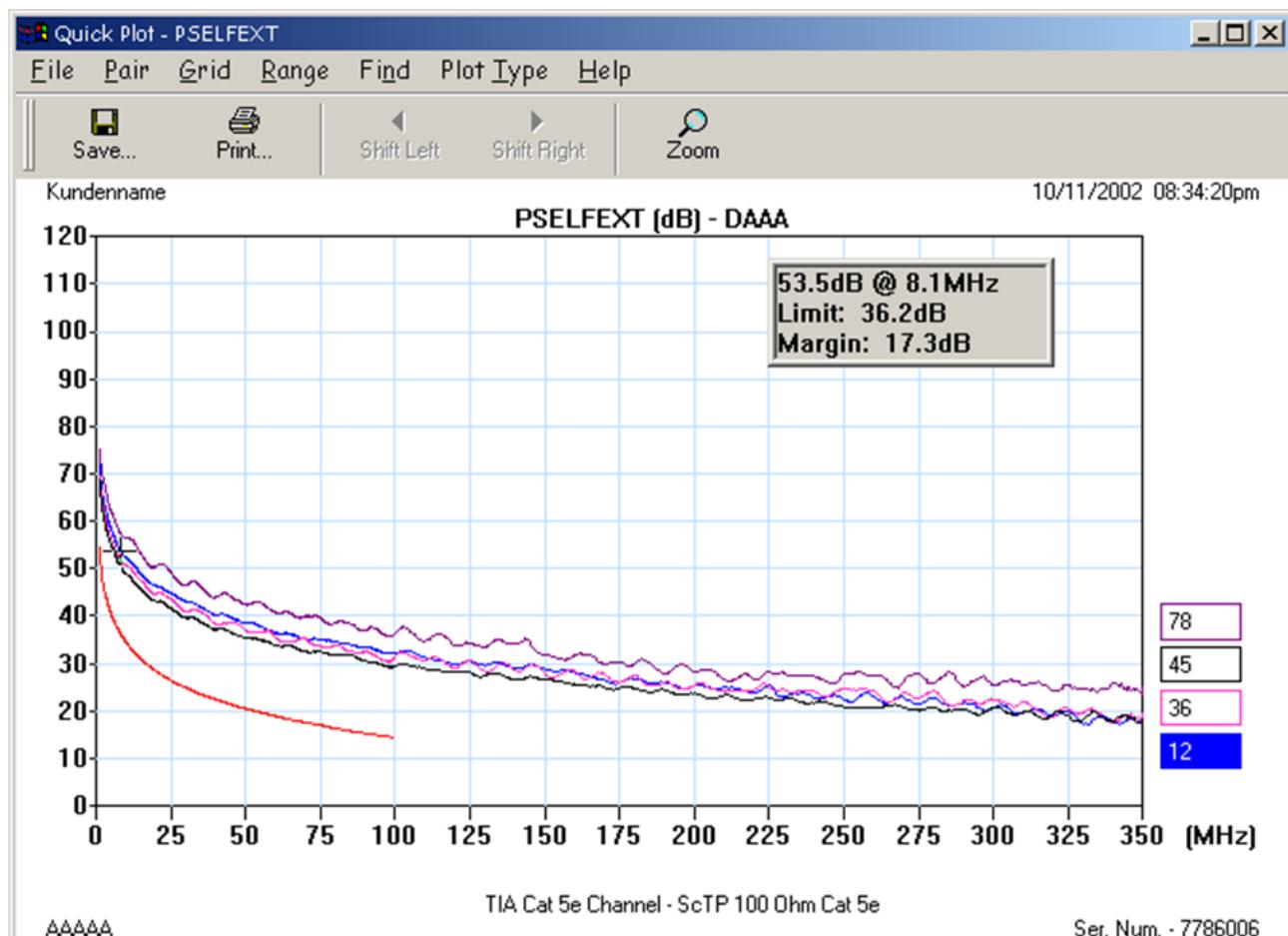


Abbildung 157: PSELFEXT-Messung

PSELFEXT ist eine Berechnung. Es werden für jedes Paar die ELFEXT-Werte, die über die restlichen 3 Paare ermittelt werden addiert. Somit gibt es für eine 4-Paarige Leitung 4 PSELFEXT-Werte.

9.12 - Propagation Delay

(deutsch: Ausbreitungs / Übertragungs-Verzögerung)

Der Grund dafür sind die Induktivitäts- und Kapazitäts-Beläge in der Leitung. Die NVP (Nominal Velocity of propagation (deutsch: Nenn-Ausbreitungs-Geschwindigkeit)) wird für jedes Adernpaar in Nanosekunden ermittelt. Sie ist die Grundlage für eine Längenmessung einer Leitung. Ist die NVP bekannt kann durch die Laufzeit eines Signals von einem Ende zum anderen die Länge ermittelt werden. Außerdem kann für die Erkennung von Leitungsdefekten dieses Verfahren herangezogen werden.



Abbildung 158: Propagation Delay

Die Verzögerung ist der Hauptgrund für die Längenbegrenzung über mehrere Segmente in Netzwerken. Natürlich haben nicht nur die Leitungen sondern auch die Netzwerkgeräte hierbei einen großen Einfluss. Alle Leitungen innerhalb einer strukturierten Verkabelung haben ein NVP von 0,6c bis 0,9c. Dabei ist c die Lichtgeschwindigkeit (299792km/s).

9.13 - Propagation Delay Skew

(deutsch: Ausbreitungs- / Übertragungs-Verzögerungs-Verzerrung)

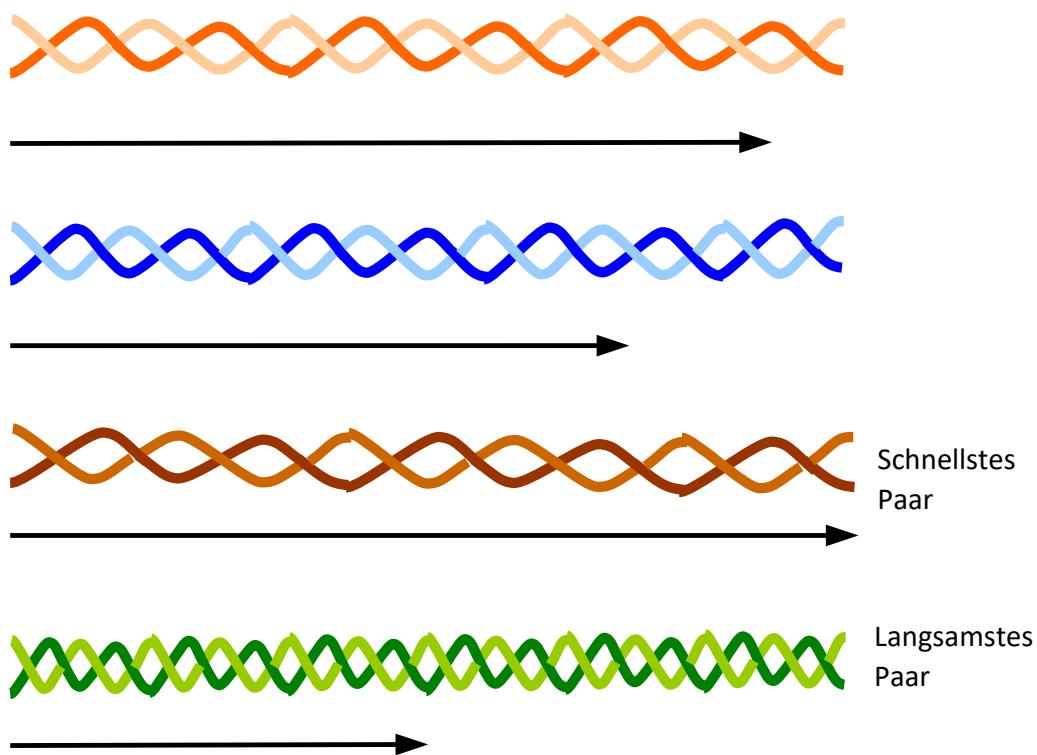


Abbildung 159: Propagation Delay-Skew

Werden Signale auf mehreren Paaren gleichzeitig gesendet, ist es wichtig, dass sie möglichst gleichzeitig ankommen. Durch Unterschiede in der Verdrillung ist hier eine Streuung bei den Laufzeiten festzustellen. Möglichst kleine Unterschiede sind anzustreben. Bei einer Messung einer 4 paarigen Leitung werden 4 Messwerte ermittelt. Das Paar mit der kürzesten Laufzeit hat den Wert 0 μs .

9.14 - HDTDR (High Definition Time Domain Reflectometry)

Damit kann die Länge, sowie der Wellenwiderstand entlang einer Leitung, ermittelt werden. Es wird von einem Testgerät ein kurzer Impuls von 2 ns auf die Leitung gelegt. Dort wo die Impedanz sich entlang der Leitung ändert, wird die Welle reflektiert.

Besonders am Leitungsende wird, je nach Abschlusswiderstand, die Welle positiv (Leitung offen), negativ (Kurzschluss) oder gar nicht reflektiert (Leitung mit Wellenwiderstand abgeschlossen)

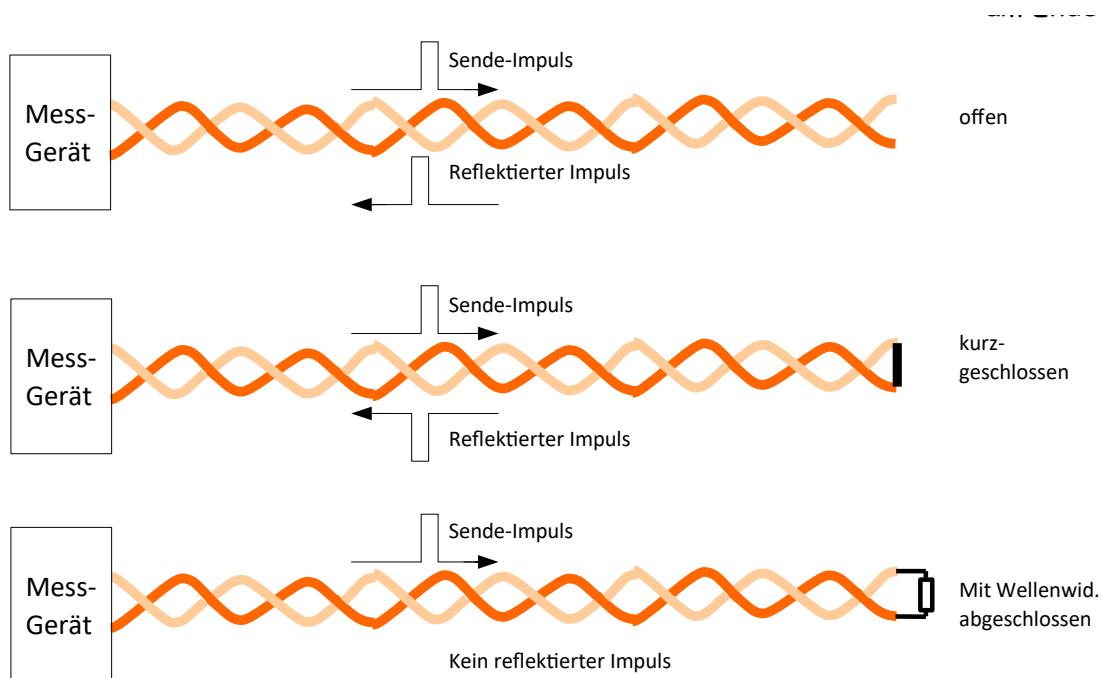


Abbildung 160: HDTDR-Messung

Zur Ermittlung einer Leitungslänge muss die Ausbreitungsgeschwindigkeit der Leitung bekannt sein. Wird am Ende eine Reflexion erzwungen, ist über die Impuls-Laufzeit die Länge ermittelbar.

Stecker oder Leitungsanomalien (Quetschungen) erzeugen ebenfalls Reflexionen.

9.15 - HDTDX (High Definition Time Domain Crosstalk)

Dieses Verfahren dient zum Auffinden der Position an der Nebensprechen in der Leitung auftritt. Die Messung wird von beiden Enden aus durchgeführt um genauere Ergebnisse zu erzielen.

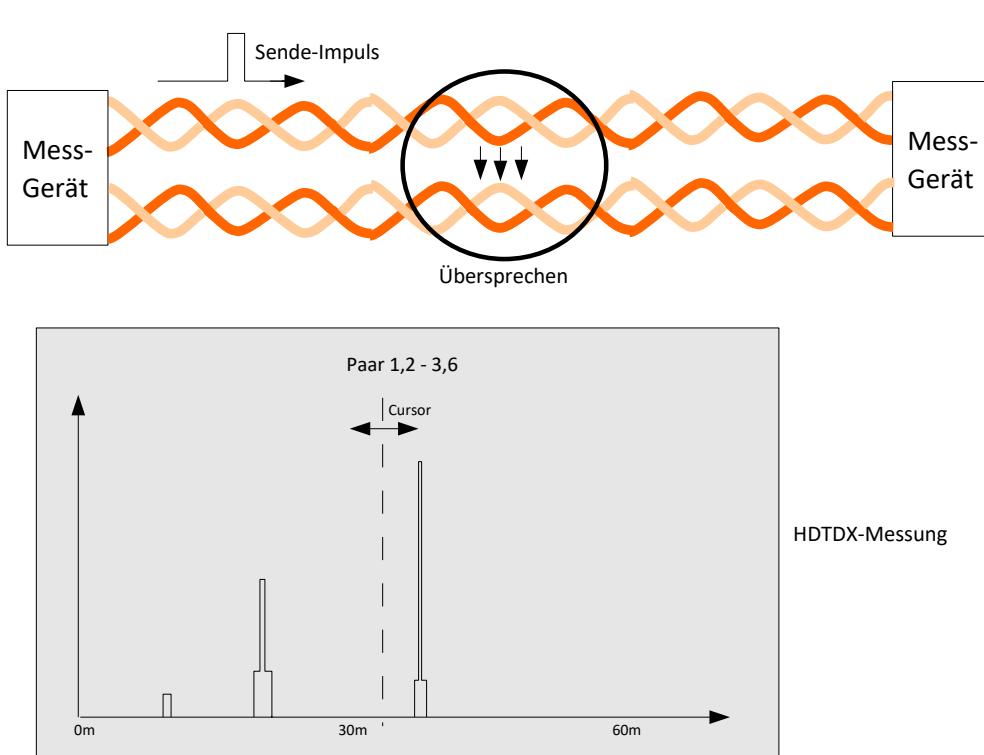


Abbildung 161: HDTDX-Messung

9.16 - Return Loss (RL)

RL ist die Messung aller Reflexionen, die durch Fehlanpassungen der Impedanzen hervorgerufen werden.

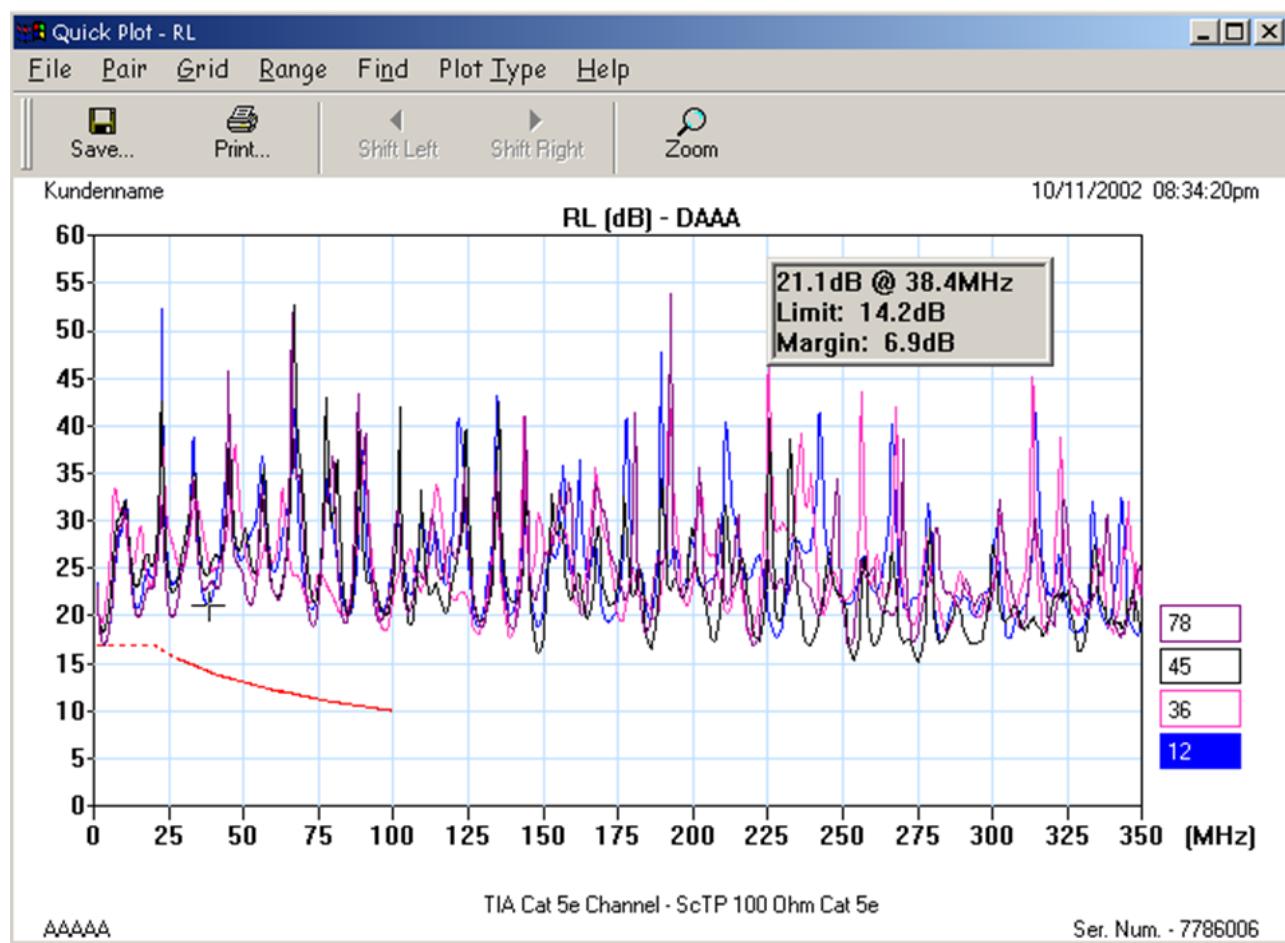


Abbildung 162: RL-Messung

9.17 - DC Loop Resistance

(deutsch: Gleichstrom-Schleifenwiderstand)

Bei dieser Messung wird am fernen Ende ein Kurzschluss angelegt. Danach kann der Gleichstromwiderstand eines Paares gemessen werden. Bei Signalen steht die Dämpfung im Vordergrund.

9.18 - Alien Crosstalk

Nahe aneinander liegende Leitungen in einem Kabelkanal beeinflussen sich auch gegenseitig (Die Beeinflussung der Paare einer Leitung wird mit NEXT- / FEXT-Messungen ermittelt).

Eine solche Konstellation ist nur unter Laborbedingungen nachvollziehbar. Es gibt derzeit keine festgelegten Grenzen für das Nebensprechen über Leitungsgrenzen hinweg.

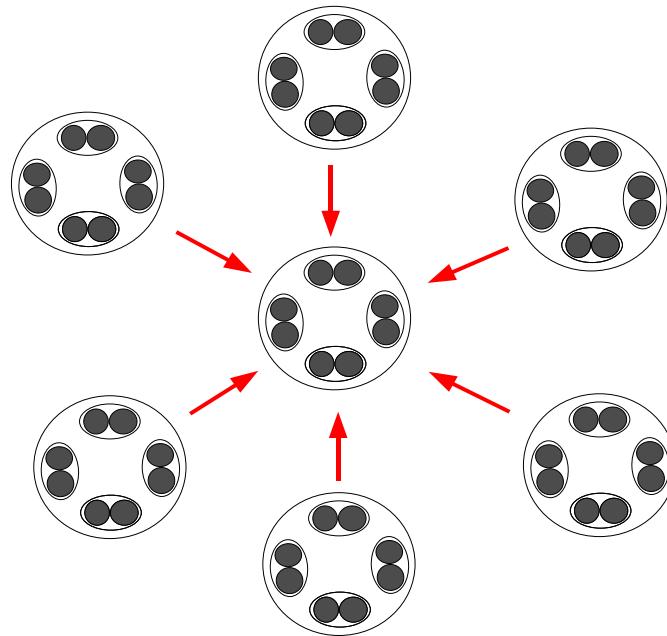


Abbildung 163: Alien-Crosstalk

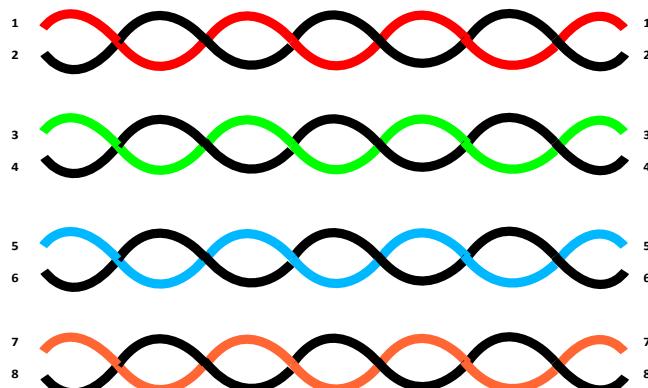
9.19 - Wire-Map-Fehler

Die Reihenfolge, wie die einzelnen Drähte in den Steckern angeschlossen wurden, kann von außen gemessen werden und in einem Verkabelungsplan (engl. Wire Map) dargestellt werden.

Da bei Twisted Pair die Drähte paarweise auf fest zugeordnete Pins aufgelegt werden müssen, können durch Vertauschung Fehler entstehen.

9.19.1 - Split Pairs

Werden die Drähte einfach der Reihe nach, wie sie in der Leitung vorkommen aufgelegt, werden die Paare auseinander gerissen.



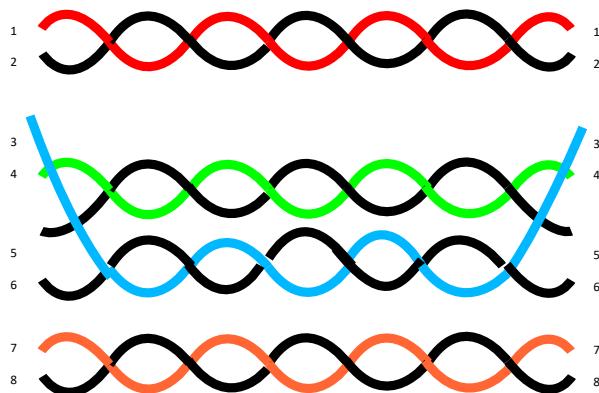
In der linken Darstellung sind die Paare an den Pins 3,4 und 5,6 falsch belegt!

Bei einer geringen Datenrate ist diese Verkabelung unkritisch. Erst bei größeren Datenraten im Full-Duplex-Betrieb wirkt sich der Fehler richtig aus.

Split-Pairs können nur mit einer HDTDX-Messung gefunden werden!

Der Draht am Pin 3 muss mit dem Draht an Pin 6 gepaart werden. Genauso ist der Draht an Pin 4 mit dem Draht an Pin 5 zu paaren. Split Pairs können mit einfachen Wire-Map-Messgeräten nicht gefunden werden da letztendlich die richtigen Pins miteinander verbunden werden

Abbildung 164: Split Pairs bei RJ45-Stecker-Belegung



In der linken Darstellung ist die Verdrahtung richtig durchgeführt.

Abbildung 165: Richtige Verdrahtung bei Twisted Pair-Leitungen mit RJ45-Steckern

9.19.2 - Anwendung unterschiedlicher Normen Normen von EIA/TIA 568

Diese Norm gibt es leider in unterschiedlicher Ausführung mit den Namenserweiterungen A und B.

Wird nun eine Leitung auf der einen Seite nach EIA/TIA 568A und auf der anderen Seite nach EIA/TIA 568B verkabelt. Da der A- und der B-Standard sich in den Paaren welche für Twisted-Pair verwendet werden in der Nummerierung der Paare unterscheidet kann es dazu kommen, dass anstelle einer Straight-Through(1:1) Leitung eine Crossover-Leitung entsteht. Dies führt dazu, dass ein an einen Switch angeschlossener PC nicht funktioniert.

9.19.3 - Kurzschluss und Leitungsunterbrechung

Sowohl ein Kurzschluss, als auch eine Leitungsunterbrechung, kann bei einer einfachen Wire-Map -Messung erkannt werden.

9.20 - Güte / Qualitätseinteilungen von Kabel

9.20.1 - Amerikanischer Ansatz

Alle Einzelkomponenten, wie Leitungen, Stecker, Dosen, Patchfeld usw. werden für sich getestet und einer Kategorie (engl.: Category) zugeordnet. Die Categories werden durchnummiert und Grenzfrequenzen zugeordnet, welche über diese Bauteile noch übertragbar sind.

Category	Grenzfrequenz [MHz]	Anwendung bei
CAT3	10	Telefon / 10 BASET
CAT4	16	Token Ring
CAT5	100	100BASE-TX
CAT6	250	1000BASE-TX
CAT6e	500	10GBASE-T bis 55m
CAT6a	625	10GBASE-T bis 100m
CAT7	600	10GBASE-T bis 100m
CAT8	1200	25 Gbps / 40 Gbps über 30m

Dabei ist keine Aussage über die Qualität des gesamten Links möglich. Beim Installieren können durch unsachgemäße Bearbeitung Beeinträchtigungen auftreten, die kleine Grenzfrequenzen und somit eine niedrigere Klasse erforderlich machen.

9.20.2 - Europäischer Ansatz

Hierbei wird der gesamte Link als Einheit angesehen und aufgrund seiner Qualitätsmerkmale in Klassen eingeteilt.

Klasse	Grenzfrequenz	Enthält Kategorie
A	0,1	3,4,5
B	1	3,4,5
C	16	3,4,5
D	100	5
E	250	6
F	600	7

9.20.3 - Bedingungen für die Einordnung in Qualitätsklassen

Für jede Qualitätsklasse ist ein Verlauf der Messwerte über den Frequenzverlauf vorgeschrieben. In der folgenden Tabelle sind die Messwerte für Dämpfung, NEXT, ACR und RL in tabellarischer Form aufgelistet.

		Frequenz in MHz						
		1	16	100	250	500	600	1000
Klasse D	Attenuation	4	9,1	24				
	NEXT	63,3	43,6	30,1				
	ACR	59,3	34,6	6,1				
Klasse E	RL	17	17	10				
	Attenuation	4	8,3	21,7	35,9			
	NEXT	65	53,2	39,9	33,1			
Klasse Ea	ACR	61	44,9	18,2	-2,8			
	RL	19	18	12	8			
	Attenuation	4	8,1	20,8	33,8	49,3		
Klasse F	NEXT	65	53,2	39,9	33,1	27,9		
	ACR	61	45,1	19,2	-0,7	-21,4		
	RL	19	18	12	8	8		
Klasse Fa	Attenuation	4	8,1	20,8	33,8	49,3	54,6	
	NEXT	65	65	62,9	56,9	52,4	51,2	
	ACR	61	56,9	41,1	23,1	3,1	-3,4	
	RL	19	18	12	8	8	8	
	Attenuation	4	8	20,3	32,5	46,7	51,4	67,6
	NEXT	65	65	65	59,1	53,6	51,1	47,9
	ACR	61	57	46,1	26,6	6,9	-0,7	-19,7
	RL	19	18	12	8	8	8	8

Die grafische Aufbereitung zeigt die Abweichungen übersichtlicher an. Je höher die Leistungsklasse, desto restriktiver ist der vorgeschriebene Kurvenverlauf, der mindestens einzuhalten ist.

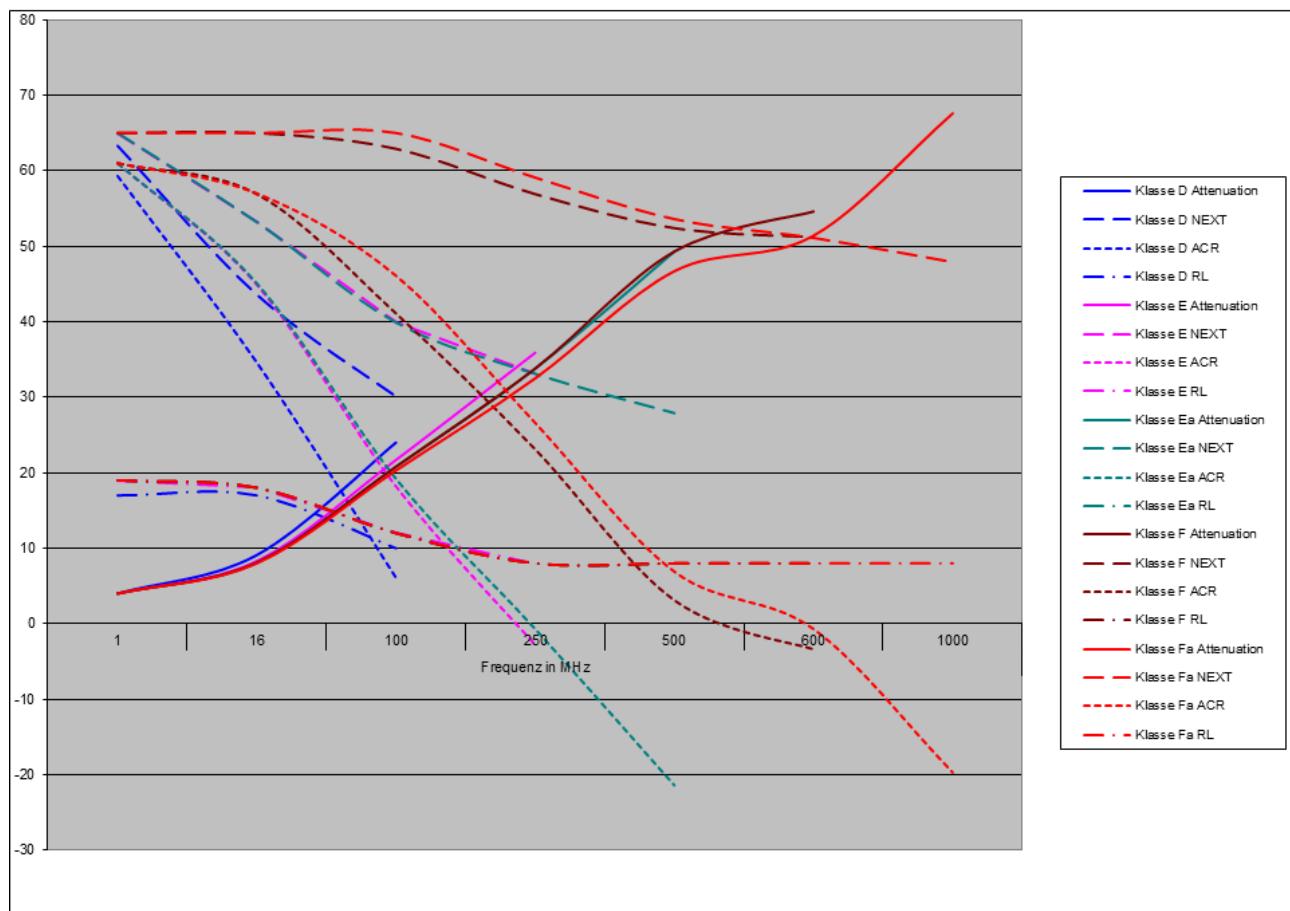


Abbildung 166: Verlauf in dB über der Frequenz

Bei den Kurven kann man erkennen, dass sie nur bis zu den für die Kasse festgelegten Grenzfrequenzen verlaufen.

10 - Zugriffsverfahren

Sobald der Datenaustausch über ein Shared Media erfolgt, muss der Zugriff auf das Medium geregelt werden! Dazu wurden mehrere Verfahren entwickelt. Die nachfolgende Abbildung zeigt einen Überblick.

In der MAC-Layer (Teil der 2. ISO-RM-Schicht) werden die Zugriffsverfahren, mit denen die Netzwerkgeräte auf das Netzwerk zugreifen, bearbeitet.

Die Zugriffsverfahren lassen sich in zwei Gruppen aufteilen. Deterministische und nicht deterministische Verfahren.

Die deterministischen Verfahren arbeiten mit einem Protokoll, das den Zugriff auf das Netzwerk regelt.

Somit wird koordiniert und konfliktfrei (kollisionsfrei) auf das Netzwerk zugegriffen.

Die nicht deterministischen Verfahren greifen unkoordiniert, und somit konkurrierend, auf das Netzwerk zu. Dies kann zu Kollisionen führen!

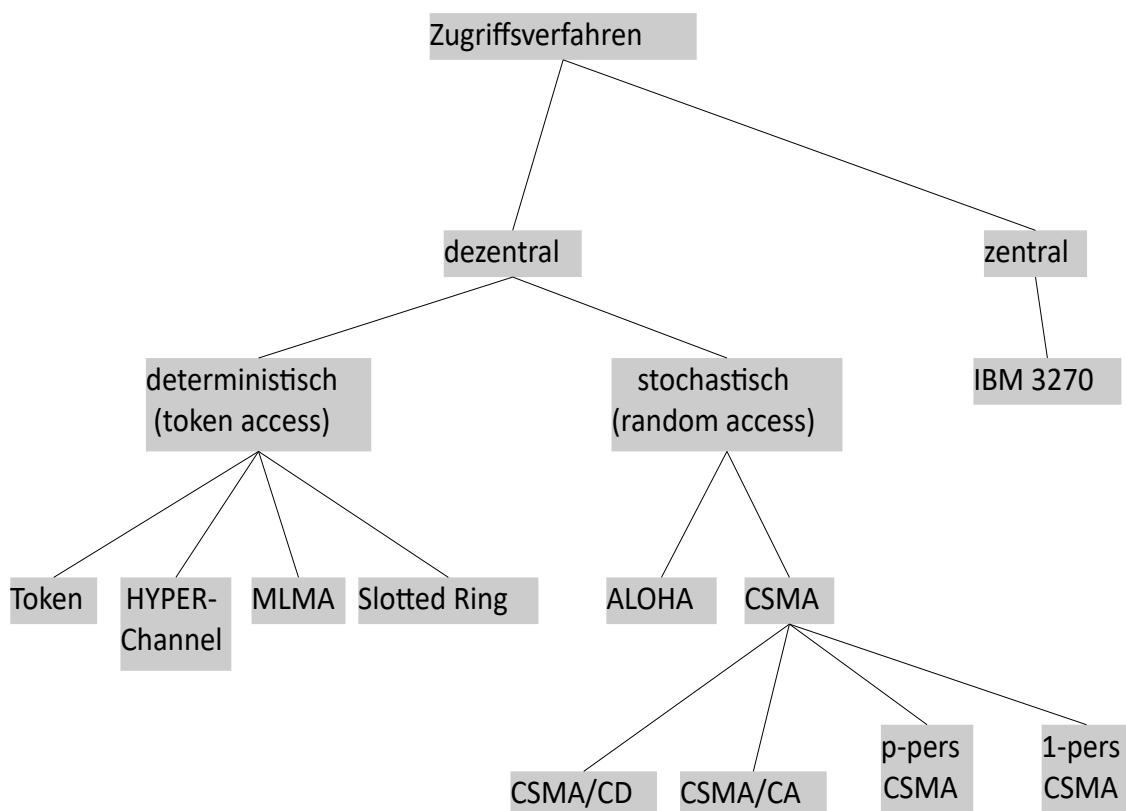


Abbildung 167: Zugriffsverfahren

10.1 - Pure ALOHA

10.1.1 - Historisches

An der Universität von Hawaii wurde ein Zugriffsverfahren namens ALOHA (deutsch: „Hallo“) entwickelt, um die über mehrere Inseln verteilten Standorte der Universität mit einem funkbasierter Netzwerk miteinander zu verbinden. In seiner Grundform wurde es als „Pure ALOHA“ (deutsch: reines ALOHA) bekannt. Hierbei kann jeder, jederzeit mit dem Senden beginnen. Dies hat zur Folge, dass Kollisionen auftreten. Da bei einer Kollision der Empfänger die Daten nicht korrekt empfängt, kann durch einen Cyclic Redundancy Check (CRC) erkannt werden, dass der Frame (deutsch: Rahmen) fehlerhaft ist. Der fehlerhafte Frame wird verworfen und deshalb auch nicht an den Sender zurück quittiert. Nach einer zufälligen Zeit wird der Frame vom Sender wiederholt.

10.1.2 - Kollisionen

Bei Kollisionen handelt es sich um mehrere Datenpakete die

- zeitgleich
- am gleichen Ort
- mit gleichen Frequenz
- der gleichen Kodierung
- von verschiedenen Stationen

übertragen werden.

Treten Kollisionen auf, dann kann mit den kollidierten Frames (deutsch: Rahmen) nichts angefangen werden. Die zu übertragende Information, kann beim Empfänger nicht mehr vollständig aufbereitet werden. Die Konsequenz aus einem kollidierten Paket ist dessen Wiederholung. Wiederholungen sind schlecht, da die Netzlast weiter erhöht wird und die zur Verfügung stehende Kanalkapazität weiter eingeschränkt wird.

Betrachtet man bei Pure ALOHA die Effizienz des Zugriffsverfahrens stellt sich die Frage, wie viele Rahmen fallen einer Kollision zum Opfer und wie viele kommen unversehrt beim Empfänger an. Dazu muss man sich die Vorgehensweise etwas genauer ansehen. Sie werden zu beliebigen Zeitpunkten übertragen.

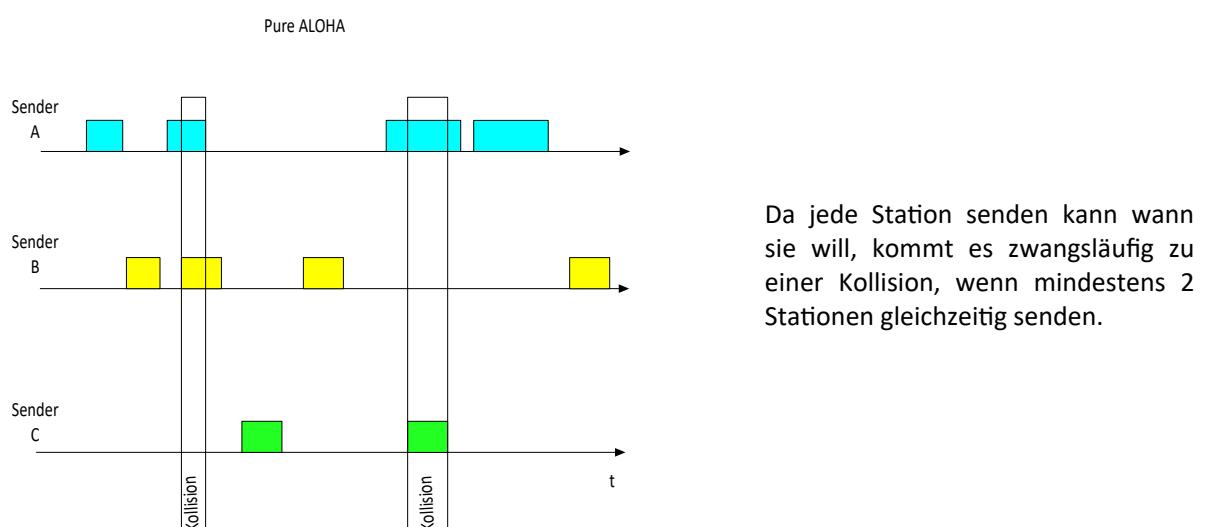


Abbildung 168: Pure ALOHA - Kollisionen

Zugriffsverfahren

Bei der folgenden Betrachtung wird vorausgesetzt, dass alle Rahmen die gleiche Größe und damit die gleiche Übertragungsdauer t_d haben.

Ein Rahmen B (in der Abbildung der graue Rahmen) kollidiert nicht, wenn kein anderer Rahmen innerhalb der Rahmenübertragungszeit t_0+t_d bis $t_0 + 2t_d$ übertragen wird.

Wenn in der Zeit zwischen t_0 und t_0+t_d begonnen wird einen zweiten Rahmen zu senden, kollidieren der erste und der zweite Rahmen.

Ebenso wenn ein anderer Rahmen C zwischen t_0+t_d und t_0+2t_d gesendet wird, kollidiert dieser Rahmen mit dem grauen Rahmen.

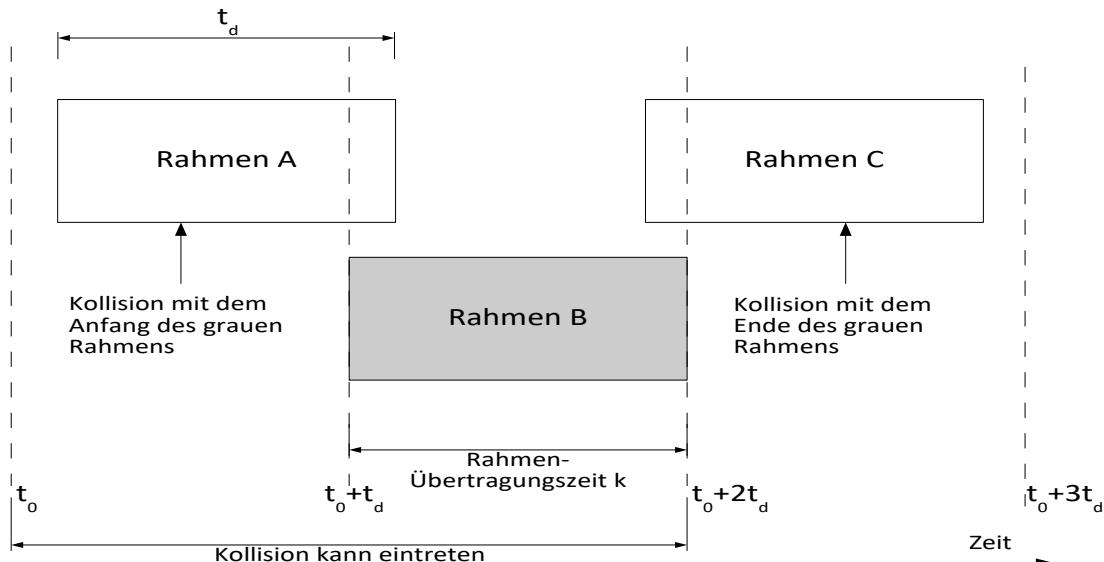


Abbildung 169: Kollision (Kritische Zeit)

Die Wahrscheinlichkeit (Pr), dass innerhalb einer gegebenen Rahmenübertragungszeit k Rahmen produziert werden, ergibt sich durch die Poisson-Verteilung:

$$Pr[k] = (G^k e^{-G}) / k! \quad (89)$$

Damit ist die Wahrscheinlichkeit für 0 Rahmen genau e^{-G} .

Innerhalb der Zeitspanne $2k$, werden im Durchschnitt $2G$ Rahmen gesendet.

Die Wahrscheinlichkeit, dass innerhalb der gefährlichen Zeitspanne kein anderer Datenverkehr begonnen wird, ergibt sich mit $P_0 = e^{-2G}$.

Unter Verwendung von $S = GP_0$ erhält man:

$$S = G * e^{-2G} \quad (90)$$

Der maximale Datendurchsatz ergibt sich bei $G=0,5$ mit $S=1/2e$. Dies ergibt einen Wert von 0,184. Dies bedeutet, dass der maximale Datendurchsatz 18% von der möglichen Kanalnutzung beträgt.

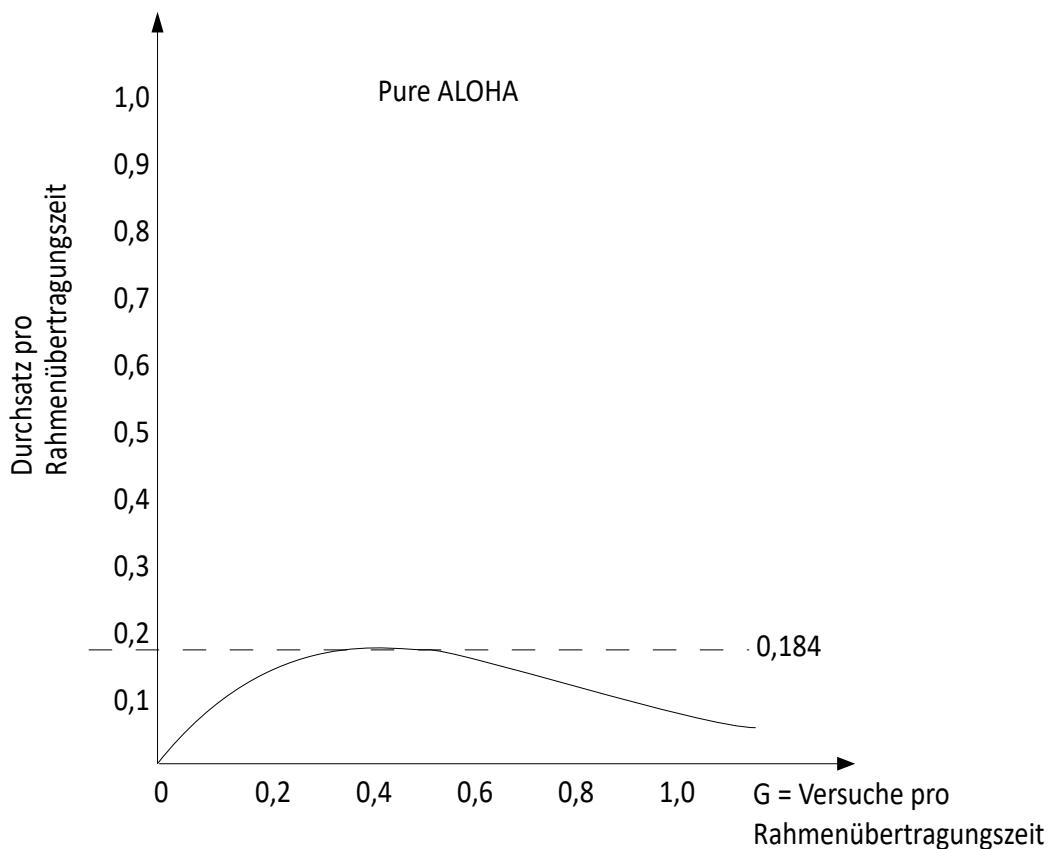


Abbildung 170: Pure Aloha Datendurchsatz

Bei einem Wert von $G = 0,5$ Versuchen, innerhalb der Übertragungszeit eines Rahmens, erreicht dieses Verfahren also ein Maximum von 18,4% Datendurchsatz.

10.2 - Slotted ALOHA

Um den mageren Datendurchsatz von Pure ALOHA zu verbessern, wurde ein Verfahren namens „Slotted ALOHA“ (S-ALOHA) (deutsch: ALOHA mit Zeitschlitzten) entwickelt. Dabei wird die Zeit in Intervalle eingeteilt, die der Übertragungszeit eines Rahmens entsprechen. Die Stationen müssen die Zeitschlitzte miteinander abstimmen / synchronisieren. Will eine Station Daten senden, muss sie warten bis der Beginn eines Zeitschlitztes kommt, um mit dem Senden zu beginnen. Da jetzt die Kollisionen nur noch zu Beginn eines Zeitschlitztes auftreten können, halbiert sich die Zeit in der ein Rahmen kollidieren kann auf die Hälfte der Zeit bei Pure ALOHA.

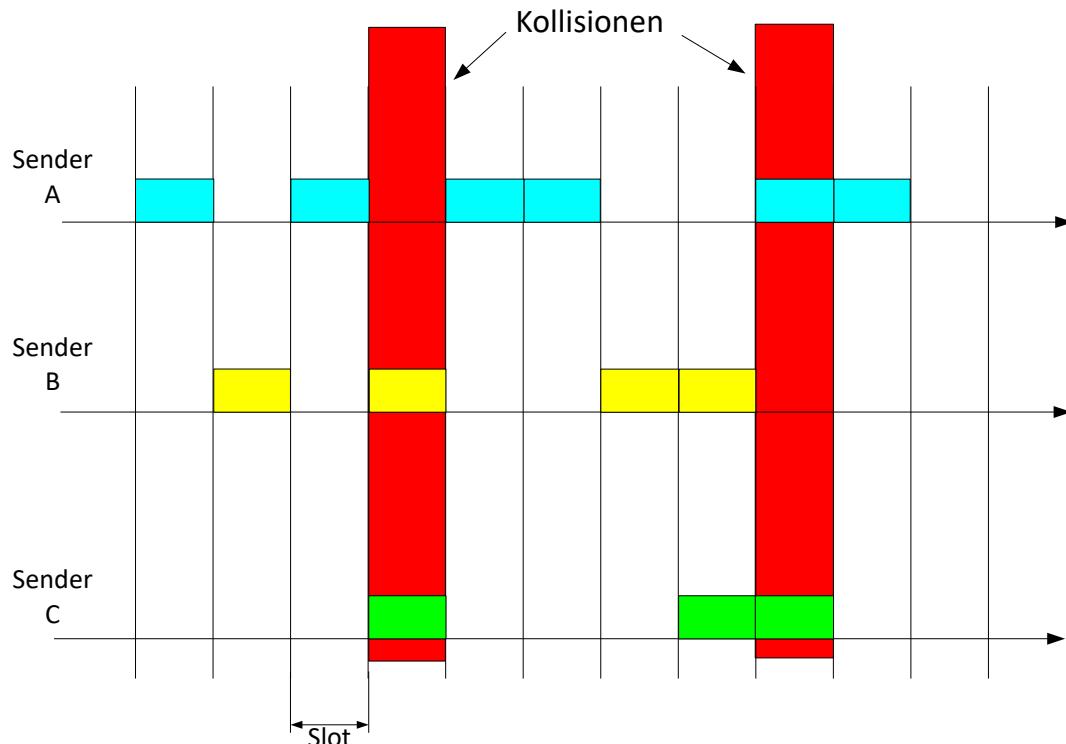


Abbildung 171: Slotted ALOHA

Die Wahrscheinlichkeit, dass kein anderer Rahmen im gleichen Zeitschlitz wie ein zu sendender Rahmen gesendet wird, ist e^{-G} . Damit ergibt sich $S = Ge^{-G}$. S-ALOHA hat seinen Spitzenwert bei $G = 1$.

Die Wahrscheinlichkeit für einen leeren Zeitschlitz ist damit 36,8%.

Die Wahrscheinlichkeit für eine erfolgreiche Datenübertragung ist ebenfalls bei 36,8%.

Für die Slots sind natürlich Taktgeber erforderlich.

10.3 - CSMA-Protokolle

Um eine weitere Verbesserung der Zugriffsverfahren zu erreichen wurde CSMA entwickelt. Hierbei steht CSMA für Carrier Sense Multiple Access. „CS“ bedeutet, dass ein Sender, bevor er sendet, den Kanal abhören muss. Es darf nur dann gesendet werden, wenn der Kanal frei ist. Ist das Medium für die Inter-Frame-Gap-Zeitspanne (IFG) (9,6 µs bei 10-Mbps-Ethernet, 960 ns bei 100-Mbps-Fast-Ethernet und 9 ns bei 1000 Mbps) nicht belegt, wird es als frei betrachtet. Dadurch kann zumindest ein Teil der Kollisionen vermieden werden. Weiterhin ist in der Abkürzung „MA“ hinterlegt, dass alle Stationen auf den Kanal gleichberechtigt und konkurrierend zugreifen dürfen.

In den folgenden Beispielen ist zum Zeitpunkt t_0 eine Station gerade am Senden. Während des Sendens wollen weitere Stationen auch senden. Die Auflösung dieser Situation kann unterschiedlich erfolgen.

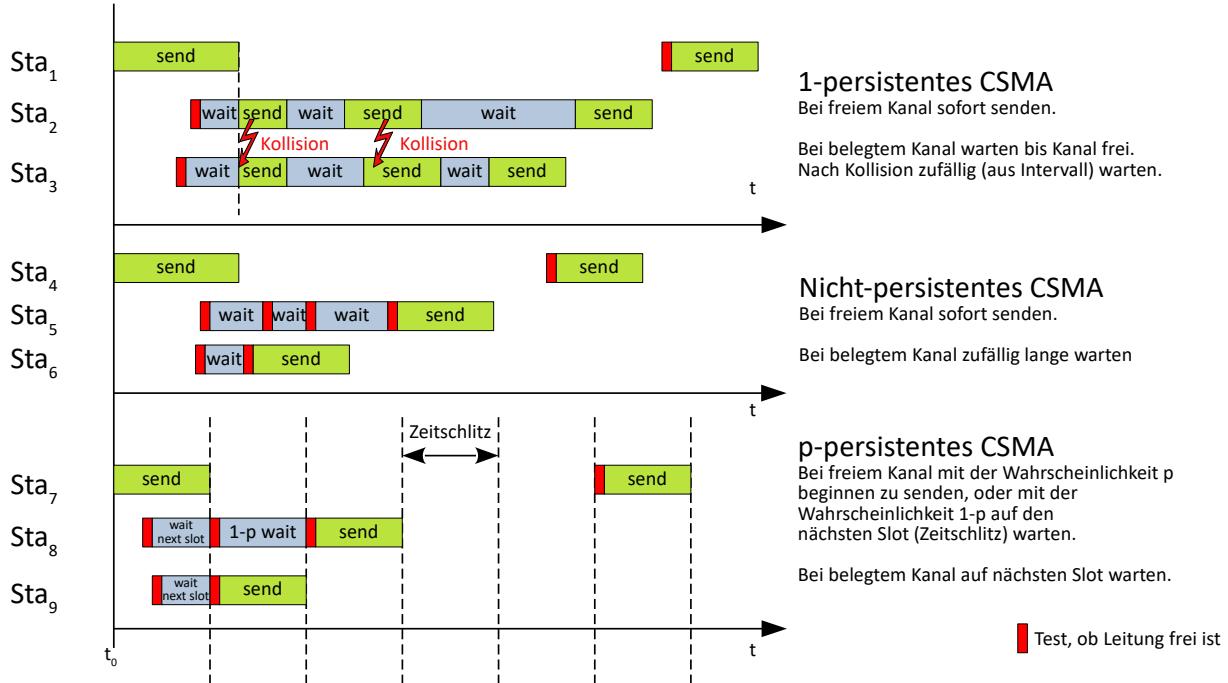


Abbildung 172: CSMA-Verfahren

10.3.1 - 1-persistent CSMA

Wenn eine sendewillige Station Daten übertragen möchte, hört sie zunächst den Kanal ab.

Ist der Kanal frei, kann sofort ein Rahmen übertragen werden. Es wird immer, also mit der Wahrscheinlichkeit von 1 gesendet. Daher kommt der Name 1-persistentes CSMA.

Sofort nach dem Sendeende und dem IFG versuchen wartende Stationen zu senden. Haben mehrere Stationen gewartet, beginnen sie gleichzeitig mit dem Senden. Dies hat sofort eine Kollision zur Folge.

Sollte eine Kollision auftreten, warten die Stationen eine zufällige Zeitspanne und beginnen danach sofort erneut mit dem Daten-Übertragungsversuch.

Dieses Verfahren ist das aggressivste. Solange nur wenige Stationen senden wollen, ist es performant. Sobald jedoch mehr als eine Station pro Rahmen-Übertragungszeit senden will, treten immer mehr Kollisionen auf.

10.3.2 - Nicht-persistentes CSMA

Wenn eine sende willige Station Daten übertragen möchte, hört sie zunächst den Kanal ab.

Falls das Medium frei ist, wird sofort gesendet. Ansonsten wird eine zufällige Zeitspanne gewartet um erneut zu testen.

Dieses Verfahren ist nicht so hartnäckig (persistent) wie das 1-persistenten Verfahren. Dadurch kommen bei einem belegten Kanal die einzelnen Stationen nur verzögert zum Zug. Dafür treten weniger Kollisionen auf.

10.3.3 - p-persistent CSMA

Für dieses Verfahren werden Zeitschlüsse benötigt. Wenn eine Station senden will, hört sie zunächst den Kanal ab.

Ist der Kanal belegt, wird auf den nächsten Zeitschlitz gewartet.

Ist der Kanal frei, wird mit der Wahrscheinlichkeit p mit dem Senden begonnen, oder mit der Wahrscheinlichkeit $q = 1 - p$ auf den nächsten Zeitschlitz gewartet.

Ist dann der Zeitschlitz dann frei, wird mit der Wahrscheinlichkeit p gesendet, oder mit der Wahrscheinlichkeit $q = 1 - p$ wiederum gewartet.

10.3.4 - Vergleich der unterschiedlichen Zugriffsverfahren

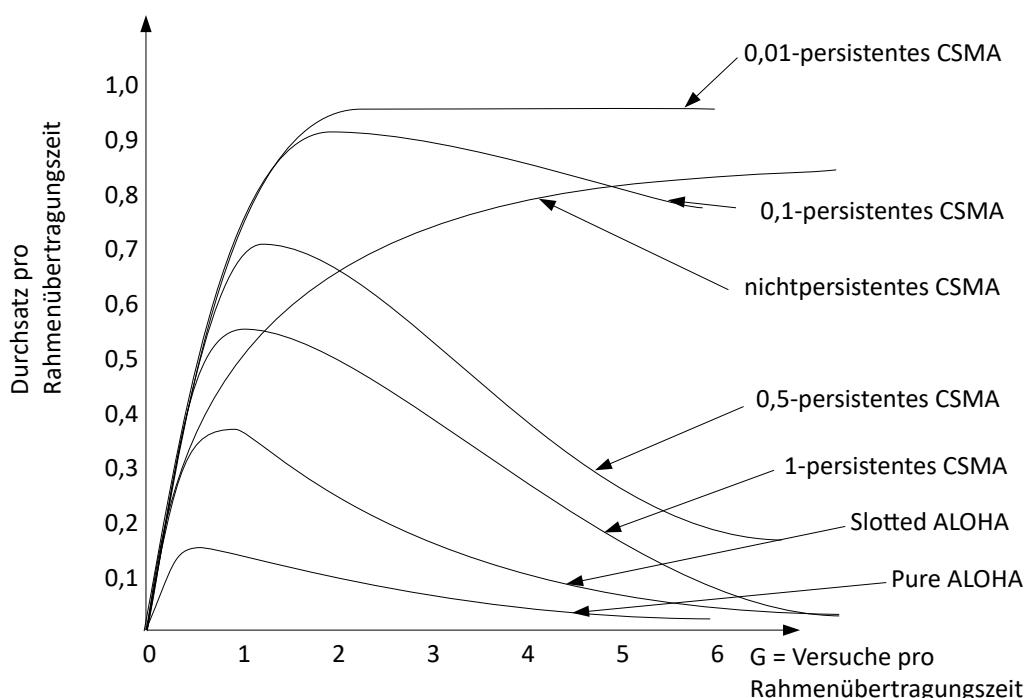


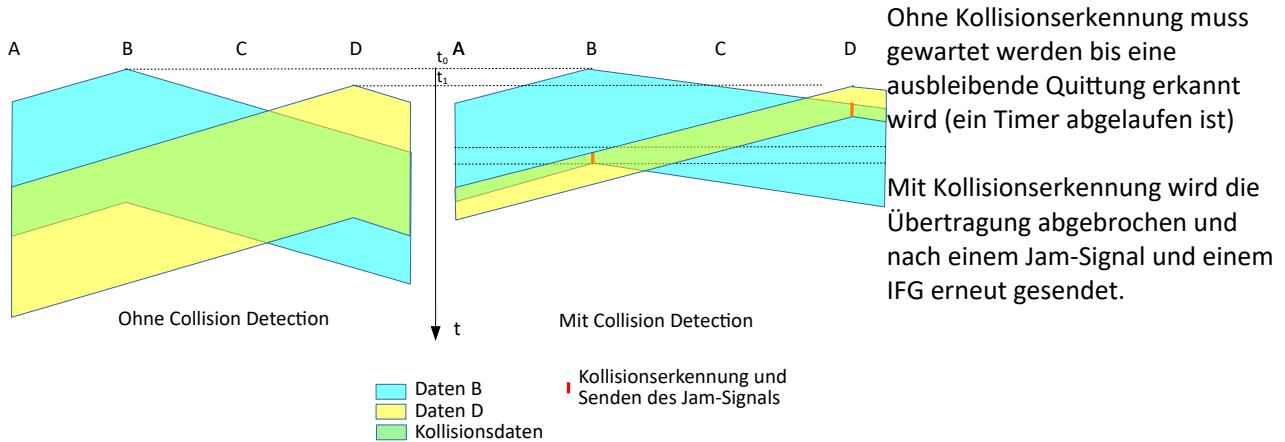
Abbildung 173: Zugriffsverfahren im Vergleich

Am schlechtesten schneiden die Aloha-Verfahren ab da sie relativ unkoordiniert auf das Medium zugreifen. Bei den CSMA-Verfahren sind die p-persistenten Verfahren besser. Allerdings ist das auch von der Teilnehmeranzahl, deren Sendeverhalten und den Paketgrößen abhängig. Wenige Teilnehmer mit kurzen Paketen sind mit einem 1-Persistenten-CSMA gut bedient.

10.3.5 - CSMA/CD

Keines der obigen Verfahren kann ausschließen, dass Kollisionen entstehen! Um Kollisionen erkennen zu können muss, während des Sendens der Daten, der Kanal abgehört werden!

Erkennt der Sender eine Kollision, bricht er die Datenübertragung sofort ab und sendet ein Jam-Signal (dt. Stausignal = 4Byte mit 10101010) aus. Damit können alle anderen Stationen erkennen, dass eine Kollision stattgefunden hat und brechen evtl. ihr Senden ab.



Treten nach dem Senden von 64 Bytes trotzdem noch Kollisionen auf, spricht man von „Late Collisions“ oder auch „Long Collisions“. Diese treten dann auf, wenn Netzwerkkarten defekt sind oder die räumliche Ausdehnung eines Netzwerk-Segmentes zu groß geworden ist. Late Collisions sind sehr problematisch, da sie nicht erkannt werden und somit die Frames nicht wiederholt werden. Letztendlich bedeutet dies ein Datenverlust!

10.3.5.1 - Implementierung bei Ethernet

Es gibt viele Möglichkeiten Netzwerk-Geräte an ein Netz anzuschließen. Bei einem Medium, auf das von mehreren Teilnehmern gleichberechtigt zugegriffen wird, muss mit einem Zugriffsverfahren auf das Übertragungsmedium im Half-Duplex-Modus zugegriffen werden. Das unter Ethernet verwendete Zugriffsverfahren bei Half-Duplex-Betrieb ist ein 1-persistentes CSMA/CD.

Werden für die Verbindung von 2 Geräten Crossover-Kabel oder mehreren Geräten Switches verwendet, kann auf ein Zugriffsverfahren verzichtet und der Full-Duplex-Mode verwendet werden, denn dann werden alle Verbindungen als 1:1-Verbindungen angesehen.

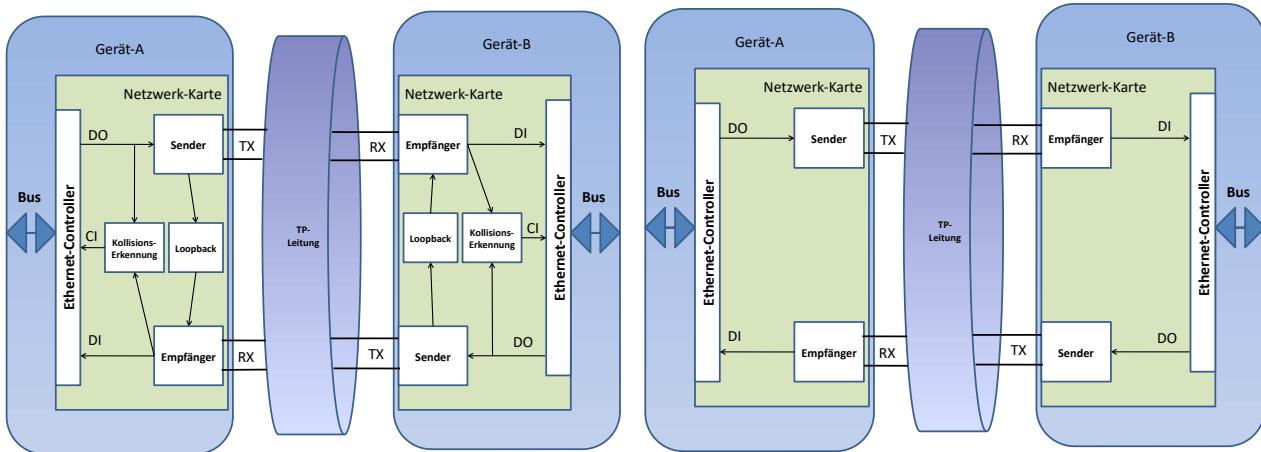


Abbildung 175: Kollisionserkennung bei Half-Duplex

Abbildung 174: Keine Kollisionserkennung bei Full-Duplex

Zugriffsverfahren

Beim Half-Duplex-Betrieb können Kollisionen auftreten. Dies ist zum einen im 1-persistenten CSMA begründet. Zum anderen kollidieren Daten dann, wenn bei einem Bussystem die Stationen weit voneinander entfernt sind. Da die Signale auf der Leitung Zeit benötigen, um sich auszubreiten, können zwei Stationen die weit auseinander liegen nicht erkennen, dass eine Station gerade angefangen hat zu senden. So ist es möglich, dass mehrere Stationen gleichzeitig beginnen zu senden.

Bei der Festlegung der Parameter für das ein Ethernet-Netzwerk spielt also die Signallaufzeit eine entscheidende Rolle. Selbst wenn zwei Stationen mit einem kleinen Zeitversatz anfangen zu Senden, benötigen die Bits, bis sie bei der anderen Station ankommen und kollidieren, eine bestimmte Laufzeit. Diese Signallaufzeit führt zur Festlegung der Dimensionen eines Netzwerks.

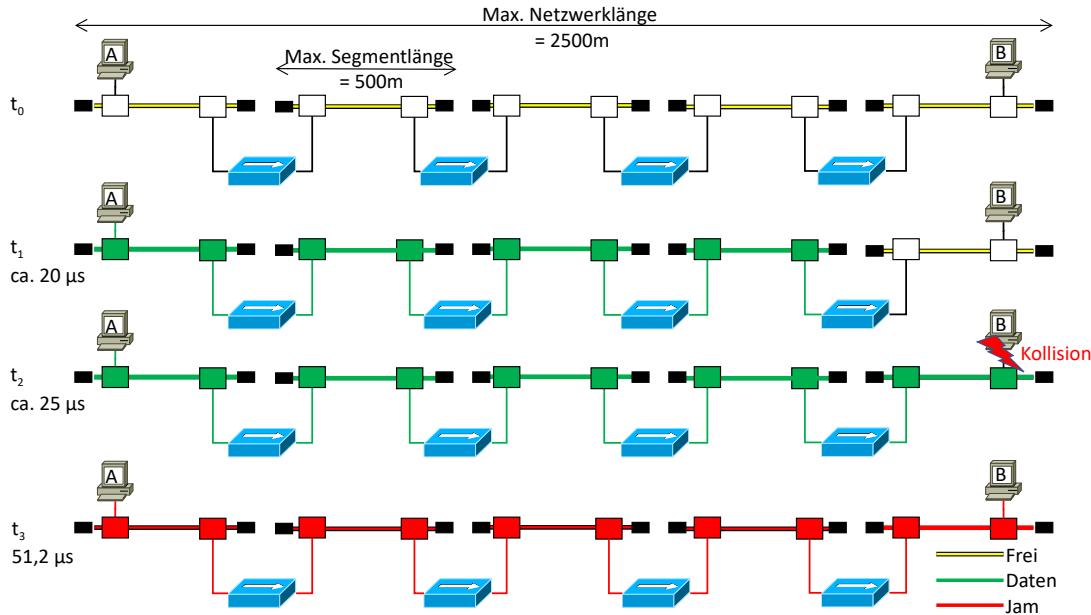


Abbildung 176: Zusammenhang zwischen Signallaufzeit und Netzwerk-Dimensionen

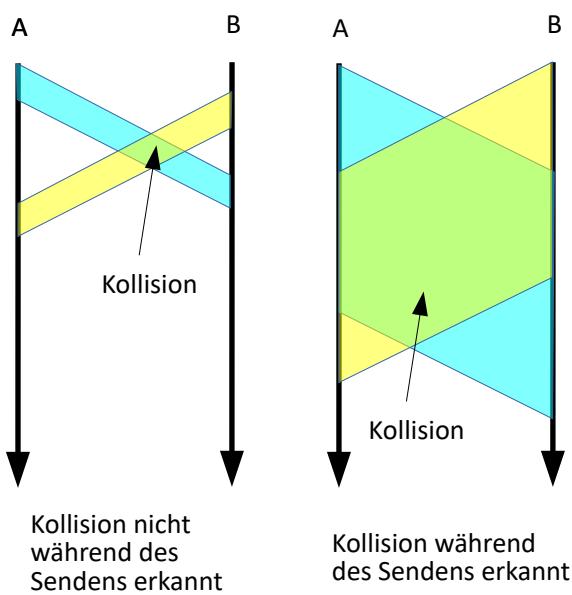
10.3.5.2 - Ablauf einer Kollision bei Ethernet mit 10Mbps

Ein Segment kann die maximale Länge von 500m haben. Es ist möglich mit Repeatern bis zu maximal 5 Segmente miteinander zu verketten.

Zum Zeitpunkt t_0 beginnt Station A zu senden da die Leitung frei ist. Die Daten breiten sich über das gesamte Netzwerk aus. Zum Zeitpunkt t_1 (nach ca. 20µs) will Station B auch Daten senden und kann den Kanal als frei erkennen. Zum Zeitpunkt t_2 (nach ca. 25µs) hat Station B mit dem Senden begonnen und erkennt sofort eine Kollision. Darauf hin bricht sie das Senden ab und sendet ein **Jam-Signal**, das sich in Richtung zur Station A hin ausbreitet. Zum Zeitpunkt t_3 (nach ca. 51,2 µs) kann auch die Station A das Jam-Signal erkennen und bricht seinerseits die Übertragung ab.

Wichtige Größen sind hierbei:

- **IFG (Inter Frame Gap; deutsch Lücke zwischen den Rahmen) auch IPG (Inter Packet Gap; deutsch: Lücke zwischen den Paketen)** Zwischen den Rahmen sind Wartezeiten einzuhalten, damit die Netzwerkkarten die Möglichkeit haben, die einzelnen Rahmen sauber voneinander zu unterscheiden.
- Maximallänge eines Frames. Damit andere Stationen ebenfalls senden können, ist die maximale Framegröße bei Ethernet auf 1518 Bytes begrenzt. Eine Ausnahme bilden hier **Jumbo-Frames** mit einer Länge von bis zu 16000 Bytes. Jumbo-Frames sind nicht standardisiert!
- Die **Maximale Ausdehnung eines Netzwerks** ergibt sich aus der maximalen Signallaufzeit von einem Ende zum anderen und wieder zurück. Mit der sogenannten Round-Trip-Time (RTT) wird der Maximalwert von 2500m definiert, den die maximale physikalische Ausdehnung eines Netzwerksegments haben darf. Bei 10 Mbps (10Base5) wir somit eine RTT von 51.2 µs festgelegt. Das kann erreicht werden indem 5 Segmente (mit je 500m) mit 4 Repeatern zu einer Kette aneinander gehängt werden. Die 51.2 µs entsprechen der Zeit, die für die Übertragung von 512 Bit benötigt werden, was der minimalen Größe eines Frames mit 64 Byte und der maximalen Ausdehnung der Kollisionsdomäne von 2500m entspricht.
- **Minimale Frame-Länge.** Die Netzwerkkarte muss mindestens so lange die Leitung beim Senden überprüfen, wie ein Frame vom einen Ende eines Netzwerks bis zum anderen und wieder zurück braucht, um sicher zu gehen, dass keine Kollision aufgetreten ist. Dazu muss ein Frame die Mindestgröße von 64 Bytes (= 512-Bit-Times) haben.



Bei der Kollisionserkennung ist natürlich Voraussetzung dass eine evtl. auftretende Kollision während des Sendens erkannt wird.

Im linken Beispiel ist der Sender A schon mit dem Senden fertig bevor die Kollision auftritt. Damit kann die Kollision nicht erkannt werden.

Abbildung 177: Mindestpaketgröße um Kollisionen zu erkennen

- **Collision Window** Ist die Zeit, in der ein Frame aufgrund der RTT und der Netzwerkausdehnung einer Kollision zum Opfer fallen kann.

Zugriffsverfahren

Für verschiedene Ethernet-Datenübertragungsraten gelten folgende Werte:

Geschwindigkeit	IFG	Collision Window	Mindest Framegröße	Slotzeit [Bit-times]	Maximale Framegröße
10 Mbps	9,6 µs	51,2 µs	64 Bytes	512	1518 Bytes
100 Mbps	0,96 µs	5,12 µs	64 Bytes	512	1518 Bytes
1000 Mbps	0,096µs	5,4 µs mit Carrier Extension	64 Bytes 512 Bytes bei Carrier Extension	512	1518 Bytes

Während der Dauer eines Collision-Window können Kollisionen auftreten. Das bedeutet, dass mindestens 64 Bytes = 512 Bit gesendet werden müssen.

Die Wartezeit nach der Erkennung einer Kollision wird mit einem exponentiellen Backoff-Algorithmus bestimmt. Dazu wird die so genannte Slotzeit S, als Übertragungszeit eines minimalen Ethernetframes (64 Byte) festgelegt. Weiterhin wird ein Kollisionszähler n eingeführt, der mithält, wie oft ein Frame einer Kollision zum Opfer fiel.

Die Back-off-Time berechnet sich zu: Backoff-Time = i * S

i = zufälliges Element aus {0 < i < 2k}

k = min (n, 10)

Beispiele:

n = 1: → i ist zufällig aus {0,1} ausgewählt → Back-off-Time = 0*S oder 1*S

n = 2: → i ist zufällig aus {0,1,2,3} ausgewählt → Back-off-Time = 0*S, 1*S, 2*S oder 3*S.

n = 3: → i ist zufällig aus {0,1,2,3,4,5,6,7} ausgewählt → Back-off-Time = 0*S, 1*S, 2*S, 3*S, 4*S, 5*S, 6*S oder 7*S.

CSMA/CD gibt nach mehr als 16 Kollisionen auf und meldet der überlagerten Schicht einen Fehler, obwohl nach der obigen Vorgehensweise 20 Versuche möglich sind.

Wiederholungen:

- 1 $51,2 = 51,2 \mu s$
- 2 $4 * 51,2 = 204,8 \mu s$
- 3 $8 * 51,2 = 409,6 \mu s$
- 4 $16 * 51,2 = 819,2 \mu s$
- 5 $32 * 51,2 = 1638,4 \mu s$
- 6 $64 * 51,2 = 3276,8 \mu s$
- 7 $128 * 51,2 = 6553,6 \mu s$
- 8 $256 * 51,2 = 13107,2 \mu s$
- 9 $512 * 51,2 = 26214,4 \mu s$
- 10 $1024 * 51,2 = 52428,8 \mu s$
- 11 $1024 * 51,2 = 52428,8 \mu s$
- 12 $1024 * 51,2 = 52428,8 \mu s$
- 13 $1024 * 51,2 = 52428,8 \mu s$
- 14 $1024 * 51,2 = 52428,8 \mu s$
- 15 $1024 * 51,2 = 52428,8 \mu s$

CSMA/CD gibt nach mehr als 16 Kollisionen auf. Das bedeutet $366848 \mu s = 0,366s$ reine maximale Wartezeit. Hinzukommen noch die Zeiten für die Kollisionserkennung von jeweils $51,2 \mu s$

10.4 - CSMA/CA

Hierbei steht CA für Collision Avoidance (deutsch: Kollisions Vermeidung). Es wird bei den WLANs (wireless LANs) verwendet. In diesem Zusammenhang sind folgende Begriffe wichtig:

- Backoff Time

Hierbei handelt es sich um eine Wartezeit. Diese Zeit wird durch einen Pseudo-Zufallszahlengenerator ermittelt. Sollte es mehrere Zugriffs-Versuche benötigen um ein Paket zu senden, dann wächst die Backoff Time exponentiell bis zu einer maximalen Größe an. (Exponential Backoff) an.

- DIFS (DCF Inter Frame Spacing)

Zeit, die nach dem Senden eines Frames verstreichen muss, bevor eine Station senden darf.

- CW (Contention Window)

Zeitspanne nach dem DIFS. Im CW läuft bei jeder sendewilligen Station die Backoff Time ab. Während der Timer abläuft, wird der Kanal weiterhin noch abgehört, um evtl. andere sendende Stationen zu erkennen. Ist die Backoff Time abgelaufen und der Kanal ist noch frei, beginnt eine Station mit dem Senden.

- SIFS (Short Inter Frame Spacing)

Wartezeit, die eine Station nach dem Empfang wartet, bevor die Daten mit einem ACK quittiert werden. Die SIFS ist immer kürzer als die DIFS. Damit ist sichergestellt, dass Frames, unmittelbar nachdem sie gesendet wurden, vom Empfänger quittiert werden können.

Dieses Verfahren kann nicht vermeiden, dass Kollisionen entstehen. Ein Gerät, das gerade funk, kann nicht gleichzeitig empfangen. Kollisionen können deshalb nicht wie bei CSMA/CD erkannt werden. Eine Kollisionserkennung kann in Funknetzen nur durch einen Rückkanal erfolgen. Deshalb wird ein Unicast-Paket vom Empfänger immer quittiert. Bleibt eine Quittung aus, wird der Sendevorgang wiederholt. Dies geschieht bis zu einer maximalen Anzahl von Übertragungsversuchen. Ist dann immer noch keine Quittung eingetroffen, wird das Paket verworfen.

Anhand eines Beispiels sollen die Abläufe erklärt werden.

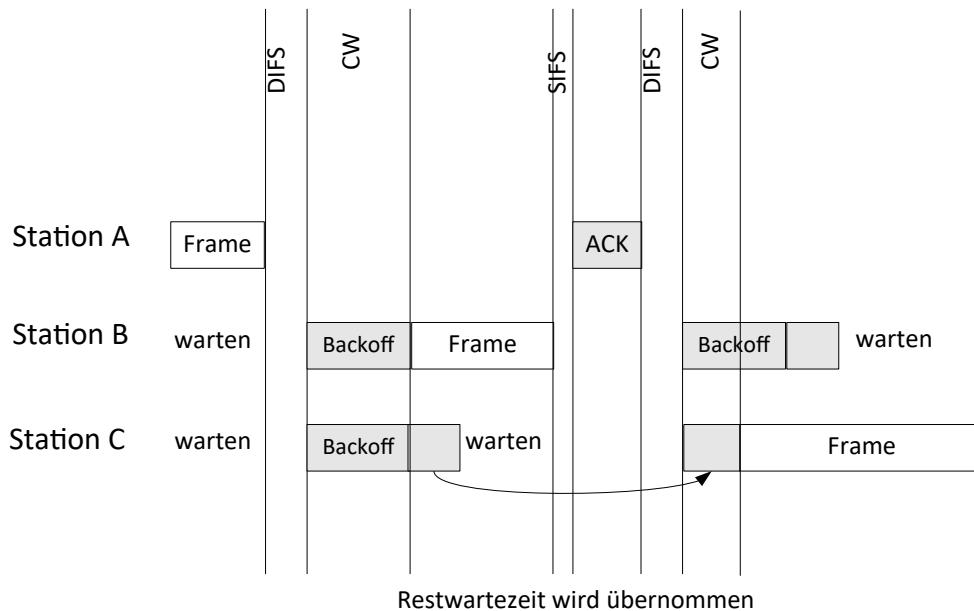


Abbildung 178: Kanalzugriff

Zugriffsverfahren

Drei Stationen befinden sich in einem Funknetz.

Station A sendet gerade. Die Stationen B und C wollen ebenfalls senden und ermitteln die Zeiten für ihre Backoff-Timer.

Solange Station A sendet, warten die beiden anderen Stationen.

Sobald die Station A ihre Daten gesendet hat, läuft die DIFS ab. Danach laufen in den Stationen B und C die Backoff-Timer ab.

Der Backoff-Timer von B läuft zuerst ab und somit kann B direkt nach Ablauf des Timers mit dem Senden beginnen.

Die Station B sendet nun Daten an die Station A.

Die restliche Wartezeit der Station C wird für den nächsten Sendeversuch gespeichert. Dies bewirkt eine hohe Wahrscheinlichkeit, dass Station C als nächste senden darf.

Nachdem die Station B ihre Daten gesendet hat, werden die Daten nach einer kurzen Wartezeit (SIFS) von der Station A durch ein ACK bestätigt.

10.5 - CSMA/CR

Hier steht „CR“ für Collision Resolution. Dies bedeutet, dass Kollisionen erkannt und aufgelöst werden können.

Dieses Zugriffsverfahren kommt bei Feldbussen, wie z. B. dem CAN (Controller Area Network) in Fahrzeugen zum Einsatz. Kollisionen werden durch Bitarbitrierung erkannt. Dadurch wird sichergestellt, dass am Ende jeder Arbitrierungsphase der Teilnehmer mit der höchsten Priorität das Medium nutzen kann. Dabei können Kollisionen auftreten, jedoch haben sie keine Auswirkung.

10.6 - Token-Zugriffsverfahren

Hierbei handelt es sich um ein deterministisches Verfahren, denn es kann vorausgesagt werden, wie lange eine Datenübertragung dauert.

Wer auf ein Token-Netzwerk zugreifen will, muss dazu die Berechtigung haben. Diese Berechtigung läuft in Form eines freien Token auf dem Netzwerk entlang und jede Station hat die Möglichkeit, dieses Token zu nehmen und damit die Sende-Berechtigung zu erlangen.

Ein Token ist eine eindeutige Bitfolge, die auf einem Ring kreist oder auf einem Bus hin und her bewegt wird. (Token Ring oder Token Bus)

Im Allgemeinen wird das Token-Verfahren beim Token Ring angewendet. Der Token Bus ist zwar spezifiziert, ist jedoch kaum anzutreffen.

Ablauf

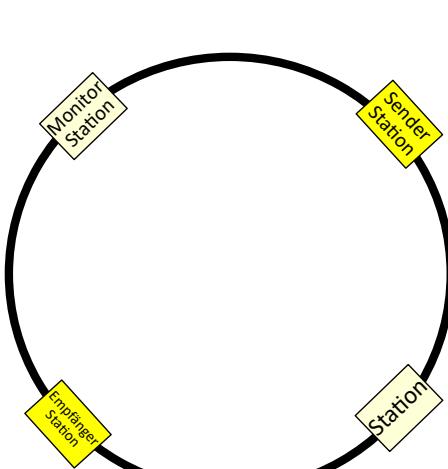


Abbildung 180: Token-Ring: Teilnehmer

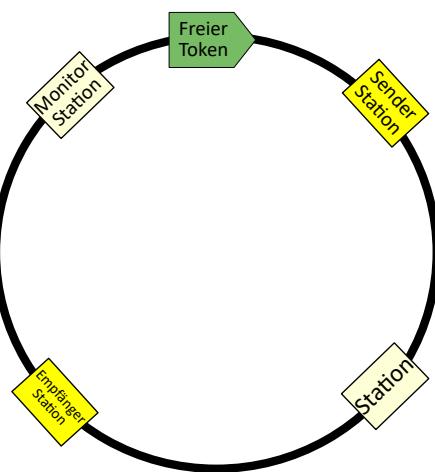


Abbildung 179: Frei-Token

- Sobald eine Station senden will, wartet sie so lange, bis ein freies Token vorbeikommt. Das freie Token wird von einer Monitor-Station erzeugt und verwaltet. Dieses freie Token wandelt sie in ein belegtes Token um und sendet dieses Token an die nächste Station weiter. Daran hängt die sendende Station ihre Daten, die sie senden will. Dies tut sie so lange, bis entweder alle Bits übertragen sind, oder die maximal zulässige Zeit abgelaufen ist.

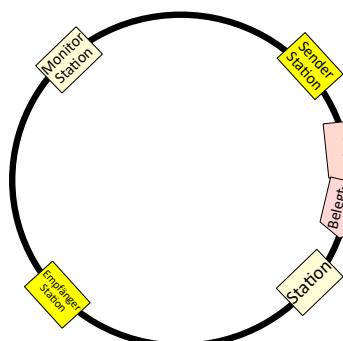


Abbildung 183: Daten werden auf dem Ring weiter geleitet

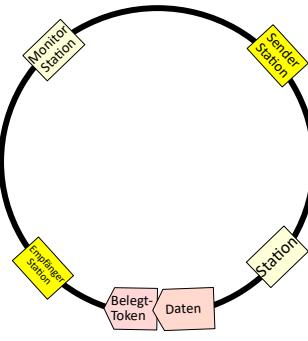


Abbildung 181: Unbeteiligte Stationen leiten die Daten weiter

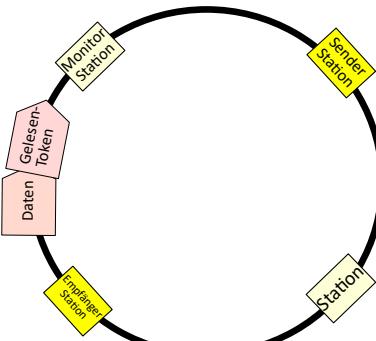


Abbildung 182: Empfänger kopiert die Daten und ändert Token

- Die Daten werden von den einzelnen Stationen bis zum Empfänger weiter geleitet.
- Der Empfänger kopiert die Daten vom Ring und setzt an das Ende des Frames entsprechende Bitflags, die signalisieren, dass der Frame identifiziert und korrekt kopiert wurde. (Address Recognition Bit und Frame Copied Bit)

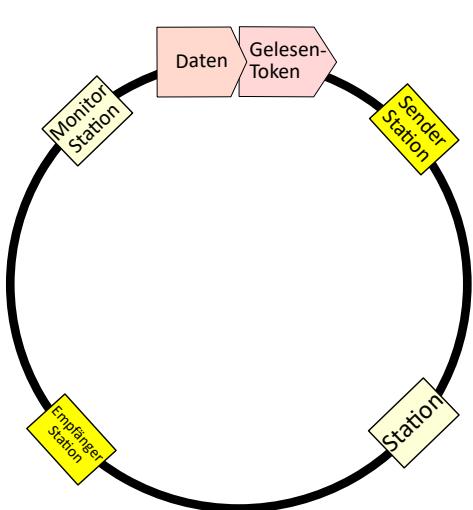


Abbildung 184: Lese-Information wird zum Sender weiter geleitet

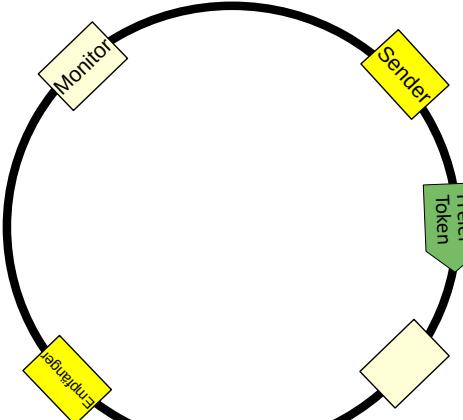


Abbildung 185: Nach erfolgreicher Übertragung erzeugt der Sender ein freies Token

- ➊ Die Information, dass die Daten gelesen wurden, wird bis zum Sender weiter gereicht.
- ➋ Die Sendestation nimmt das gesendete Bit vom Ring.
- ➌ Danach nimmt sie den belegten Token vom Ring und sendet eine freie Token an die nächste Station.

Der Token Ring ist mit zwei Geschwindigkeiten anzutreffen 4 Mbps und 16 Mbps.

Für die 16 Mbps-Version gibt es noch die die Option des Early-Token-Release. Dabei wird bereits nach dem Empfang des gesendeten Frames vom Empfänger ein neues freies Token gesendet. Dieses und weitere Verfahren (Z. B. Multiple Token) wurden zur Performancesteigerung entwickelt.

Jede Station die am Ring hängt, wird von allen Frames durchlaufen. Fällt eine Station aus, ist der Ring zumindest kurzfristig unterbrochen.

Als zentrale Überwachungsstation wurde die Monitorstation eingeführt. Sie überwacht den Ring und reagiert auf verschiedene Fehlersituationen.

- ➊ Verlorenes Token durch Rauschen oder Signalstörung
Neugenerieren des Token nach Timerablauf
- ➋ Kreisendes belegtes Token durch Rauschen oder Stationsfehler
Entfernen des Token, falls es zwei Mal den Monitor passiert. Neugenerieren eines freien Token.
- ➌ Doppeltes Token durch Rauschen oder Stationsfehler
Überprüfen des Absenders. Entfernung und Rekonfiguration des Frames.
- ➍ Ausfall des Monitors selbst: Durch Hard- oder Softwarefehler
Übernahme durch Standby-Monitor nach Timerablauf bzw. aushandeln eines neuen Monitors.

Bei einem Leitungs- oder Stationsausfall, muss der Fehler überbrückt werden. Dies kann zumindest teilweise automatisch gemacht werden. Ansonsten sind manuelle Eingriffe notwendig.

11 - Topologien

11.1 - Allgemeines

Als Topologie bezeichnet man die Art und Weise, wie die Netzwerknoten miteinander zusammengeschaltet werden.

11.2 - Merkmale

Um Topologien zu unterscheiden bieten sich mehrere Merkmale an.

11.2.1 - Durchmesser

Gibt die maximale Anzahl der möglichen Hops an.

Dies lässt Rückschlüsse auf die physikalische Ausdehnung und die maximale Transferzeit für Daten zu.

11.2.2 - Grad

Damit ist die Anzahl der Links pro Knoten gemeint. Ist die Anzahl für alle Knoten gleich ist die Topologie regulär. Daraus lassen sich auch die Kosten für das Netzwerk ableiten.

11.2.3 - Bisektionsweite

Die Bisektionsweite gibt die minimale Anzahl von Links an, die durchgeschnitten werden müssen, um ein Netz mit N Knoten in zwei Netze mit jeweils $N/2$ Knoten zu teilen.

Damit ist sie ein Maß für die Leistungsfähigkeit eines Netzes, da in vielen Algorithmen die Knoten der einen Netzhälfte mit den Knoten der anderen Hälfte kommunizieren. Je niedriger also die Bisektionsweite, desto ungünstiger wirkt sich dies auf den Zeitbedarf für den Datenaustausch zwischen beiden Netzhälften aus.

11.2.4 - Symmetrie

Sieht eine Topologie aus Knoten- oder Link-Sicht in jeder Richtung gleich aus, ist es symmetrisch.

Knoten und Links verhalten sich in einem symmetrischen Netz gleich, egal welchen Knoten oder Link man betrachtet. Dies hat Auswirkungen auf die Programmierung, die Lastverteilung und das Routing, da es keine Spezialfälle zu betrachten gibt.

11.2.5 - Skalierbarkeit

Hier geht es um den Aufwand der bei Erweiterungen zu leisten ist. Eine Vergrößerung kann auch mit Leistungseinbußen (z.B. Laufzeiten) einher gehen.

Grundsätzlich sind bei Änderungen alle Tätigkeiten im Zusammenhang IMACD (Insert / Move / Add / Change / Disposal) zu betrachten.

11.2.6 - Konnektivität

Gibt die Anzahl der Knoten / Links an die eliminiert werden müssen, damit das Netz nicht mehr funktioniert.

Topologien

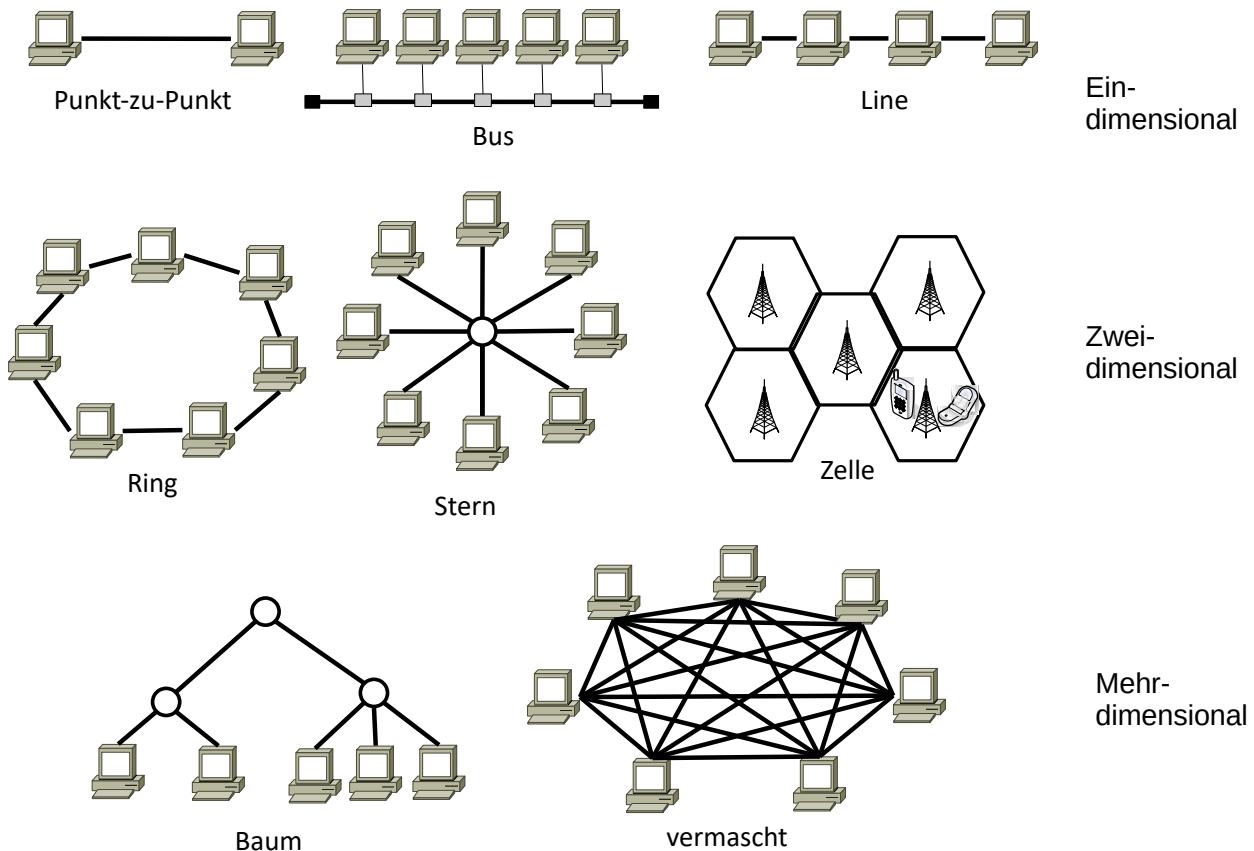


Abbildung 186: Topologieformen

Damit ist die Anzahl der unabhängigen Wege beschrieben, was auch ein Maß für die Ausfallsicherheit der Topologie darstellt.

Folgenden Topologien können unterschieden werden:

● **Punkt-zu-Punkt**

Diese einfachste Form der Verbindung von zwei Geräten erfordert bei einer Kupfer-basierten Verbindung nur eine spezielle Leitung (Crossover-Leitung). Bei einer Funk-basierten Verbindung ist die Ad-hoc-Topologie zu wählen. Da nur zwei Geräte miteinander kommunizieren, kann auf Medien-Zugriffsverfahren verzichtet werden. Fällt ein Gerät aus, kommt der Datenaustausch zum Erliegen. Erweiterungen sind nicht möglich.

● **Bus**

Diese Form stellt die Urform des Ethernet dar. Jedes Gerät greift über einen Transceiver auf das Medium Bus zu. Alle erforderlichen Funktionen, wie etwa das Medienzugriffsverfahren, leiten sich daraus ab, denn es handelt sich hierbei um ein „Shared Media“. Eine zentrale Geräte zur Koordinierung des Zugriffs gibt es nicht. Fällt ein Gerät aus, können alle anderen Geräte weiter miteinander kommunizieren. Wird der Bus unterbrochen, ist keine Kommunikation mehr möglich, da die verbleibenden Bussegmente nicht mehr korrekt abgeschlossen sind. Änderungen können zur Unterbrechung führen.

● **Linie**

Die auch Daisy-Chain genannte Topologie wird in der Automatisierungs- und Sicherheits-Technik verwendet. Bis auf die Hosts am Ende haben alle Teilnehmer zwei Partner. Fällt eine Verbindung oder auch ein Host aus, funktioniert die Topologie nicht mehr. Änderungen können zur Unterbrechung führen.

● **Ring**

Der Zugriff auf dieses Medium ist ebenfalls zu koordinieren. Dazu ist eine Managerstation zu empfehlen. Eine Unterbrechung des Rings führt zum Erliegen des Datenverkehrs. Der Vorteil der Ring-Topologie ist, dass die maximale Dauer des Datentransfers gewährleistet werden kann. Änderungen führen zur Unterbrechung während er Arbeiten.

● **Stern**

Bei der Stern-Topologie gibt es einen zentralen Netzwerk-Knoten. Diese Topologie ist abhängig von den verwendeten Netzwerk-Komponenten, denn es hat Konsequenzen für einen evtl. erforderlichen Einsatz eines Medien-Zugriffsverfahrens. Bei Verwendung von Hubs ist ein Medien-Zugriffs-Verfahren zu verwenden, da es sich um ein „Shared Media“ handelt. Bei Switches ist kein Medien-Zugriffsverfahren erforderlich. Änderungen können unterbrechungsfrei durchgeführt werden.

● **Baum**

Diese Topologieform ist eine Erweiterung der Stern-Topologie. Daher gelten die gleichen Bedingungen wie bei der Stern-Topologie. Diese Topologie ist die am häufigsten verwendete.

● **Vermascht**

Diese Topologieform bietet die größte Ausfallsicherheit. Allerdings ist hierbei auch der größte Aufwand erforderlich. Ein Medienzugriffsverfahren ist nicht erforderlich, da zwischen den verwendeten Switches oder Routern Punkt-zu-Punkt-Beziehungen bestehen.

● **Zelle**

Eine Zelle ist die Grundform bei den Funknetzwerken und gekennzeichnet durch eine Antenne und bewegliche Clients. Da es sich um ein Shared Media handelt ist ein Medienzugriffsverfahren erforderlich. Eine Erweiterung kann einfach durch anmelden am Medium erfolgen. Allerdings sinkt dadurch die durchschnittliche Datenübertragungsrate.

Topologie	Erweiterbarkeit	Zugriffs-verfahren	Anwendung
Punkt-zu-Punkt Point-to-Point (PtP)	n. a.	n. a.	Ad-hoc-Verbindung von nur zwei Geräten
Bus	Ja, Host durch neuen Transceiver Segment durch Repeater (max4)	Ja, z.B. CSMA/CD	10Base5 10Base2
Linie Daisy-Chain	Ja, neues Gerät	Ja, z.B. beim CAN-Bus CSMA/CR	CAN-Bus
Ring	Ja, neues Gerät	Ja, Token Passing	Token Ring (IEEE802.5)
Stern	Ja, neues Gerät	Bei Hub: CSAM/CD Bei Switch: n. a.	10Base-T 100Base-T 1000Base-T
Baum	Ja, neues Gerät	Bei Hub: CSAM/CD Bei Switch: n. a.	10Base-T 100Base-T 1000Base-T
Vermascht	Ja, neues Gerät		Internet
Zelle	Ja, neues Gerät	Ja, z.B. CSMA/CA	WLAN GSM

Topologien

Der Begriff Topologie wird unter unterschiedlichen Gesichtspunkten verwendet.

- Physikalische Topologie

Die physikalische Topologie beachtet mit welchen Komponenten die Netzwerke aufgebaut werden und wie diese miteinander verbunden sind. Hierbei wird detailliert auf die einzelnen Netzwerkkomponenten eingegangen. Auch redundante Anbindungen werden hier dargestellt.

- Logische Topologie.

Bei der logischen Topologie ist die Funktionsweise und damit der Datenfluss im Netzwerk entscheidend. Es gibt zum Beispiel Bus-Topologien oder Ring-Topologien. Die logische Struktur stellt z. B. die Adressierung der Netzwerk-Teilnehmer dar.

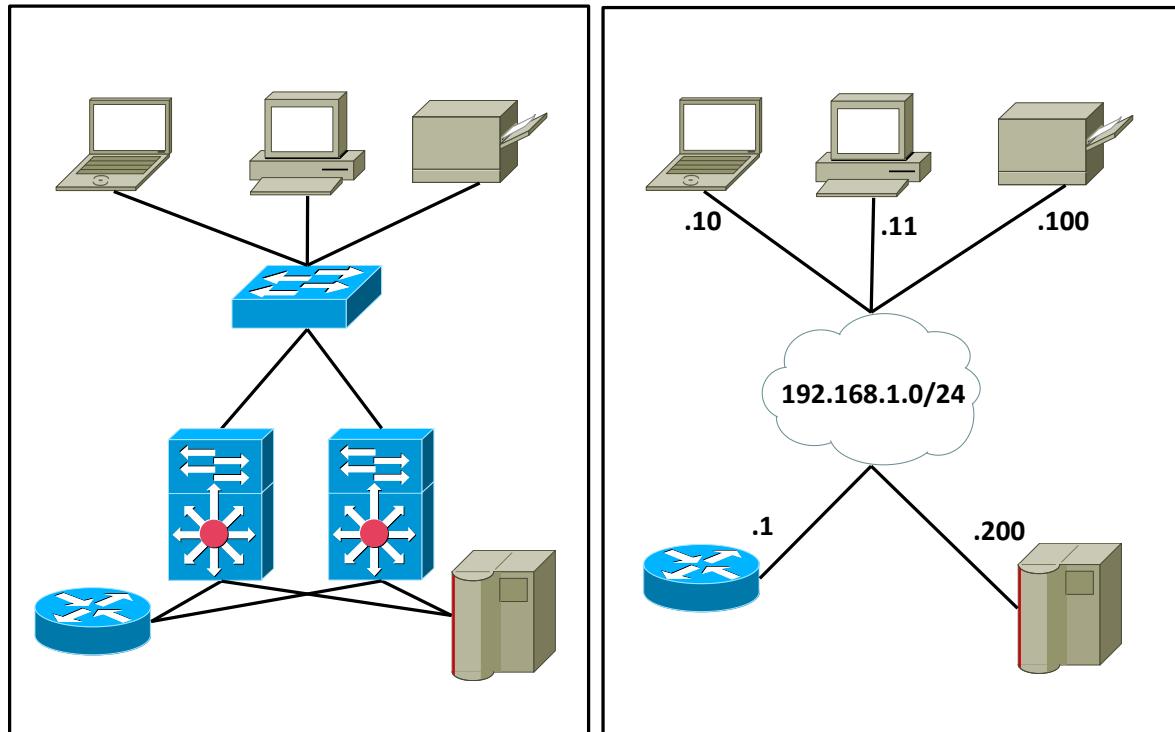


Abbildung 187: Physikalische und logische Topologie

11.3 - Logische Topologie

Bei dieser Betrachtungsweise ist die Funktionsweise eines Netzwerks, oder auch der Datenfluss über mehrere Netzwerke hinweg, entscheidend. Es gibt zum Beispiel Bus-Topologien oder Ring-Topologien. Hier werden Themen wie Medienzugriffsverfahren usw. betrachtet. Es besteht ein Zusammenhang zwischen der logischen Topologie und der Verkabelungstopologie. Je nach Netzwerk-Protokoll können unterschiedliche Ausprägungen realisiert werden.

Netzwerk-Protokoll	Logische Topologie	Physikalische Topologie
Token Ring	Ring	Ring, Stern
High Speed Token Ring	Ring	Ring, Stern
FDDI	Ring	Ring, Stern
Ethernet (10 Mbps)	Bus	Bus, Stern, Punkt zu Punkt
Fast Ethernet (100 Mbps)	Bus, Punkt zu Punkt	Stern, Punkt zu Punkt
Gigabit Ethernet (1000 Mbps)	Bus, Punkt zu Punkt	Stern, Punkt zu Punkt
ATM	Virtual Path / Channel	Ring, Stern

11.4 - Physikalische Topologie

Die physikalische Topologie beachtet mit welchen Komponenten die Netzwerke aufgebaut werden und wie diese miteinander verbunden sind. Hierbei wird detailliert auf die einzelnen Netzwerkkomponenten eingegangen. Auch redundante Anbindungen werden hier dargestellt.

Die Topologie folgt den Anforderungen einer einfach wartbaren Struktur. Das ist im allgemeinen eine Stern- / Baum-Struktur.

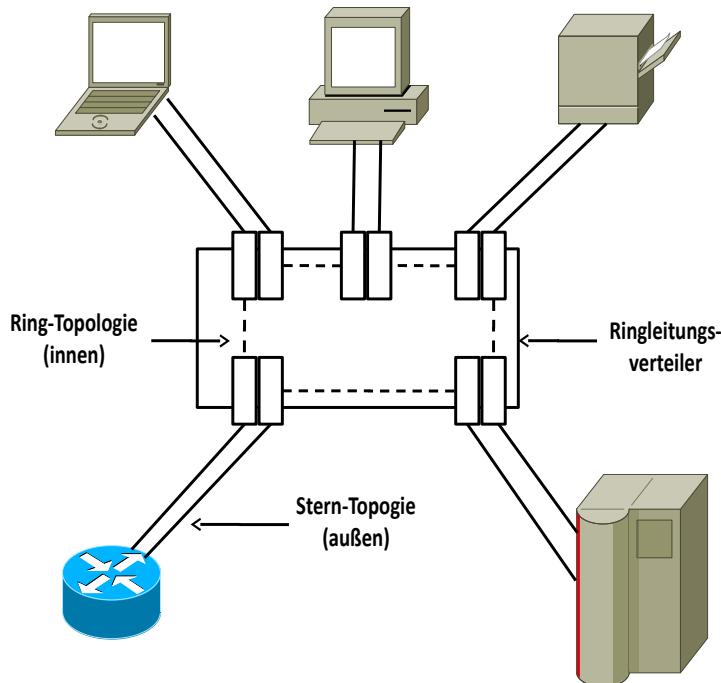


Abbildung 188: Ring-Topologie mit äußerer Stern-Struktur

Aus der obigen Tabelle kann entnommen werden, dass je nach Netzwerk-Protokoll eine andere Topologie zur Anwendung kommt. Dabei erschließt der äußere, sichtbare Aufbau nicht immer die innere Logik einer Topologie. So kann z. B. Ethernet in seiner 10 Mbps-Variante als Bus (10Base5), als Punkt-zu-Punkt oder als Stern realisiert werden. Dies ist abhängig von den eingesetzten Netzwerkgeräten.

11.5 - Topologie-Vergleich

Topologie	Beispiele von Realisierungen	Medien-Zugriffsverfahren	Bemerkung
Bus	10Base-T 10Base2 10Base5	CSMA/CD	
Punkt-zu-Punkt	10Base-T Verbindung zweier Rechner 1000Base-T	Kein Zugriffsverfahren erforderlich	
Linie	CAN-Bus	CSMA/CR	
Ring	Token-Ring FDDI CDDI	Token Passing	
Stern	Siehe Baumstruktur	Siehe Baumstruktur	Sonderform der Baumstruktur
Baum	10Base-T / 100Base-T / 1000Base-T mit Hubs / Switches	CSMA/CD bei Hubs. Kein Zugriffsverfahren bei Switches	Zwischen den Switches bestehen Punkt-zu-Punkt Verbindungen
Vermascht	Proprietäre Ethernet-Lösungen Mesh (HP) / MPLS / ATM	Kein Zugriffsverfahren erforderlich	
Zelle	IEEE-802.11 (WLAN)	CSMA/CA	

Eigenschaften verschiedener Realisierungen von unterschiedlichen Topologien

Bezeichnung	Medium	Datenrate [Mbps]	Max. Ausdehnung	Max. Knotenzahl pro Seg.	Max. Frame-/Zellen-Länge
Ethernet	LWL / Kupfer	10/100/1000/10000	2,5 km (Cu) 40 km (LWL)	1024	1518 Bytes
FDDI	LWL bei < 100m Kupfer	100	100 km	1000	9000 Bytes
Token Ring	Kupfer	16/4	500 m	100	2000 Bytes 5000 Bytes
ATM	LWL	155/622			53 Bytes

12 - Kupferverkabelung

12.1 - Symmetrische / Unsymmetrische Leitungen

Hierbei ist nicht der geometrische Aufbau der Leitung gemeint, sondern das elektrische Verhalten der Leitungen, bezogen auf die Erde.

12.1.1 - Symmetrische Leitungen

Ein symmetrischer Leiter besteht immer aus zwei Adern und der Bezugserde. Durch die Netzwerk-Schnittstellen werden die beiden Adern so angesteuert, dass sie das gleiche Signal, jedoch mit entgegengesetzter Polarität, haben. Im Idealfall addieren sich die beiden Signalamplituden zu 0. Da die Bezugserde beim Empfänger nicht verwendet wird, sind diese Leitungen auch gegen elektromagnetische Störungen im Idealfall unempfindlich.

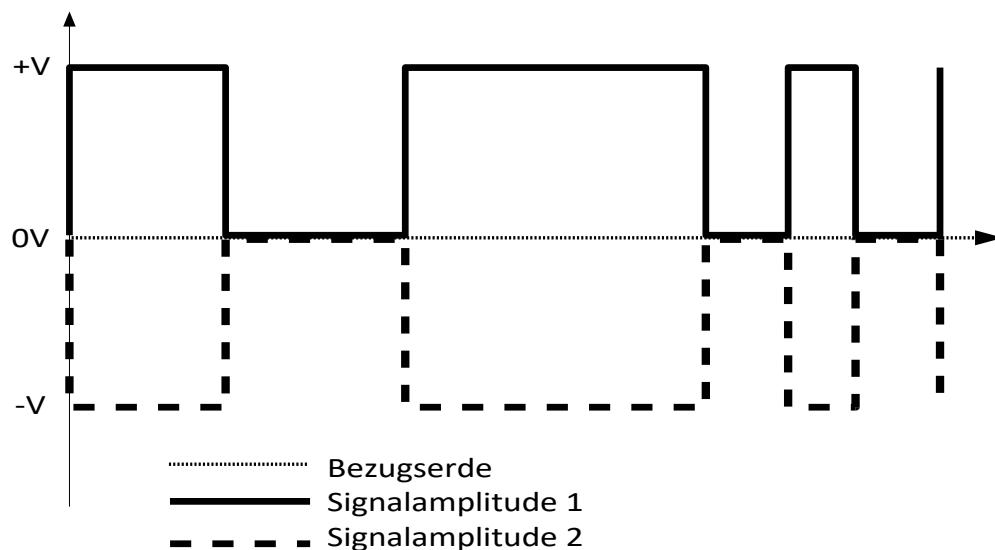


Abbildung 189: Symmetrische Leitungen

12.1.2 - Unsymmetrische Leitungen

Unsymmetrische Leitungen haben, bezogen auf die Erde nicht ständig den Wert 0. Hier wird die Schirmung zur Rückführung des Stroms mit eingebunden. Der Außenschirm wird auch als Außenleiter bezeichnet. Diese Leitungen sind anfällig gegen Störungen und Erdpotential-Probleme.

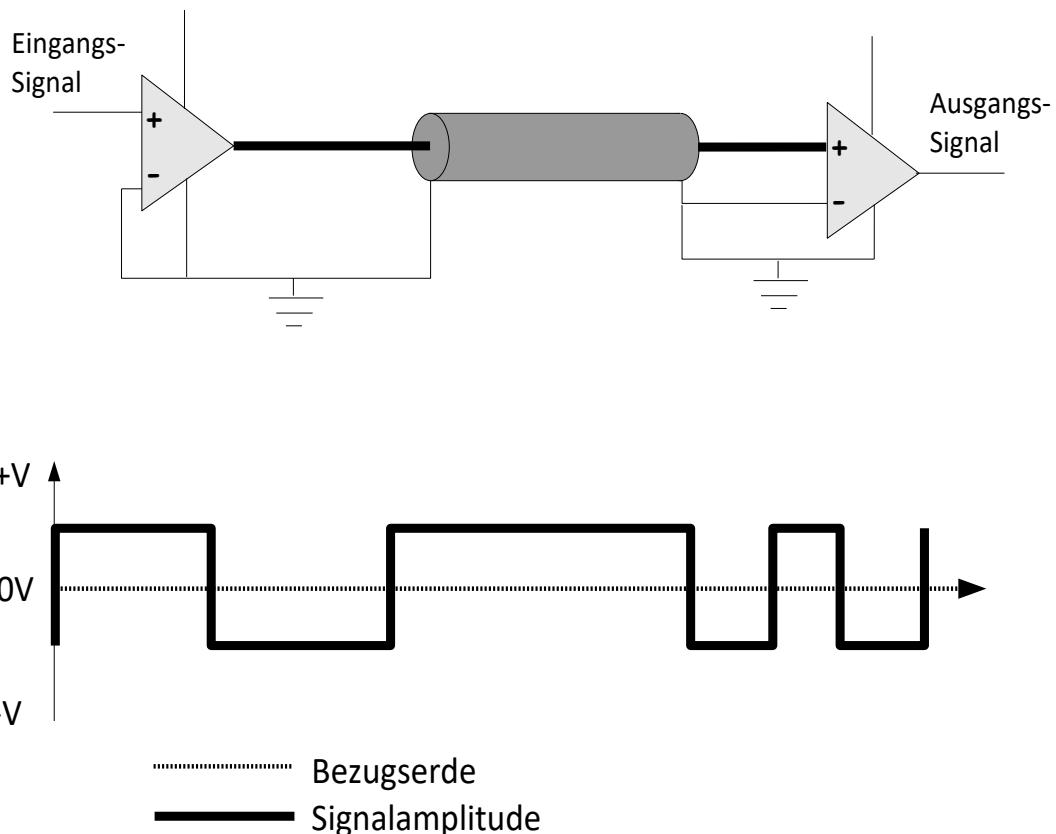


Abbildung 190: Unsymmetrische Leitungen



Abbildung 3: BALUN

Adapter zwischen den Leitungssystemen

Für die Umsetzung von symmetrischen auf unsymmetrische Leitungen gibt es so genannte Baluns. Der Name setzt sich aus den Wörtern **balanced** und **unbalanced** zusammen.

12.2 - Koaxialkabel

12.2.1 - Yellow-Cable

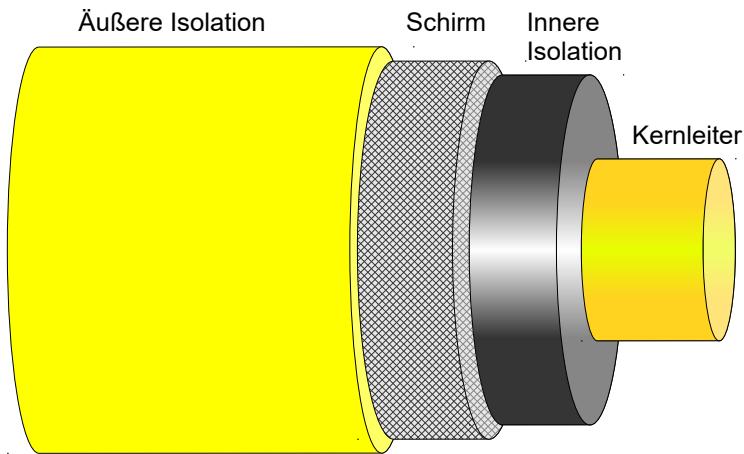


Abbildung 191: Yellow-Cable

Der Wellenwiderstand, die so genannte Impedanz, beträgt 50Ω . Im Handel wird diese Leitung mit RG8A/U bezeichnet. Es handelt sich hierbei um einen unsymmetrischen Leiter.

IEEE-802.3 schreibt die gelbe Farbe nicht vor, empfiehlt sie aber. Graue Kabel sind ebenso anzutreffen. Man wollte eine Signalfarbe verwenden, da die Leitungen bei 10Base5 angebohrt werden um Transceiver zu setzen, was bei stromführenden Leitern fatal wäre.

Wird für 10Base5 eingesetzt. Dort ist die maximale Segmentlänge 500m.

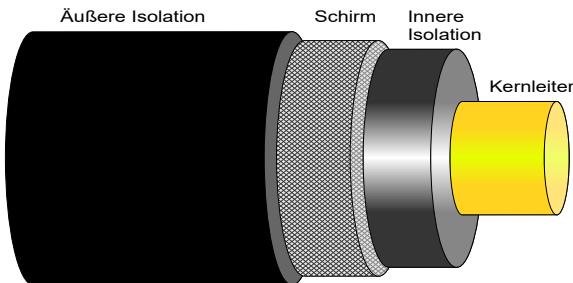


Abbildung 192 – CheaperNet-Kabel

12.2.2 - CheaperNet-Cable

Die Impedanz der Leitung beträgt im Allgemeinen 50Ω . Es handelt sich um eine unsymmetrische Leitung. Die genaue Bezeichnung lautet RG58.

Das 10Base2-Kabel sieht ähnlich aus, darf aber mit RG58/U-Kabel nicht gemischt werden.

RG59B wird für das Kabelfernsehen verwendet und hat eine Impedanz von 75 Ohm.

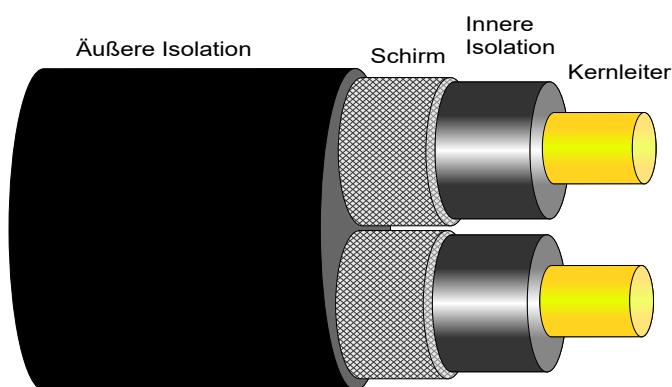
RG62A wird als Arcnet-Kabel bezeichnet und hat eine Impedanz von 93 Ohm.

Kabel	Impedanz	Geschwindigkeit (bez. auf c)
RG-58A/U	50Ω	0.66 oder 0.78
RG-58C/U	50Ω	0,66
RG-58/U	53.5Ω	0.66 oder 0.696

Bei 10Base2 ist die maximale Segmentlänge 185m.



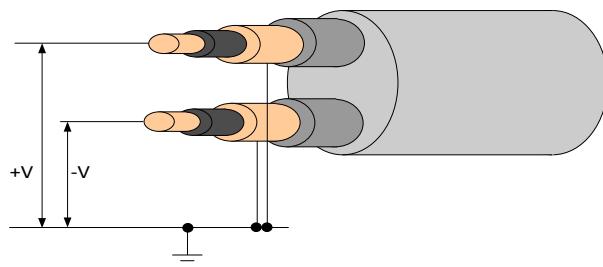
12.2.3 - Twin-Koax-Leitung



Diese Leitung ist nur noch selten in Altanlagen anzutreffen. Hierbei beträgt die Impedanz 105Ω .

Bei 1000Base-CX fand diese Lösung Anwendung bei der Verkabelung in Rechenzentren. (Maximallänge = 25m)

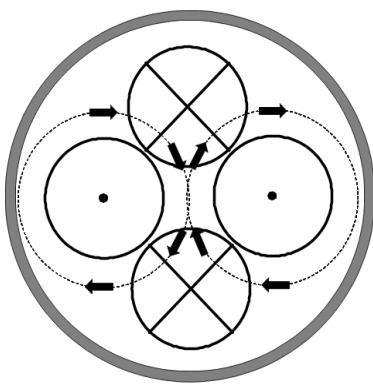
Abbildung 193 – Twin-Koaxial-Leitung



Die Bezeichnung ist AC_BAL. Daraus kann bereits abgeleitet werden, dass es sich um eine symmetrische Leitung (engl. balanced) handelt.

Abbildung 194: Symmetrische-Twin-Koax-Leitung

12.3 - Sternvierer



Drähte die in 4er-Gruppen miteinander verdrillt werden, kommen im Telefon-Bereich zum Einsatz und werden auch Stern-Vierer genannt. Diese Leitungen sind nur bis maximal 10Mbps zu gebrauchen!

Abbildung 195: Sternvierer

12.4 - Twisted Pair Kabel (TP)

Bei Twisted-Pair-Leitungen handelt sich um symmetrische Leitungen.

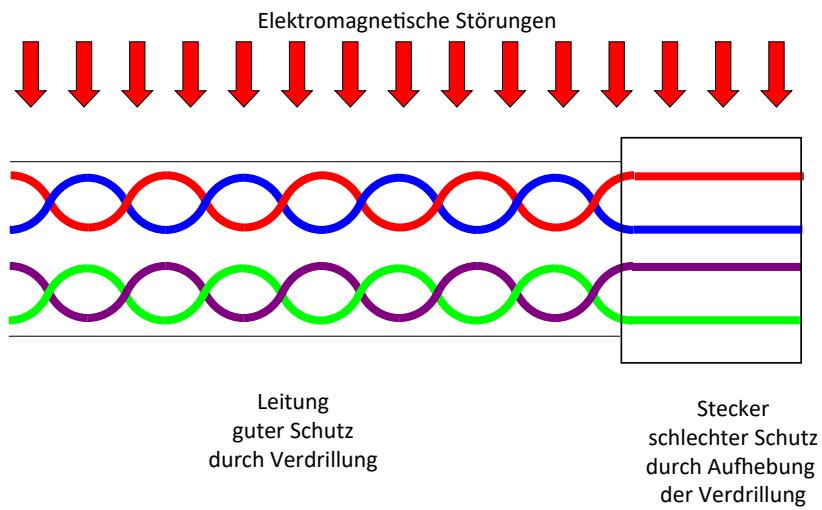


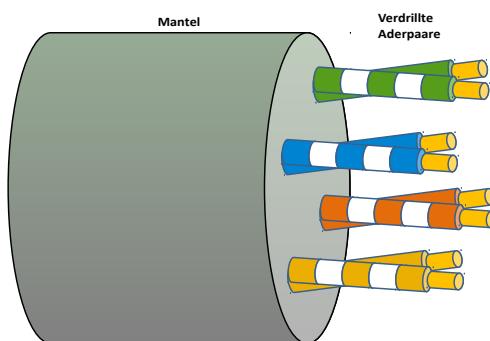
Abbildung 196: Twisted-Pair-Leitung

Hierbei werden Drähte paarweise miteinander verdrillt.

Dabei werden die Einflüsse durch die Tatsache, dass Sie über eine Verdrillung von beiden Seiten gleich einwirken, eliminiert.

Über die verdrillte Leitung hinweg können so Störungen eliminiert werden. An den Steckern, wo die Verdrillung aufgehoben werden muss, sind Störungseinflüsse messbar.

12.4.1 - Unshielded-TP-Kabel (UTP)



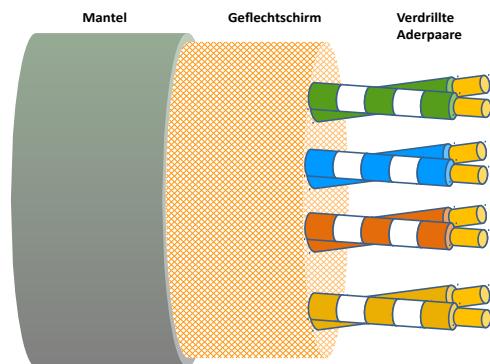
Die Impedanz für TP-Leitungen beträgt immer 100 Ohm.

Dem Namen nach handelt es sich hier um ungeschirmte Leitungen bei denen die Aderpaare miteinander verdrillt sind.

Je nach Verwendung oder Kodierung der Signale, sind unterschiedliche Frequenzen und somit, wegen der unterschiedlichen Dämpfung, unterschiedliche Segmentlängen möglich.

Abbildung 197: UTP-Kabel

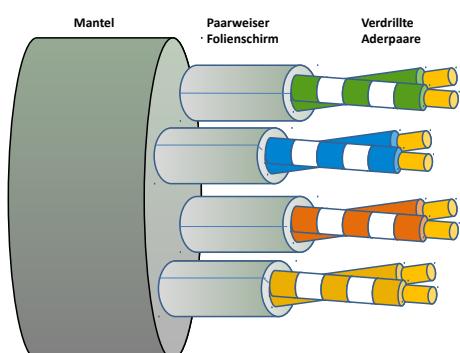
12.4.2 - Shielded-TP-Kabel (STP)



Hierbei sind die Adernpaare wiederum miteinander verdrillt. Die obige Abbildung zeigt, wie alle verdrillten Adernpaare mit einem Geflechtschirm, gegen elektromagnetische Einflüsse geschützt werden.

Abbildung 198: STP-Kabel

12.4.3 - Unshielded Foiled TP (UFTP)

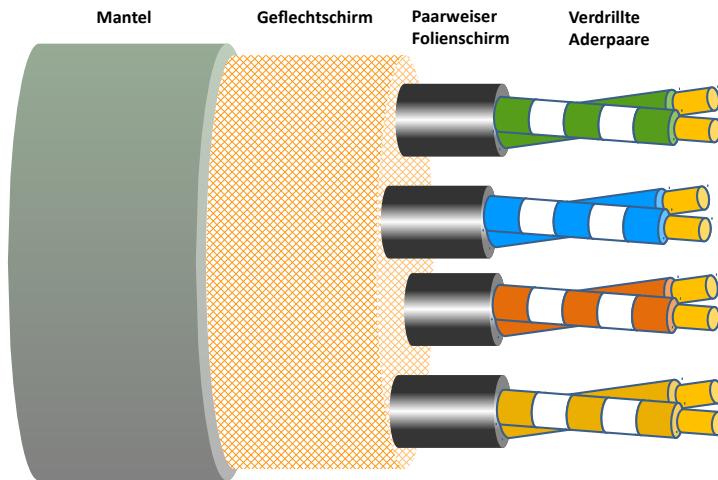


Sind die einzelnen Paare mit einem Folienschirm gegeneinander abgeschirmt, spricht man von einem Unshielded Foiled Twisted Pair oder auch PiMF (Pair in Metal Foil)

Abbildung 199: PiMF

12.4.4 - Screened shielded TP (SSTP/SFTP)

Geflecht und paargeschirmtes Datenkabel



Durch die doppelte Schirmung werden unterschiedliche Störeinflüsse erfolgreich unterdrückt. So werden über einen Folien- und einen Geflechtschirm magnetische und elektrische Strahlungen effektiv abgeschirmt. Die gegenseitige Beeinflussung der Adernpaare (siehe auch NEXT und FEXT), kann so wirksam minimiert werden.

Abbildung 200: SSTP/SFTP-Kabel

Übersicht über die Verwendung der unterschiedlichen Leitungstypen

Kabeltyp	EIA/TIA 568 Kategorie, Kat. Category, Cat.	DIN EN 50173 Klasse	Max. Frequenz	Impedanz	Anwendung / Bemerkung
UTP-1	Cat.1	-	0,3 ... 3,4 kHz	100 Ohm	analoge Sprachübertragung
UTP-1	-	A	100 kHz	100 Ohm	analoge Sprachübertragung
UTP-2	Cat.2	B	1 MHz	100 Ohm	ISDN
UTP-3	Cat.3	C	16 MHz	100 Ohm	10Base-T, 100Base-T4, ISDN
UTP-4	Cat.4	-	20 MHz	100 Ohm	16 Mbit Token Ring
STP	IBM Typ 1/9		20 MHz	150 Ohm	4 und 16 Mbit Token Ring
S/FTP	Cat.5	D	100 MHz	100 Ohm	100Base-TX, SONET, SOH
	Cat.5e	D	100 MHz	100 Ohm	1000Base-T
S/FTP	Cat.6	E	250 MHz	100 Ohm	155-Mbit-ATM, 622-Mbit-ATM
	Cat.6 _e	E	500 MHz	100 Ohm	-
	Cat.6 _a	F	625 MHz	100 Ohm	10GBase-T
S/FTP	Cat.7	F	600 MHz	100 Ohm	GG45-Stecker
S/FTP	Cat.7 _a	F	1000 MHz	100 Ohm	40GBase-T, 100GBase-T
S/FTP	Cat 8	G	1600 – 2000 MHz		Max. 30m! 40GBase-T, 100GBase-T

12.5 - Übersicht über Kabeltypen nach IEEE-802.3 bei LAN's

Für eine vollständige Darstellung wurden hier die LWL-Kabel ebenfalls dargestellt.

12.5.1 - 10 Mbps - Verkabelung

Bezeichnung	Daten-Rate In Mbps	Kabel	Topologie	Max. Segment-Länge	Max. Knotenanz./Seg.
10Base2	10	Dünnes Koaxialkabel	Bus	185 m	30
10Base5	10	AUI-Kabel	Endgerät-Transceiver	50m	
10Base5	10	AUI-Kabel mit Schnittstellenvervielfacher	Endgerät-SSV	40m	
10Base5	10	Dickes Koaxialkabel	Bus	500 m	100
10Base-T	10	2 verdrillte Aderpaare	Stern	100 m	1024
10Base-F	10	Glasfaserpaar	Punkt zu Punkt	2000 m bei * = 850nm mit MM-Faser 5000m bei * = 1300nm mit MM-Faser 20000m bei * = 1300nm mit SM-Faser	1024
10Broad36	10	Dickes Koaxialkabel	Bus	3600	?

12.5.2 - 100 Mbps - Verkabelung

Bezeichnung	Daten-Rate In Mbps	Kabel	Topologie	Max. Segment- Länge	Max. Knotenanz./Seg.
100Base-Fx	100	LWL	Punkt zu Punkt	412 m MM HD (ohne Repeater) 305m MM HD (mit 1 Repeater) 210m MM HD (mit 2 Repeater) 2000m MM FD 20-40km SM (FD CF ohne Repeater)	1024
100Base-Sx	100	LWL	Punkt zu Punkt	300m MM/SM mit * = 850nm	
100Base-T2 CAT5	100	2 verdrillte Aderpaare	Punkt zu Punkt	100m (Switch- Switch) 200m MM HD (mit 1 Repeater) 210m MM HD (mit 2 Repeater)	1024
100Base-T4 CAT3	100	4 verdrillte Aderpaare	Punkt zu Punkt	205 m	1024

12.5.3 - 1000Mbps / 1Gbps - Verkabelung

Bezeichnung	Daten-Rate In Mbps	Kabel	Topologie	Max. Segment-Länge	Max. Knotenanz./Seg.
1000Base-CX	1.000	Geschirmtes Twinax-Kabel	Punkt zu Punkt	25 m	1024
1000Base-T	1.000	4 verdrillte Aderpaare	Punkt zu Punkt	100 m	1024
1000Base-LX 62,5µ Faser	1.000	Long Wavelength Duplex-Multimode-Glasfaser	Punkt zu Punkt	2m - 440m	1024
1000BASE-LX 50µ Faser	1.000	Long Wavelength Duplex-Multimode-Glasfaser	Punkt zu Punkt	2m - 550m	1024
1000BASE-LX 10µ Faser	1.000	Long Wavelength Duplex-Monomode-Glasfaser	Punkt zu Punkt	2m - 3000m	1024
1000Base-SX 62,5µ Faser	1.000	Short Wavelength Duplex-Multimode-Glasfaser	Punkt zu Punkt	2m - 260 m	1024
1000BASE-SX 50µ Faser	1.000	Short Wavelength Duplex-Multimode-Glasfaser	Punkt zu Punkt	2m - 550m	1024
1000BASE-LX 10µ Faser	1.000	Long Wavelength Duplex-Monomode-Glasfaser	Punkt zu Punkt	2m - 3000m	1024

12.5.4 - 10Gbps - Verkabelung

Bezeichnung	Daten-Rate [Gbps]	Kabel	Topologie	Max. Segment-Länge	Max. Knotenanz./Seg.
10GBase-T	10	4 verdrillte Aderpaare	Punkt zu Punkt	100 m mit CAT6a oder höher	1024
10GBase-T	10	4 verdrillte Aderpaare	Punkt zu Punkt	55 m mit CAT 6e	1024

12.5.5 - Aufbau der Topologie-Bezeichnung

Die Bezeichnung baut sich folgendermaßen auf:

< Datenrate [Mbit] >< Übertragungsverfahren >< Maximallänge/100m | -Topologie >

12.5.5.1 - Datenraten

- ➊ 10 Die Auslegung ist auf **10 Mbps** begrenzt.
- ➋ 100 Die Auslegung ist auf **100 Mbps** begrenzt. (Megabit-Ethernet)
- ➌ 1000 Die Auslegung ist auf **1 Gbps** begrenzt. (Gigabit-Ethernet)
- ➍ 10G Die Auslegung ist auf **10 Gbps** begrenzt. (10 Gigabit-Ethernet)
- ➎ 100G Die Auslegung ist auf **100 Gbps** begrenzt. (100 Gigabit-Ethernet)

12.5.5.2 - Übertragungsverfahren

➊ Base

Es wird eine **Basisband-Zeichengabe** benutzt. Dies bedeutet, dass nur eine Übertragungs-Frequenz benutzt wird was zur Folge hat, dass immer nur eine Station senden kann. Die Sende-Berechtigung wird über ein Zugriffsverfahren wie CSMA/CD oder Token geregelt.

➋ Broad

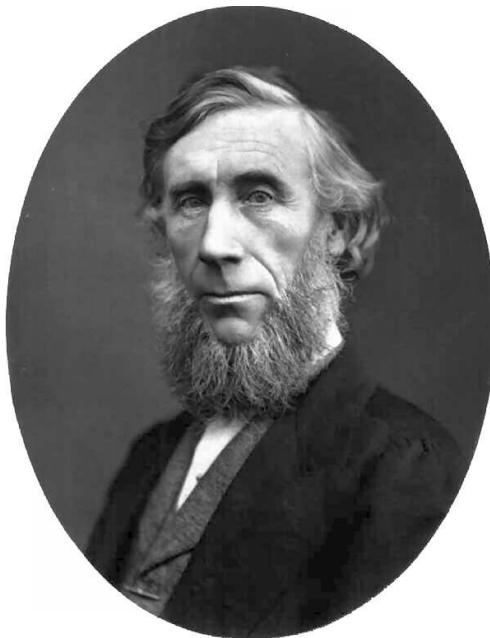
Es wird eine **Breitbandband-Zeichengabe** benutzt. Hier werden mehrere Frequenzen genutzt. Dies hat zur Folge, dass mehrere Stationen gleichzeitig senden können. Allerdings muss jedes Signal auf eine Trägerfrequenz aufmoduliert werden. Da dies sehr aufwändig ist, wurde nur ein Standard (10Broad36) definiert, der allerdings keine Marktakzeptanz fand.

12.5.5.3 - Maximallänge

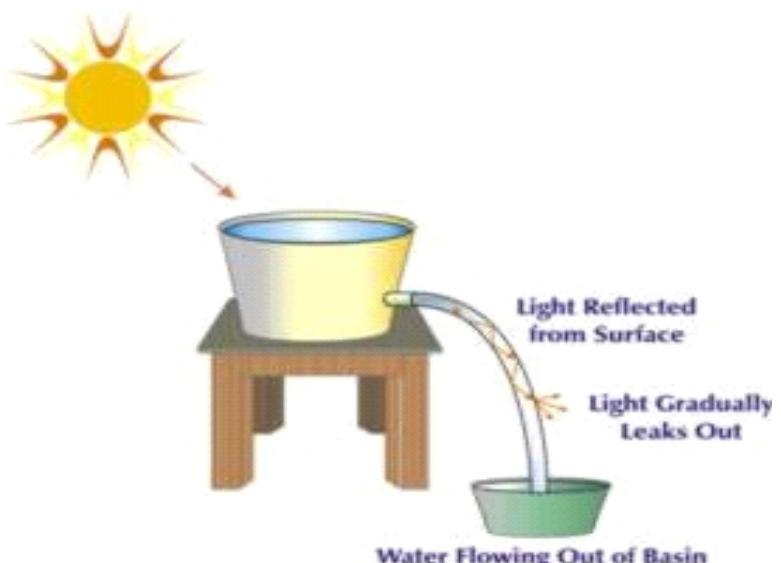
- 2 Maximale Ausdehnung 200m (genau 185m)
- 5 Maximale Ausdehnung 500m
- 36 Maximale Ausdehnung 3600m
- T Twisted-Pair (max. 100m)
- F Fiber-Optic
- LX Long Wavelength Fiber-Optic (max. 1500m)
- SX Short Wavelength Fiber-Optic (max. 500m)
- FD Full Duplex
- HD Half Duplex
- CF Collision Free
- MM Multimode LWL
- SM SingleMode LWL

13 - Lichtwellenleiter

13.1 - Historisches



John Tyndall (1820-1893) machte **1870** ein Experiment bei dem Licht in einem Wasserstrahl als Übertragungsmedium geleitet wurden. Die Lichtquelle war dabei die Sonne.



In den **1950er** Jahren wurden erste Fasern mit hohen Verlustraten hergestellt. Durch das Aufbringen eines Glasmantels (engl.: cladding) um den Glaskern konnten die Verluste dramatisch gesenkt werden. Durch den großen Brechungsindexunterschied zwischen Glasmantel und Glaskern wird ein Lichtstrahl vollständig reflektiert.

Durch die Entwicklung von LEDs und Laserdioden in den **1960er** Jahren bekam diese Technologie einen ersten Auftrieb.

1970 stellte Corning Glass Works (USA) und Nippon Electric Co. (NEC Japan) die ersten brauchbaren Glasfasern mit Dämpfungswerten von 20 dB/km her. Diese Glasfasern arbeiteten alle noch im ersten Fenster bei 850nm.

Im Laufe des restlichen Jahrzehnts wechselten die Hersteller in das dritte Fenster bei 1550nm um die Verluste weiter zu verringern.

13.2 - Allgemeines

Die Grundlage für die Datenübertragung mit Licht, beruhen auf der Lichtbrechung, sowie der Reflexion von Licht. In optisch dichteren Medien bewegt sich das Licht langsamer, als in optisch dünnen Medien.

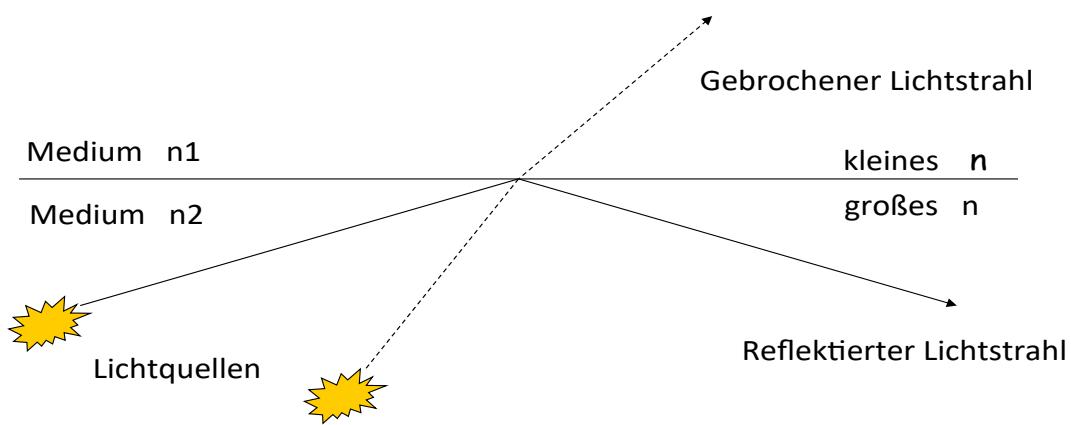


Abbildung 201 - Lichtbrechung

Aus den verschiedenen Geschwindigkeiten der lichtdurchlässigen Medien (v) verglichen mit der Ausbreitungsgeschwindigkeit im Vakuum (c) ergibt sich die Brechzahl (n).

$$n = c/v \quad (91)$$

Der Brechungsindex verschiedener Medien

Medium	Brechungsindex
Glas	1,5
Wasser	1,33
Vakuum	1

13.2.1 - Vorteile der Lichtwellenleiter gegenüber Kupferkabel

- Lichtwellenleiter können beliebig mit anderen Versorgungsleitungen parallel verlegt werden. Es wirken keine elektromagnetischen Störeinflüsse.
- Wegen der optischen Übertragung existieren keine elektrischen Potentialprobleme.
- Entfernungsbedingte Verluste durch Induktivitäten, Kapazitäten und Widerständen treten nicht auf.
- Nahezu Frequenz-unabhängige Leitungsdämpfung der Signale.
- Übertragungsraten sind durch mehrere Trägerwellen mit unterschiedlichen Wellenlängen (Farbspektrum) fast unbegrenzt erhöhbar.
- Lichtwellenleiter haben eine erheblich geringere Dämpfung und eignen sich somit für weite Strecken.

Nachteile der Lichtwellenleiter gegenüber Kupferkabel

- Teurer als Kupferleitungen. Die Kosten für Material und der Aufwand bei der Montage sind höher.
- Lichtimpulse lassen sich nicht zwischenspeichern. Wegen fehlender optischer Signalspeicher und Verarbeitungselementen muss eine aufwendige optisch/elektrisch und elektrisch/optische Signalumwandlung statt finden.

Die derzeit verwendeten Glasfasern weisen, je nach Typ, verschiedene Fenster im Dämpfungsverlauf über die Wellenlänge auf. Bei einer Wellenlänge von 850nm, 1300nm und 1500nm, zeigen sich durch Streuung und Absorption kleinere Dämpfungswerte.

Insgesamt sind 7 Wellenlängenbereiche festgelegt.

Von IEEE wurde im F1-Fenster (850 nm) festgelegt, dass Gigabit-Ethernet übertragen wird.

Von der ITU wurden 6 Wellenlängenbereiche in den oberen beiden optischen Fenstern (F2 = 1300nm, F3 = 1500nm) festgelegt.:.

F2:

O-Band Original-Band 1260-1360 nm

F3:

E-Band Enhanced-Band 1360-1460 nm

S-Band Shortwave-Band 1460-1530 nm

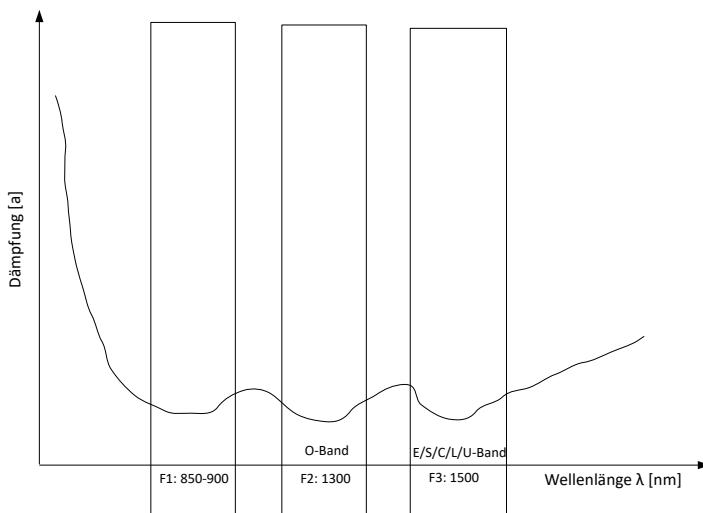
C-Band Conventional-Band 1530-1565 nm

L-Band Longwave-Band 1565-1625 nm

U-Band Ultra-Longwave-Band 1625-1675 nm

Typische Dämpfungswerte liegen bei 3dB/km im F1-Fenster und 0,1dB/km in F2-Fenster.

Diese Fenster werden für die Datenübertragung verwendet. Dazu sind speziell für diese Wellenlängen produzierte LEDs oder Laserdioden im Einsatz.



Lichtwellenleiter bzw. Glasfaserkabel sind nach ITU-T G.651 bis G.657, ISO/IEC 11801 und 24702 und IEC 60793 international genormt, sowie nach DIN VDE 0888 national genormt

Abbildung 202 – Dämpfungsverlauf bei verschiedenen Wellenlängen

Lichtstrahlen, können verschiedene Wege nehmen und somit unterschiedlich lange Zeit durch ein Glasfaserkabel benötigen. Licht, das in einem Winkel nahe des maximalen Einfallswinkels in den LWL eintritt, wird Licht hohen Modes genannt und oft reflektiert. Dieser Lichtstrahl hat den längsten Weg zurückzulegen und braucht somit auch die längste Zeit. Licht, welches entlang der optischen Achse des LWL in den LWL eintritt, wird Licht niedrigen Modes genannt, und gar nicht oder sehr selten umgelenkt. Dieser Lichtstrahl kommt als erster am Ziel an. Die unterschiedliche Ausbreitungsgeschwindigkeit der einzelnen Lichtstrahlen eines Impulses führt zu einer Dehnung des Eingangs-Impulses. Dies wird Dispersion genannt und bedeutet letztendlich eine Signal-Verzerrung. Siehe folgende Abbildung.

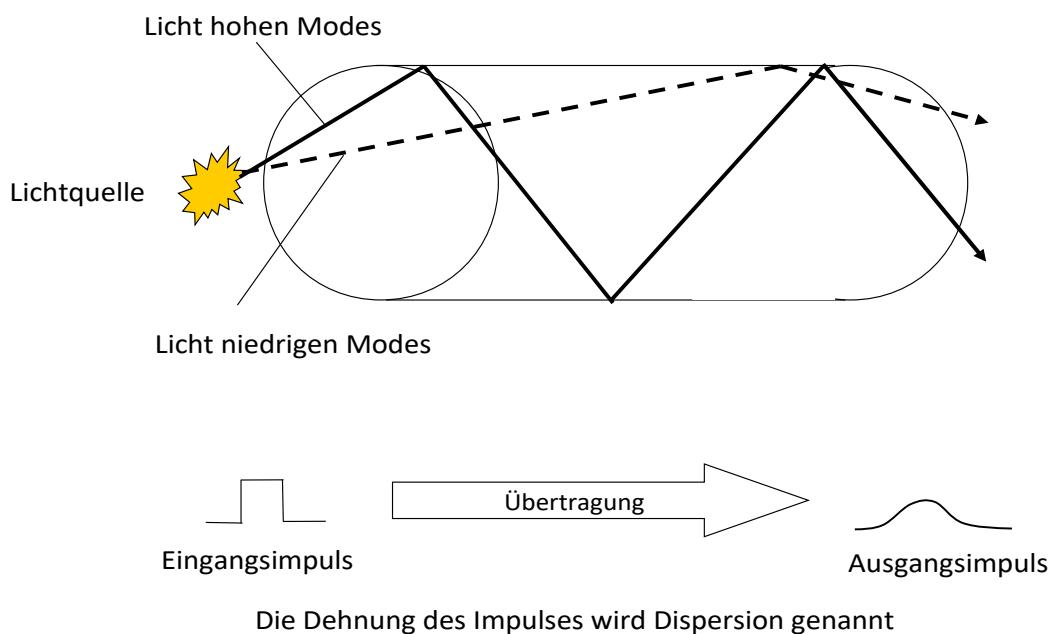


Abbildung 203 – Reflexion der Lichtstrahlen in Glasfaser

13.2.2 - Multimode-Fasern

Die Multimode-Fasern werden als Stufenindex und als Gradienten-Faser hergestellt. In der folgenden Abbildung ist zu sehen, wie das Licht in mehreren verschiedenen Winkeln, in die Glasfaser eintritt. Es wird, je nach Winkel, verschieden oft umgelenkt. Dies bedeutet, dass ein Lichtimpuls am Ende der Faser, mit unterschiedlichen Laufzeiten ankommt. Die unterschiedlichen Lichtstrahlen werden auch Lichtmoden genannt.

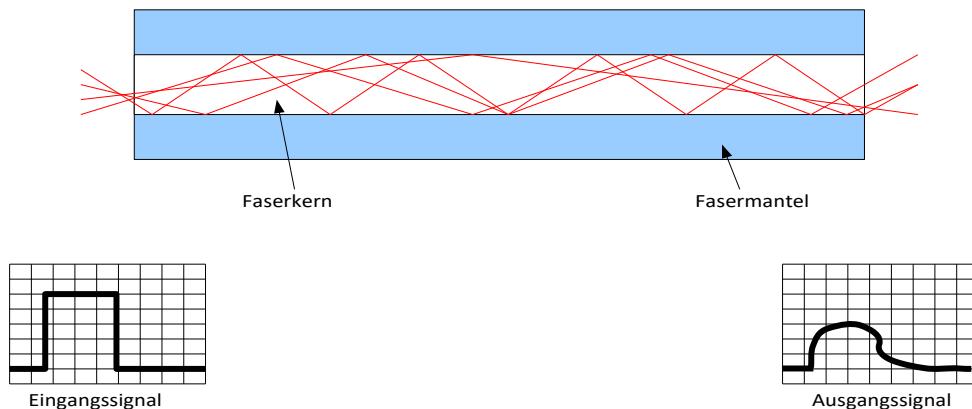


Abbildung 204 – Multimode-Faser

Die Multimode-Stufenindexfaser ist einfach herzustellen und deshalb billig. Sie hat allerdings die größte Dispersion. In der folgenden Abbildung ist zu sehen, wie der Brechungsindex über den Faserquerschnitt verteilt ist.

Die Dispersion beträgt ca. 50 ns/km.

Die Dämpfung beträgt etwa 6 dB/km.

Die typische Reichweite ohne Repeater beträgt nur wenige 100m.

Typische Durchmesser für Kern/Mantel sind:
100/200µm
200/400µm
400/500µm.

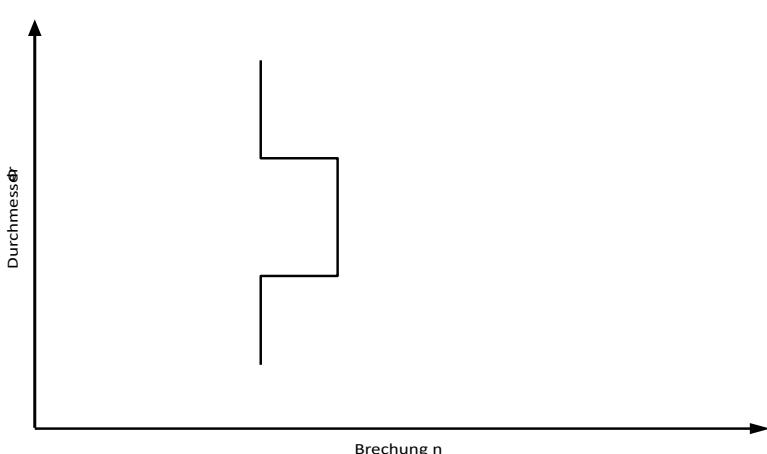


Abbildung 205 – Brechungsindex-Verlauf bei Multimodefaser

13.2.3 - Gradienten-Faser

Bei der Gradientenfaser (folgende Abbildung) ist der Brechungsindex im Faserkern, nicht wie bei den Stufenindexfasern, überall gleich, sondern der Brechungsindex nimmt mit dem Durchmesser zu. Damit wird der Lichtstrahl, je weiter er sich von der Kernmitte entfernt, stärker gebrochen. Dies bedeutet, dass der Lichtstrahl nicht am Übergang Kern/Mantel gebrochen wird, sondern kontinuierlich im Kern. Die Gradientenfaser ist im Herstellungs-Prozeß schwieriger und deshalb teurer als die Multimode-Stufenindexfaser. Die Dispersionswerte sind jedoch besser. (Das Ausgangssignal ist größer und etwas schmäler)

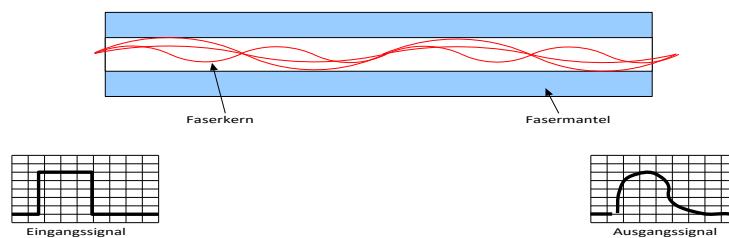


Abbildung 206 – Gradienten-Faser

In der folgenden Abbildung ist der Brechungsindex-Verlauf über den Faserquerschnitt dargestellt und dabei wird sichtbar, dass der Brechungsindex sich über den Querschnitt hinweg ständig ändert.

Die Dispersion beträgt ca. 5 ns/km.

Die Dispersion beträgt ca. 5 ns/km.

Die Dämpfung beträgt etwa 3 dB/km.

Die typische Reichweite beträgt nur wenige 10 km ohne Repeater.

Typische Durchmesser für Kern/Mantel sind:
50/125µm
62,5/125µm.

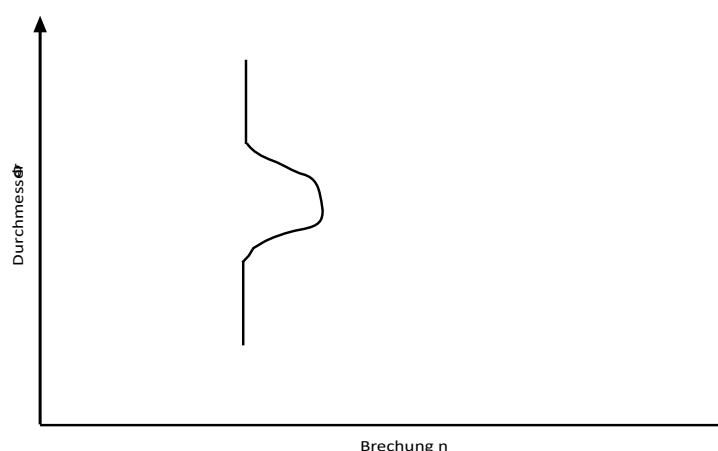


Abbildung 207 – Brechungsindex-Verlauf bei Multimodefaser

13.2.4 - Monomode-Fasern

Monomodefasern leiten nur ein Lichtmode. Monomode-Fasern sind immer Stufenindexfasern. Wie in der folgenden Abbildung angedeutet, ist der Kernquerschnitt dünner, was nur einem Lichtstrahl erlaubt, ihn zu durchqueren. Sie sind mit $9-10\mu$ im Kern wesentlich dünner als die Multimode-Fasern (50μ oder $62,5\mu$) und

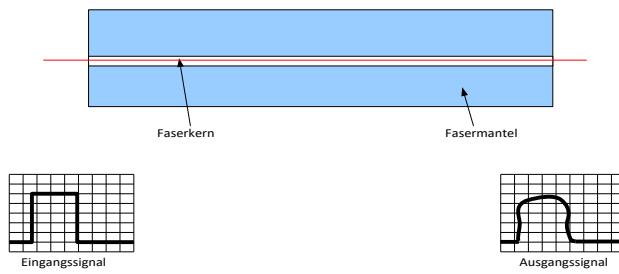


Abbildung 208 – Monomode-Faser

damit aufwendiger in der Herstellung und in der Verarbeitung. Dies hat natürlich auch seinen Preis.

Der Verlauf des Brechungsindex in der folgenden Abbildung zeigt den gleichen rechteckigen Verlauf wie bei der Multimode-Faser. Allerdings ist der Bereich mit erhöhtem Brechungsindex schmäler.

Die Dispersion beträgt ca. $0,1 \text{ ns/km}$.

Die Dämpfung beträgt etwa $0,1 \text{ dB/km}$.

Die typische Reichweite beträgt nur wenige 50 km ohne Repeater.

Der Typische Wert der Durchmesser für Kern/Mantel ist:
 $9/125\mu\text{m}$.

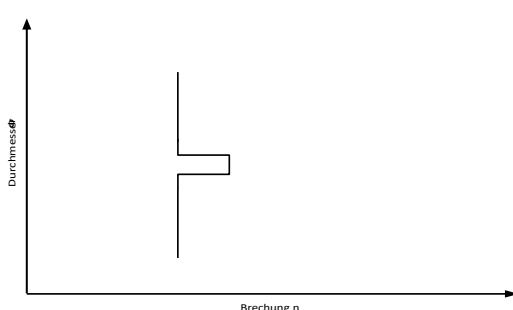


Abbildung 209 – Brechungsindex-Verlauf bei Monomode-Faser

13.3 - Lichtquellen

Die verwendeten unterschiedlichen Lichtquellen haben ein unterschiedliches Einstrahl-Verhalten.

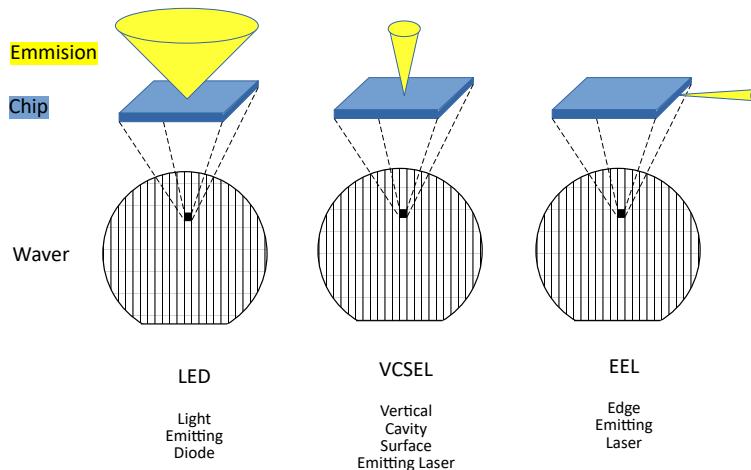


Abbildung 210: Einstrahlverhalten

LEDs sind billig in der Herstellung, streuen ihr Licht sehr breit. Dies führt zu einer starken Dispersion.

VCSELS (Vertical Cavity Surface Emitting Laser) sind LASER-Dioden die ihr Licht vertikal zur Epitaxieschicht aussenden. Damit ist das Einstrahl-Verhalten günstiger und die Disperion kleiner.

Ein LASER erzeugt einen stark gebündelten Lichtstrahl ohne Dispersion. Allerdings sind LASER am teuersten in der Herstellung.

Das Einstrahlverhalten von LEDs und VCSELS in Multimode-Fasern führt gewöhnlicherweise zu Problemen. Dies liegt daran das sich die Moden stark verbreiten können. Dies führt zu Längenrestriktionen. Eine Verlängerung der Strecken ist mit so genannten Mode-Conditioning Kabeln möglich. Es handelt sich dabei um Patchkabel bei denen ein Modenfilter eingebaut ist.

13.4 - Lieferbare Formen

13.4.1 - Übersicht über die lieferbaren Einzelfasern

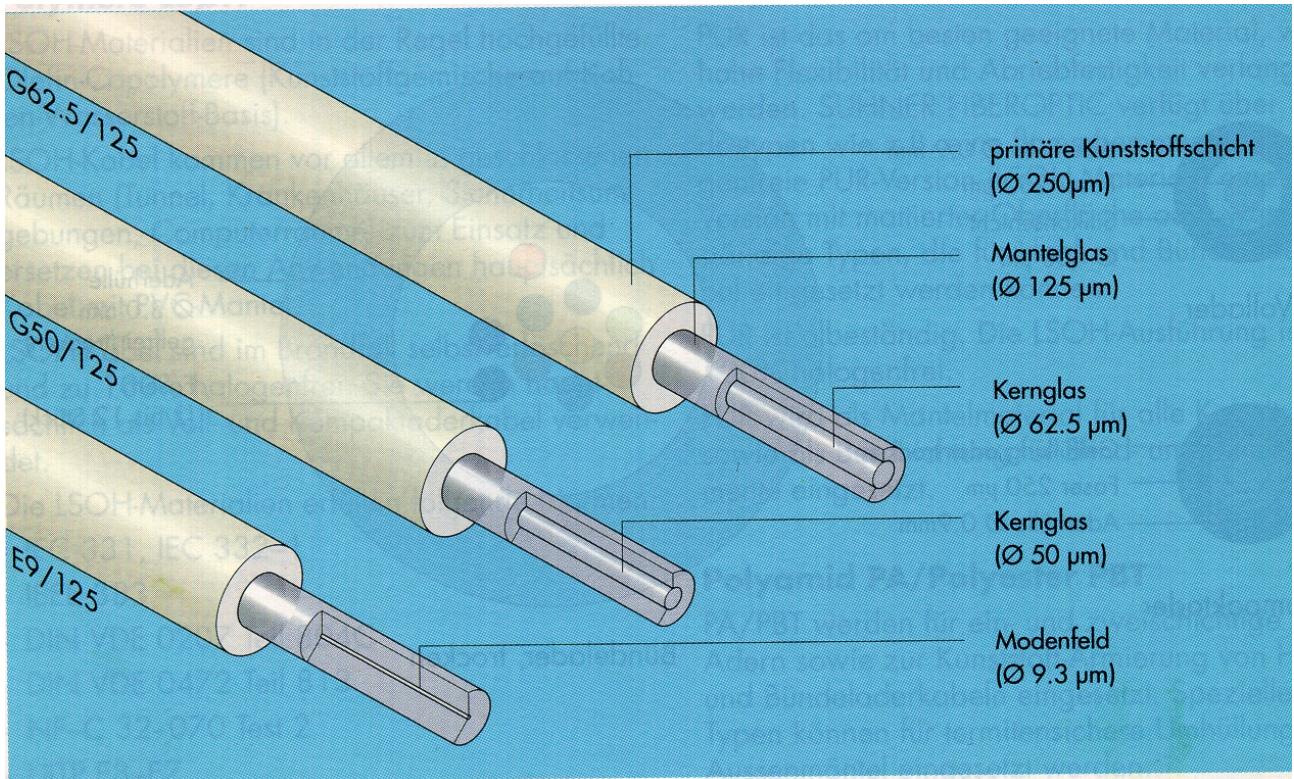


Abbildung 211: Übersicht Einzelfasern

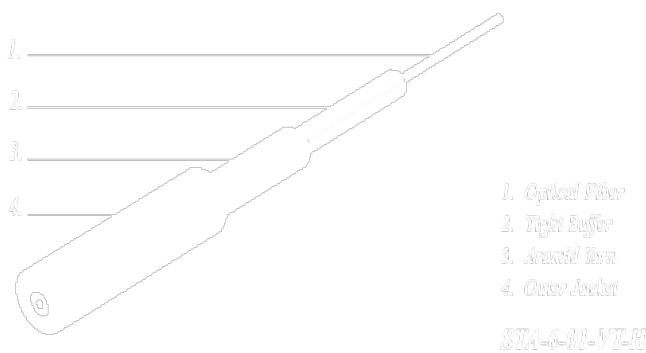
Der Durchmesser des Mantelglases ist immer 125µm.

Für den Durchmesser des Kernglases gibt es 3 verschiedenen Größen:

9,3 - 10 µm für Singlemode-Fasern

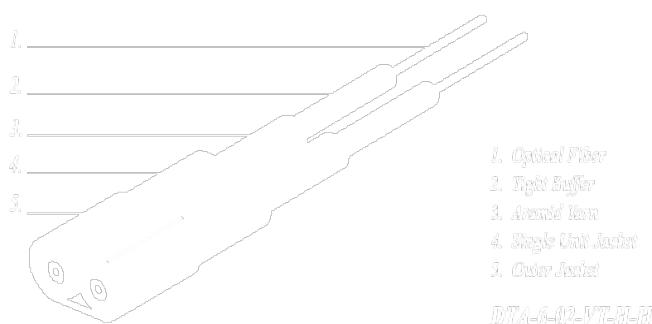
50 µm für Multimode-Fasern in Europa

62,5 µm für Multimode-Fasern in USA.



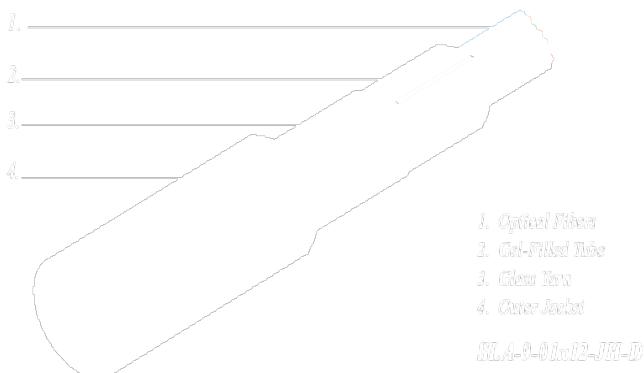
13.4.2 - Simplexkabel

Hierbei handelt es sich um eine einzelne LWL-Faser. Sie ist Zug-entlastet und ummantelt. Das Simplexkabel wird auch Einzelfaserkabel genannt.



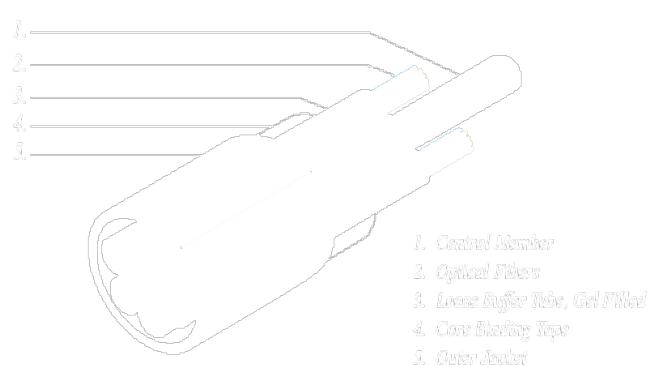
13.4.3 - Duplexkabel

Zwei Einzelfaserkabel mit Verbindungssteg oder zusätzlichem Außenmantel.



13.4.4 - Breakout-Kabel

4 bis 20 Einzelfaserkabel verseilt mit gemeinsamem Außenmantel. Wird auch Bündelfaserkabel genannt.



13.4.5 - Bündelader-Kabel

Hierbei werden mehrere Fasern in Bündeln zusammengefasst. Mehrere Bündel sind dann in einem Kabel zusammengefasst.

Quelle: Superior Cables GmbH

13.4.6 - Bezeichnungscodes für Innenkabel nach DIN / VDE 0888

<u>I</u>	Innenkabel
<u>V</u>	Vollader
<u>H</u>	Hohlader, ungefüllt
<u>W</u>	Hohlader, gefüllt
<u>Y</u>	PVC-Mantel
<u>H</u>	Mantel aus halogenfreiem Material
<u>n</u>	Anzahl der Fasern
<u>E</u>	Einmodenfaser
<u>G</u>	Gradientenfaser
<u>P</u>	Plastikfaser
<u>n/</u>	Kerndurchmesser
<u>n</u>	Manteldurchmesser
<u>B</u>	Wellenlänge = 850nm
<u>E</u>	Wellenlänge = 1300 nm
<u>H</u>	Wellenlänge = 1550 nm
<u>n</u>	Bandbreite [Mhz*km] bei MM oder Dispersion [ps/(km*nm)]	

13.5 - Bezeichnungscodes für Aussenkabel nach DIN / VDE 0888

A-	Außenkabel
H	Hohlader, ungefüllt
W	Hohlader, gefüllt
B	Bündelader, ungefüllt
D	Bündelader, gefüllt
S	metallenes Element in Kabelseele
F	Füllmasse des Verseilhohlräums in der Kabelseele
Q	Quellflies
2Y	PE-Mantel
(L)2Y	Schichtenmantel
(ZN)2Y	PE-Mantel mit nichtmetallenen Zugentlastungselem.
(L)(ZN)2Y	Schichtenmantel mit nichtmetallenen Zugentlastungselem.
B	Bewehrung
BY	Bewehrung mit PVC-Schutzhülle
B2Y	Bewehrung mit PE-Schutzhülle
n	Faseranzahl
E	Stufenindexfaser
G	Gradiantenfaser
P	Plastikfaser
n/	Kerndurchmesser
n	Manteldurchmesser
n	Dämpfungskoeffizient [dB / km]
B	Wellenlänge=850 nm
F	Wellenlänge=1300 nm
H	Wellenlänge=1550 nm
n	Bandbreite [Mhz+km] bei MM o. Dispersion [ps/(km*nm)]
LG	Lagenverteilung

13.6 - Herstellung

Glasfasern werden in einem Zugverfahren mit einer Schmelztechnik hergestellt.

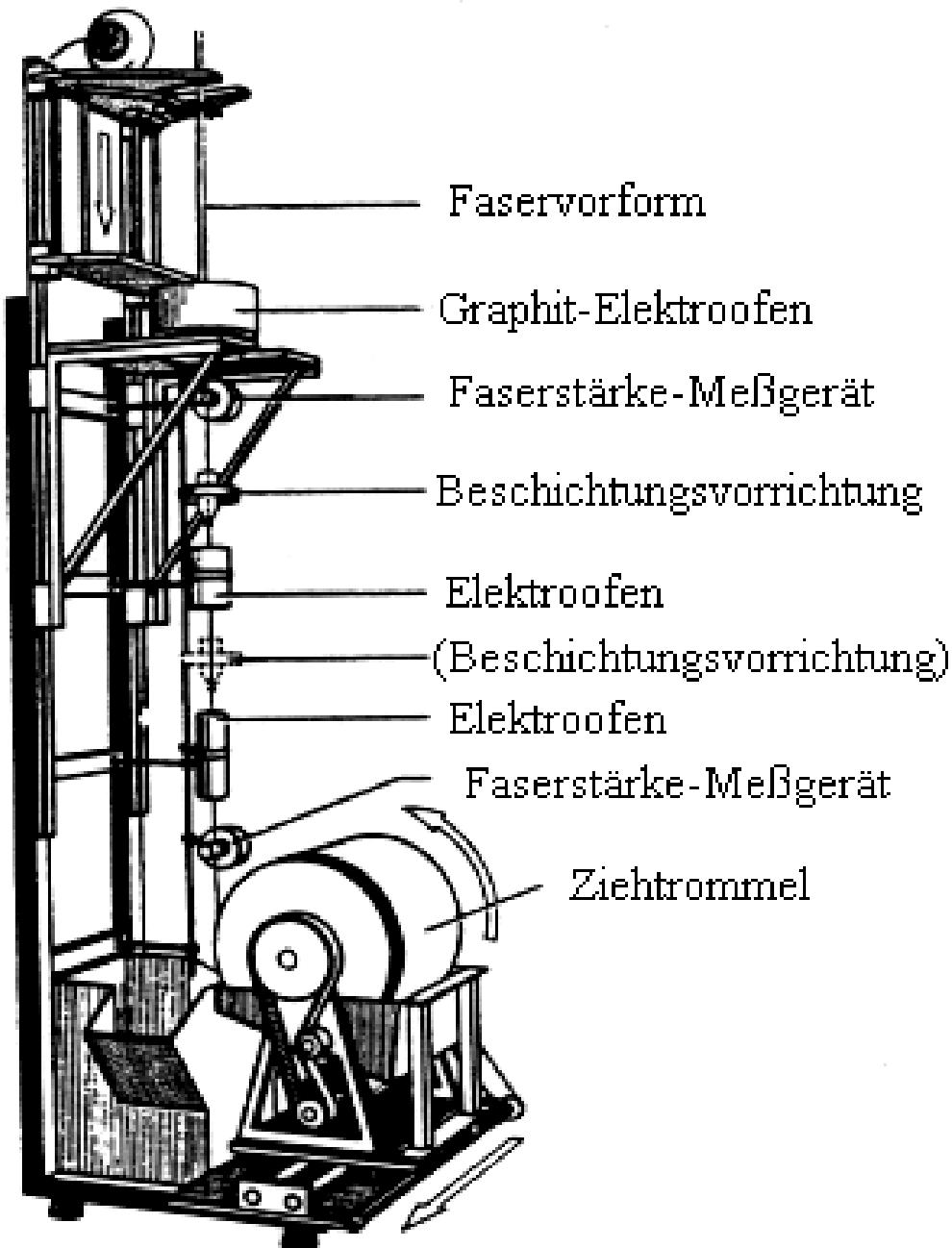


Abbildung 212: Glasfaser-Zugofen

Durch einen konstanten Zugkraft erhält die Faser einen konstanten Durchmesser. Bevor die Faser aufgewickelt wird erhält sie das Primary-Coating um vor Beschädigungen geschützt zu werden.

Quelle: www.glasfaserinfo.de

13.7 - Verbindung von LWL-Fasern

Die Verbindung von Glasfasern ist wesentlich aufwändiger als bei einer Kupferverkabelung. Sowohl die Verlängerung einer Faser als auch das Verbinden mit einem Pigtail ist mit einem so genannten Spleiss vorzunehmen. Ein Pigtail ist eine vorkonfektionierte Verbindung eines kurzen Faserteils mit einem Stecker oder einer Kupplung. Dazu sind die Glasfasern zuerst genau auszurichten. Dies ist in allen 3 Ebenen vorzunehmen. Da die Fasern sehr dünn sind und kaum mit dem bloßen Auge zu sehen sind werden hierbei Mikroskope verwendet. Sind die Faserenden genau aufeinander ausgerichtet, werden sie mit einem Lichtbogen miteinander verschmolzen. Gute Spleissverbindungen haben einem Dämpfungswert von weniger als 0,1 dB.

Fibers Stripped of Coating, Cleaned,
and Cleaved, are Brought Together

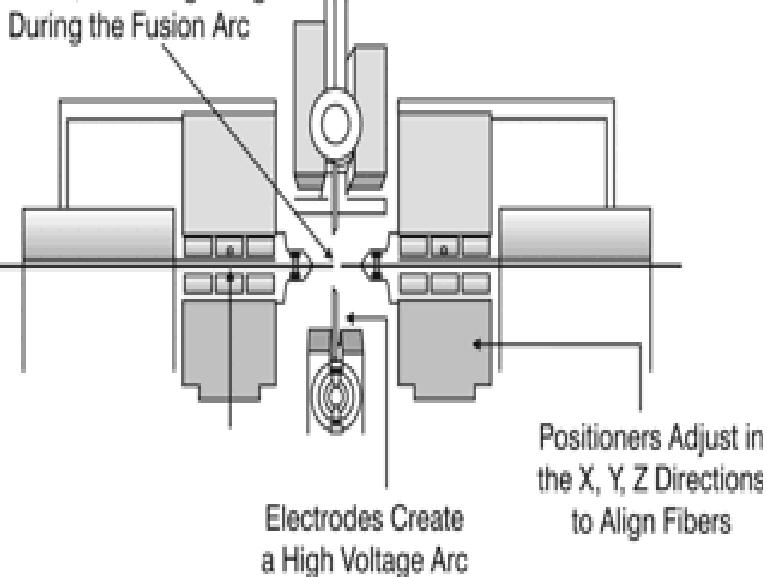


Abbildung 213: Spleissvorgang

Der fertige Spleiss wird in einer so genannten Spleissbox geschützt untergebracht.

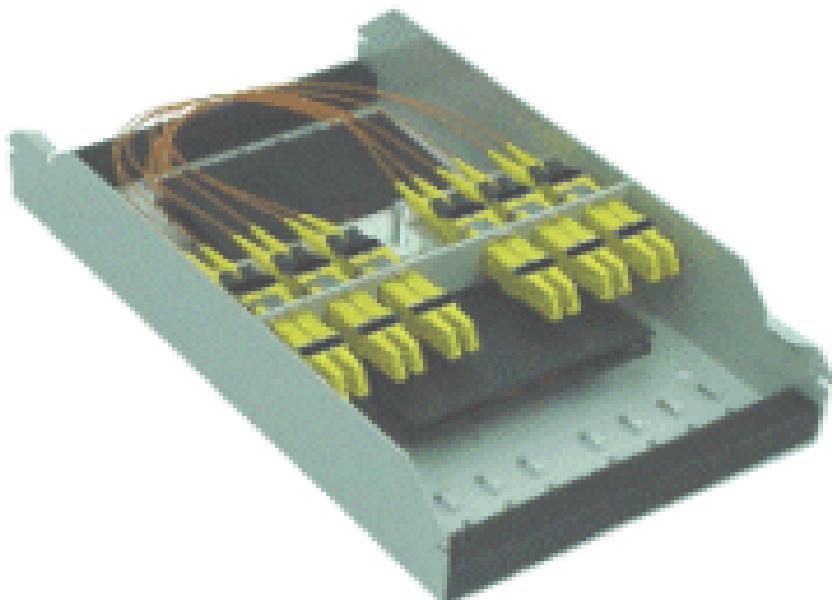


Abbildung 214: Spleissbox

13.8 - Messungen

Natürlich ist bei LWL eine Abnahme der Strecke nach der Installation genauso erforderlich wie bei einer Kupferverkabelung. Dazu wird ein OTDR (Optical Time Domain Reflectometer) verwendet.

Ein Lichtimpuls wird in die Faser eingebracht. Durch Reflexionen und die Laufzeit können Faserbrüche, Spleisse, Stecker oder die Unterschreitung des Biegeradius auf den Meter genau ermittelt werden.



Bild: Nettest Inc.

13.9 - LWL Link-Klassen

13.9.1 - Link-Längen

Die garantierte Link-Längen stehen in Abhängigkeit vom Dienst und der verwendeten Faser-Qualität.

Service	Max. Cannel attenuation			ISO/EC Link Support							
	Multimode		Single mode	OM1		OM2		OM3		OS1	
	850nm	1300nm	1300nm	850nm	1300nm	850nm	1300nm	850nm	1300nm	850 nm	1300 nm
100BaseFX		11 (6.0)			OF2000		OF 2000		Off2000		
1000BaseSX	2,6 (3,56)	-	-	500 50µm 275 62,5µm		OF5 00		OF 500			
1000BaseLX		2,35	4,56		OF 500		OF 500		OF 500	OF 2000	
10GBASE-SR	1,6 (62,5) 1,8 OM2 1,6 OM3	-	-					OF 300			

13.9.2 - LWL-Faserklassen

Faser-Typ	Kerndurchmesser	OFLBandbreite		Effektive Laserbandbreite
		850 nm		850 nm
OM1	50µm oder 62,5µm	200	500	-
OM 2	50 µm	500	500	-
OM 3	50 µm	1500	500	200

13.9.3 - Linklänge in Abhängigkeit vom Standard und verwendeten Fasertyp

Standard	FaserTyp	Kerndurchmesser	Maximale Länge
1000BASE-SX	Multimode	62,5 µm	260 m
1000BASE-SX	Multimode	50 µm	525 m
1000BASE-LX	Multimode	62,5 µm	550 m
1000BASE-LX	Multimode	50 µm	550 m
1000BASE-LX	Singlemode	9 µm	5000 m
10GBASE-EW	Singlemode	9 µm	40 km (WAN)
10GBASE-ER	Singlemode	9 µm	40 km (LAN)
10GBASE-LW	Singlemode	9 µm	10 km (WAN)
10GBASE-LR	Singlemode	9 µm	10 km (LAN)
10GBASE-LX4	Multimode	50 µm	300m (LAN)
10GBASE-LX4	Singlemode	9 µm	10 km (LAN)
10GBASE-SW	Multimode	50 µm	65 m (WAN)
10GBASE-SR	Multimode	50 µm	65 m (LAN)

In Fällen, bei denen nur eine Faser (single Strand) zur Verfügung steht, gibt es eine Lösung bei der mit unterschiedlichen Wellenlängen gearbeitet werden kann, um die unterschiedlichen Richtungen zu trennen. Dabei werden zwei unterschiedliche SPFs paarweise eingesetzt.

- ➊ 1000Base-BX10-D sendet mit 1490nm und empfängt mit 1310nm.
- ➋ 1000Base-BX10-U sendet mit 1310nm und empfängt mit 1490nm.

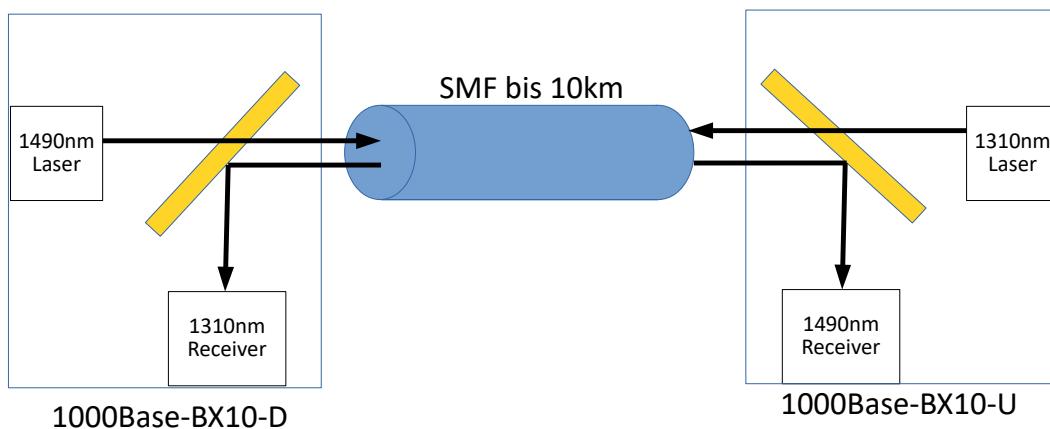


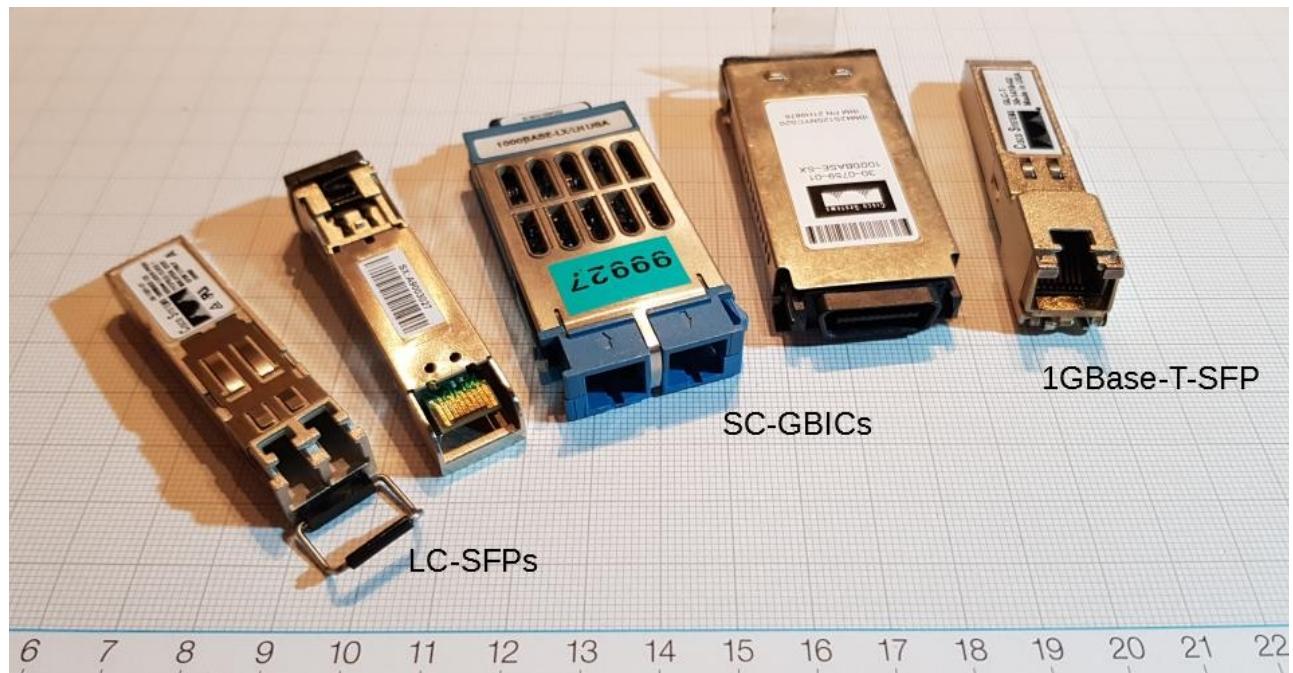
Abbildung 215: Single-Strand-Verbindung

13.9.4 - Transceiver-Module

Bei modernen Geräten sind die Transceiver nicht fest in den Geräten verbaut sondern als Modul ausgeführt.

Im Laufe der Zeit haben sich unterschiedliche Module entwickelt. Sie sind „hot swappable“, d. h. Sie können im laufenden Betrieb getauscht werden. Außerdem bieten sie eine Vielzahl unterschiedlicher Stecker-Möglichkeiten sowie Reichweiten. Viele bieten die Möglichkeit des DOM (Digital Optical Monitoring) womit „!Realtime-Parameter“ wie Ausgangsleitung, Eingangsleistung, Temperatur und Versorgungsspannung überwacht werden können.

Kurzbezeichnung	Bezeichnung	Verwendung	Hinweis
GBIC	Gigabit Interface Converter	1Gbps	
SFP	Small-Form-Factor-Pluggable	1Gbps	
QSFP	Quad Small Form-factor Pluggable	4Gbps	
SFP+	Enhanced Small Form-factor Pluggable	Max. 16Gbps 10Gbps (Ethernet) 4/16Gbps (FC)	
XFP		10Gbps	Wie SFP aufgebaut, jedoch größer und für 10Gbps
XENPAK		10Gbps	
X2		10Gbps	Nachfolger von XENPAK
QSFP+	Enhanced Quad Small Form-factor Pluggable	40Gbps	
13.10 - SFP 28	Small Form-factor Pluggable 28	25Gbps	



13.11 - Steckverbinder

Die meisten Steck-Verbindungen sind Stecker-Stecker-Verbindungen. Dabei ist eine möglichst geringe Signaldämpfung (auch Einfügedämpfung; engl. insertion loss), eine hohe Rückflussdämpfung (engl. Return loss), sowie eine hohe Reproduzierbarkeit der Parameter über mehrere hundert Verbindungszyklen gewünscht.

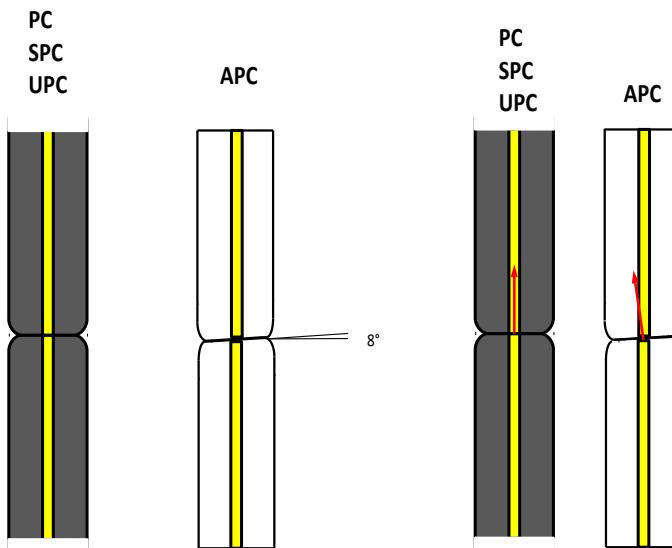


Abbildung 216: Bauformen: PC/SPC/UPC - APC

www.fiberc.com/connectors.html.

13.11.1 - ST-Stecker



Die zylindrischen Hülsen zur Faser-Aufnahme, die so genannten Ferrulen, bestehen aus Metall oder Keramik und sind federnd gelagert. Die Fasern werden in die Ferrulen eingeklebt. An der Stirnseite sind sie geschliffen und poliert. Moderne Ferrulen haben abgerundete Endflächen und sollen sicherstellen, dass durch einen physikalischen Kontakt die Dämpfungseigenschaften optimal sind. Diese Stecker haben auch den Anhang PC, für Physical Contact. Weitere Optimierungen sind mit den Namen Super Physical Contact (SPC) und Ultra Physical Contact (UPC) verfügbar. Damit heißen solche Stecker z.B. ST/PC.
Es gibt noch die Schrägschliff-Variante, die eine um 8° gekippte Stirnfläche aufweist. Die Namens-Ergänzung heißt Angled Physical Contact (APC). Dadurch wird die Rückflussreflexion über das Mantelglas hinaus gebrochen. Stecker mit dieser Bauform haben z.B. den Namen LC/APC.

Die folgenden Bilder sind von

Der „Straight Tip“ (deutsch: gerades Ende/Anschluß) - Stecker wurde von AT&T spezifiziert (BFOC/2,5 IEC -874-10) und kann sowohl für Monomodefasern als auch für Multimodefasern verwendet werden. Dieser Stecker ist schon länger auf dem Markt und hat eine weite Verbreitung gefunden. Aus Gründen der Präzision und der Verdreh-Sicherheit sollte nur der Steckertyp ST3 verwendet werden. Die Typen 1 und 2 weisen die durchgehende Nase nicht auf, und können daher verdreht werden!

13.11.2 - FSMA-Stecker



Der FSMA- (auch SMA-) Stecker ist einer der ersten LWL-Stecker, der international standardisiert wurde. Er ist genormt durch das Dokument IEC -SC 86B(CO)20. Bei dem FSMA-Stecker handelt es sich um einen Schraubstecker, bei dem die Faser in einer relativ langen metallischen Ferrule mit einem Stiftdurchmesser von 3,175 mm geführt wird, die an der Kontaktfläche plan geschliffen ist.

13.11.3 - SC-Stecker



SC steht für Subscriber Connector; deutsch Teilnehmer-Verbinder.

Durch die Nasen und Nuten kann ein Verwechseln der Send- und Receive-Leitungen ausgeschlossen werden. Kann Probleme machen, falls er in der Buchse nicht richtig eingerastet ist. Bei Problemen ist der richtige Sitz des Steckers in der Buchse zu überprüfen.

13.11.4 - FC-Stecker



Der Fiber Connector ist ein LWL-Stecker der sowohl für Multimode-Fasern (ITU-Empfehlung G.651) als auch Monomode-Fasern (CCITT-Empfehlung G.652) einsetzbar ist.

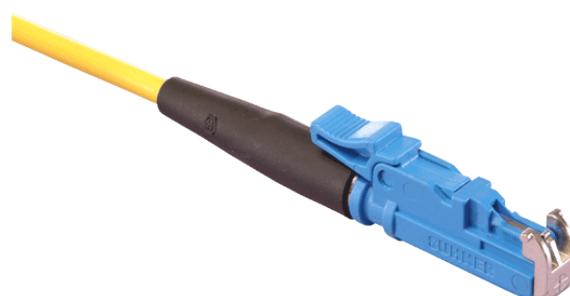
Dieser Stecker hat keine Verdrehschutz. Seine Dämpfung liegt typischerweise bei 0,5 dB .

13.11.5 - LC-Stecker



Der Lucent Connector wurde von der Fa. Lucent als Konkurrenzprodukt zum MT-RJ Stecker entwickelt. Er ist sehr kompakt und in Duplex- als auch in Simplex-Bauform zu erhalten. Er hat eine Keramikferrule mit 1,25mm Durchmesser. Verwendung findet dieser Stecker häufig im Fiberchannel-Umfeld.

13.11.6 - E2000 Stretcker



Dieser Stecker wurde von der Fa. Diamond SA (Schweiz) entwickelt. Eine Schutzklappe, die sich beim Einstechen automatisch öffnet, schützt die Glasfasern vor Verschmutzung. Dieser Stecker ist für Monomode- als auch für Multimodefasern geeignet. Er ist sowohl als Duplexstecker als auch als Einzelstecker verfügbar. Bei diesem Stecker ist darauf zu achten, dass es bereits Schrägschliffvarianten mit unterschiedlichen Winkeln als auch Stirnflächenkopplung auf dem Markt gibt.

13.11.7 - MT-RJ Stecker



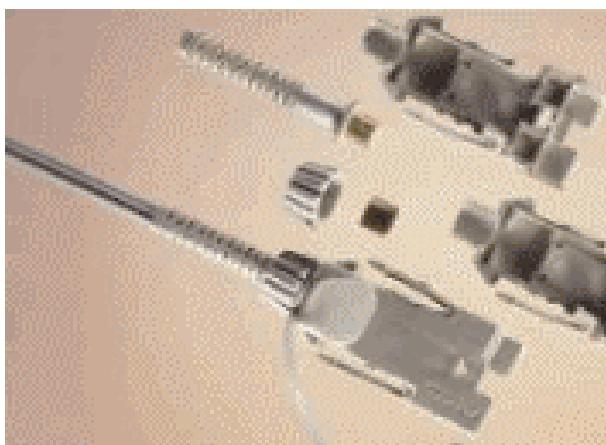
Dieser Stecker ist für Monomode- als auch für Multimodefasern geeignet. Er ist ein Duplexstecker und hat einen Verriegelungsmechanismus wie beim RJ45-Stecker. Durch die kleinere Bauform im Vergleich zum SC-Stecker sind in den Patchfeldern wesentlich höhere Portdichten möglich. Dieser Stecker soll den SC-Stecker im Tertiär-Bereich ablösen.

13.11.8 - ESCON-Stecker



Dieser Stecker wurde von IBM für die Verkabelung von Großrechnern verwendet.

13.11.9 - MIC-Stecker



Der MIC-Stecker findet in ATM und FDDI-Netzen Verwendung. Seit Übernahme des ANSI -Standards X3.166 durch ISO (ISO 9314-3) ist der Stecker auch international genormt. Die Verbindung des Steckers mit der Faser wird durch eine Ferrule aus Zirkonia hergestellt. Eine aufsteckbare Schutzkappe schützt die Ferrule vor Verschmutzung.

13.11.10 - Pigtail mit ST-Stecker

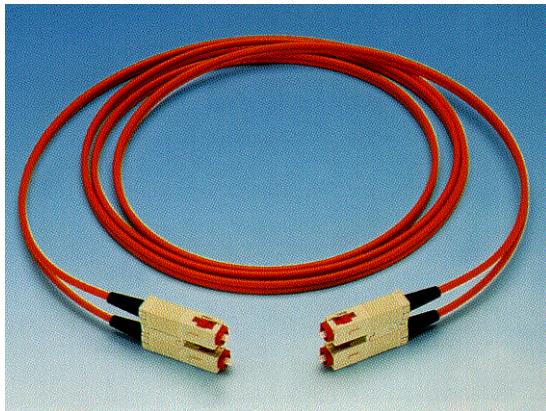
Mit Pigtaills werden die verlegten Kabel in der Spleissbox abgeschlossen.
Die Pigtaills werden in einem Spleissverfahren mit den Fasern verschmolzen.



Abbildung 217: Pigtail

13.11.11 - Patchkabel

Für die Anbindung von Netzwerk-Geräten an ein Patchfeld, gibt es fertig konfektionierte Patchkabel. Bei der Bestellung sind Steckertyp(en), Leitungslänge und Faserdurchmesser (9μ , 50μ oder $62,5\mu$) anzugeben.



Hier ein LWL-SC-SC-Beispiel.

Abbildung 218: LWL SC-SC-Patchleitung

13.11.12 - Übersicht über die unterschiedlichen Steckertypen

Steckertyp	Einsatzort	Typische Dämpfung Single-/Multimode	Steck- zyklen	Häufigkeit	Ferrule	Faserstärke	Verdreh- schutz
	LAN	< 0,15 / < 0,2dB	2000	sehr oft	Metall / Keramik	9 / 50-62,5µm	ja
<u>SC</u>	LAN / WAN	< 0,1 / < 0,2dB	2000	sehr oft (Europa Standard)	Metall / Keramik	9 / 50-62,5µm	ja
<u>FC/PC</u>	LAN	< 0,1 / < 0,15dB	2000	selten (Asien Standard)	Metall / Keramik	9 / 50-62,5µm	nein
<u>MIC FDDI</u>	LAN	< 0,15dB	2000	häufig	Keramik	9 / 50-62,5µm	ja
<u>LC</u>	LAN	< 0,1 / < 0,15dB	1000	immer häufiger	Metall / Keramik Kunststoff	9 / 50-62,5µm	ja
DIN	WAN	< 0,1 / < 0,15dB	2000	nur im deutschsprachigen Raum	Metall / Keramik	9 / 50-62,5µm	ja
<u>FSMA</u>	LAN	< 0,2dB	2000	selten	Metall / Keramik	50-62,5µm	nein
<u>E2000</u>	LAN / WAN	< 0,12 / < 0,2dB	1000	immer häufiger	Keramik	9 / 50-62,5µm	ja
<u>MT-RJ</u>	LAN	< 0,1 / < 0,2dB	?	oft	Keramik / Kunststoff	9 / 50-62,5µm	ja
<u>Volition</u>	LAN	< 0,2dB	500	häufig	ohne Ferrule	9 / 50-62,5µm	ja
<u>ESCON</u>	LAN	?	?	selten	Keramik	9 / 50-62,5µm	ja
<u>Mini-BNC</u>	LAN	< 0,3dB	?	sehr selten	Metall	9 / 50-62,5µm	ja
MU (Mini-SC)	LAN	< 0,1 / 0,15dB	1000	sehr selten	Metall / Keramik Kunststoff	9 / 50-62,5µm	ja

14 - Ethernet

14.1 - Historisches

Ethernet hat durch seine lange Entwicklungsgeschichte viele Veränderungen durchlaufen. Mit der ersten Entwicklung Anfang der siebziger Jahre von Robert Metcalfe bei XEROX sollten Drucker mit 2,94MHz/s angebunden werden. Es basierte auf einem experimentellen Funknetz namens Aloha (dt. Hallo) der Universität Hawaii um die Inselstandorte der Universität zu verbinden.

Ein Medienzugriffsprotokoll war auf Hawaii nicht vorgesehen. Jeder der senden wollte, konnte dies sofort tun, was zu einer maximalen Auslastung des Übertragungskanals von 18% führte. Wurde versucht, den Kanal weiter auszulasten, führte dies zu Kollisionen, die mit der Wiederholung der Daten bearbeitet werden mussten, was zu einer weiteren Verschlechterung der Auslastung führte. Robert Metcalfe hatte das erkannt und für Ethernet ein Medienzugriffsverfahren namens CSMA/CD vorgesehen. Dabei wird zuerst überprüft, ob der Kanal frei ist (CS = Carrier Sense). Ist er frei, kann jeder sofort senden (MA = Multiple Access). Ist er belegt, muss gewartet werden. Das verhindert jedoch nicht, dass trotzdem Kollisionen stattfinden können. Deshalb muss noch eine Kollisionserkennung implementiert werden, die während des Sendens überwacht, ob eine Kollision stattfindet (CD = Collision Detection). Bei einer Kollisionserkennung, wird das Senden der Daten unterbrochen und es findet eine Wiederholung statt.

In Abbildung 219 ist die älteste, noch erhaltene, Abbildung von Ethernet zu sehen. Das gelbe Koaxalkabel (THE ETHER) ist an seinen beiden Enden mit einem Abschlusswiderstand (TERMINATOR) versehen um Reflexionen auf dem Bus zu vermeiden. Auf das Koaxalkabel wird mit einem TAP (deutsch: Anzapfung) physikalisch zugegriffen. Dabei wird die Koaxial-Leitung so angebohrt, dass der Kernleiter und die Schirmung getrennt angeschlossen werden kann. Tap und Transceiver bilden zusammen die MAU (Media Attachment Unit. Dt. Medium-Zugriffseinheit). Auf der Rechnerseite (STATION) wurde der Controller auf den vorhandenen Bus (ISA / PCI / ...) gesteckt. Auf dem Controller ist das Interface untergebracht. Mit der Interface-Leitung (INTERFACE CABLE / DROP-CABLE) wird das Interface mit dem Transceiver verbunden.

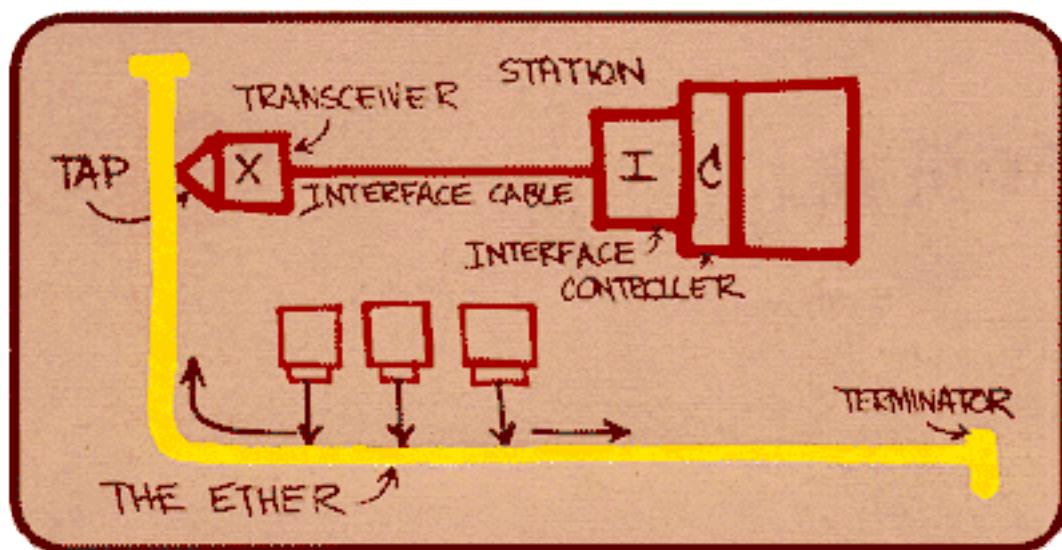


Abbildung 219: Ältestes noch erhaltenes Bild von Ethernet

14.2 - 10 Mbps-Ethernet

Am 13. Dezember 1979 wurde Ethernet von Robert Metcalfe als Multipoint Data Communication System with Collision Detection unter der US-Patentnummer 4 063 220 für die XEROX Corporation patentiert.

Ein Konsortium aus den Firmen DEC (Digital Equipment Corporation¹), Intel und XEROX (die so genannte DIX-Gruppe) entwickelte auf dieser Basis ein 10 Mbps/s-Ethernet. Im September 1980 wurde eine Spezifikation veröffentlicht. Diese Version wird heute als Ethernet 1 bezeichnet.

Im Februar 1980 war beim Institute of Electrical and Electrical Engineer (IEEE) eine Arbeitsgruppe (IEEE-802) eingerichtet, die sich mit der Vernetzung von Systemen beschäftigte. Eine Untergruppe (IEEE-802.3) hatte den Auftrag übernommen, den Vorschlag der DIX-Gruppe, in einen international anerkannten Standard zu überführen. Der erste Entwurf namens Carrier Sense Multiple Access with Collision Detection (CSMA/CD) wurde im Dezember 1980 vorgelegt. Am 23. Juni 1983 wurde Ethernet als Standard IEEE-802.3 verabschiedet.

Da es bei Ethernet keine zentrale Taktsteuerung gibt, muss der Empfänger den Takt aus dem empfangenen Datenstrom zurückgewinnen. Dazu dienen die ersten 7 Bytes eines Pakets, die so genannte Präambel. Durch die Übertragung von abwechselnden Einsen und Nullen kann der Empfänger ein Taktsignal erzeugen. Damit der Empfänger weiß, wo die Taktinformation endet und Daten anfangen ist im 8. Byte der Präambel, dem Start-Frame-Delimiter (SFD), das letzte Bit auf Eins gesetzt. Dies ist das Zeichen dafür, dass im Folgenden die MAC-Adressen, also die Information für die nächsten Ebenen im Datenteil folgen.

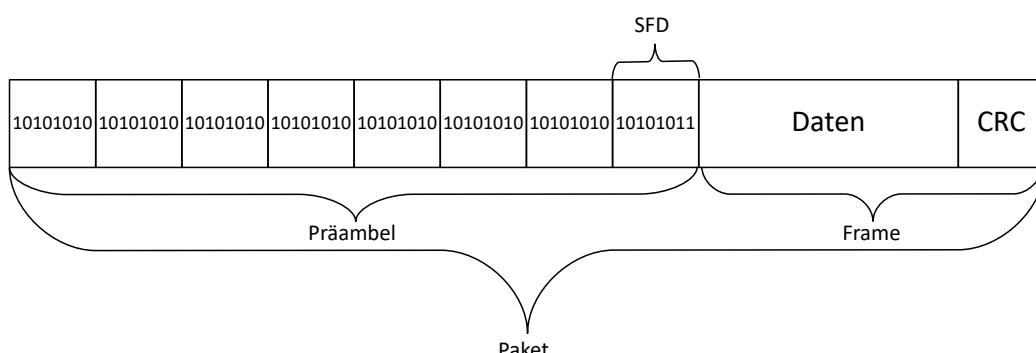


Abbildung 220: Aufbau eines Pakets mit 10 Mbps auf Ebene 1

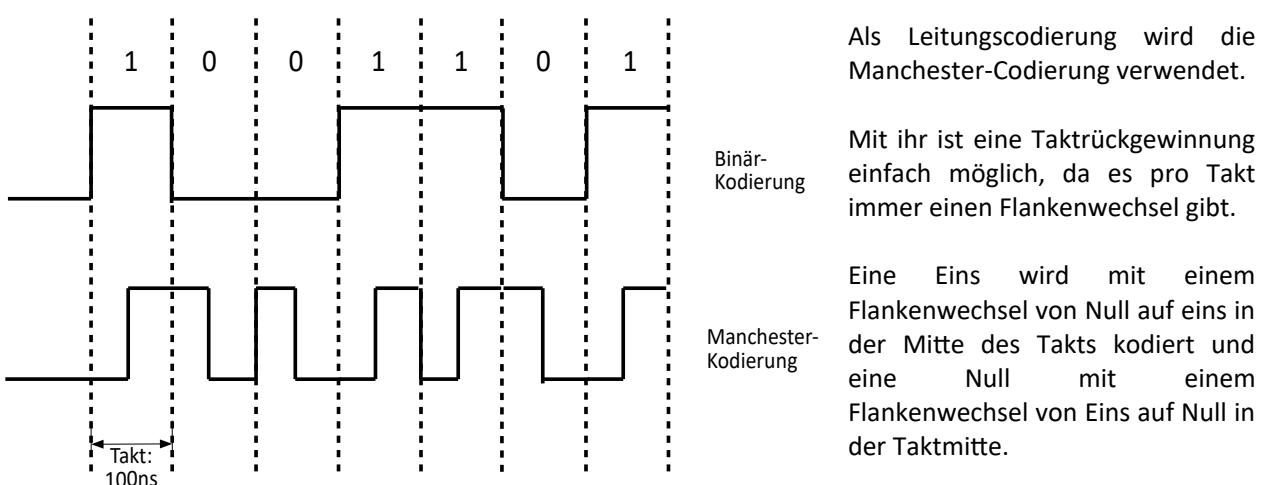


Abbildung 221: Manchester-Kodierung

¹ DEC wurde 1998 von Compaq übernommen und ist somit seit 2002 ein Teil von HP.

14.2.1 - 10 Mbps-Aufteilung auf die Schichten im OSI-Referenzmodell

Ethernet deckt die beiden unteren Schichten des OSI-RM ab. Schaut man sich die Aufteilung der einzelnen Funktionen an, fällt folgendes auf.

Beide Schichten realisieren ihre Funktionen in Hardware.

- ➊ Die Data-Link-Layer (Ebene 2) realisiert die Adressierungs-Themen, den Medienzugriff und die Sicherung der Daten mittels des Cyclic Redundancy Checks. (CRC).
- ➋ Die PHY-Ebene (Ebene 1) ist für die physikalische Anpassung zuständig.

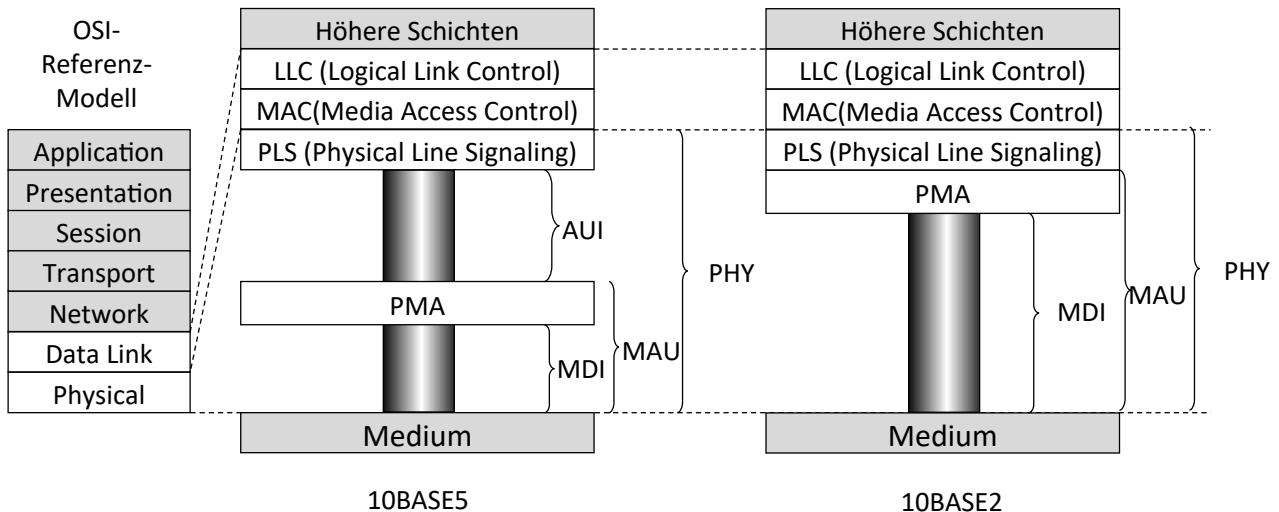


Abbildung 222: 10 Mbps Coaxialkabel-Varianten

14.2.1.1 - LLC

Die LLC-Schicht dient der Bearbeitung der DSAP und SSAP im Rahmen der Funktionen für IEEE-802.1.

14.2.1.2 - MAC

Die MAC-Schicht erbringt die Funktionen zur Adressierung mittels der MAC-Adressen und dem Medien-Zugriffsverfahren (CSMA/CD) sowie der Sicherung über den CRC.

14.2.1.3 - PLS

Die PLS-Schicht (Physical Line Signaling) ermittelt den Zustand der Leitung (Belegt, Frei, Kollision, usw.) und liefert damit dem Medien-Zugriffsverfahren CSMA/CD die Grundlagen.

14.2.1.4 - PMA

Das Physical Medium Attachment (PMA) ist die eigentliche Hardwareschnittstelle auf das Medium. Bei 10Base5 ist das der Transceiver mit dem das Koaxialkabel angebohrt wird.

Bei 10Base2 ist der Transceiver auf die Controller-Karte gewandert und damit ist das PMA der BNC-Stecker auf den das T-Stück für den Busanschluss gesteckt wird.

14.2.2 - 10Mbps-Koaxiallösungen

Die ersten beiden Lösungen beim IEEE802.3-Standard wurden mit unsymmetrischen Koaxialleitungen realisiert.

14.2.2.1 - 10Base5

In dieser ersten Version wurde Ethernet mit einem RG8 Koaxialkabel mit 50Ω Wellenwiderstand und einer Bus-Topologie realisiert. Wie aus der Spezifikation 10Base5 hervorgeht, beträgt die Datenrate 10 Mbps bei einer maximalen Segmentlänge 500 m. Die Gesamtlänge kann mit maximal 4 Repeatern auf maximal 2500 m vergrößert werden.

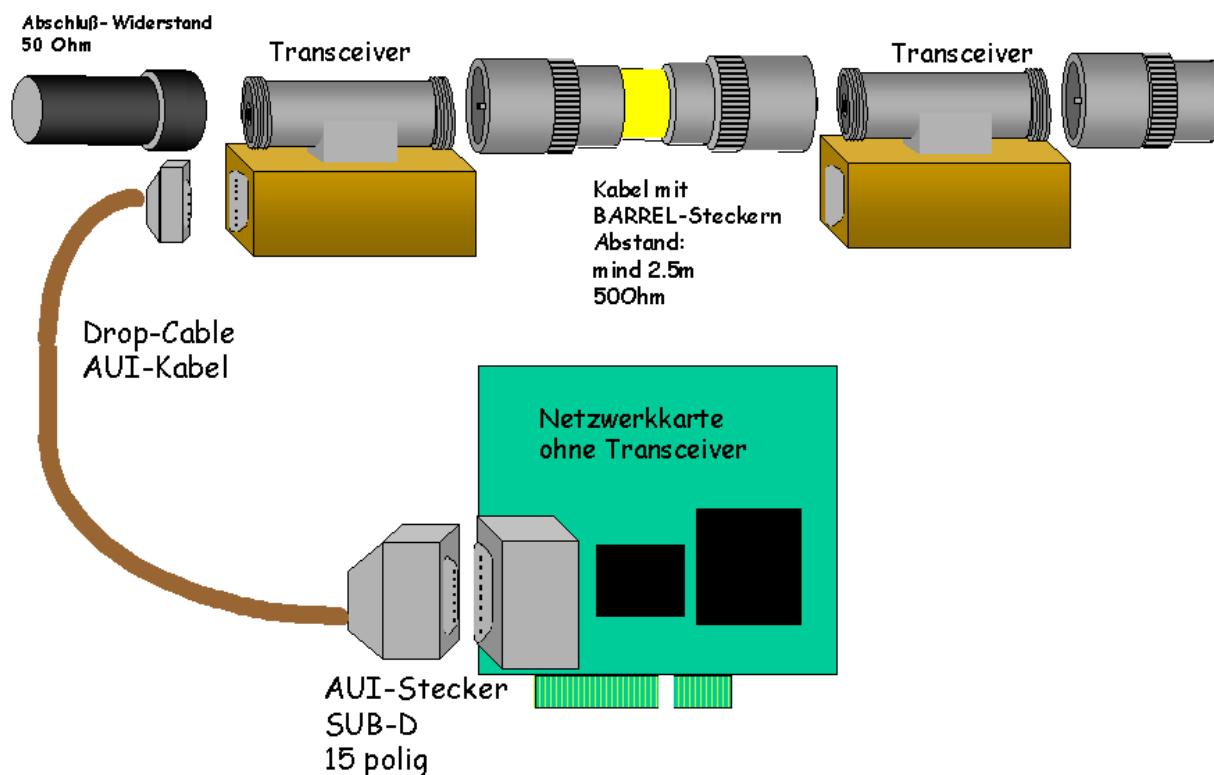


Abbildung 223: 10Base5

10Base2

10Base5 hatte die Nachteile, dass das Buskabel sehr sperrig bei der Verlegung, schwieg beim Anschluss und die Komponenten teuer in der Anschaffung waren. Vor allem im Büroumfeld war dieser Standard nicht besonders praktikabel.

Im November 1985 wurde deshalb die erste Verbesserung mit der Bezeichnung 10Base2 als IEEE-802.3a eingeführt. Dabei wurde die Datenrate von 10 Mbps als auch die Basisband-Zeichengabe beibehalten.

Während bei 10Base5 der Transceiver noch ein eigenständiges Gehäuse hatte und über eine AUI-Leitung zu verbinden war, ist bei 10Base2 der Transceiver auf der Netzwerk-Karte integriert und das Buskabel wird mit einem T-Stück direkt mit der Netzwerk-Karte verbunden. Damit verschwindet die AUI-Schnittstelle. Als Leitung wurde die 6 mm dünne und damit flexiblere RG-58-Leitung festgelegt. Obwohl die Bezeichnung auf eine Segmentlänge von 200 m hindeutet, ist die maximale Segmentlänge, wegen der größeren Dämpfung der Leitung, auf 185m begrenzt.

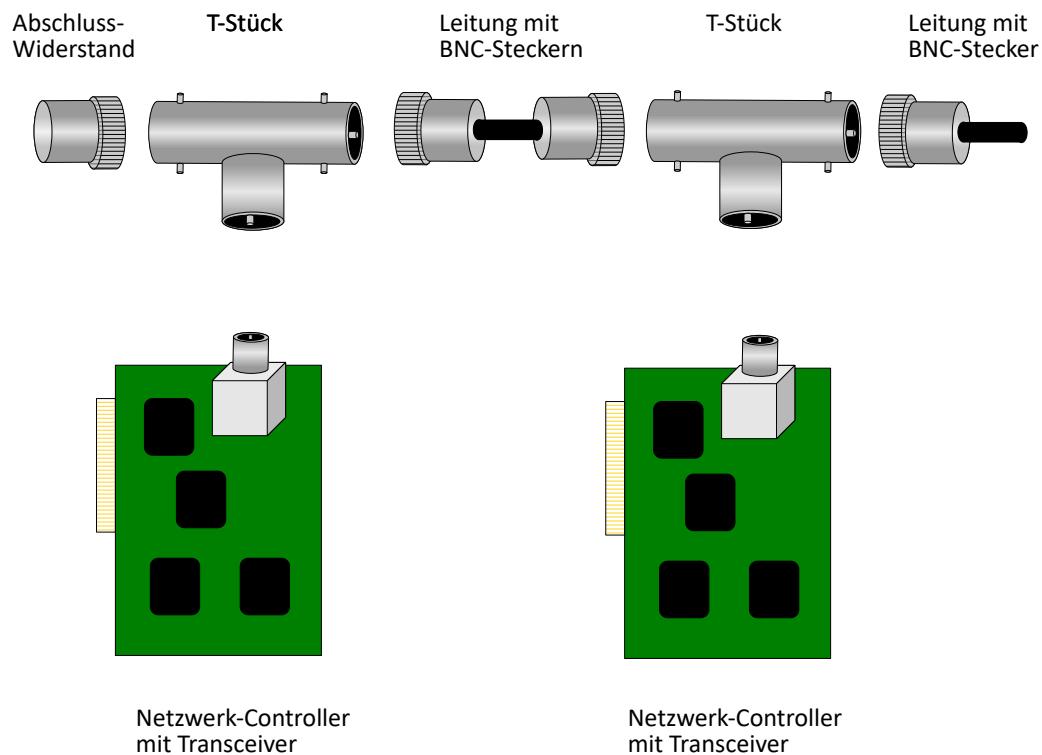


Abbildung 224: 10Base2

14.2.3 - 10 Mbps-Ethernet mit Twisted-Pair-Leitungen

Die Ethernet-Varianten mit Koaxialleitungen waren fehleranfällig und teuer in der Beschaffung der Hardware. Vor allem die T-Stücke waren durch die mechanische Belastung fehleranfällig. Andere Technologien hatten bereits Lösungen mit Twisted-Pair-Leitungen was eine Realisierung bei Ethernet nahelegte.

Im September 1990 wurde mit dem Standard IEEE-802.3i der Standard 10Base-T eingeführt. Als Medium wurde eine UTP-Leitung (Unshielded Twisted Pair) festgelegt. Als Schnittstelle wurde der RJ45-Stecker, der aus dem Telefonumfeld entstammt, definiert. Bei den Leitungen handelt es sich um verbesserte Telefondrähte von denen jeweils zwei Adern miteinander verdrillt sind. 10Base-T verwendet 2 Adernpaare, also 4 Drähte. Ein Adernpaar wird zum Senden und das andere Adernpaar zum Empfangen von Daten verwendet.

Bei den Twisted-Pair-Leitungen handelt es sich symmetrische Leitungen. Das bedeutet, dass die beiden Drähte mit einem Komplementärsignal, also einem symmetrischen Signal zum Potential Erde, versehen werden.

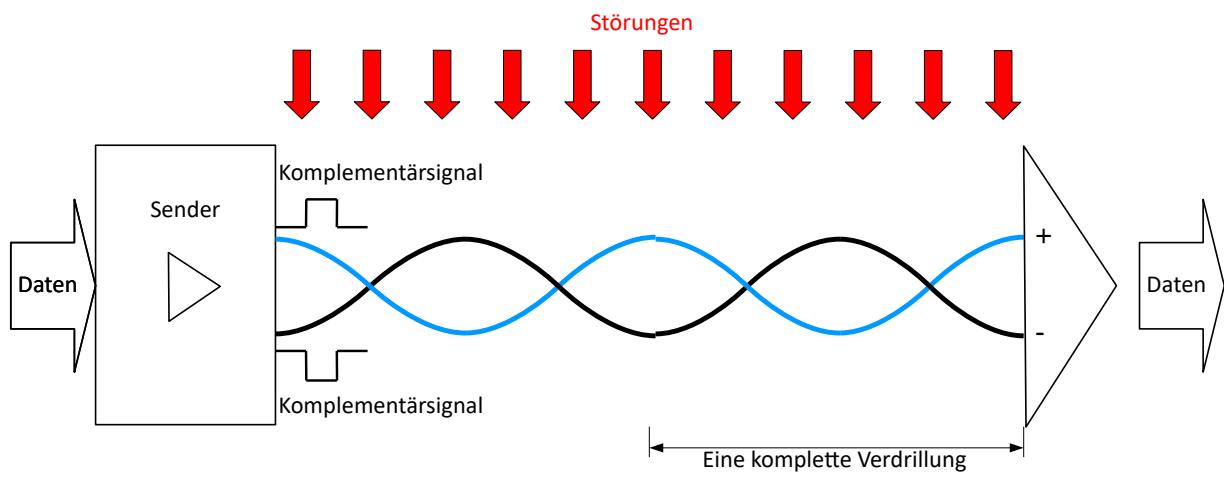


Abbildung 225: Eliminierung von Störungen durch Verdrillung

Das gesendete Komplementärsignal hat auf dem ersten Draht die Pegel von 0V – +2,8V – 0V. Auf dem zweiten Draht werden komplementär dazu die Pegel 0V - -2,8V – 0V angelegt.

Zusammen mit der Verdrillung ergibt sich trotz eines Störsignals beim Empfänger :

$$((+ \text{Nutzsignal}) + (+ \text{Störsignal})) - ((- \text{Nutzsignal}) + (+ \text{Störsignal})) = 2 * \text{Nutzsignal} \quad (92)$$

Dabei sorgt die Verdrillung dafür, dass das Störsignal über eine Verdrillung hinweg klein bleibt bzw. sich aufhebt.

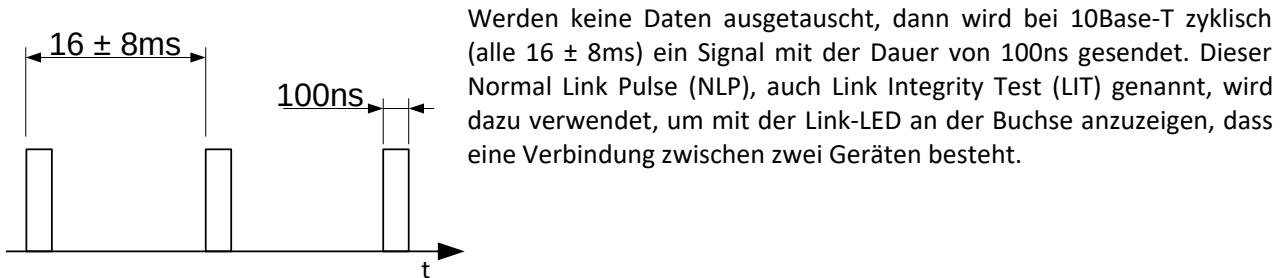


Abbildung 226: Link Integrity Test (LIT) / Normal Link Pulse (NLP)

Ethernet

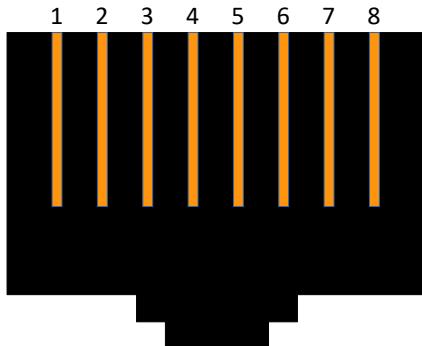


Abbildung 227: Pin-Numerierung einer RJ45-Buchse

Pin	Belegung
1	TD+ (Datenausgang)
2	TD- (Datenausgang)
3	RD+ (Dateneingang)
4	Bei 10Base-T nicht belegt
5	Bei 10Base-T nicht belegt
6	RD- (Dateneingang)
7	Bei 10Base-T nicht belegt
8	Bei 10Base-T nicht belegt

Tabelle 2: RJ45-Pinbelegung

Die Pin-Belegung der RJ45 Buchse ist für alle Endgeräte gleich. Das bedeutet, dass an Pin 1 und 2 die Daten gesendet werden und an Pin 3 und 6 die Daten empfangen.

Würde bei einer Verbindung von zwei Geräten immer die selben Pins miteinander verbunden werden, so würde der Sender auf den Sender und der Empfänger auf den Empfänger geschaltet werden, was natürlich zu einer nicht funktionierenden Verbindung führt.

Deshalb gibt es, für die Verbindung von Geräten mit gleicher Schnittstelle, so genannte Crossover-Leitungen, welche die richtigen Verbindungen herstellen.

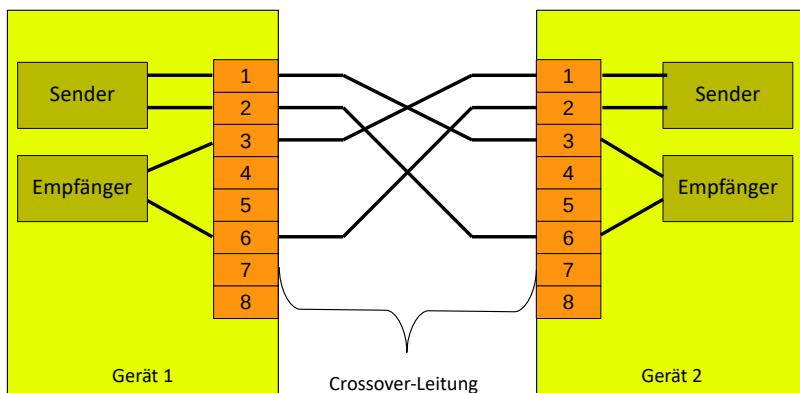
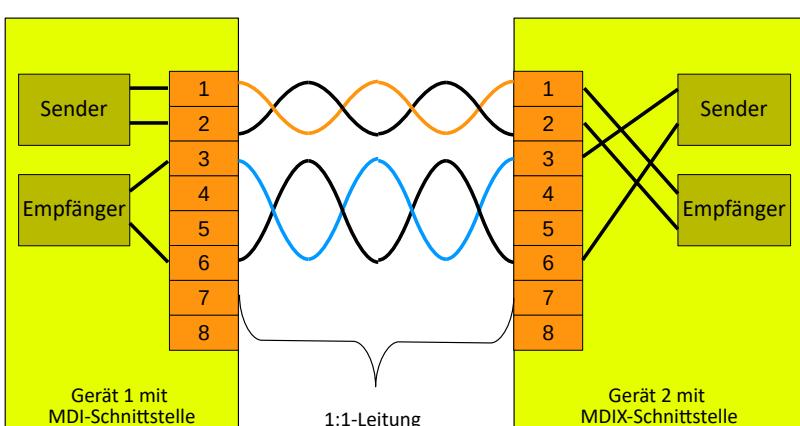


Abbildung 228: Crossover-Verbindung

Die MDI-Schnittstelle (Media Dependent Interface) mit den links gezeigten Pinbelegungen ist bei Endgeräten wie PCs, Drucker, Routern oder Notebooks zu finden. Mit der Verdrahtung der Crossover-Leitung werden die richtigen Verbindungen hergestellt. Dabei sind die zusammengehörigen Paare mit den Pins 1 und 2 sowie 3 und 6 miteinander zu verdrillen.

Die Herstellung ist aufwändig.



Um die Pinbelegung der Leitungen für die Herstellung möglichst einfach zu halten, haben Netzwerkgeräte bei denen viele Anschlüsse zusammenkommen, wie Hubs und Switches, Ports die mit MDIX bezeichnet sind wie beim Gerät 2. Dabei wird die gekreuzte Verbindung zwischen Sender und Empfänger im Netzwerk-Gerät hergestellt, so dass Leitungen benutzt werden können, die immer die selben Pins miteinander verbinden (so genannte

Abbildung 229: Straight-Through-Verbindung
236

1:1- oder Straight-Through-Leitungen).

14.2.4 - 10 Mbps- mit Glasfasern

Die Alternative zu Kupfer ist Glasfaser (LWL = Lichtwellenleiter). 1993 wurden mit dem Standard IEEE802.3j die 10 Mbps-LWL-Varianten eingeführt.

Bei der Anwendung von Glasfasern entfallen einige Probleme.

- Galvanische Trennung
- Potentialprobleme
- Dämpfungsprobleme und damit Längenprobleme
- Sicherheit gegenüber elektromagnetischen Störungen

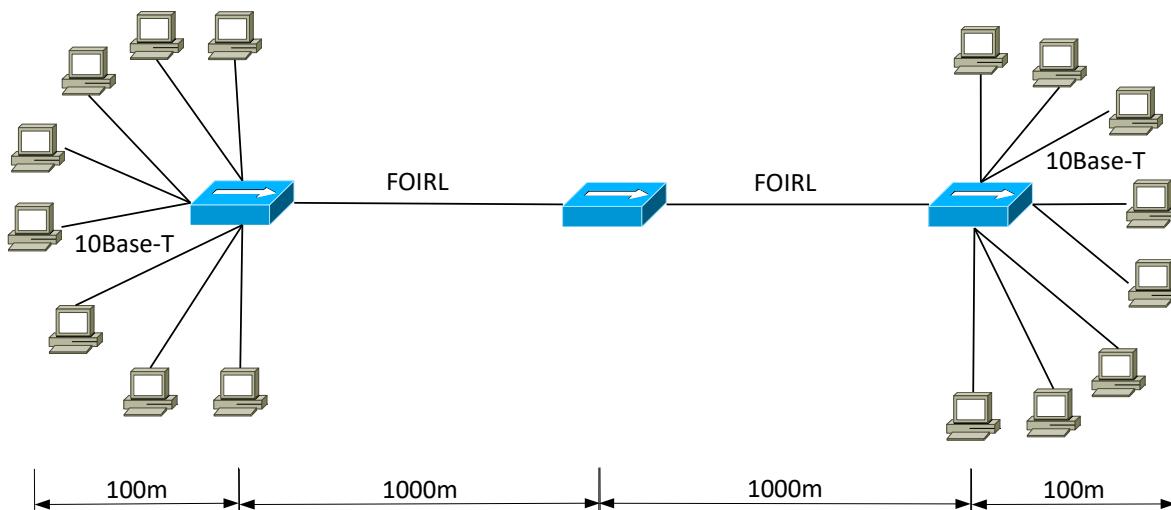


Abbildung 230: Ausdehnung von 10Base-T mittels FOIRL

Es gibt mehrere Varianten von Glasfasern bei 10 Mbps:

- FOIRL (Fibre Optic Inter Repeater Link)

Damit kann eine Verbindung zwischen zwei Reatern (Hubs) auf bis zu 1000 m vergrößert werden. Als Lichtquelle wurden LEDs mit einer Wellenlänge von 850 nm verwendet. Als Fasertyp kommt eine Gradienten Multimode Faser mit einem Durchmesser von 62,5/125 µm zum Einsatz.
- 10Base-FL

Diese Variante entspricht FOIRL mit dem Unterschied, dass die überbrückbare Distanz von 1000 m auf 2000 m anwächst.
- 10Base-FB

Diese Lösung war für den Backbone-Einsatz gedacht. Es gibt Reichweiten bis zu 2000 m.
- 10Base-FP

Diese Lösung besteht aus passiven glasfaserbasierten Sternverteilern. Es wurden allerdings keine Produkte dazu auf den Markt gebracht.

14.2.4.1 - Kenngrößen für 10 Mbps-Ethernet

Kenngröße	10Base-5	10Base-2	10Base-T	10Base-FL	10Base-FB	10Base-FP
Topologie	Bus	Bus	Stern	Stern	Stern	Stern
Signalisierungs-technik	Basisband	Basisband	Basisband	Basisband	Basisband	Basisband
Codierungs-Verfahren	Manchester	Manchester	Manchester	Manchester	Manchester	Manchester
Kabeltyp	RG-8 Koaxialleitung	RG-58 Koaxialleitung	Twisted-Pair	LWL-MMF 62,5/125 µm	LWL-MMF 62,5/125 µm	LWL-MMF 62,5/125 µm
Impedanz Wellenlänge	50 Ω	50 Ω	100 Ω	850 nm	850 nm	850 nm
Maximale Segmentlänge	500 m	185 m	100 m	2000 m	2000 m	500 m
Max. Anz. Stationen pro Segment	100	30	2	2	2	33
Anschluss	Sub-D-15 mit Drop-Cable + Transceiver	T-Verbinder	RJ45-Stecker	ST-Stecker	ST-Stecker	ST-Stecker

Tabelle 3: Kenngrößen für 10 Mbps-Ethernet

14.3 - 100 Mbps-Ethernet

14.3.1 - 100Base-TX (Fast Ethernet)

Im Juni 1995 wurde der 100 Mbps-Ethernet-Standard von IEEE als IEEE-802.3u veröffentlicht. Um die 10-fache Datenübertragungsrate herauszustellen, wurde 100 Mbps-Ethernet auch mit Fast-Ethernet bezeichnet. Obwohl viele Neuerungen für die 100 Mbps-Variante eingeführt wurden, ist sie zu 10 Mbps abwärtskompatibel. Dafür wurde zwischen MAC-Ebene und PLS eine neue Subebene, die Reconciliation-Layer, eingezogen.

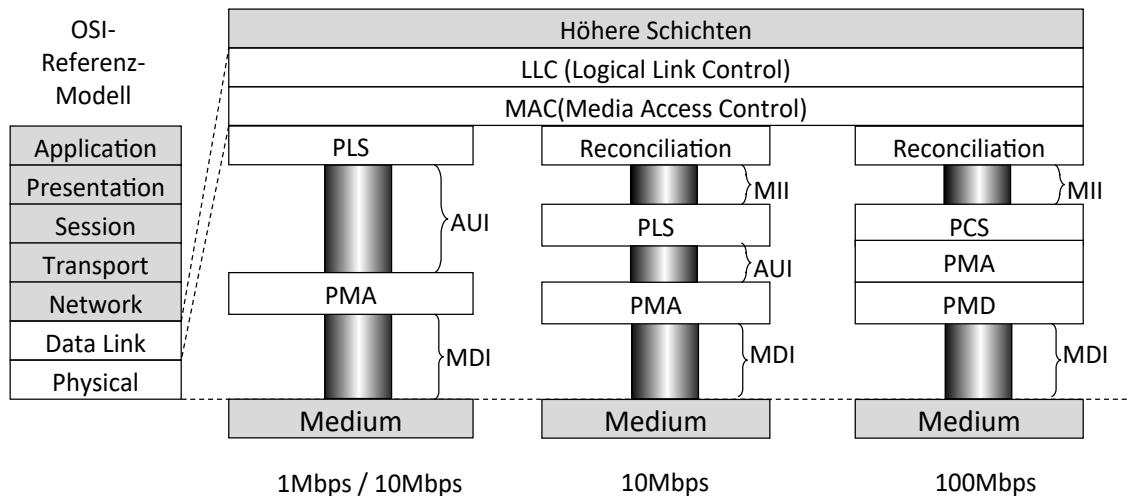
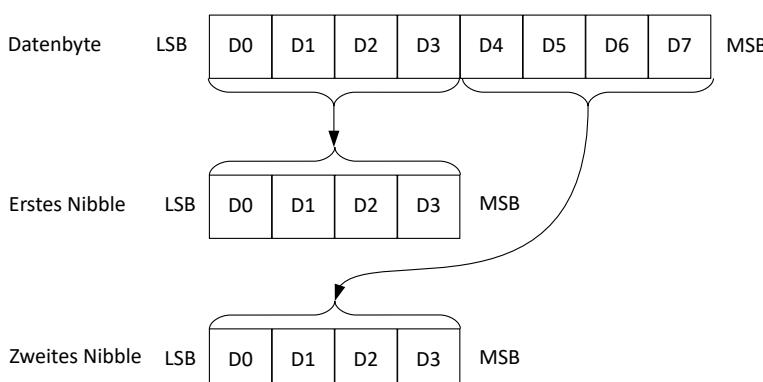


Abbildung 231: Einführung neuer Sublayer für 100 Mbps

14.3.1.1 - Reconciliation Layer



In dieser Schicht wird die Anpassung an das neu erstellte Media Independent Interface (MII) durchgeführt. Damit wurde die AUI-Schnittstelle ersetzt. Im Falle eines Kommunikationspartners der nur 10 Mbps-Fähigkeiten besitzt, kann die PLS mit der MII verbunden werden. Darunter ist dann auch wieder eine AUI-Schnittstelle verfügbar.

Die Daten werden über die MII-Schnittstelle mit 4 Bits (Nibbles) zur Verfügung gestellt. Dafür müssen die Datenbytes in 4 Bit große Nibbles umgewandelt werden.

Abbildung 232: Umwandlung von Bytes in Nibbles

Die MII-Schnittstelle erlaubt die Adaptierung verschiedener physikalischer Medien mit 10 Mbps und 100 Mbps. Sie kann auf einem 40-poligen-Subminiatur-Stecker nach außen geführt werden. Dabei handelt es sich um eine Leitung vom Typ 26 AWG mit einem Wellenwiderstand von 68Ω . Als Signale werden TTL-Signale mit 5V-Pegel verwendet, womit die Schnittstelle mit CMOS-Bausteinen ausgeführt werden kann.

Pin	Signal	Pin	Signal
1	+5V	21	+5V
2	Management Data I/O (MDO)	22	Masse
3	Management Data Clock (MDC)	23	Masse
4	RX Data 3 (RXD3)	24	Masse
5	RX Data 2 (RXD2)	25	Masse
6	RX Data 1 (RXD1)	26	Masse
7	RX Data 0 (RXD0)	27	Masse
8	RX Data Valid (RX_DV)	28	Masse
9	RX Clock (RX_CLK)	29	Masse
10	RX Error (RX_ER)	30	Masse
11	TX Error (TX_ER)	31	Masse
12	TX Clock (TX_CLK)	32	Masse
13	TX Enable (TX_EN)	33	Masse
14	TX Data 0 (TXD0)	34	Masse
15	TX Data 1 (TXD1)	35	Masse
16	TX Data 2 (TXD2)	36	Masse
17	TX Data 3 (TXD3)	37	Masse
18	Collision (COL)	38	Masse
19	Carrier Sense (CRS)	39	Masse
20	+5V	40	+5V

Tabelle 4: Pinbelegung der MII-Schnittstelle

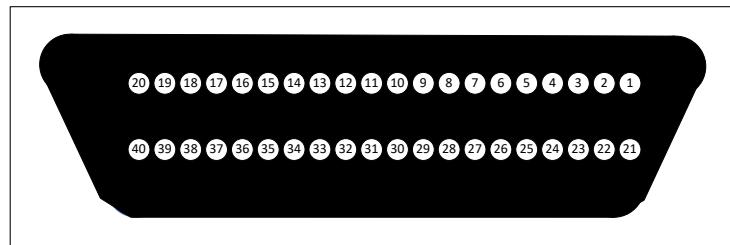


Abbildung 233: MII-D-Subminiatur-Stecker

14.3.1.2 - PCS

Hier erfolgt eine 4B/5B-Codierung.

14.3.1.3 - PMA

Die Physical Medium Attachment Sublayer ist von oben her gesehen die letzte mediumunabhängige Sublayer. Die PMA generiert Kontrollssignale, welche die Verfügbarkeit des PMD anzeigen und die Autonegotiation durchführen. Hier findet auch die Taktrückgewinnung aus den NRZI-kodierten Datenströmen statt.

14.3.1.4 - PMD

Die Physical Medium Dependent Sublayer stellt entweder eine Kupfer-, oder eine LWL-Schnittstelle bereit.

Ethernet

Um die bei 10Base-T verwendeten Leitungen weiterhin auch mit 100 Mbps nutzen zu können, musste eine andere Codierung gewählt werden. Die bei 10Mbps verwendete Manchester-Codierung hätte eine Frequenz von 100 MHZ auf der Leitung zur Folge gehabt. Von FDDI hat man die NRZI-Codierung übernommen. Dabei wird nur bei jeder 1 ein Pegelwechsel durchgeführt.

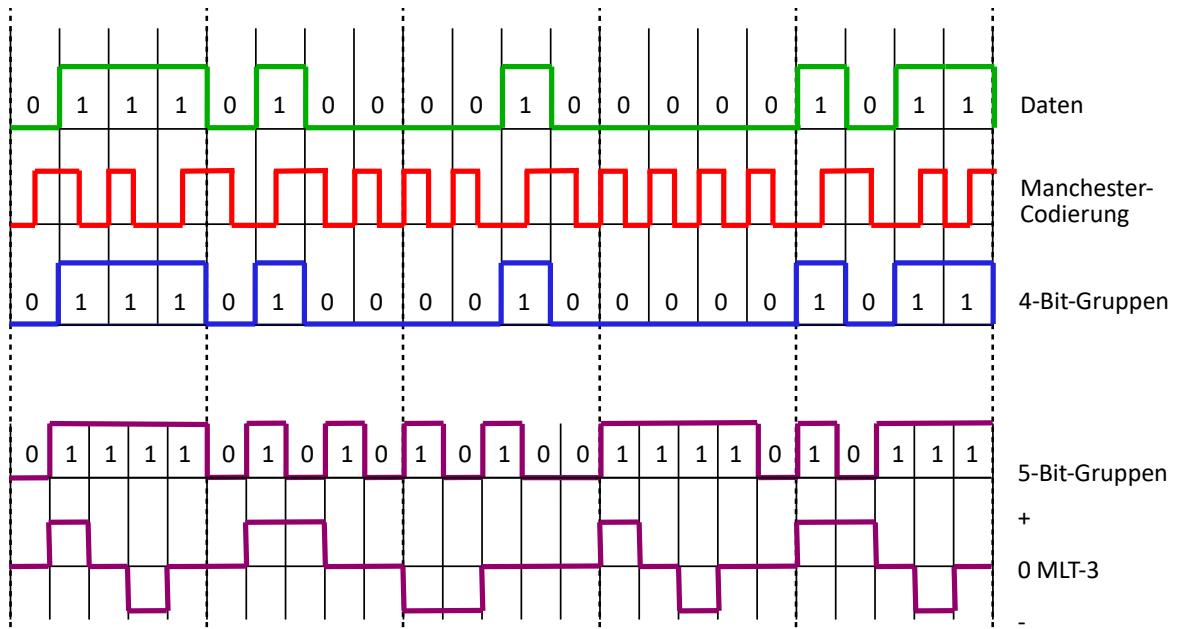


Abbildung 234: Übergang von der Manchester-Codierung zu MLT-3

Dies hat allerdings den Nachteil, dass eine Taktrückgewinnung bei einer langen Null-Folge nicht mehr möglich ist. Deshalb ist dafür Sorge zu tragen, dass es keine langen Null-Folgen gibt. Dies wird erreicht, indem ein 4-Bit-Nibble in ein 5-Bit-Symbol umgewandelt wird (siehe folgende Tabelle).

Codetyp	4B Code	Name	5B Symbole
Daten	0000	0	11110
Daten	0001	1	01001
Daten	0010	2	10100
Daten	0011	3	10101
Daten	0100	4	01010
Daten	0101	5	01011
Daten	0110	6	01110
Daten	0111	7	01111
Daten	1000	8	10010
Daten	1001	9	10011
Daten	1010	A	10110
Daten	1011	B	10111
Daten	1100	C	11010
Daten	1101	D	11011
Daten	1110	E	11100

Codetyp	4B Code	Name	5B Symbole
Quiet		Q	00000
Idle		I	11111
Start of Stream		J	11000
Start of Stream		K	10001
End of Stream		T	01101
Reset		R	00111
Set		S	11001
Halt		H	00100
Invalid			00001
Invalid			00010
Invalid			00011
Invalid			00101
Invalid			00110
Invalid			01000
Invalid			10000

Daten	1111	F	11101
-------	------	---	-------

Invalid			11001
---------	--	--	-------

Tabelle 5: 4B/5B-Codierung

Eine weitere Reduzierung der Frequenz auf der Leitung wird durch die Anwendung einer MLT-3-Codierung auf der Leitung erreicht (siehe Abbildung 234).

Ethernet

Die 4B/5B-Codierung hat auch die Möglichkeit geschaffen, zusätzliche Informationen zu übertragen und Codes festzulegen, die als ungültig erkannt werden können, womit ist eine Fehlererkennung möglich wird.

Der Beginn einer Datenübertragung wird mit einer Speziellen Symbolgruppe (JK) die als Start-of-Stream-Delimiter (SSD) bezeichnet wird, eingeleitet.

Das Ende einer Datenübertragung wird mit der Symbolgruppe (TR), die als End-of-Stream-Delimiter (ESD) bezeichnet wird, abgeschlossen.

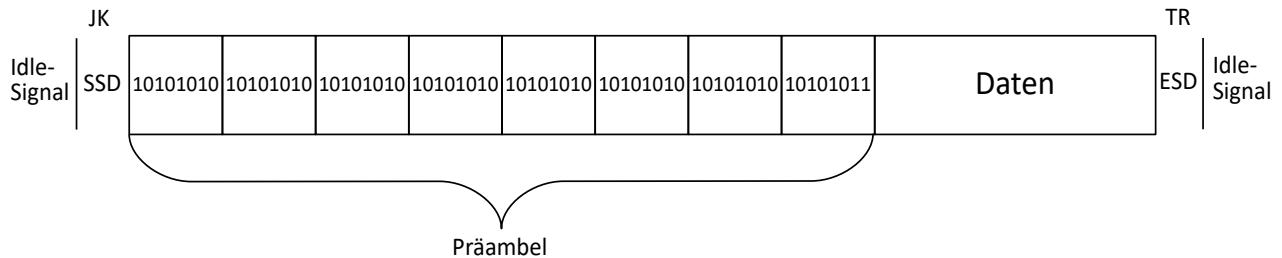


Abbildung 235: 100 Mbps-Ethernet-Paket

Die bisher verwendete Präambel bleibt erhalten und wird mitgesendet.

Werden beim 10 Mbps-Ethernet keine Daten gesendet, gibt es dort nur die NLP-Impulse auf der Leitung. Werden bei 100 Mbps-Ethernet keine Daten gesendet, findet trotzdem der Austausch von Idle-Symbolen (11111) statt. Damit kann eine Taktrückgewinnung durchgeführt werden.

14.3.1.5 - Auto-Negotiation-Handshake

Mit der Erweiterung von Ethernet auf 100 Mbps und der Anforderung, dass Geräte mit einer 10 Mbps-Schnittstelle an ein 100 Mbps-Gerät angeschlossen werden können, kam die Anforderung hinzu, die unterschiedlichen Varianten möglichst automatisch zu erkennen und die Schnittstellen automatisch an die bestmögliche Übertragung anzupassen. Dies ist bei den LWL-Varianten nicht möglich, da dort unterschiedliche Wellenlängen, die nicht geändert werden können, bei den Lichtquellen verwendet werden.

Die Firma National Semiconductor hatte 1994 Nway (oder N-way) entwickelt um die Inkompatibilitäten bei falschen Konfigurationen zu entschärfen. Nway wurde im IEEE802.3u integriert.

Bei der Twisted-Pair-Kupfervariante gab es mit den NLPs (Normal Link Pulse) bei 10 Mbps eine Möglichkeit herauszufinden, ob der Link zustande gekommen ist. Diese Funktionalität wurde erweitert um die Datenrate und den Duplexmode zwischen den Kommunikationspartnern anzupassen. Dazu wurden die NLPs zu den Fast Link Pulse (FLP) erweitert.

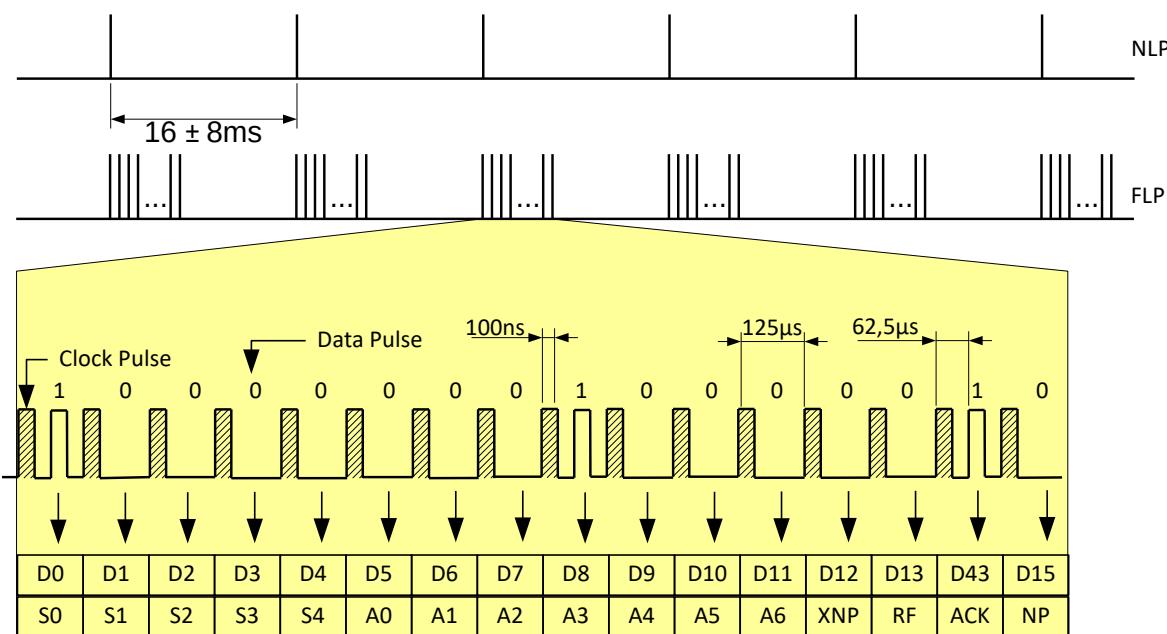


Abbildung 236: NLP und FLP mit dem Basic Link Codewort

Alle 16 ± 8 ms wird, wie bei den NLPs, eine Folge von 16 Clock-Pulsen innerhalb von 2 ms ($16 * 125 \mu s$) gesendet. Zwischen den Clock-Pulsen kann jeweils ein Bit Dateninformation mitgegeben werden (0 = kein Daten-Puls / 1 = Daten-Puls). Damit werden die 16 Datenbits (D0 – D15) eines Basic-Link-Codewortes (BLC) übertragen.

Ethernet

Die ersten 5 Bits des BLC bilden das Selektor-Feld. Sie dienen der Auswahl des zugrundeliegenden Standards. Danach folgt mit 7 Bits das Ability-Feld. Darin werden, je nach angegebenem Selektor-Feld, die Eigenschaften wie Datenrate und Duplexmode beschreiben. Es folgt ein Bit für den Extended Next Page (XNP). Weiter folgt ein Remote Fault-Bit (RF). Danach kommt ein Acknowledge-Bit (ACK). Als letztes folgt ein Next Page-Bit (NP).

S4	S3	S2	S1	S0	Selector-Beschreibung
0	0	0	0	0	Reserviert für künftige Entwicklungen
0	0	0	0	1	IEEE-802.3-Standard
0	0	0	1	0	IEEE-802.9-Standard (zurückgezogen)
0	0	0	1	1	IEEE-802.5-Standard (zurückgezogen)
0	0	1	0	0	IEEE-1394-Standard
0	0	1	0	1	INCITS
0	0	1	1	X	Reserviert für künftige Entwicklungen
0	1	X	X	X	Reserviert für künftige Entwicklungen
1	X	X	X	X	Reserviert für künftige Entwicklungen

Tabelle 6: Basic-Link Selektor-Feld

Nach der obigen Tabelle wird in Abbildung 236 IEEE802.3, also Ethernet ausgewählt. Die nächsten 7 Bits sind die so genannten Ability-Bits. Je nach ausgewähltem Standard wird im Ability-Feld (z. B. bei Ethernet) die Datenrate und der Duplexmode angezeigt.

Bit	Technologie
A0	10Base-T
A1	10Base-T Vollduplex
A2	100Base-TX
A3	100Base-TX Vollduplex
A4	100Base-T4
A5	Pause Operation für Flow-Control
A6	Asymmetrische Pause Operation für Flow Control

Tabelle 7: Ability-Feld bei 100 Mbps-Ethernet

In Abbildung 236 wurde also 100Base-TX Vollduplex ausgewählt.

Eine Komponente beginnt mit dem aussenden des Basic-Link-Codewortes ohne ACK-Bit. Nachdem die Gegenseite das Link-Codewort mit dem selben Inhalt dreimal empfangen hat, beginnt die Gegenseite mit dem Senden des Link-Codewortes mit gesetztem ACK-Bit. Ist auch das dreimal hintereinander mit gleichem Inhalt erfolgt wird durch das sechs- bis achtmalige Senden mit gesetztem ACK-Bit ein erfolgreicher Handshake angezeigt.

Bei diesem Informationsaustausch kann es vorkommen, dass jede Seite eine andere Datenrate oder einen anderen Duplexmodus signalisiert. Zur Festlegung des kleinsten gemeinsamen Nenners wird die folgende Tabelle herangezogen.

Priorität	Modus
1	10GBase-T Vollduplex
2	1000Base-T Vollduplex
3	1000Base-T
4	100Base-T2 Vollduplex
5	100Base-TX Vollduplex
6	100Base-T2
7	100Base-T4
8	100Base-TX
9	10Base-T Vollduplex
10	10Base-T

Tabelle 8: Prioritätenliste bei 100 Mbps

14.3.1.6 - Flow-Control nach IEEE802.3x

Die Bits A5 und A6 des Ability-Feldes bieten die Möglichkeit für die Steuerung des Datenstroms (Flow Control). Beim Auto-Negotiation-Ablauf wird mit den beiden Bits festgelegt, ob die Stationen die Funktion unterstützen.

Im Full duplex Mode, also bei Verbindungen, bei denen immer nur zwei Geräte miteinander kommunizieren, ist kein Zugriffsverfahren mehr notwendig und es kann vorkommen, dass ein Gerät mit der Abarbeitung der eingehenden Daten nicht mehr hinterherkommt. Mit der Einführung des Standards IEEE-802.3x gibt es die Möglichkeit einer Flow-Control (deutsch: Flusssteuerung) also, den Sender aufzufordern mit dem Senden zu warten. Dazu wird ein spezieller Pause-Frame an den Sender gesendet. Er hat als Inhalt den Wert 0x8808 im Type-Feld eingetragen. Im Pause-Frame ist die Wartezeit hinterlegt, die der Sender einlegen muss. Nach Ablauf der Pausezeit (Pause Time) sendet der Sender wieder Daten. Kommt es wieder zu einer Überlastung, kann der Ablauf wiederholt werden.

Der Pause-Frame hat einen speziellen Aufbau bei dem als Ziel-MAC-Adresse immer 01-08-C2-00-00-01 an gegeben wird. Das ist eine Multicast-Adresse die von Switches gefiltert, also nicht weiter geleitet wird. Damit bleibt dieser Frame immer in der Verbindung, die gedrosselt werden soll eingeschlossen.

Im 2 Byte großen MAC-Control-Opcode ist der Code 0x0001 hinterlegt, was darauf hinweist, dass das nächste 2 Byte große Feld die Pausezeit beinhaltet. Mit den zwei Bytes können Werte zwischen 0 und 65635 als das Vielfache der Slot-Time darstellt.

Präambel	SFD	Ziel-MAC-Adresse 01-08-C2-00-00-01	Quell-MAC-Adresse	Type 0x8808	MAC-Control Opcode=0x0001 2 Bytes	Pause Time 2 Bytes	Füller 44 Bytes	CRC 4 Bytes
----------	-----	---------------------------------------	-------------------	----------------	---	-----------------------	--------------------	----------------

Abbildung 237: Pause-Frame

Beim Flow-Control-Verfahren gibt es zwei Varianten. Wird von beiden Seiten Flow-Control unterstützt spricht man von symmetrischem Flow-Control. Beim asymmetrischen Flow-Control sendet nur eine Seite Pause Frames. Die andere Seite wertet die Frames aus und wartet mit dem Senden der Daten.

14.3.2 - Weitere 100 Mbps-Kupfer-Varianten

Es gibt noch zwei weitere Kupfer-Varianten, die jedoch keine Marktakzeptanz gefunden haben. Allerdings wurden hier Funktionen eingeführt, die bei späteren Standards wieder Verwendung fanden. Deshalb werden sie hier der Vollständigkeit halber aufgeführt.

14.3.2.1 - 100Base-T2

Diese Variante wurde als IEEE-802.3y 1997 veröffentlicht. Die Bezeichnung T2 weist darauf hin, dass hier zwei CAT-3-Adernpaare verwendet werden. Erreicht wird das mit der PAM5-Codierung, also einer Puls-Amplituden-Modulation mit 5 Level (-2V, 1V, 0V, 1V, 2V). Die Daten werden über beide Adernpaare in beiden Richtungen übertragen. Damit dies funktioniert musste ein Echo-Cancellation-Verfahren eingeführt werden. Es wird nach einem Master-Slave-Verfahren gearbeitet. Dabei verwendet der Master seinen internen Takt. Der Slave auf der anderen Seite muss den Takt aus dem übertragenen Signal erzeugen. Als MDI wird die RJ45-Schnittstelle eingesetzt.

Pin	PHY ohne interne Kreuzungsfunktion	PHY mit interne Kreuzungsfunktion	MDI
1	BI_DA +	BI_DB +	BI_DA +
2	BI_DA -	BI_DB -	BI_DA -
3	BI_DB +	BI_DA +	BI_DB +
4	Nicht benutzt	Nicht benutzt	Nicht benutzt
5	Nicht benutzt	Nicht benutzt	Nicht benutzt
6	BI_DB -	BI_DA -	BI_DB -
7	Nicht benutzt	Nicht benutzt	Nicht benutzt
8	Nicht benutzt	Nicht benutzt	Nicht benutzt

Tabelle 9: Pinbelegung des MDI bei 100Base-T2

14.3.2.2 - 100Base-T4

Der Name weist bereits darauf hin, dass hier 4 Adernpaare verwendet werden. Über 3 Adernpaare werden Daten gesendet und über das verbleibende Adernpaar werden Kollisionsmeldungen übertragen.

Pin	PHY ohne interne Kreuzungsfunktion	PHY mit interne Kreuzungsfunktion	MDI
1	TX_D1 +	RX_D2 +	TX_D1 +
2	TX_D1 -	RX_D2 -	TX_D1 -
3	RX_D2 +	TX_D1 +	RX_D2 +
4	RX_D2 -	TX_D1 -	RX_D2 -
5	BI_D3 +	BI_D4 +	BI_D3 +
6	BI_D3 -	BI_D4 -	BI_D3 -

Ethernet

7	BI_D4 +	BI_D3 +	BI_D4 +
8	BI_D4 -	BI_D3 -	BI_D4 -

14.3.2.3 - 100Base-FX

Bei den LWL-Varianten können nur feste Datenraten verwendet werden. Damit gibt es keine Abwärtskompatibilität. Hier können Distanzen von bis zu 412m erreicht werden. Dabei wird im Vollduplex Modus gearbeitet. Als Übertragungsmedium werden Gradienten-Multimode-Fasern mit den Durchmessern 62,5/125 µm und 50/125µm. Als Lichtquelle werden LEDs mit einer Wellenlänge von 1300nm verwendet. Die Datenübertragung wird mit einem NRZI-Code durchgeführt.

14.3.2.4 - 100Base-FX für große Distanzen

Es gibt noch eine LWL-Variante für Distanzen von bis zu 15km. Dazu wird einen Singlemode-Stufenindex-Faser mit 9/125 µm und eine Laserdiode mit einer Wellenlänge von 130nm verwendet.

14.3.2.5 - Kenngrößen für 100 Mbps-Ethernet

Kenngröße	100Base-TX	100Base-T2	100Base-T4	100Base-FX	100Base-FX für große Distanzen
Topologie	Stern	Stern	Stern	Stern	Stern
Signalisierungstechnik	Basisband	Basisband	Basisband		
Codierungs-Verfahren	NRZI 4B/5B über MLT-3	2 * PAM5	8B/6T	NRZI 4B/5B	NRZI 4B/5B
Kabeltyp	TP-CAT-5	TP-CAT-3	TP-CAT-3	LWL-MMF 62,5/125 µm oder 50/125 µm	LWL-SMF 9/125 µm
Impedanz Wellenlänge	100Ω	100Ω	100Ω	LED 1300 nm	Laser 1300 nm
Maximale Segmentlänge	100 m	100 m	100 m	2.000 m (Vollduplex) 412 m (Halbduplex)	15.000 m
Max. Anz. Stationen pro Segment	2	2	2	2	2
Anschluss	RJ45	RJ45	RJ45	Duplex-SC / Duplex-ST	Duplex-SC / Duplex-ST

Tabelle 10: Kenngrößen für 100 Mbps-Ethernet

14.4 - 1000 Mbps-Ethernet

Um sicher zu stellen, dass Ethernet eine Erfolgsgeschichte bleibt, bekamen die Entwickler der nächsten Generation die Aufgabe, dass 1000Base-X abwärtskompatibel sein sollte.

Damit musste eine Möglichkeit geschaffen werden, alte Geräte, die nur 10 Mbps und 100 Mbps beherrschen, an die neue Variante anzuschließen.

Das ist bei den LWL-Varianten nicht umsetzbar, da die Lichtquellen mit festen Wellenlängen arbeiten.

Im Kupferbereich ist es jedoch gelungen die alten Varianten mit dem neuen Gigabit-Ethernet zu verbinden. Das war auch wichtig, da es eigentlich nur Endgeräte mit einer Kupferanbindung gibt.

Für die Kupferanbindung war allerdings auch noch gefordert worden das Zugriffsverfahren und die Frameformate beizubehalten. Die Idee war CSMA/CD weiterhin betreiben zu können um Hubs mit 1000 Mbps auf den Markt bringen zu können. Bei der Umsetzung dieser Forderung entstanden die größten Probleme. Deshalb wurde Gigabit-Ethernet zuerst in einer IEEE-Norm (IEEE-802.3z) für LWL mit einer kurzen Kupfervariante (25m) veröffentlicht. Die 1000Base-T-Variante (IEEE -802.3ab) mit einer Leitungslänge von 100 m kam erst später.

14.4.1 - IEEE-802.3z

Für die Verwendung von CSMA/CD müssen Grenzwerte festgelegt werden, damit eine Kollision sicher erkannt werden kann. Dazu gehört die minimale Framegröße mit 64Byte. Damit wird sichergestellt, dass während die Bits ausgesendet werden, eine Kollision am maximal entfernten anderen Ende, noch sicher erkannt werden kann. Die Festlegung der minimalen Framegröße hängt von den Bitzeiten ab, die benötigt werden, um ein Bit zu übertragen.

Davon abgeleitet ergibt sich dann die maximale Ausdehnung aller zusammengeschalteten Segmente als Kollisionsdomäne. Bei 1000 Mbps-Ethernet würde sich damit eine maximale Segmentlänge von ca. 20 m ergeben.

Datenrate	Bitzeiten	Maximale Ausdehnung
10 Mbps	100 ns	ca. 2000 m
100 Mbps	10 ns	ca. 200 m
1000 Mbps	1 ns	ca. 20 m

Tabelle 11: Größe einer Kollisionsdomäne bei unterschiedlichen Datenraten ohne Anpassung

Dies war nicht akzeptabel, da die vorhandenen Twisted-Pair-Installationen bereits Distanzen von maximal 100 m überbrücken konnten. Deshalb musste die minimale Framegröße für Ethernet bei Verwendung von CSMA/CD im Halbduplexbetrieb erweitert werden.

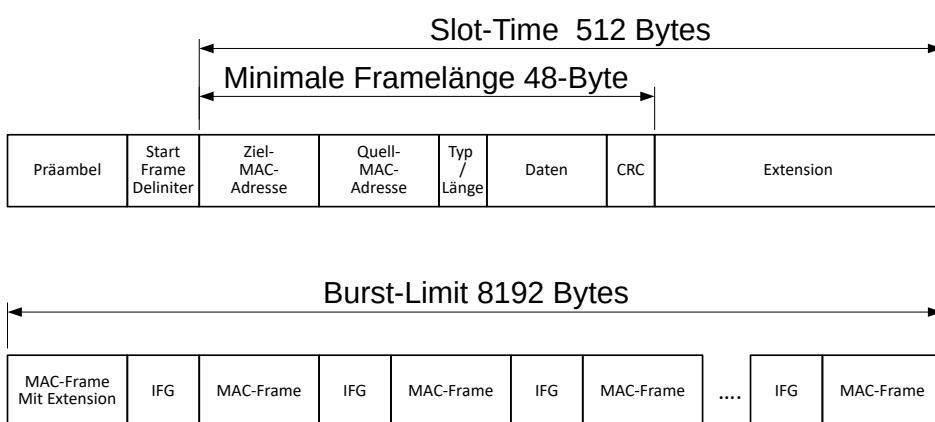


Abbildung 238: Extension-Frame und Burst-Limit

Dazu wurde an den vorhandenen Frame eine Extension angehängt, die abhängig von der Größe des Datenteils ermittelt wurde. Damit konnte eine Kollision sicher erkannt werden.

Ethernet

Allerdings war das bei kurzen Datenpaketen eine Verschwendungen der Bandbreite. Um diesen Effekt abzumildern wurde für Gigabit-Ethernet das Frame-Bursting eingeführt. Dabei wird der Erste Frame mit Extension gesendet. Weitere Frames werden nach einem Inter-Frame-Gap (IFG) ohne Extension gesendet. Um zu vermeiden, dass eine Station das LAN zu lange belegt, wurde das Frame-Burst-Limit mit 65536 Bit = 8192 Bytes eingeführt. Der IFG beträgt 96ns was 12 Bytes entspricht. Damit lassen sich 6 Frames mit maximaler Größe senden.

Wohlgemerkt, das ist nur bei einem Halbduplexbetrieb erforderlich! Hubs mit 1000 Mbps wurden durch die Einführung von Switches nicht mehr in großen Stückzahlen realisiert. Bei Switches kommt CSMA/CD nicht mehr zum Einsatz, da es sich hierbei immer um eine Punkt zu Punkt Verbindung zwischen Switch und Endgerät handelt. Damit haben sowohl Extension-Frames sowie Frame-Bursting nur eine historische Bedeutung.

14.4.1.1 - Physical-Layer

Die für Fast-Ethernet eingeführte MII wurde für Gigabit-Ethernet durch das Gigabit-Media-Independent-Interface (GMII) ergänzt. Chipsätze die mehrere Geschwindigkeiten unterstützen haben die MII und AUI auch noch implementiert.

Die Datenbreite beträgt beim GMII 8 Bit. Damit wird die doppelte Datenbreite vom MII verwendet. Die Frequenz auf der Leitung beträgt 125MHz und ist damit um den Faktor 5 größer als bei 100 Mbps. Mit der doppelten Datenbreite und der fünffachen Frequenz ist es möglich die 10fache Datenrate von Fast-Ethernet zu übertragen.

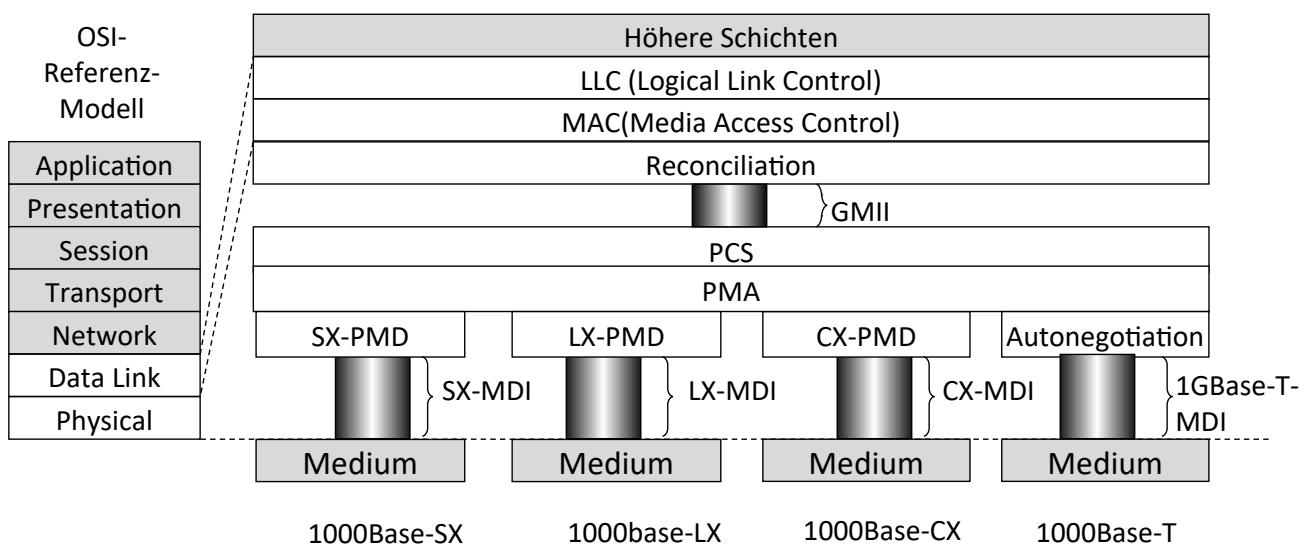


Abbildung 239: GMII-Einführung

14.4.1.2 - PCS

Bei den LWL-Varianten wird in der Physical-Coding-Sublayer(PCS) eine Umwandlung der 8 Bit breiten Daten auf 10 Bit durchgeführt. Die 8B/10B-Codierung entspricht der 4B5B-Codierung von Fast-Ethernet. Bei der 1GBase-T-Variante wird keine 8B/10B-Codierung vorgenommen.

14.4.1.3 - PMA

Das Physical Media Attachment wandelt die parallelen 10Bit in ein serielles Datenformat um. Im PMA erfolgt auf der Empfängerseite die Taktrückgewinnung aus dem empfangenen Signal. Bei der 1GBase-T-Variante wird hier die Autonegotiation vorgenommen.

14.4.1.4 - PMD

Die Physical Media Dependent Sublayer gibt es bei IEEE802.3z in drei Varianten:

- SX-PMD Multimode-Glasfaser mit einer Wellenlänge von 850nm
- LX-PMD Multimode oder Monomode-Glasfaser mit einer Wellenlänge von 1300nm
- CX-PMD ist eine kupferbasierte Übertragung auf einer Twinax-Leitung
- T ist die Lösung mit Twisted-Pair-Leitungen

Die 8B/10B-Codierung wurde dem Fibre-Channel-Standard ANSI X3.230:1994 entlehnt. Hier ist die weitgehende Gleichspannungsfreiheit und die Möglichkeit der Taktrückgewinnung gegeben.

Die 10Bit großen Blöcke sind in 2 Unterblöcke aufgeteilt. Dabei handelt es sich um einen 5B/6B-NRZ-Code und einen 3B/4B-NRZ-Code

Code Group Name	Octet Wert	Octet Bits HGF EDCBA	Current RD - abcdei fghj	Current RD + abcdei fghj
D0.0	00	0 0 0 00000	100111 0100	011000 1011
D1.0	01	0 0 0 00001	011101 0100	100010 1011
D2.0	02	0 0 0 00010	101101 0100	010010 1011
D3.0	03	0 0 0 00011	110001 1011	001110 0100
D4.0	04	0 0 0 00100	110101 0100	001010 1011
D5.0	05	0 0 0 00101	101001 1011	010110 0100
D6.0	06	0 0 0 00110	011001 1011	100110 0100
D7.0	07	0 0 0 00111	111000 1011	000111 0100
D8.0	08	0 0 0 01000	111001 0100	000110 1011
D9.0	09	0 0 0 01001	100101 1011	011010 0100
D10.0	0A	0 0 0 01010	010101 1011	101010 0100
D11.0	0B	0 0 0 01011	110100 1011	001011 0100
D12.0	0C	0 0 0 01100	001101 1011	110010 0100
D13.0	0D	0 0 0 01101	101100 1011	010011 0100
D14.0	0E	0 0 0 01110	011100 1011	100011 0100
D15.0	0F	0 0 0 01111	010111 0100	101000 1011

Tabelle 12: Ausschnitt aus der 8B/10B-Codierung

Eine erzeugte Codegruppe hat mindestens 4, jedoch nie mehr als 7 Pegelwechsel. Damit werden die Lauflängen der Nullen und Einsen beschränkt. (Run Length Limited). Der Gleichspannungsanteil ergibt sich aus der Differenz von Einsen (mit einem hohen Signalpegel) und den Nullen (mit einem niedrigen Signalpegel). Die Ungleichheit zwischen Einsen und Nullen innerhalb einer Codegruppe nennt man Disparity.

$$\text{Disparity} = \text{Anzahl der Einsen} - \text{Anzahl der Nullen} \quad (93)$$

Die Disparity bei den verwendeten Codewörtern darf nur die Werte 2, 0 oder +2 annehmen. So hat z. B. der Octet-Wert 00 zwei mögliche Ergebnisse mit der Disparity = 0 (100111 0100 oder 011000 1011). Der Octet-Wert 03 hat ein Ergebnis mit einer Disparity von +2 (110001 1011) und ein Ergebnis mit -2 (001110 0100)

Ethernet

Es wird eine laufende Disparity (Running Disparity = RD) ständig mitgeführt. Bei einem 8B/10BCode darf die RD nur Werte von -1 oder +1 annehmen.

Mit einem angenommenen Wert von RD = -1 und den folgenden Regeln kann die Maximale Schwankung von -1 und +1 eingehalten werden:

- ➊ Ein Code mit einer Disparity von 0 kann unabhängig von der RD gesendet werden.
- ➋ Ein Code von -2 kann nur bei einem RD-Wert von +1 gesendet werden.
- ➌ Ein Code von +2 kann nur bei einem RD-Wert von -1 gesendet werden.

In Tabelle 12: Ausschnitt aus der 8B/10B-Codierung ist zu sehen, dass die beiden rechten Spalten komplementäre Ergebnisse beinhalten. Welches der beiden Ergebnisse verwendet wird, hängt vom aktuellen RD-Wert ab.

Im folgenden Beispiel ist der aktuelle RD-Wert=-1. Es sollen die Daten 00, 03, 07 und 09 gesendet werden.

Alter RD-Wert	Zu übertragende Daten	Ausgewählter Code	Disparity des ausgewählten Codes	Neuer RD-Wert
-1	00	10011 10100	0	-1
-1	03	11000 11011	+2	+1
+1	07	0011 10100	-2	-1
-1	09	10010 11011	+2	+1

Tabelle 13: Auswirkung der Auswahl des Codes auf den RD-Wert

Wie bei Fast-Ethernet werden nicht alle Symbole für die Übertragung von Daten genutzt. Bei Gigabit-Ethernet kommen neue Symbole oder Gruppen von bis zu 4 Symbolen. Damit lassen sich die folgende Signale setzen

- ➊ Idle
- ➋ Carrier Extend
- ➌ Start of Packet
- ➍ End of Packet

Nicht alle Bitkombinationen sind zulässig. Unzulässige empfangene Symbole werden als Violation erkannt und registriert. Ein erhöhtes Aufkommen von Violations deutet auf eine schlechte Verbindung hin.

14.4.1.5 - 1000Base – LWL-Varianten

Bei den LWL-Varianten gibt es keine Auto-Negotiation bezüglich der Geschwindigkeit. Diese ist immer fest eingestellt. Es wird also nur der Duplex-Mode und die Flow Control abgehandelt. Es werden keine Fast Link Pulse (FLP) verwendet, sondern spezielle Codeworte. Zum Einsatz kommen SC-Stecker.

14.4.1.5.1 - Bandbreiten-Längenprodukt

War bei der maximalen Leitungslänge unter 100 Mbps die Dämpfung ausschlaggebend, ist bei Gigabit-Ethernet die Dispersion gravierender. Bei der Dispersion ist die Länge eine elementare Größe. Je länger die Glasfaser ist, desto größer ist die Dispersion. Die Hersteller haben deshalb das Bandbreiten-Längen-Produkt eingeführt. Damit kann bei vorgegebener Datenrate (Bandbreite) die maximal erreichbare Distanz angegeben werden. Je nach verwendeter Glasfaser haben die MM-LWL ein Bandbreiten-Längen-Produkt von 160 bis 500 MHz * km. Damit können Reichweiten von 220 m bis 550 m erreicht werden.

14.4.1.5.2 - 1000Base-SX

Das „S“ von 1000Base-SX steht für Short Wavelength, was auf die verwendete Wellenlänge von 830nm hinweist. Damit lassen sich je nach verwendeter Gradienten Multimode-Faser Distanzen von 220 m (62,5 /125µm) und 550 m (50/125µm) erreichen. Durch die günstige Lösung ist diese Variante weit verbreitet.

14.4.1.5.3 - 1000Base-LX

Das „L“ von 1000Base-LX steht für Long Wavelength, was auf die verwendete Wellenlänge von 1270nm hinweist. Dabei kann sowohl eine Multimode-Faser als auch eine Single-Mode-Faser verwendet werden. Die damit erreichbaren Distanzen sind 550 m (MM-LWL) und 5000 m (SM-LWL).

14.4.1.5.4 - 1000Base-T

Da diese Variante technisch sehr anspruchsvoll ist, dauerte sie etwas länger in der Erstellung und wurde deshalb in einem späteren Standard (IEEE802.3ab) im Juni 1990 verabschiedet. Schließlich sollten einige altgewohnte Eigenschaften übernommen werden:

- 100 m Segmentlänge
- CSMA/CD als Medienzugriffsverfahren
- Abwärtskompatibilität (Es soll ein 10 Mbsp-Gerät angeschlossen werden können)
- Flusskontrolle

Dazu mussten einige Maßnahmen umgesetzt werden.

- Wegfall der 8B10B-Codierung zur Senkung der Bitrate von 1250 Mbps auf 1000 Mbps auf der Leitung
- Trellis-Codierung um mit zusätzlicher Redundanz Fehler zu beheben.
- Scrambling zur gleichmäßigen Verteilung der Signalzustände auf dem Übertragungsmedium
- Einsatz eines PAM-5-Leitungscodes (Leitungscode mit 5 Pegeln (-1V, -0,5V, 0V, 0,5V, 1V))
- Aufteilung der Daten auf 4 Adernpaare mit einer Übertragung in beide Richtungen
- Echo-Cancellation
- NEXT-Cancellation

Um in beiden Richtungen gleichzeitig Daten auszutauschen muss mit einer Hybridschaltung der Sende- und der Empfangsbaustein zusammengeführt werden. Damit ist es auch wichtig, dass alle 4 Adernpaare in den Leitungen und den Steckern vorhanden und verbunden sind.

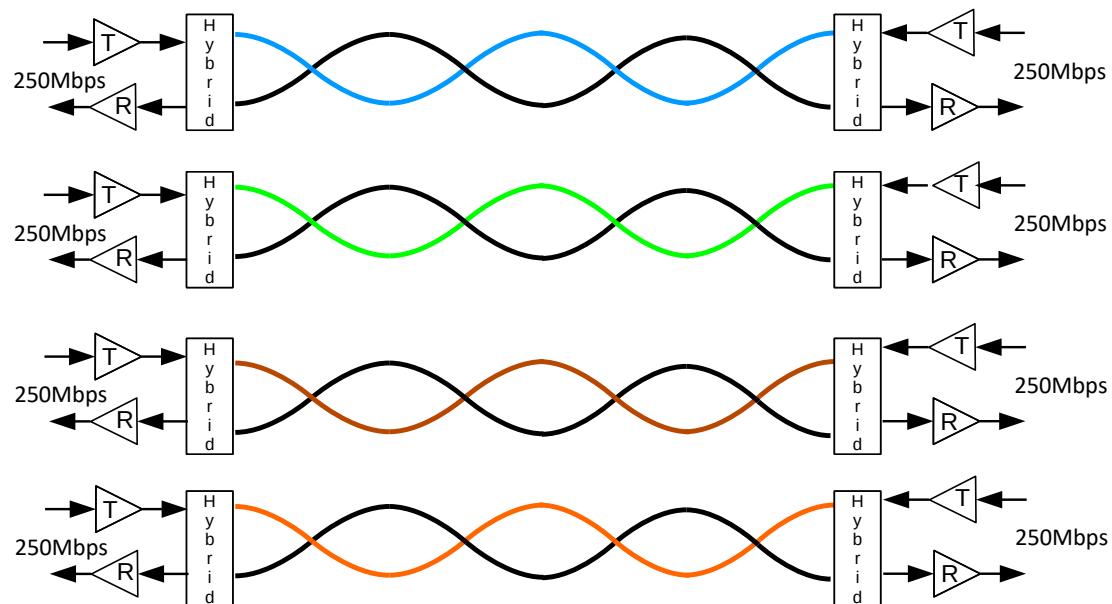


Abbildung 240: Nutzung von allen 4 Adernpaaren in beiden Richtungen bei Gigabit-Ethernet

Ethernet

Um in beiden Richtungen gleichzeitig senden und empfangen zu können, muss beim Empfänger das gesendete Signal vom empfangenen Signal abgezogen werden. Dieses Verfahren wird Echo-Cancellation genannt und z. B. auch bei Kopfhörern genutzt, um Umgebunggeräusche auszufiltern. Zusätzlich findet noch in digitalen Signalprozessoren (DSPs) eine NEXT- und eine FEXT-Cancellation statt.

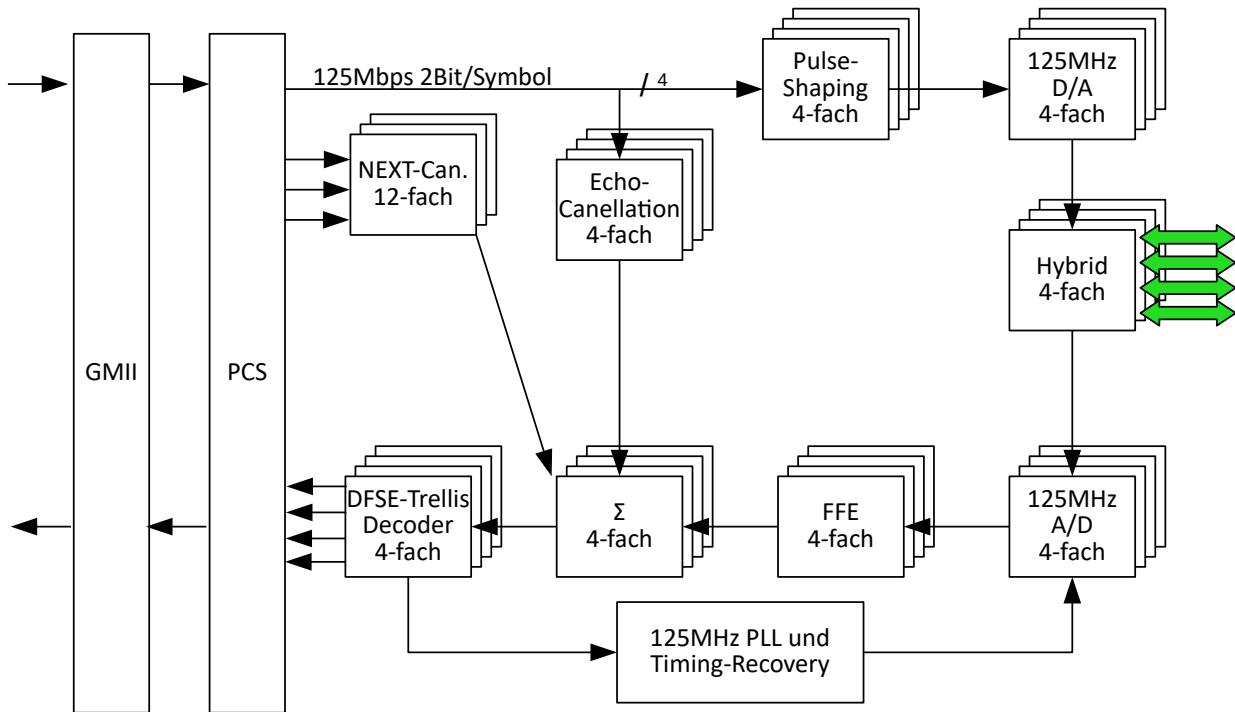


Abbildung 241: Bausteine der 1000Base-T-PHY

Die Kommunikationspartner handeln auch einen Master und einen Slave aus. Der Master bezieht seinen Takt von einem internen Taktgeber. Der Slave erzeugt aus dem empfangenen Signal den Takt. Siehe hierzu auch das Timing Recovery in Abbildung 241: Bausteine der 1000Base-T-PHY .

Im PCS wird durch einen Scrambler dafür gesorgt, dass die elektromagnetische Abstrahlung reduziert wird. Außerdem wird dabei sichergestellt, dass keine übereinstimmenden Symbole auf den 4 Adernpaaren auftreten. Zur Synchronisation der Scrambler für Senden und Empfang wird das Idle-Signal verwendet.

14.4.1.5.5 - 4D-PAM5-Leitungscodierung

Die 8 Bit, welche den Scrambler verlassen, werden auf die vier Adernpaare aufgeteilt. Damit sind pro Adernpaar 250 Mbps zu transportieren. Damit dies gelingt, wird ein Code verwendet, der die 2 Bits, die pro Adernpaar anfallen, mit einer 4D-PAM5-Codierung also 5-wertigen Symbolen übertragen. Es stehen $5^4 = 625$ mögliche Symbolkombinationen zur Verfügung. Für die Übertragung sind $2 * 2^8$ Bit = 512 Bit erforderlich, da die Daten redundant übertragen werden. Damit bleiben 113 Symbolkombinationen für Kontrollfunktionen und Fehlererkennung übrig.

Daten	Ungerade TA, TB, TC, TD	Gerade TA, TB, TC, TD
00000 001	0, 0, 0, +1	0, 0, 0, 0
00001 001	-2, 0, 0, +1	-2, 0, 0, 0
00010 001	0, -2, 0, +1	0, -2, 0, 0
00011 001	-2, -2, 0, +1	-2, -2, 0, 0
00100 001	0, 0, -2, +1	0, 0, -2, 0
00101 001	-2, 0, -2, +1	-2, 0, -2, 0

Tabelle 14: Ausschnitt aus der 4D-PAM5-Codierung

Die Daten werden, je nach vorhergehendem Signal, in ein gerades oder ungerades Symbol umgesetzt. In Tabelle 14: Ausschnitt aus der 4D-PAM5-Codierung sind die logischen Werte dargestellt. Auf der Leitung werden die Spannungspegel -1V, -0,5V, 0V, +0,5V, +1V verwendet. Dies bedeutet, dass der kleinste Spannungsunterschied 0,5V beträgt, was die Anforderungen an die Signalerkennung erheblich steigert.

Dies wird in der folgenden Abbildung deutlich, bei dem die Auswirkung der Leitungsdämpfung auf PAM5-Signale auf einem Leitungspaar dargestellt sind.

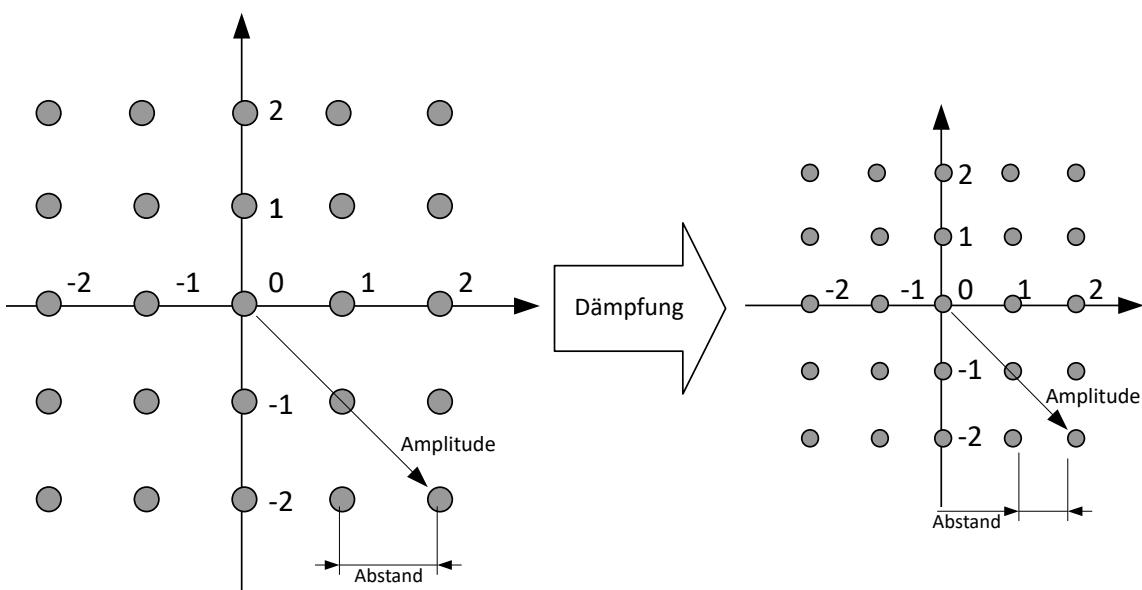


Abbildung 242: Beeinflussung des Signals durch die Leitungsdämpfung

Ethernet

Um der Dämpfung und somit der Verringerung des Abstandes entgegenzuwirken, wird wie in Tabelle 14: Ausschnitt aus der 4D-PAM5-Codierung zwischen geraden und ungeraden Symbolen unterschieden. Damit erhöht sich der Abstand.

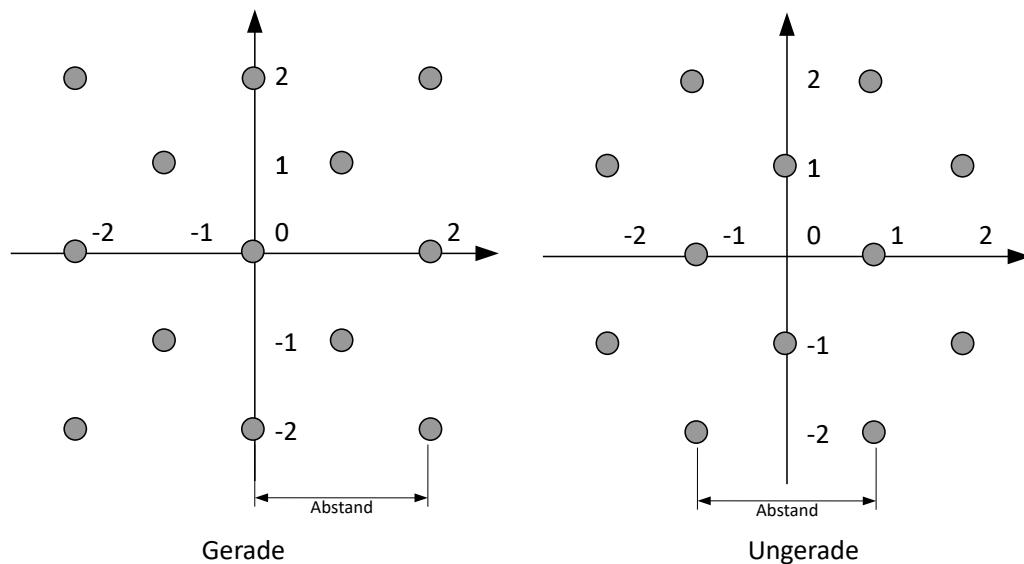


Abbildung 243: Erhöhung des Abstandes durch gerade und ungerade Symbole

Setzt man für die geraden Werte (-2, 0, +2) ein Y und für die ungeraden Werte (-1, und +1) ein X ergibt sich für die Werte aus Abbildung 243: Erhöhung des Abstandes durch gerade und ungerade Symbole die folgende Abbildung.

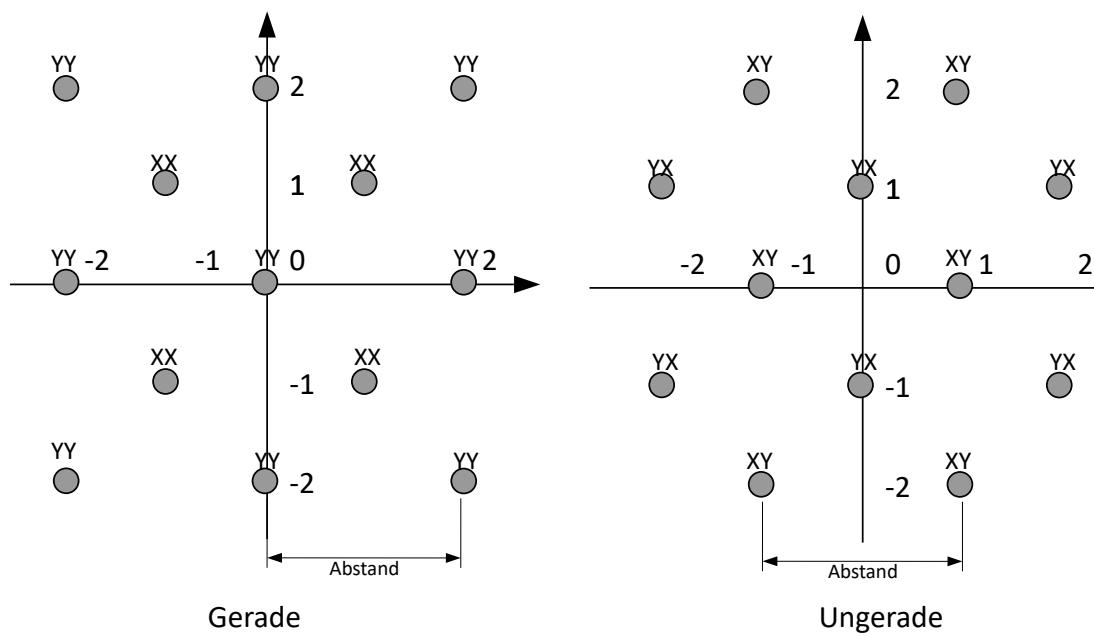


Abbildung 244: Zuordnung von Y auf gerade und X auf ungerade Symbole

Schaut man sich die geraden Symbole an, kann man feststellen, dass XX und YY invers sind.

Dreht man die Darstellung um 45° , kann man durch eine weitere Aufteilung, in normale und inverse Symbole den Abstand weiter aufteilen.

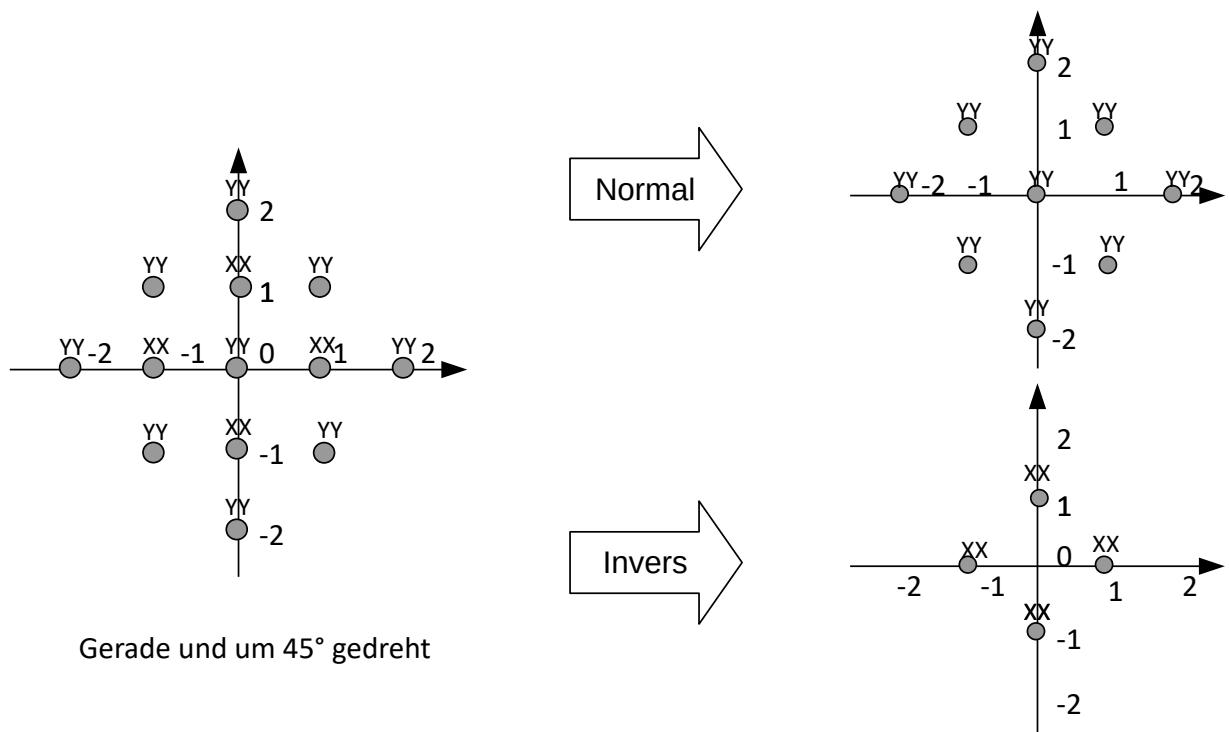


Abbildung 245: Um 45° gedreht und in normale und inverse Symbole unterteilt

Subset	Mögliche Werte
D0	XXXX oder YYYY
D1	XXXY oder YYYYX
D2	XXYY oder YYXX
D3	XXYX oder YYXY
D4	XYYX oder YXXX
D5	XYYY oder YXXX
D6	XYYX oder YXYX
D7	XYXX oder YXYY

Tabelle 15: Wertzuordnung zu den Subsets

Bei der 4D-PAM5-Codierung werden die Symbolkombinationen in 8 Subsets aufgeteilt. Es gibt 4 gerade Subsets (D0, D2, D4 und D6) und 4 ungerade Subsets (D1, D3, D5 und D7). Jedes Subset hat zwei Wertzuordnungen. Die jeweiligen Zuordnungen sind invers zueinander. X erlaubt Werte von -1 und 1. Y erlaubt Werte von -2, 0 und 2. In der ersten Zeile von Tabelle 15: Wertzuordnung zu den Subsets entstehen im ersten Fall (-1 oder 1) $2 \cdot 2 \cdot 2 \cdot 2 = 16$ Möglichkeiten. Im Zweiten Fall (-2, 0 oder 2) entstehen $3 \cdot 3 \cdot 3 \cdot 3 = 81$ Möglichkeiten.

Ethernet

Subset	TA,TB, TC, TD	Anzahl	TA,TB, TC, TD	Anzahl	Summe
D0	XXXX	16	YYYY	81	97
D1	XXXY	36	YYX	36	72
D2	XXYY	36	YYXX	36	72
D3	XXYX	36	YYXY	36	72
D4	XYYX	24	YXXX	54	78
D5	YYYY	24	YXXX	54	78
D6	XYXY	54	YXYX	24	78
D7	XYXX	54	YXYY	54	78

Tabelle 16: Anzahl der Symbolkombinationen in Abhängigkeit vom Subset

1000Base-T verwendet aus jedem Subset 64 Symbolkonstellationen. Die übrigen Symbolkonstellationen werden für Kontrollfunktionen verwendet.

Condition	Sdn[5:0]	Sdn[6:8] = [000]	Sdn[6:8] = [010]	Sdn[6:8] = [100]	Sdn[6:8] = [110]
Normal	000000	0, 0, 0, 0	0, 0, +1, +1	0, +1, +1, 0	0, +1, 0, +1
Normal	000001	-2, 0, 0, 0	-2, 0, +1, +1	-2, +1, +1, 0	-2, +1, 0, +1
Normal	000010	0, -2, 0, 0	0, -2, +1, +1	0, -1, +1, 0	0, -1, 0, +1
Normal	000011	-2, -2, 0, 0	-2, -2, +1, +1	-2, -1, +1, 0	-2, -1, 0, +1
Normal	000100	0, 0, -2, 0	0, 0, -1, +1	0, +1, -1, 0	0, +1, -2, +1
Normal	000101	-2, 0, -2, 0	-2, 0, -1, +1	0, +1, -1, 0	-2, +1, -2, +1
Normal	000110	0, -2, -2, 0	0, -2, -1, +1	0, -1, -1, 0	0, -1, -2, +1
Normal	000111	-2, -2, -2, 0	-2, -2, +1, +1	-2, -1, -1, 0	-2, -1, -2, +1
Normal	001000	0, 0, 0, -2	0, 0, +1, -1	0, +1, +1, -2	0, +1, 0, -1
Normal	001001	-2, 0, 0, -2	-2, 0, +1, -1	-2, +1, +1, -2	-2, +1, 0, -1
Normal	001010	0, -2, 0, -2	0, -2, +1, -1	0, -1, +1, -2	0, -1, 0, -1
Normal	001011	-2, -2, 0, -2	-2, -2, +1, -1	-2, -1, +1, -2	-2, -1, 0, -1
Normal	001100	0, 0, -2, -2	0, 0, -1, -1	0, +1, -1, -2	0, +1, -2, -1
Normal	001101	-2, 0, -2, -2	-2, 0, -1, -1	-2, +1, -1, -2	-2, +1, -2, -1
Normal	001110	0, -2, -2, -2	0, -2, -1, -1	0, -1, -1, -2	0, -1, -2, -1
Normal	001111	-2, -2, -2, -2	-2, -2, -1, -1	-2, -1, -1, -2	-2, -1, -2, -1

Tabelle 17: Ausschnitt aus der geraden Symboltabelle

Die Auswahl des Subsets erfolgt über die Trellis-Codierung. Für die Trellis-Codierung werden nach dem Scrambler die 8 Datenbits um ein neuntes Datenbit erweitert. Dazu werden die 8 Bits des aktuellen und der drei vorhergehenden Datenwertes miteinander verknüpft.

Ethernet

Das Trellis-Diagramm entspricht einem Codebaum mit Knotenpunkten bei dem jeweils zwei Verzweigung (0 und 1) abgehen, welche die Zustände der Codegruppen darstellen.

In der folgenden Abbildung entspricht 0 einer gestrichelten Linie (die hier oben verläuft) und eine 1 einer durchgezogenen Linie (die unten verläuft)

Damit ist sichergestellt dass z.B. bei einer 11-Gruppe nur eine 01 oder eine 10-Gruppe folgen kann. Somit ergibt die Eingangs-Datenfolge 00111 die Ausgangsdatenfolge 00,00,11,01,10

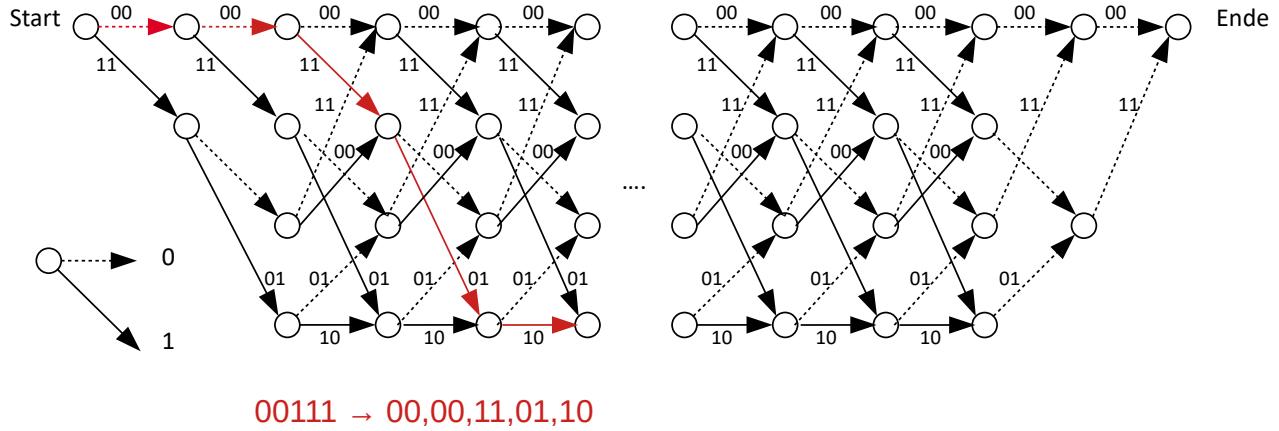


Abbildung 246: Trellis-Diagramm

Nach diesem Schema wird bei 1000Bast-T das Subset ausgewählt.

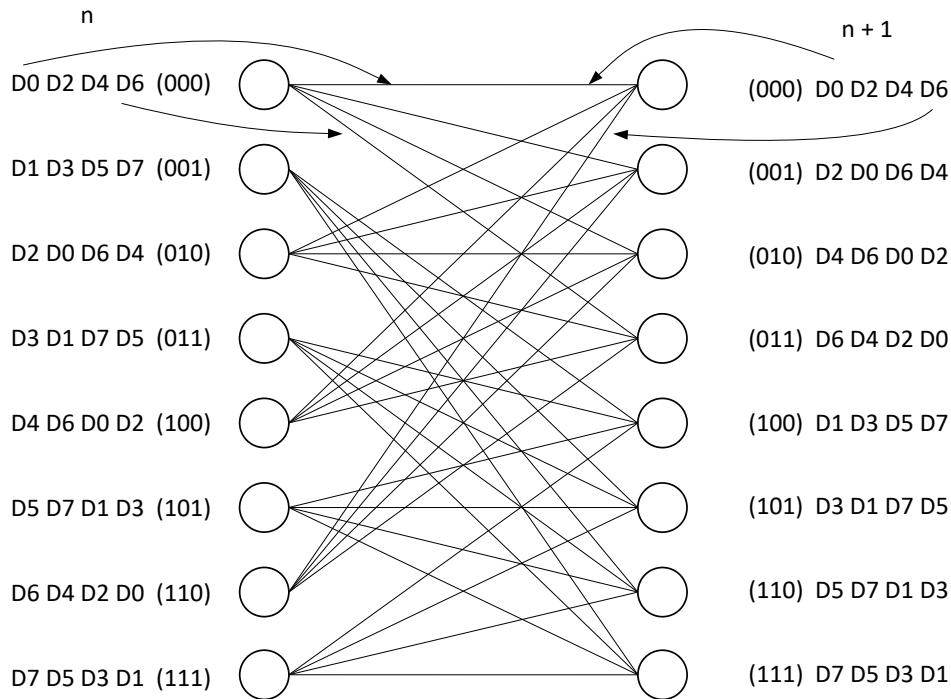
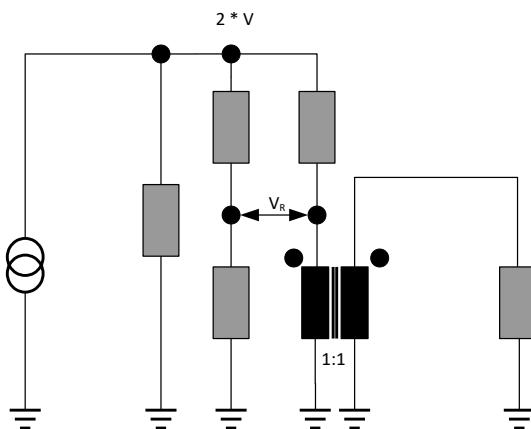


Abbildung 247: Trellis-Diagramm von 1000Base-T

Das Gegenstück zur Trellis-Codierung ist auf der Empfängerseite der Viterbi-Algorithmus. Dabei wird nicht nach einem Regelwerk vorgegangen sondern die am wahrscheinlichsten übertragene Datenfolge ermittelt. Zusätzlich kann durch die Trellis-Codierung ein eventuell aufgetretener Fehler korrigiert werden. Werden z. B. hintereinander zwei gerade Symbole empfangen, fallen die Symbolzweige zusammen und es wird der Zweig mit dem geringsten Abstand vom empfangenen Symbol gewählt.

14.4.1.5.6 - Hybridfunktion



Die Hybridschaltung ermöglicht es, dass gleichzeitig gesendet und empfangen werden kann.

Das ist auf allen 4 Adernpaaren möglich. Bei Brückenschaltungen lässt sich ein Restecho nicht vermeiden. Deshalb ist noch eine zusätzliche Echo-Cancellation erforderlich.

Abbildung 248: Brückenschaltung mit Hybridfunktion für ein Adernpaar

14.4.1.5.7 - Echo Cancellation

Die Beseitigung des Echoes wird in den DSPs realisiert. Dabei wird das eigene gesendete Signal zugrunde gelegt und vom empfangenen Signal abgezogen.

Es muss auch sichergestellt sein, dass die Signallaufzeiten der Adernpaare keine allzu großen Unterschiede aufweisen. Maximal 50 ns sind zulässig. Deshalb ist die Pair-Skew-Messung bei den Leistungsmessungen wichtig. Innerhalb der 50 ns gleichen die DSPs mit der Pair-Skew-Correction-Function die Unterschiede aus.

14.4.1.5.8 - Crosstalk-Minimierung

Das Nebensprechen (Crosstalk (NEXT /FEXT)) wird beim Senden von einem Adernpaar auf die anderen 3 Paare übertragen. Deshalb ist es für die Übertragung von Gigabit-Ethernet auf der Leitung wichtig, dass das Nebensprechen so gering wie möglich ist. NEXT, FEXT, PSNEXT und PSFEXT sind wichtige Gütemerkmale für Leitungen die Gigabit-Ethernet übertragen sollen. Im DSP wird deshalb auch eine FEXT-Cancellation realisiert. Da jedes Adernpaar 3 Nachbarpaare hat, ist die FEXT-Cancellation 12 Mal vorhanden.

14.4.1.5.9 - Startup einer 1000Bast-T-Schnittstelle

Nach dem zurücksetzen der 1000Base-T-Schnittstelle und dem Empfang des Fast Link Pulses (FLP) führt sie die folgenden Schritte durch:

1. Automatische MDI/MDIX-Einstellung
2. Auto Negotiation
3. Festlegung der Datenübertragungsrate (10, 100 oder 1000 Mbps)
4. Festlegung der Master/Slave-Rolle
5. Einstellung der DSP-Filter

14.4.1.5.9.1 - MDI/MDIX -Erkennung und Einstellung

Ob eine 1:1- oder Crossover-Wiremap für die Verbindung verwendet wird, kann optional ermittelt werden. Die Informationen der FLPs werden zuerst auf dem BI_DA Pfad gesendet und auf dem Pfad BI_DB empfangen. Damit ist die Schnittstelle auf MDI eingestellt.

Sollte keine Information ankommen, wird auf den Pfad BI-DB als Sender umgeschaltet und BI-DA auf Empfang eingestellt. Damit ist die MDIX-Einstellung vorgenommen.

Pin	PHY	MDI	MDIX
1	BI_DA+ (TP0+)	BI_DA+	BI_DB+
2	BI_DA- (TP0-)	BI_DA-	BI_DB-
3	BI_DB+ (TP1+)	BI_DB+	BI_DA+
4	BI_DC+ (TP2+)	BI_DC+	BI_DD+
5	BI_DC- (TP2-)	BI_DC-	BI_DD+
6	BI_DB- (TP1-)	BI_DB-	BI_DA-
7	BI_DD+ (TP3+)	BI_DD+	BI_DC+
8	BI_DD- (TP3-)	BI_DD-	BI_DC-

Tabelle 18: Zuordnung der Signale bei MDI- / MDIX-Belegung

14.4.1.5.9.2 - Auto-Negotiation

Die Auto-Negotiation-Funktion ist für die Aushandlung der Datenübertragungsrate Flow-Control und Master-Slave-Rolle zuständig.

Zuerst wird versucht die Aushandlung nach IEEE802.3ab (also 1000Base-T) durchzuführen

Schlägt das fehl wird versuche nach Fast-Ethernet auszuhandeln (also 100Base-Tx)

Sollte auch das nicht funktionieren, wird mit der Parallel-Detection-Function 10 Mbps oder 100 Mbps und der Halbduplex-Modus eingestellt.

Die Auto-Negotiation-Funktion für 1000Base-T tauscht eine Base-Page eine Message Next Page und zwei unformatted Next Pages aus. Nur die Flow Control wird über die Base Page festgelegt. Weitere relevante Information werden in den zwei unformatted Next Pages übertragen.

Die erste unfomatted Page enthält Informationen, ob es sich um eine Einport-Komponente oder Multiportkomponente handelt sowie eventuelle manuelle Einstellungen und Informationen zur Master/Slave-Rolle.

Bit	Bedeutung
U4	1000Base-T Halbduplex
U5	1000Base-T Vollduplex
U2	1000Base-T Multiport-Komponente
U1	1000Base-T Master Slave manuelle Konfiguration
U0	1000Base-T manuelle Master-Slave sol verwendet werden

Tabelle 19: Inhalt der ersten unformatierten Next Page

Bit	Bedeutung
U10	1000 Base-T Master-Slave Seed Bit 10 (MSB)
U9	1000 Base-T Master-Slave Seed Bit 9
U8	1000 Base-T Master-Slave Seed Bit 8
U7	1000 Base-T Master-Slave Seed Bit 7
U6	1000 Base-T Master-Slave Seed Bit 6
U5	1000 Base-T Master-Slave Seed Bit 5
U4	1000 Base-T Master-Slave Seed Bit 4
U3	1000 Base-T Master-Slave Seed Bit 3
U2	1000 Base-T Master-Slave Seed Bit 2
U1	1000 Base-T Master-Slave Seed Bit 1
U0	1000 Base-T Master-Slave Seed Bit 0 (LSB)

Tabelle 20: Inhalt der zweiten unformatiertne Next Page

Ethernet

Die Aushandlung der Master-/Slave-Rolle geht nach folgenden Regeln:

1. Eine Multiport-Komponente hat für die Master-Rolle eine höhere Priorität als eine Einzelport-Komponente
2. Sind die Komponententypen gleich, entscheidet die höhere Seed
3. Die Komponente mit der höheren Seed erlangen die Master-Rolle
4. Die Komponente mit der niedrigeren Seed erlangen die Slave-Rolle
5. Sind beide Seeds gleich wird durch ein Link_Status_1GigT-Fehler eine erneute Aushandlung angestoßen
6. Schlagen 7 Versuche fehl das als Master-Slave-Fehler

Lokale Komponente	Entfernte Komponente	Lokal	Entfernt
Einzelport-Komponente	Multiport-Komponente	Slave	Master
Einzelport-Komponente	Manuell Master	Slave	Master
Manuell Slave	Manuell Master	Slave	Master
Manuell Slave	Manuell Master	Slave	Master
Multiport-Komponente	Manuell Master	Slave	Master
Manuell Slave	Einzelport-Komponente	Slave	Master
Multiport-Komponente	Einzelport-Komponente	Master	Slave
Multiport-Komponente	Manuell Slave	Master	Slave
Manuell Master	Manuell Slave	Master	Slave
Manuell Master	Einzelport-Komponente	Master	Slave
Einzelport-Komponente	Manuell Slave	Master	Slave
Manuell Master	Multiport-Komponente	Master	Slave
Multiport-Komponente	Multiport-Komponente	Seed	Seed
Einzelport-Komponente	Einzelport-Komponente	Seed	Seed
Manuell Slave	Manuell Slave	Fehler	Fehler
Manuell Master	Manuell Master	Fehler	Fehler

Tabelle 21: Zuordnung von Master und Slave

14.5 - 10Gbps-Ethernet

Wie bereits bei Gigabit-Ethernet gab es zuerst eine LWL-basierte Variante die im Juni 2002 als IEEE802.3ae veröffentlicht wurde. Es handelt sich dabei nicht mehr um eine reine LAN-Lösung sondern es wurde der WAN-Bereich mit einbezogen. Im Juni 2006 wurde mit IEEE802.3an die Twisted-Pair-Lösung nachgeschoben und im März 2007 kam mit IEEE802.3ap noch eine Backplane-Lösung hinzu.

Zusätzlich hat man sich von Altlasten befreit. Da keine Repeater (Hubs) mehr vorgesehen waren, konnte der Halb-Duplex-Modus mit dem erforderlichen Medien-Zugriffsverfahren CSMA/CD entfallen.

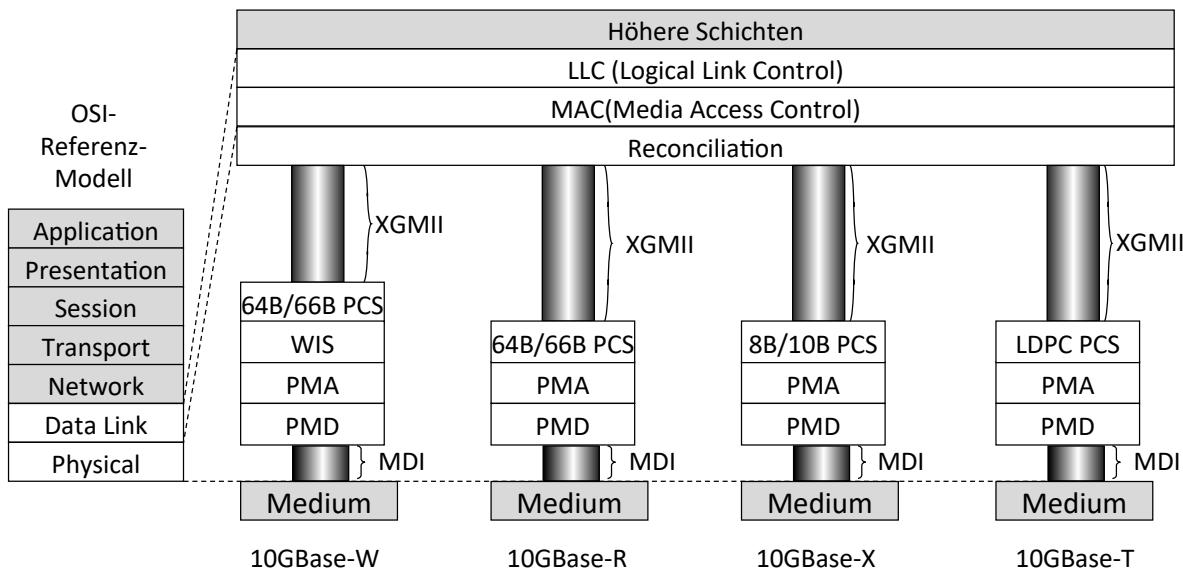


Abbildung 249: Sublayer bei 10 Gigabit-Ethernet

Die GMII wurde durch die XGMII ersetzt. Das römische X steht für 10. Für die XGMII-Schnittstelle wurde der Funktionsumfang und die Datenbreite erweitert.

Es gibt für die 10GBase-Lösungen 4 Ausprägungen:

- ➊ Die WAN-Schnittstelle unter 10GBase-W
- ➋ Die LAN LWL-Schnittstelle unter 10GBase-X
- ➌ Die serielle Schnittstelle unter 10GBase-R
- ➍ Die Kupferbasierte TP-Lösung unter 10Gbase-T

Auffällig ist, dass es für fast jede Variante eine eigenes PCS-Verfahren gibt. Die Umsetzung der 32 Bit breiten Daten der XGMII in Codegruppen erfolgt angepasst an die physikalischen Medium-Eigenschaften des PMD.

Die PMA wandelt die Codegruppen auf der Sendeseite in serielle Daten um und auf der Empfängerseite wieder zurück. Außerdem ist die PMA bei den Slaves für Taktrückgewinnung zuständig.

Die PMDs sind bei LWL in Duplex-SC-, oder Duplex-LC-Stecker ausgeführt.

Alle drei optischen Fenster bei Glasfasern werden genutzt. Es gibt für jede Wellenlänge eine Variante, die für das WAN-Umfeld genutzt werden kann und eine, die nicht für ein WAN genutzt werden kann.

- „S“ (short) Für kurze Wellenlängen (850 nm)
- „L“ (Long) Für lange Wellenlängen (1310 nm)
- „E“ Extra long) Für extra lange Wellenlängen (1550 nm)

Die Unterschiede liegen vor allem im Transceiver-Preis. Die Dämpfung spielt bei den Glasfasern keine Rolle mehr. Vielmehr ist die Dispersion die begrenzende Größe bei die erzielbaren Distanz.

Bezeichnung	Beschreibung der PHY-Typs
10GBase-SR	Serielle 850 nm-Variante ohne WAN-Anpassung
10GBase-SW	Serielle 850 nm-Variante mit WAN-Anpassung
10GBase-LR	Serielle 1310 nm-Variante ohne WAN-Anpassung
10GBase-LW	Serielle 1310 nm-Variante mit WAN-Anpassung
10GBase-ER	Serielle 1550 nm-Variante ohne WAN-Anpassung
10GBase-EW	Serielle 1550 nm-Variante mit WAN-Anpassung
10GBase-LX4	1310 nm WWDM-Variante für den LAN-Betrieb

Tabelle 22: LWL-Varianten bei 10Gigabit -Ethernet

14.5.1.1 - 10GBase-R

Bei den 10GBase-Varianten ohne WAN-Anbindung durchlaufen die Daten nach dem Scrambler eine 64B/66B-Codierung. Dabei werden 64Bit zu einer Codegruppe zusammengefasst und mit 2 Byte großen Präambel ergänzt. Die erzeugten Codes ermöglichen eine zuverlässige Fehlererkennung und werden in Daten- und Kontroll-Blöcke unterschieden. Die Datenblöcke sind 8 Bytes groß, während die Kontrollblöcke 7 Bytes groß sind. Die Unterscheidung erfolgt über die 2 Bit des SYNC-Feldes. Das SYNC-Feld ist bei den Datenblöcken auf 01 gesetzt. Bei den Kontrollblöcken ist es auf 10 gesetzt. Inhalte des SYNC-Feldes von 00 oder 11 sind ungültig.

14.5.1.1.1 - 10GBase-SR

Diese Variante entspricht den bisher bekannten Glasfaserlösungen. Die Daten werden im ersten Fenster bei 850nm übertragen. Je nach verwendetem Transceiver sind unterschiedliche Distanzen möglich, die sich allerdings auch im Preis niederschlagen.

Mit den herkömmlichen Multimode-Fasern (62,5/125 µm oder 50/125 µm) kann beim kostengünstigen 10GBase-SR 82m überbrückt werden. Dabei werden Vertical Cavity Surface Emitting Laser (VCSEL) eingesetzt. Verwendet man die modernen New Fiber Cable (Hochreine Gradientenfasern mit einem Bandbreiten-Längenprodukt von 2000 Mhz*km) können bis zu 300 m überbrückt werden.

Glasfasertyp	Bandbreiten-Längen-Produkt	Erzielbare Distanz
MMF 62,5/125µm	160 MHz * km	2 m – 26 m
MMF 62,5/125µm	200 MHz * km	2 m – 33 m
MMF 50/125µm	400 MHz * km	2 m – 66 m
MMF 50/125µm	500 MHz * km	2 m – 82 m
MMF 50/125µm	2000 MHz * km	2 m – 300 m
SMF 9/125µm	-	2 m – 10.000 m

Tabelle 23: Erzielbare Distanzen bei 10GBase-SR

14.5.1.1.2 - 10GBase-LR

Diese Variante arbeitet im zweiten Fenster bei 1310 nm. Dabei kommen sogenannte Farby-Perot-Laser zum Einsatz. Mit Singlemode-Fasern (9/125 µm) können Daten von 2 m bis zu 10.000 m weit übertragen werden.

10GBase-ER

Die teuerste Lösung arbeitet im dritten Fenster (1550 nm) mit einem Distributed Feedback Laser (DFB-Laser) und Singlemode-Fasern (9/125 µm). Damit lassen sich Distanzen von 2 m bis zu 40.000 m überbrücken.

14.5.1.2 - 10GBase-LX4

Mithilfe des Bandbreiten-Längen-Produkts kann ermittelt werden welche Distanzen überbrückt werden können. Um akzeptable Distanzen überbrücken zu können wurde 10GBase-LX4 entwickelt. Dabei wird, wie bei der TP-Variante, die Information auf 4 Kanäle verteilt um die Bandbreite zu reduzieren. Damit können vorhandene Multimode-Fasern verwendet werden.

Glasfaser	Bandbreiten-Längen-Produkt	Erzielbare Distanz
MMF 62,5/125 µm	500 Mhz * km	2 bis 300 m
MMF 50/125µm	400 MHz * km	2 bis 240 m
MMF 50/125 µm	500 MHz * km	2 bis 300 m
SMF 9/125µm	-	2 bis 10.000 m

Tabelle 24: Distanzen bei 10GBase-LX4

Die 4 Kanäle werden mit unterschiedlichen Wellenlängen auf einer Faser mittels des Wide-Wavelength-Division-Multiplexing-Verfahrens (WWDM) durchgeführt. Bekannt war das Verfahren bereits aus dem WAN-Bereich. Wie in Abbildung 250: WWDM-Verfahren bei 10GBase-LX4 gezeigt, werden die 4 Kanäle (L0, L1, L2 und L3) beim Senden auf unterschiedliche Wellenlängen verteilt und beim Empfänger wieder zusammengeführt.

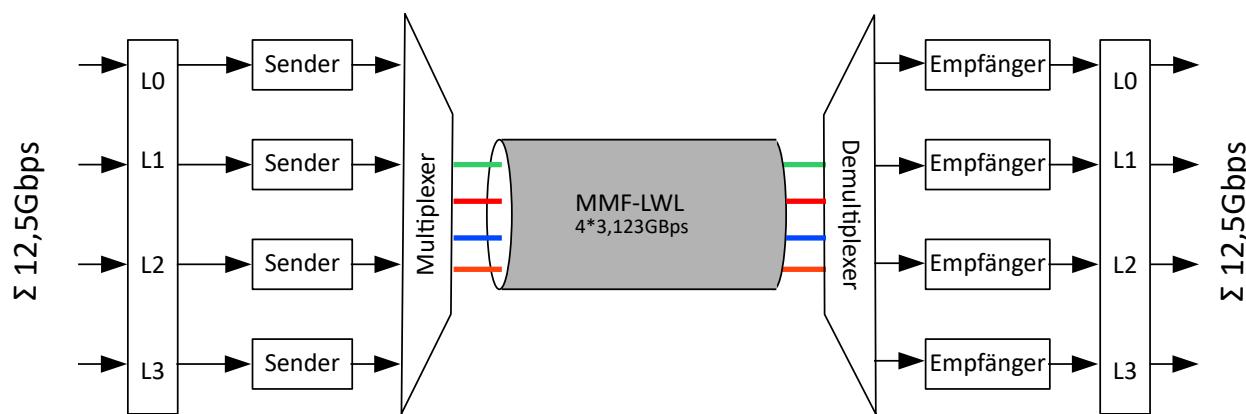


Abbildung 250: WWDM-Verfahren bei 10GBase-LX4

In der folgenden Tabelle ist die Aufteilung der Kanäle auf die verwendeten Wellenlängen aufgezeigt.

Kanal	Wellenlängenbereich
L0	1269,0 nm – 1282,4 nm
L1	1293,5 nm – 1306,9 nm
L2	1318,0 nm – 1331,4 nm
L3	1342,5 nm – 1355,9 nm

Tabelle 25: Aufteilung der Kanäle auf Wellenlängen

Wie in Abbildung Abbildung 249: Sublayer bei 10 Gigabit-Ethernet gezeigt wird bei der 10GBase-X-Variante zuerst eine 8B/10B-Codierung vorgenommen. Damit der so entstandene Overhead wieder ausgeglichen wird, werden pro Kanal die Daten mit 3,125Gbps übertragen. Über die 4 Kanäle hinweg summiert, entstehen so 12,5Gbps. (Multipliziert man die 12,5Gbps mit 8/10 ergibt sich wieder 10Gbps.

14.5.1.3 - 10GBase-W

Ethernet wurde erstmals mit 10Gigabit-Ethernet auch im WAN-Bereich eingeführt. Während früher die Plesiochrone Digitale Hierarchie (PDH) verbreitet war ist heutzutage die Synchronous-Digital-Hierarchy-System / Synchronous-Optical-Network-Technology (SDH/SONET) weit verbreitet anzutreffen. SDH und SONET sind in etwa kompatibel. SONET wird überwiegend in Nordamerika eingesetzt. SDH bietet gegenüber PDH die Möglichkeit höhere Datenübertragungsraten zu übertragen und andere Dienste leichter zu integrieren. Dies wird durch eine einheitliche Rahmenstruktur ermöglicht.

Mit dem WAN Interface Sublayer (WIS) erfolgt die Anpassung von Ethernet an SDH/SONET. Dabei muss die Datenrate von 10Gbps an die bei SDH/SONET verwendete Datenrate von 9,95328 Gbps (Payload-Datenrate von 9,58464) angepasst werden. Die Anpassung erfolgt mittels der so genannten Stretch-Funktion, bei der 104 zusätzliche IDLE-Symbole eingefügt werden. Dadurch wird der Frame-Abstand von 96 Bit auf 200Bit vergrößert. Auf der Senderseite werden bei der 64B/66B-Codierung die IDLE-Symbole entfernt und in das SDH/SONET-Übertragungsformat gepackt. Auf der Empfängerseite werden die IDLE-Symbole wieder eingefügt.

Die Rahmen werden bei SDH Synchronous Transport Module (STM) genannt. Ein STM entspricht einer Byteweisen Strukturierung in Spalten und Zeilen. Die STM-1-Grundstruktur wird in 270 Spalten und 9 Zeilen aufgeteilt. Die Übertragung selbst erfolgt zeilenweise (Beginnen wird links oben und abgeschlossen rechts unten).

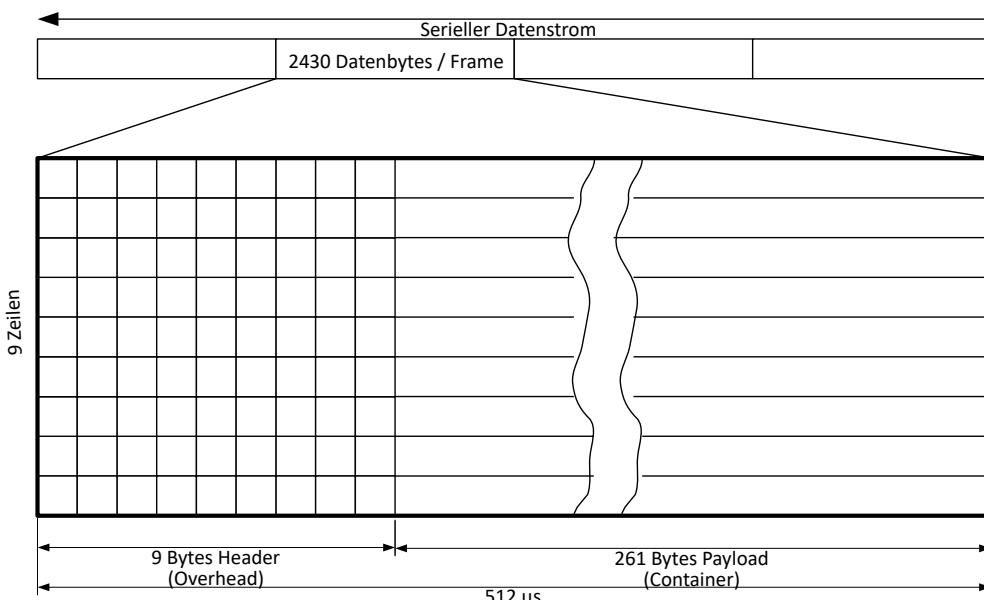


Abbildung 251: STH-Rahmen mit STM-1-Struktur

Die Overhead-Bytes werden bei der Übertragung zur Steuerung, Kontrolle und Synchronisation genutzt. Die Overhead-Bytes werden in Regenerator Section Overhead (RSOH), Multiplex Section Overhead (MSOH) und AU-Pointer unterschieden.

Die RSOH werden von den Regeneratoren genutzt, die wie Repeater arbeiten und ein abgeschwächtes Signal wieder aufhübschen.

Die MSOH dienen dazu unterschiedliche Dienste in den STH-Rahmen zu integrieren. Die AU-Pointer dienen dazu die Position der Nutzdaten unterschiedlicher Dienste im SDH-Rahmen mit Stopf-Bytes (Füll-Bytes) festzulegen.

Bei 10 Gigabit-Ethernet wird die STM-64/STS-192-Ramenstruktur angewendet. Damit kommt man auf eine Datenrate von 9953,29Mbps (siehe Tabelle 26: Gegenüberstellung der SDH/SONET-Rahmenstrukturen)

SDH	SONET	Faktor	Datenrate
-	STS-1	1/3	51,84 Mbps
STM-1	STS-3	1	155,52 Mbps
STM-3	STS-9	3	466,56 Mbps
STM-4	STS-12	4	622,08 Mbps
STM-6	STS-18	6	933,12 Mbps
STM-8	STS-24	8	1244,16 Mbps
STM-16	STS-48	16	2488,37 Mbps
STM-64	STS-192	64	9953,28 Mbps

Tabelle 26: Gegenüberstellung der SDH/SONET-Rahmenstrukturen

14.5.1.3.1 - STM-64/STS-192-Rahmen

Verglichen mit einem STS-1-Rahmen ist der Header bei diesem Rahmen 64-mal so groß. Damit hat er eine Länge von 576 Bytes und der Payload-Bereich hat eine Länge von 16.704 Bytes.

Jede Zeile beginnt mit einem 1 Byte langen Path Overhead (POH), einem 63 Byte langen Bereich mit festem Inhalt gefolgt von einem Bereich mit einer Länge von 16.640 Bytes in dem die Container der Nutzdaten abgelegt werden. In den Containern werden die eigentlichen Ethernet-Daten von der Präambel bis zum CRC-Feld übernommen. Mit der POH-Erweiterung werden die Container zu virtuellen Containern (VC). 10Gigabit-Ethernet verwendet, die so genannten VC-4-64 Container.

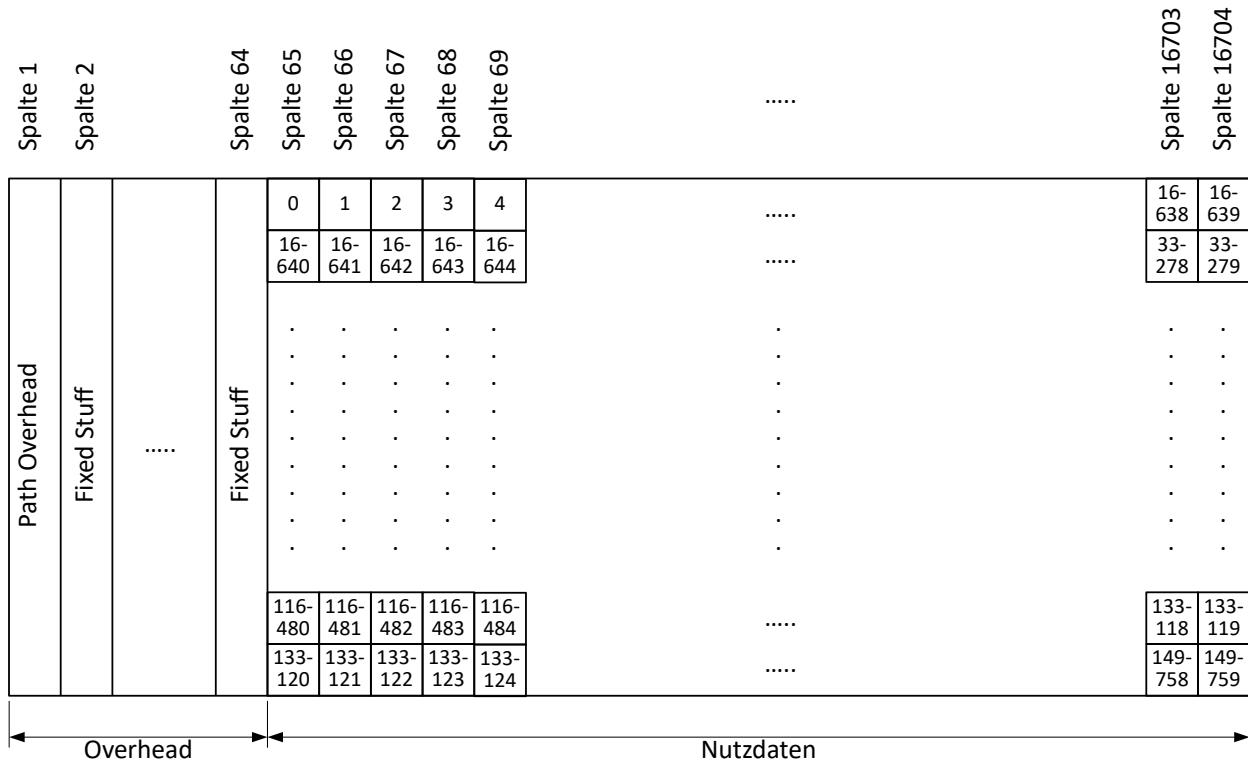


Abbildung 252: 10Gigabit-Ethernet Payload Envelope mit Path Overhead innerhalb eines STM

Ethernet

Im WAN-Bereich findet die 10GBase-LW-Lösung mit Monomodefasern (9/125µm) einen Einsatz bis 10 km. Für große Distanzen wird 10GBase-EW angewendet. Hier kommt man mit Monomode-Fasern (9/125µm) bis zu 40 km weit.

10GBase-CX-4

Im Februar 2004 wurde eine erste Kupferlösung als 10Gbase-CX-4 standardisiert. Dabei werden die Daten auf 4 Adernpaaren gesendet und auf weiteren 4 Adernpaaren empfangen. Damit müssen pro Adernpaar nur 2,5Gbps übertragen werden. Es wird die 8B/10B-Codierung verwendet. Als Stecker dient der 4X-Connector mit 16 Signal-Pins wie er bereits von InfiniBand her bekannt ist.



Abbildung 253: 4X-Buchsen (wie sie auch bei InfiniBand verwendet werden) (Quelle: Wikipedia)



Abbildung 254: 4X-Stecker (Quelle: DELL)

Der

Wermutstropfen bei dieser Lösung ist, dass nur eine maximale Distanz von 15 m überbrückt werden kann. Das ist in einem Serverraum evtl. noch tragbar. Für eine Lösung in der Fläche ist das allerdings nicht vorstellbar.

14.5.1.4 - 10GBase-T

So schön die Glasfaserlösungen bei 10Gigabit auch sind, so haben sie doch den Nachteil, dass sie teuer sind. Außerdem ist die Tertiär-Verkabelung in der Fläche meist nur in Kupfer realisiert. Wie bei den vorangegangenen Standards wurde von IEEE im November 2002 die Arbeitsgruppe 802.3an beauftragt eine Kupferlösung zu entwickeln. Im Juni 2006 wurde dann die der Standard verabschiedet. Vorgaben waren 100 m Distanz mit 4 Steckverbindungen. (90 m Installationsleitung und zwei 5 m Patchleitungen)

Als Leitungscode wurde PAM16, also eine Puls Amplituden Modulation mit 16 Signalniveaus, festgelegt. Das bedeutet bei dem Spannungsbereich vom 1 V bis +1V einen Abstand von 130 mV. Damit sind Störeinflüsse bei der Signalübertragung wesentlich gravierender als bei den älteren Standards.

Kandidaten für Störeinflüsse sind NEXT, FEXT, Reflexionen usw. Diese Störungen können durch Filterfunktionen herausgefiltert werden, da bekannt ist was gesendet wird und somit auf solche Störungen reagiert werden kann. Allerdings gibt es noch Störungen, die nicht gefiltert werden können, da sie von außen auf das Übertragungssystem einwirken. Hierzu gehört z. B. Alien Crosstalk (AXTALK). Durch die geringen Signalabstände bei 10GBase-T sind diese Einflüsse erstmals gravierend. Dies ist der Grund für die Verwendung von Fehler korrigierenden Codes. Je besser die Fehler korrigierenden Codes sind, desto weniger Redundanz muss bei der Datenübertragung mitgegeben werden. 10GBaseT verwendet gleich mehrere Codierungsverfahren.

14.5.1.4.1 - 10GBase-PHY

Wie in Abbildung 249: Sublayer bei 10 Gigabit-Ethernet dargestellt, sind die einzelnen Sublayer neu erstellt worden.

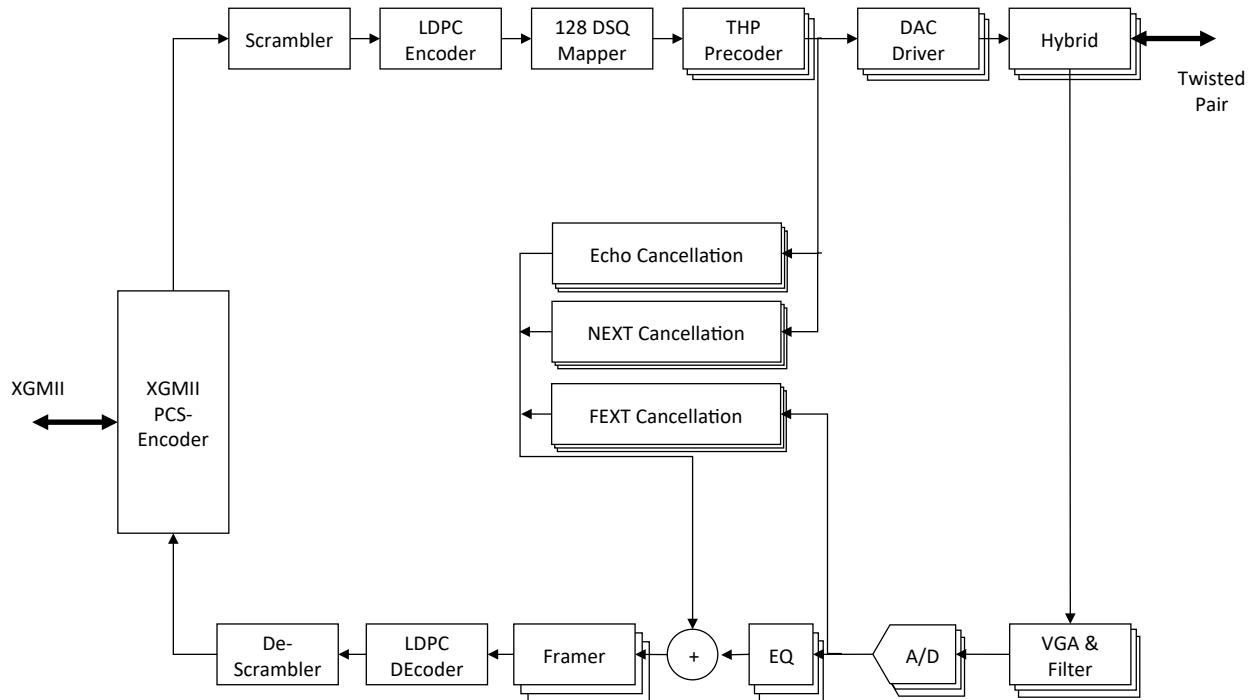


Abbildung 255: DSP-Funktionen bei 10GBase-T

Zentrales Bauteil ist dabei ein Digitaler Signal Processor (DSP) der die Funktionen und Codierungen durchführt. Der PCS übernimmt mit zwei Datentransfers 8 Datenbytes über die 32-Bit XGMII-Schnittstelle. Die 64 Bit werden mit einem vorangestellten Kontrollbit zu einem 65 Bit langen Codewort erweitert. Die 65-Bit-Blöcke werden dem Scrambler zugeführt der dafür sorgt, dass auf den vier Adernpaaren nicht die gleichen Symbole auftreten und zwischen den eingehenden und ausgehenden Datenströmen keine Übereinstimmung besteht. Das Scrambling sorgt auch dafür, dass die Signalenergie gleichmäßig über das Frequenzspektrum verteilt wird und so Signalspitzen vermieden werden.

DSQ-128 kann als zweidimensionale Konstellation betrachtet werden, deren mögliche Signalraumpunkte über zwei aufeinander folgende PAM16-Symbole gebildet werden, die gegeneinander versetzt sind. Zwei PAM16-Signale beinhalten 256 ($16 * 16$) Signalraumpunkte. Von denen ist aber nur die Hälfte zulässig. Damit ist DSQ-128 einem Subset von PAM16 mit den über zwei DSQ-128 Dimensionen (2D-DSQ-128) die Informationen von 2^7 Bits darstellen lassen.

Jedes 2D-DSQ-128-Symbol enthält also zwei PAM16-Komponenten (PAM16_A und PAM16_B).

Der DSQ-128-Signalraum kann erstellt werden indem die Hälfte (also die andere PAM-16-Konstellation) entfällt. Bildlich kann man sich das vorstellen wie ein Schachbrett, bei dem eine Farbe gestrichen wurde.

Durch das Weglassen der Hälfte der Signalraumpunkte erhöht sich der Abstand der verbleibenden Signalraumpunkte.

PAM16A und PAM16B können jeden Wert aus dem Wertebereich $\{-15, -13, -11, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, 11, 13, 15\}$ annehmen.

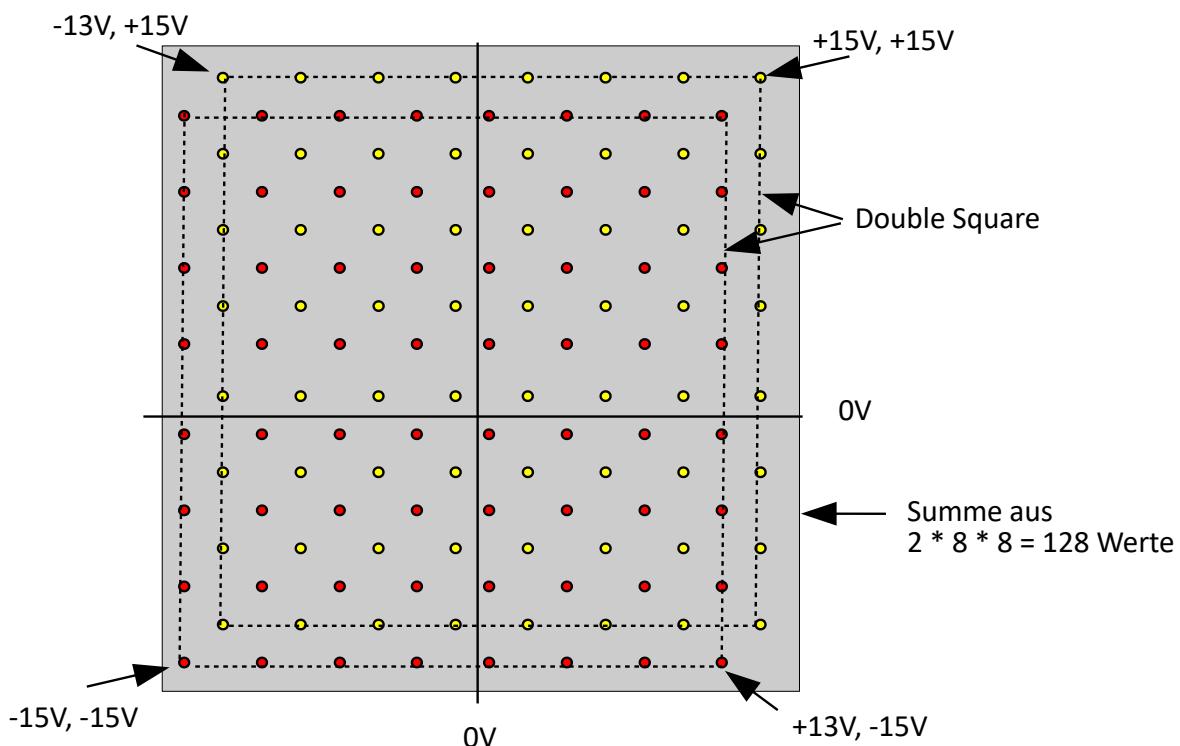


Abbildung 256: 2D-DSQ-128 Symbole

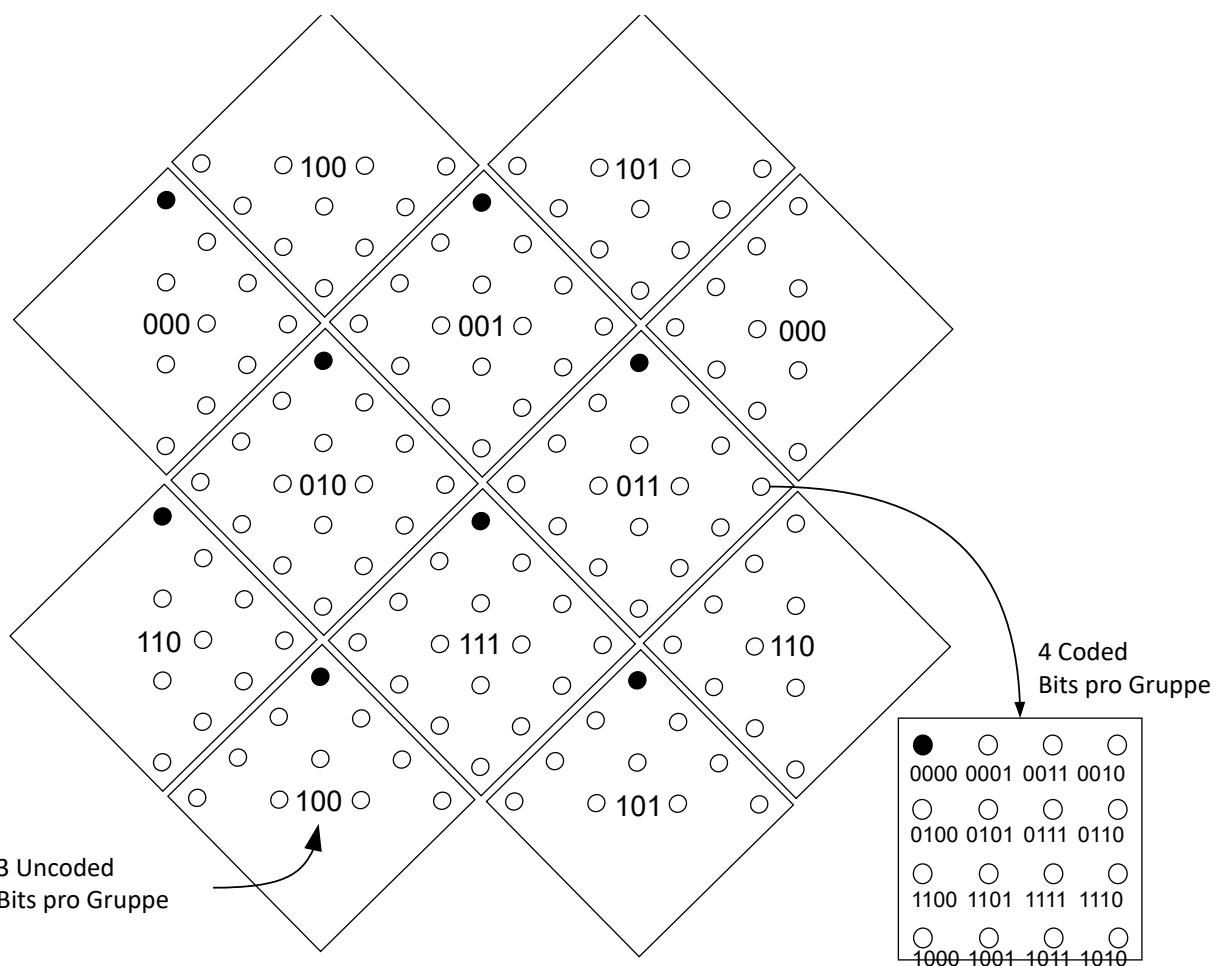


Abbildung 257: Auswahl eines Signalraumpunktes bei DSQ128

Die Signalpunkte eines DSQ128-Signalraumes lassen sich in 8 gleichseitige Parallelogramme (vier vollständige und 8 halbe) aufteilen.

Die mittleren Parallelogramme enthalten 16 Signalpunkte. Die Parallelogramme an den Rändern werden an den Kanten umgeschlagen und zu einem vollständigen Parallelogramm mit ebenfalls 16 Signalpunkten zusammengefasst.

Die 3 uncodierten Bits wählen das Parallelogramm aus. Die 4 codierten Bits wählen den Signalraumpunkt innerhalb des Parallelogramms aus. Dies hat den Vorteil, dass der Abstand der Parallelogramme groß genug ist und die 3 uncodierten Bits nicht durch die LDPC-Codierung geschützt werden müssen. Es reicht also aus die 4 Bit für die Auswahl des Signalraumpunktes innerhalb eines Parallelogramms mit der LDPC-Codierung zu schützen was den Overhead verringert und somit zur Kanaleffizienz beiträgt.

Bei der LDPC-Codierung werden die Daten in zwei Bereiche unterteilt ($3 * 512 = 1536$ Bit bleiben uncodiert und 1723 Bit, die codiert werden). Bei der Codierung werden die Daten nicht verändert, sondern lediglich den 1723 zu codierenden Bits, 325 Paritätsbits hinzugefügt. Der Empfänger kann damit Fehler erkennen und zu einem gewissen Teil auch korrigieren.

Nach dem Scrambling werden fünfzig 65-Bit-Code-Blöcke zusammengefasst. Davor wird noch ein Auxiliary-Channel-Bit gesetzt. Dahinter werden noch 8 CRC-Bits angehängt.

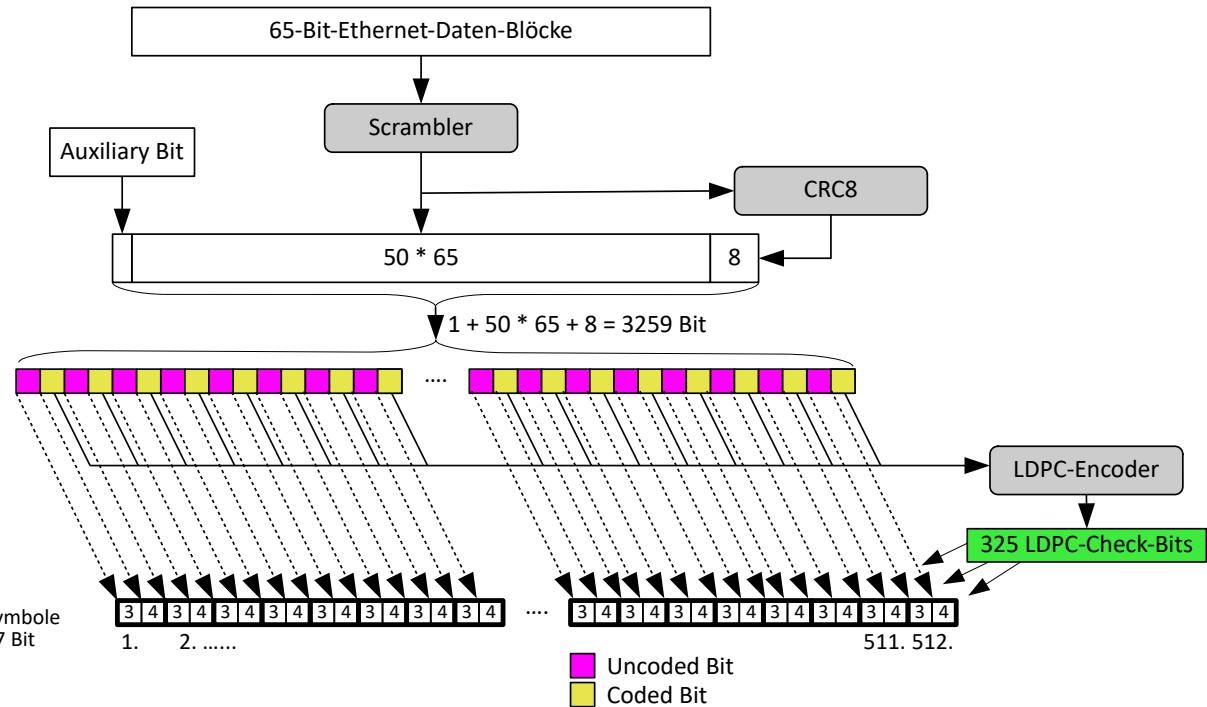


Abbildung 258: Bildung der LDPC-Frames

Das Ergebnis sind die 1536 uncodierten Bits und 2048 (1723 + 325) codierten Bits, zusammen also 3584 Bits, die zu einen Frame mit 512 7-Bit-Symbolen (2D-DSQ128-Symbole) zusammen gefasst werden. Diese werden wiederum auf 256 4D-PAM16-Symbole abgebildet. Dabei werden jeweils die beiden PAM-16-Komponenten eines DSQ128-Symbols über zwei aufeinander folgende Taktperioden auf demselben Kanal übertragen.

Nach der Bearbeitung durch den PCS erfolgt im PMA mit einem Tomlinson-Harashima Precoding (THP) eine Vorcodierung um den Signalpegel zu kontrollieren. THP beseitigt Intersymbol-Interferenzen, welche durch Dämpfung und Signalverzerrung erzeugt werden.

Die Echo-Cancellation erfolgt in 2 Stufen. Einmal durch die Brückenschaltung und danach nochmals im DSP, da es nach dem Hybrid noch Restanteile des Echos gibt.

Durch die große Rechenleistung im DSP kommt es zu einer entsprechenden Wärmeentwicklung. Besonders bei hoher Portdichte, wie sie in Switches vorkommt, ist das ein Problem. IEEE-802.3an sieht deshalb ein Power-Management vor. In Abhängigkeit von der Dämpfung (also auch der Leitungslänge) kann die Sendeleistung in 2-dB-Schritten angepasst werden. Es gibt 8 Level welche die Sendeleistung von 0 bis -14 dB reduzieren. Die Anpassung erfolgt mit Trainingssequenzen. Dabei werden Informationen über die Reserven beim Signalausabstand und die Power-Backoff-Level ausgetauscht.

Ethernet

Wie bei den vorangegangenen Standards gibt es beim Takt für jede Verbindung einen Master und einen Slave. Der Master erzeugt den Takt aus einem internen Takt während der Slave den Takt aus den Verbindungsdaten extrahieren muss. Das wird über die Auto-Negotiation-Funktion ausgehandelt und kann entweder durch manuelle Einstellung oder durch eine Gewichtung (mittels Seed) konfiguriert werden.

Die Auto-Negotiation erfolgt über eine 32 Bit große unformatted Extended Next Page direkt nach der Base Page.

Bit	Bedeutung
U31 - U21	Reserviert (0)
U20	PMA Trainings Anforderung. 1 = PMA-Trainings Sequenz (PRBS) bei jedem Frame reinitialisiert 0 = Fortlaufende Reinitialisierung
U19	Reserviert (0)
U18	PHY Sort Reach Mode (für bis zu 30 m Leitungslänge)
U17	Loop-Timing-Unterstützung Die Taktinformation kann vom Slave aus dem Datenstrom generiert werden.
U16	10GBase-T Vollduplex
U15	1000Base-T Halbduplex
U14	1000Base-T Vollduplex
U13	Anschlusstyp 1 = Mehr-Port 0 = Einzel-Port
U12	10GBase-T Master Slave-Konfiguration 1 = Master 0 = Slave
U11	10GBase-T Master-Slave-Rolle nach manueller Konfiguration
U10	Master Slave Seed Bit 10 (MSB)
U9	Master Slave Seed Bit 9
U8	Master Slave Seed Bit 8
U7	Master Slave Seed Bit 7
U6	Master Slave Seed Bit 6
U5	Master Slave Seed Bit 5
U4	Master Slave Seed Bit 4
U3	Master Slave Seed Bit 3
U2	Master Slave Seed Bit 2
U1	Master Slave Seed Bit 1
U0	Master Slave Seed Bit 0 (LSB)

--	--

Tabelle 27 Unformatted Extended Next Page für die Konfiguration von 10GBase-T

14.5.1.4.2 - Master Slave Priorisierung

Ähnlich wie bei 1GBase-T erfolgt bei 10GBase-T die Priorisierung von Master und Slave. Siehe folgende Tabelle.

Lokale Komponente	Entfernte Komponente	Lokale Rolle	Entfernte Rolle
Einzelport-Komponente	Multiport-Komponente	Slave	Master
Einzelport-Komponente	Manuell Master	Slave	Master
Manuell Slave	Manuell Master	Slave	Master
Manuell Slave	Multiport-Komponente	Slave	Master
Multiport-Komponente	Manuell Master	Slave	Master
Manuell Slave	Einzelport-Komponente	Slave	Master
Multiport-Komponente	Einzelport-Komponente	Master	Slave
Multiport-Komponente	Manuell Slave	Master	Slave
Manuell Master	Manuell Slave	Master	Slave
Manuell Master	Einzelport-Komponente	Master	Slave
Einzelport-Komponente	Manuell Slave	Master	Slave
Manuell Master	Multiport-Komponente	Master	Slave
Multiport-Komponente	Multiport-Komponente	Seed	Seed
Einzelport-Komponente	Einzelport-Komponente	Seed	Seed
Manuell Slave	Manuell Slave	Fehler	Fehler
Manuell Master	Manuell Master	Fehler	Fehler

Tabelle 28: Master-Slave-Priorisierung

Nach der Festlegung der Master- / Slave-Rolle erfolgt die Festlegung der Sendeleistung für das Power-Management durch eine Trainingssequenz. Während der Trainingssequenz werden vom Scrambler kontinuierlich 16.384 Bit lange PAM2-modulierte Trainings Frames auf allen 4 Adernpaaren gesendet. Die Signalfolge wird als Pseudo Random Binary Sequenz (PRBS) bezeichnet. Über die Symbolsequenz wird auch geprüft, ob es sich um eine MDI oder MDIX Verbindung handelt und ggf. angepasst.

Die Pin-Belegung entspricht der Belegung wie bei 1000Base-T siehe Tabelle 18: Zuordnung der Signale bei MDI- / MDIX-Belegung.

14.5.1.4.3 - Hinweis zur Verkabelung

Das Ziel war bei der Normierung 10 GBase-T auf CAT5e-Leitungen mit einer Distanz von 100 m zu ermöglichen. Diesen Ziel wurde nicht erreicht! Auch eine Cat6-Leitung (mit max. 250 MHz) ist nicht in der Lage 10GBase-T über 100 m zu transportieren. Deshalb wurde Cat6 um 2 Erweiterungen ergänzt (Cat6e für max. 500 MHz und Cat6a für max. 625 MHz) Die maximale Distanz bei Cat6e ist 55 m und bei Cat6a 100 m.

14.5.2 - 10GBase-KX

Ein bisher fehlendes Streckenteil war bisher immer die Backplane von Geräten wie etwa Switches oder Blade-Server. Im März 2007 sollte mit IEEE-802.3ap diese Lücke geschlossen werden.

Die maximale Länge beträgt 1 m bei 2 Steck-Kontakten. Wesentliche Ethernet-Parameter, wie Frameformat, minimale und maximale Framegröße wurden beibehalten. 10GBase-KX arbeitet mit einem Kanal (Lane) und einer Signalrate von 1,25 GBaud mit dem ein Differenzsignal mit einer Amplitude von 800 mV_{ss} bis 1600 mV_{ss} übertragen wird.

14.5.2.1 - 10GBase-KX4

Diese Lösung arbeitet mit 4 Lanes und einer Signalrate von 3,125 Gbaud. Das Differenzsignal arbeitet mit Amplituden von 800 mV_{ss} bis 1200 mV_{ss}. Der Nachteil dieser Lösung liegt bei der erhöhten Anzahl von Pins bei den Steckverbindern was den Formfaktor bei den Backplane-Switches etwas verringert. Dafür sind die Kosten beim Leiterplattenmaterial geringer da eine geringere Frequenz verwendet werden kann. Als Codierung kommt eine 8B/10B-Codierung zum Einsatz.

14.5.2.2 - 10GBase-KR

Diese Lösung arbeitet mit einem Lane und einer Signalrate von 10,3125 Gbaud. Das Differenzsignal arbeitet mit einer Amplituden von 1200 mV_{ss}. Als Codierung kommt eine 64B/66B-Codierung zum Einsatz. Damit ist der Formfaktor verbessert, jedoch sind die Bauteile auf die größeren Frequenzen auszulegen.

Das PMD wird mittels eines Startup-Protokolls initialisiert. Dabei wird die Taktrückgewinnung und das Timing angepasst. Weiterhin ist es möglich, dass der Empfänger den Sende-Entzerrer anpasst um frequenzabhängige Signalverluste zu kompensieren. Danach ist die Verbindung im Datenübertragungsmodus.

Es gibt zwei Kontroll-Kanäle. Das 16 Byte lange Coeficient-Update-Feld und das 16 Byte lange Status-Report-Feld. Mit dem Coeficient-Update-Feld kann der Empfänger dem Sender Korrekturen für den Entzerrer übergeben. Mit dem Status-Report-Feld kann der Sender dem Empfänger die aktuellen Einstellungen mitteilen. Es wird übertragen ob sich die Parameter an den Grenzwerten befinden und ob sie korrigiert wurden.

PHY-Typ	Interface	Lane-Anzahl	Codierung	Signalrate [GBaud]
1000GBase-KX	GMII	1	8B/10B	1,25
10GBase-KX4	XGMII	4	8B/10B	3,125
10GBase-KR	XGMII	1	64B/66B	10,3125
40GBase-KR4	XLGMII	4	64B/66B	10,3125

Tabelle 29 Ethernet-Backplane-Lösungen

14.6 - 40/100Gigabit-Ethernet

Am 17. Juni 2010 wurde der IEEE-802.3ba-Standard verabschiedet. Vereinfacht dargestellt, handelt es sich dabei um eine Vervierfachung oder einer Verzehnfachung von 10Gigabit-Ethernet. Die 40Gigabit-Lösung entspricht einer aus dem WAN-Umfeld gewohnten Datenrate.

Insgesamt sind 8 PHYs definiert

Bezeichnung	Codierung	Lane-Anzahl	Distanz	Medium
40GBase-KR4	40GBase-R	4	mind. 1 m	Kupfer
40GBase-CR4	40GBase-R	4	mind. 7 m	Kupfer
40GBase-SR4	40GBase-R	4	mind. 100 m	LWL
40GBase-KR4	40GBase-R	4	Mind. 10.000 m	WDM-LWL
100GBase-CR10	100GBase-R	10	mind. 7m	Kupfer
100GBase-SR10	100GBase-R	10	mind. 100 m	Kupfer
100GBase-LR4	100GBase-R	4	mind. 10.000 m	WDM-LWL
100GBase-ER4	100GBase-R	4	Mind. 30 / 40 km	WDM-LWL

Tabelle 30: PHYs bei 820.3ba

Im März 2011 wurde dann noch zusätzlich eine weitere Variante mit dem Standard IEEE-802.3bg freigegeben.

Bezeichnung	Codierung	Lane-Anzahl	Distanz	Medium
40GBase-FR	40GBase-R	4	Mind. 2 -2.000 m	LWL

Tabelle 31: PHY für IEEE-802.3bg

Der Grund für die Vielzahl ist, dass man eine möglichst optimale Lösung für jeden Anwendungsfall präsentieren wollte, um auch die Kosten im Rahmen zu halten.

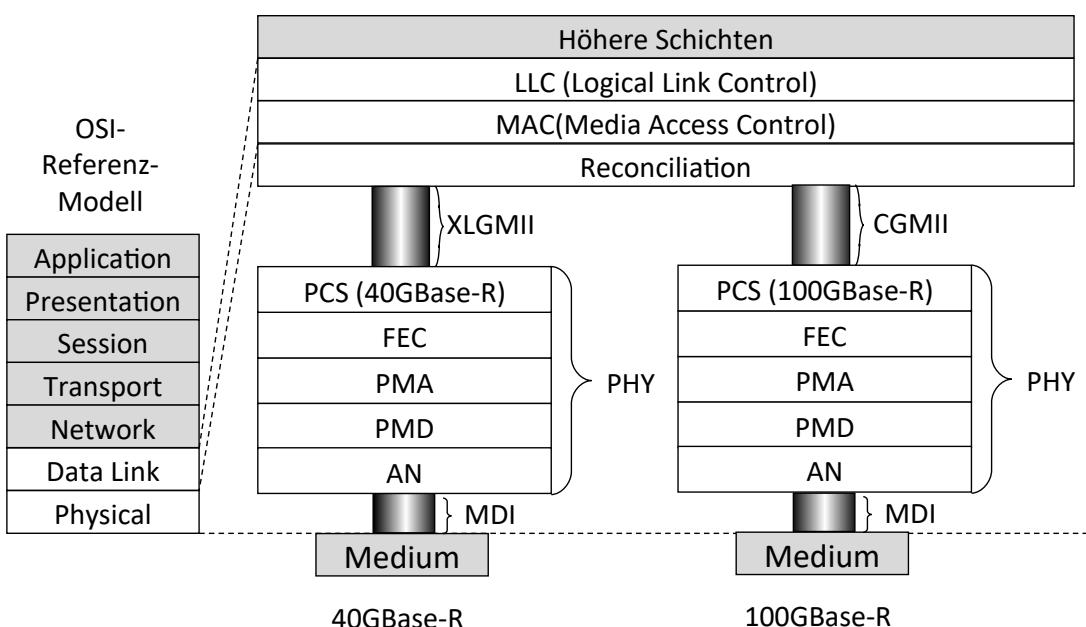


Abbildung 259: Sublayer der 40/100 Gigabit Lösungen

Die Reconciliation Layer passt die seriellen Daten an das parallele Datenformat der PCS-Sublayer an. Die Verbindung zwischen MAC und PHY ist je nach Geschwindigkeit ausgeführt (40 Gigabit Media Independent Interface (XLGMII) oder 100 Gigabit Media Independent Interface (CGMII)). Sowohl in Sende- als auch in Empfangsrichtung werden 64 Datenbits zur Verfügung gestellt. Zusätzlich gibt es noch in jeder Richtung 8 Control-Bits und ein Takt-Signal. Die 64 Bits der Sende und Empfangsrichtung sind in 8 Lanes unterteilt. Für jeden Lane ist jeweils ein Bit der 8 Control-Bits zuständig.

14.6.1.1 - PCS

Die Physical Coding Sublayer übernimmt die folgenden Aufgaben:

- ➊ 64B/66B-Coding
- ➋ Scrambling /Descrambling

Danach werden die Daten mit einem Round-Robin-Verfahren auf 4 Lanes (bei 40Gbps) oder 20 Lanes bei 100Gbps verteilt.

14.6.1.2 - FEC

Die Forward Error Correction ist optional und für die Backplane-Lösungen vorgesehen.

14.6.1.3 - PMA

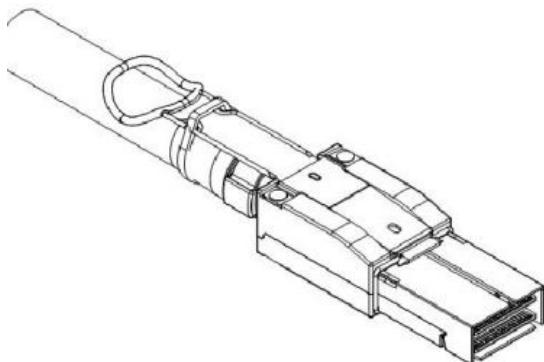
Der Physical Medium Attachment wandelt die Lane-Anzahl des PCS in die Lane-Anzahl des physikalischen Mediums um.

Beim Datenempfang ist der PMA für die Taktrückgewinnung zuständig.

14.6.1.4 - 40GBase-CR4 und 100GBase-CR10

Es gibt für 40GBase-CR4 zwei Steckervarianten

- ➊ Style-1-Variante mit einem Quad Small Form Factor Pluggable Plus (QSFP+) und 38 Pins. Laut Small Form Factor Comitee (SFF) wird der Stecker mit SFF-8436 bezeichnet.
- ➋ Style-2-Variante nach IEC 61076-3-113 mit 16 Pins.



Für 100GBase-CR10 wurde der SFF-8642 festgelegt. Es handelt sich dabei um den Mini Multilane 10 Gbps 12X Shielded Connector. Er hat vier Pinleisten mit insgesamt 84 Pins.

Abbildung 260: Mini Multilane 10 Gbps 12X

14.6.1.5 - 40GBase-SR4 und 100GBase-SR10



Diese preisgünstige Glasfaserlösung arbeitet im ersten LWL-Fenster (850nm) mit 50/125µm Fasern. Mit OM3-Fasern ist eine Distanz von 100 m erreichbar. Mit OM4-Fasern sind 150 m erreichbar. Als Leitungen werden so genannte Ribbon-Fiber eingesetzt. Diese bestehen aus mehreren parallel liegenden Glasfasern mit identischen Eigenschaften in einer Leitung. Ribbon-Fiber gibt es als Monomode und als Multimodefasern mit bis zu 72 Fasern. Senderseitig werden VCSEL eingesetzt.

Als Stecker kommt der Multi Path Push-On (PMO) – Stecker zum Einsatz. Er ist von seinen Dimensionen mit dem RJ45-Stecker vergleichbar.

Für 100GBase-SR10 ist ein Stecker mit 24 Fasern vorgesehen. Dabei werden die 24 Fasern in 2 Reihen aufgeteilt. Die obere Reihe ist für die Empfangskanäle und die untere Reihe ist für die Sendekanäle vorgesehen. Der Standard sieht auch Stecker mit nur 12 Fasern vor. Dabei sind zwei Stecker neben-, oder übereinander zu positionieren.

Abbildung 261: MPO-Stecker
(Quelle: Lindy)

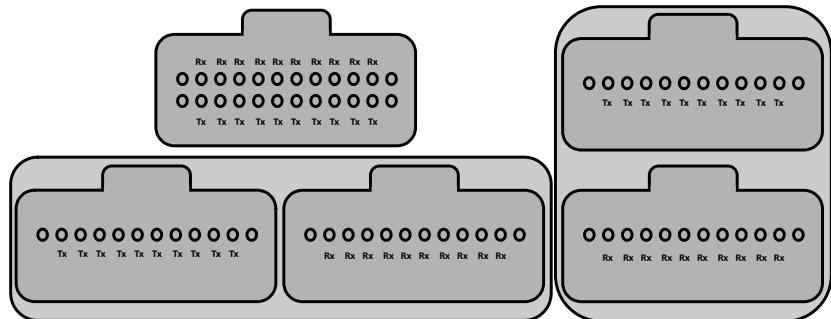


Abbildung 262: MPO-Stecker-Optionen für 100GBase-SR10

14.6.1.6 - 40GBase-LR4

Diese Variante fasst 4 Lanes mit dem Wavelength-Division-Multiplex-Verfahren (WDM) zusammen. Es wird eine Singemode-Faser (9/125 µm) verwendet. Damit sind Distanzen von 2 bis 10.000 m möglich.

14.6.1.7 - 100GBase-LR4 und 100GBase-ER4

Dabei werden zwei Singemode-Fasern und Distributed Feedback Laser (DFB) mit WDM verwendet. Die 4 Lanes transportieren je 25,78125 Gbaud/s. 100GBase-LR4 hat eine Reichweite von 2 bis 10.000 m. 100GBase-ER4 hat eine Reichweite von 2 bis maximal 40.000 m.

14.6.1.8 - 40GBase-FR

Dieser Standard wurde nachträglich als IEE802.3bq und wird vornehmlich für Carriern-Lösungen und Client-Interfaces verwendet. Das sind Verbindungen die zwischen Rechenzentren verwendet werden. Es lassen sich Distanzen von 2 bis 2.000 m überbrücken. Es wird nur ein Lane verwendet. Dabei wird eine Brutto-Datenübertragungsrate von 41,25 Gbps verwendet.

14.6.1.9 - 40GBase-KR

Für diese Backplane-Lösung werden 4 Lanes mit je 10,3125 Gbaud/s verwendet.

14.6.1.10 - Auto-Negotiation bei 40/100Gbit-Ethernet

Die PHYs für 40GBase-CR4, 100GBase-CR10 und 40GBase-KR4 funktionieren wie bisher beschrieben.

Die Standards 1000Base-KX, 10Gbase-KX4, 10GBase-KR, 40GBase-KR4, 40GBase-CR4 und 100GBase-CR10 arbeiten anstelle mit Link-Pulsen mit einem Codierungsverfahren, das Differential Manchester Encoding (DME) genannt wird. Darüber werden so genannte DME-Pages ausgetauscht.

DME-Pages haben eine Länge von 49 Bits (48 Datenbits und ein Pseudo Random Bit)

Die 48 Datenbits enthalten folgende Informationen:

Bit	Name	Hinweis
D0 - D4	Selector-Bits	Siehe: Tabelle 6: Basic-Link Selektor-Feld
D5 - D9	Echo Nonce	Pseudo-Random-Nummer Anzeige, falls ACK gesetzt war. Gilt als zusätzliche Bestätigung der Übertragung des Technology-Ability-Feldes. Ist das ACK Bit auf 0 werden D5 – D9 auch auf 0 gesetzt.
D10 - D12	C-Felder	Symmetrische Pause und Flow-Control
D13	Remote Fault Feld	Signalisierung von der Gegenseite, dass ein Fehler erkannt wurde
D14	ACK Feld	Bestätigung des Fehlerfreien Empfangs des Link-Codewortes
D15	Next Page	Hinweis, dass nach dem Basic-Codewort weitere Pages gesendet werden.
D16 - D20	Transmitted Nonce (T0 - T4)	Zur Übertragung einer Pseudo-Random-Nummer zwischen 0 bis 31. Der Inhalt wird jedes Mal neu gesendet, wenn sich der Inhalt des Technology-Ability-Feldes geändert hat.
D21 - D45	Technology Ability	
D46 - D47	FEC-Capability	

Tabelle 32: DME-Page

Bit	PHY-Typ
A0	1000Base-KX
A1	10GBase-KX4
A2	10GBase-KR
A3	40GBase-KR4
A4	40GBase-CR4
A5	100FBase-CR10
A6 - A24	Für Künftige Erweiterungen

Tabelle 33: Technology-Ability-Feld

Priorität	PHY-Typ	Leistungsmerkmal
1	100GBase-CR10	100 Gbps über 10 Lanes
2	40GBase-CR4	40 Gbps über 4 Lanes
3	40GBase-KR4	40 Gbps über 4 Lanes
4	10GBase-KR	10 Gbps über 1 Lane
5	10GBase-KX4	10 Gbps über 4 Lanes
6	1000Base-KX	1 Gbps über 1 Lane

Tabelle 34: Prioritätenauflösung

14.7 - 200/400Gigabit-Ethernet

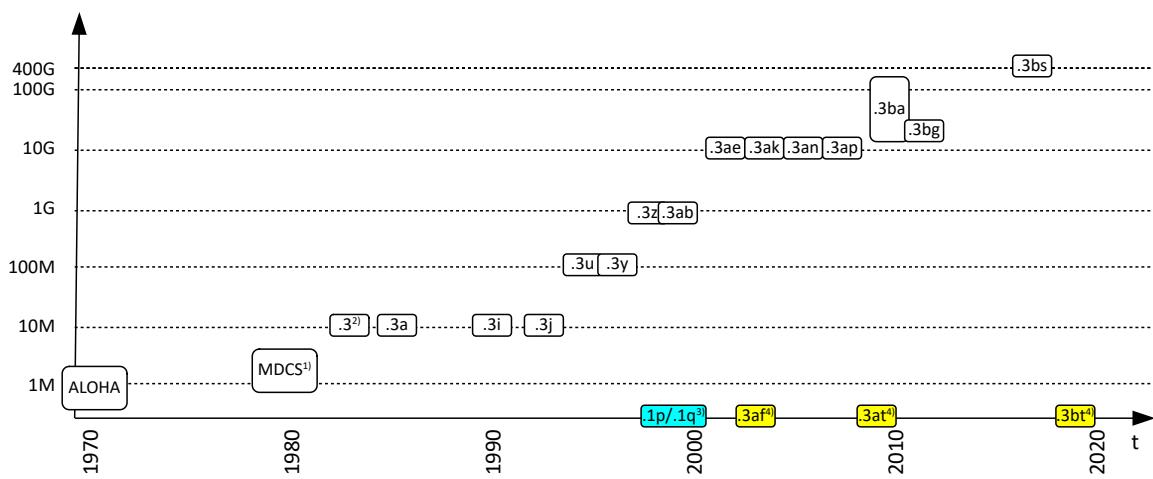
Am 06.12.2017 wurde der IEEE-802.3bs-Standard verabschiedet. Damit sind 200 und 400 Gigabit-Ethernet über LWL möglich.

14.8 - Übersicht über die Historie

Wie in den vorangegangenen Kapiteln zu lesen ist, hat Ethernet eine bewegte Vergangenheit hinter sich. Bis auf die ersten Koaxial-Lösungen, sind fast alle Lösungen noch käuflich erwerbar. Allerdings sind Lösungen mit Repeatern (Hubs) nicht mehr zeitgemäß. Den steigenden Anforderungen konnte stets mit der Erhöhung der Datenrate entsprochen werden.

Dies hat auch die Anforderungen an die passive Verkabelung in die Höhe getrieben. Kupferlösungen scheinen an ihre Grenzen zu kommen.

Das war allerdings nach jedem neuen Standard der Fall und die Geschichte ist ja noch nicht zu Ende.



- ¹⁾ Multipoint Data Communication System = Erste Ethernetvariante
- ²⁾ Entspricht IEEE-802.3 (bei allen anderen Einträgen wird IEEE802 weggelassen)
- ³⁾ VLANs = IEEE802.1p und IEEE802.1q
- ⁴⁾ PoE (Power over Ethernet)

Abbildung 263: Timeline der Ethernet-Entwicklungen

Aktuelle IEEE-Norm	Alte IEEE-Norm	Medientyp	Jahr	Daten-Übertragungs-Rate [Mbps]	Max. Segment-Länge [m]	Max. Netzsegment-Größe [m]	Max. Stations-Anzahl	Duplex-Mode	Medium	Wellen-Imp. [Ω]	Stecker	Anmerkung
IEEE-802.3 Clause 8	802.3	10BASE5	1983	10	500	2.500	100	Half	Kupfer-Koaxial-Leitung RG8A/U	50	Barrel N-Type	Mind. Stationsabstand 2,5m
		StarLAN 10	1983	10					Kupfer-Twisted Pair			obsolet
IEEE-802.3 Clause 10	802.3a	10BASE2	1985	10	185	925	30	Half	Kupfer-Koaxial-Leitung RG58	50	BNC	Mind. Stationsabstand 0,5m
IEEE-802.3 Clause 14	802.3i	10BASE-T	1990	10	100			Half	Kupfer-Twisted Pair CAT-3	100	8P8C (RJ45)	Verkabelung nach TIA568A/B
		FOIRL										Fiberoptic interrepeater link (FOIRL) Ursprünglicher Standard für Ethernet über Glasfaserkabel
IEEE-802.3 Clause 15	802.3j	10BASE-FL	1992	10								Über-Begriff für die 3 folgenden Ausprägungen
IEEE-802.3 Clause 18		10BASE-FL	1992	10								Revidierte FOIRL Version
IEEE-802.3 Clause 17		10BASE-FB		10								Für Backbones gedacht. Obsolet
IEEE-802.3 Clause 16		10BASE-FP		10								Obsolet
		100BASE-T		100	100				Kupfer-Twisted Pair			Überbegriff für die 3 folgenden Ausprägungen

Aktuelle IEEE-Norm	Alte IEEE-Norm	Medientyp	Jahr	Daten-Übertragungs-Rate [Mbps]	Max. Segment-Länge [m]	Max. Netzsegment-Größe [m]	Max. Stations-Anzahl	Duplex-Mode	Medium	Wellen-Imp. [Ω]	Stecker	Anmerkung
								CAT-3				
IEEE-802.3 Clause 32	802.3bw	100BASE-T2		100				Full	Kupfer-Twisted Pair CAT-5			Obsolet
IEEE-802.3 Clause 24	802.3u	Fast Ethernet 100BASE-TX	1995	100	100				Kupfer-Twisted Pair CAT-5	8P8C (RF45)		Verkabelung nach TIA568A/B
IEEE-802.3 Clause 23		100BASE-T4		100	100			Half	Kupfer-Twisted Pair CAT-3	8P8C (RF45)		Verkabelung nach TIA568A/B Obsolet
	802.3x	Full Duplex and flow control			100					8P8C (RF45)		Verkabelung nach TIA568A/B
IEEE-802.3 Clause 32	802.3y	100BASE-T2 100 Mbit/s (12.5 MB/s) über low quality twisted pair			100			Full		8P8C (RF45)		Verkabelung nach TIA568A/B
IEEE-802.3 Clause 26	802.3u	100BASE-FX	1995		400			Half (Repeater-Betrieb) Full (Switch-Betrieb)				
	802.3u	100BASE-SX	1995		550							
IEEE-802.3 Clause 58		100BASE-BX10				40.000		EINE Single-Mode-				SFP-Paar mit Splitter für unterschiedlichen Wellenlängen für Senden /Empfang

Aktuelle IEEE-Norm	Alte IEEE-Norm	Medientyp	Jahr	Daten-Übertragungs-Rate [Mbps]	Max. Segment-Länge [m]	Max. Netzsegment-Größe [m]	Max. Stations-Anzahl	Duplex-Mode	Medium	Wellen-Imp. [Ω]	Stecker	Anmerkung
									Glasfaser			
IEEE-802.3 Clause 58		100BASE-LX10				10.000			Single-Mode-Glasfaser			λ=1310nm
	802.3z	1000BaseX Gigabit Ethernet über Kupfer und Glasfaser	1998									
	802.3z	1000BaseSX Gigabit Ethernet über Glasfaser	1998									
	802.3ab	1000BASE-T	1999	1.000	100				4 Kupfer-Twisted Pair			
	802.3ad	Link Aggregation										
	802.3ae	10GBase-SR 10Gbase-SW 10Gbase-LR 10Gbase-LW 10Gbase-ER 10Gbase-EW 10Gbase-LX4	2002	10.000								
	802.3an	10GBASE-T	2006	10.000								
	802.3af	Power over Ethernet										
	802.3at	Power over Ethernet										
	802.3az	Energy Efficient Ethernet										

Aktuelle IEEE-Norm	Alte IEEE-Norm	Medientyp	Jahr	Daten-Übertragungs-Rate [Mbps]	Max. Segment-Länge [m]	Max. Netzsegment-Größe [m]	Max. Stations-Anzahl	Duplex-Mode	Medium	Wellen-Imp. [Ω]	Stecker	Anmerkung
	802.3ba	100 Gigabit Ethernet										
	802.3bs	200/400 Gigabit Ethernet	2017									

Tabelle 35: Zusammenfassung der Ethernet-Versionen

15 - Kupfer-Steckverbindungen

15.1 - BNC-Stecker



Abbildung 94: BNC: Abschlusswiderstand / T-Verbinder / Stecker mit Leitung

BNC bedeutet Bayonet Neill-Concelman, was auf die beiden amerikanischen Erfinder Paul Neill und Carl Concelmann, sowie auf den verwendeten Mechanismus hinweist. Der Stecker wird nicht geschraubt, sondern unter leichtem Druck um etwa 90° gedreht und rastet mit Federdruck ein, ähnlich einer Blinker Glühlampe im Auto.

Wird in 10Base2 Rechnernetzwerken verwendet.

15.2 - Barrel-Stecker (N-Stecker)

Der N-Stecker hat seinen Namen von der amerikanischen Marine (Navy-Connector; deutsch: Marine-Verbinder). Er wird mit einer Überwurfmutter an seinem Gegenstück befestigt.

Er ist selbstreinigend, da die Spitze des Innenleiters in eine nachgiebige Hülse kleineren Durchmessers gepresst wird, und somit Verschmutzungen entfernt werden.

Wird in 10Base5 Rechnernetzwerken verwendet. Siehe auch im Kapitel Kupferleitungen/10Base5.



Abbildung 264 – Barrel-Stecker (N-Stecker)

15.3 - SUB-D-Stecker

Dieser Stecker wird in den verschiedensten Bereichen verwendet. Er hat seinen Namen von seiner Bauform. Blickt man auf die Stecker- oder Buchsen-Seite, haben die Kontakte eine Anordnung in Form eines „D“. Wird auch als Subminiaturstecker oder Trapezsteckverbinder bezeichnet. Gilt als einer der störsichersten Stecker. Hat jedoch den großen Nachteil der Baugröße. Dadurch lassen sich nicht so viele Schnittstellen auf einem Modul oder einem Gerät unterbringen. Deshalb wird er zusehends vom RJ45-Stecker abgelöst, der wesentlich kompakter ist und somit eine größere Portdichte zulässt.

Siehe auch im Kapitel Kupferleitungen/10Base5.



Abbildung 265 – SUB-D-Stecker/Buchse

Wird in seiner 9, 15 oder 25 poligen Ausführung angewendet. Die 9- und 25-poligen Stecker werden z. B. für die serielle V.24/RS232-Schnittstelle genutzt. Die parallele Druckerschnittstelle wird bei PCs verwendet. Die 15polige Ausführung (Bildmitte) wird für die AUI-Schnittstelle verwendet.

15.4 - RJ-Stecker

RJ steht für Registered Jack; deutsch registrierter Stecker. Der Stecker wurden von den Bell Laboratories in den 1970er Jahren eingeführt und von der FCC (US-amerikanische Federal Communication Commission) standardisiert. Er wurde von vielen Firmen im Telefonumfeld genutzt, so auch von der Firma Western Electric. Durch die weite Verbreitung hat sich auch auch den Name Western-Stecker, oder als Gegenstück Western-Buchse etabliert.

Der Stecker existiert in verschiedenen Bauformen.

In der Norm wird die Stecker-Bezeichnung mit RJ-xx y uPvvC beschrieben.

Wobei die folgende Zuordnungen gelten:

xx Baufom. Damit werden die Abmessungen festgelegt.

y Eigenschaften mit folgender Bedeutung:

C=Bündig abgeschlossener Stecker

W=Wandsteckdose

S=Einzelanschluss

M=Mehrfachanschluss

X=Komplexer Stecker

u Anzahl der möglichen Pins (gefolgt von einem P für Pins)

v Anzahl der belegten Pins (gefolgt von einem C für Connections)

Damit hat z. B. ein LAN-Stecker für einen 1000Base-T-Verbindung nach der Norm eigentlich die Bezeichnung RJ-48C 8P8C. Durchgesetzt hat sich jedoch die Bezeichnung RJ-45.

15.4.1 - RJ11-Stecker

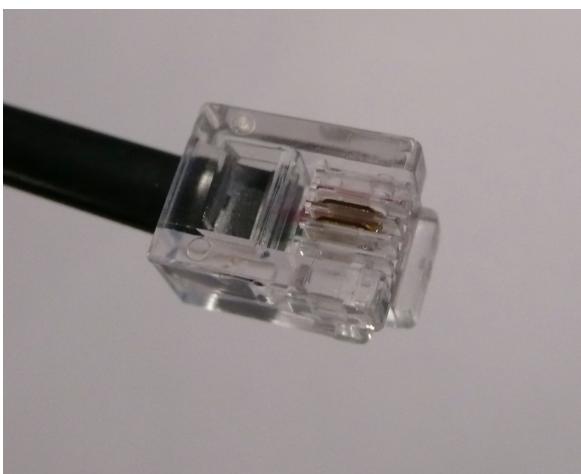


Abbildung 266 - RJ11-Stecker

Der Aufbau ist ähnlich wie der beim RJ45-Stecker. Allerdings hat er nur 4 Kontakt-Positionen.

Somit ist der Stecker in der Höhe und in der Länge wie beim RJ45 Stecker ausgefallen. Er ist schmäler als der RJ45-Stecker. Er wird im Telefonbereich verwendet.

Hier eine RJ-11C 4P2C Ausführung.

15.4.2 - RJ12-Stecker

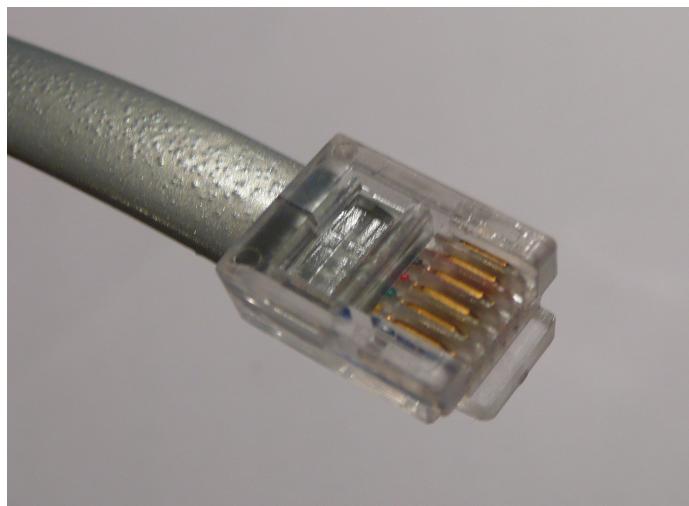


Abbildung 267 – RJ12-Stecker

Der Aufbau ist der gleiche wie beim RJ45-Stecker. Allerdings hat er in der Mitte 6 Kontakt-Positionen.

Somit ist der Stecker in der Höhe und in der Länge wie beim RJ45 Stecker ausgefallen. In der Breite ist er schmäler. Verwendung findet dieser Stecker bei Telefongeräten und Modem-Anschlüssen.

Hier eine RJ-12C 6P6C Ausführung.

15.4.3 - RJ45-Stecker

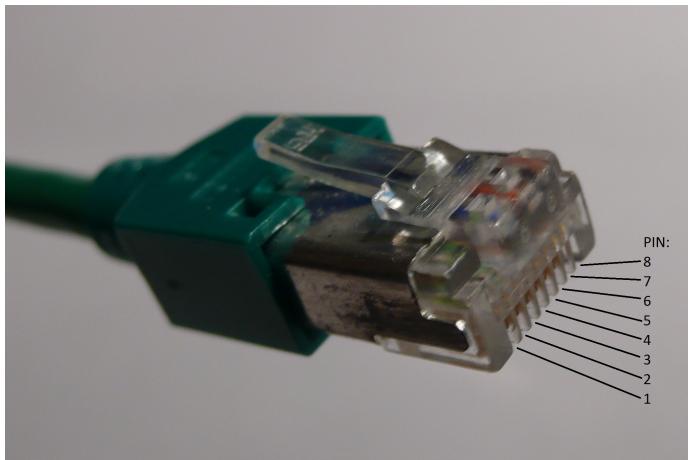


Abbildung 268 – RJ45-Stecker

Wie bereits oben beschrieben wird dieser Stecker allgemein mit RJ-45 beschrieben, obwohl es sich um einen RJ-48C- oder RJ-49C-Stecker handelt.

Er wird in 10Base-T, 100Base-Tx, 1000Base-T, Token Ring und anderen Rechnernetzwerken verwendet.

Hier eine RJ-48C 8P8C Ausführung.

Der RJ45-Stecker wird in verschiedenen Netzwerk-Spezifikationen verwendet. Die 8 Drähte werden zu 4 Paaren gruppiert. Die einzelnen Paare belegen folgende Kontakte:

15.4.3.1 - Aufteilung der Adernpaare einer Leitung nach TIA 568A

Paar-Nr	Kontakt-Nr
1	4,5
2	3,6
3	1,2
4	7,8

15.4.3.2 - Aufteilung der Adernpaare einer Leitung nach TIA 568B

Paar-Nr	Kontakt-Nr
1	4,5
2	1,2
3	3,6
4	7,8

Die beiden Varianten entstanden dadurch, dass die EIA/TIA den Standard 568A zeitlich nach dem proprietären de facto Standard 258A von AT&T eingeführt haben. EIA/TIA übernahm den AT&T Standard 258A als EIA/TIA Standard 568B.

Damit ist historisch bedingt, die EIA/TIA 568B weltweit verbreitet. In Europa dagegen ist die EIA/TIA 568A verbreitet da die Belegung mit den Farbcodes der Telefonleitungen übereinstimmt. Der Unterschied liegt in einer Vertauschung der Paare 2 und 3. Elektrisch und physikalisch sind beide Varianten gleichwertig. Wichtig ist nur, dass auf beiden Seiten einer Verkabelung, die gleiche Norm verwendet wird.

15.4.3.3 - Aufteilung der Adernpaare bei verschiedenen Topologien nach TIA 568B

Netzwerk-Spezifikation	Adernpaare
Token Ring	1 und 3
10BASE-T	2 und 3
100BASE-T	2 und 3
100BASE-T4	1, 2, 3 und 4
1000Base-T	1,2,3 und 4
10GBase-T	1,2,3 und 4
100VGAnyLAN	1, 2, 3 und 4

15.4.3.4 - Farbbelegung der verschiedenen Normungsgremien

Die Zuordnung von Pins des RJ45-Steckers zu Adernfarben wurde bei diversen Normen thematisiert. Hier ist eine Zusammenfassung der Belegungen.

Aderpaar	Pin s	EIA/TIA T568A	EIA/TIA T568B (AT&T)	IEC	REA	DIN-47-100
1	4,5	bl/ws	bl/ws	ws/bl	ws/bl	ws/bn
2	1,2	ws/gn	ws/or	sw/gn	ws/or	gr/rs
3	3,6	ws/or	ws/gn	rt/or	türkis/vi ?	gn/ge
4	7,8	ws/bn	ws/bn	ge/bn	türkis/vi ?	bl/rt

15.4.3.5 - Funktionsbelegung des RJ45-Steckers bei 10BASE-T

Sowohl Symbol als auch die Funktion sind aus der Endgerätesicht zu verstehen.

Pin	Symbol	Funktion	Richtung
1	TD+	Transmit Data Plus	Output
2	TD-	Transmit Data Minus	Output
3	RX+	Receive Data Plus	Input
4	NC	No Connection	-
5	NC	No Connection	-
6	RX-	Receive Data Minus	Input
7	NC	No Connection	-
8	NC	No Connection	-

15.4.3.6 - Funktionsbelegung des RJ45-Steckers bei Token Ring

Pin	Symbol	Funktion	Richtung
1	NC	No Connection	-
2	NC	No Connection	-
3	RX	Receive Data	Input
4	TX	Transmit Data	Output
5	TX	Transmit Data	Output
6	RX	Receive Data	Input
7	NC	No Connection	-
8	NC	No Connection	-

15.4.3.7 - Zusammenfassung

Für die unterschiedlichen Möglichkeiten der Belegung eines RJ45-Steckers gilt die folgende Tabelle.

Pin	Telefon analog	Telefon alt	T + T (CH)	DSL Splitter	ISDN (U_{k0} / U_{p0})	ISDN (S_0)	Ethernet 10BaseT	Ethernet 1000BaseT	Token Ring	TP-PMD	AS 400	3270	ATM
Schirm					(S)	(S)	S	S	S	S	(S)	(S)	S
1							TX+	D1+		TX+			X
2							TX-	D1-		TX-			X
3	W	a	1b		a2	a2	RX+	D2+	RX+			RX+	
4	a		1a	a	a1	a1		D3+	TX-		TX+	TX+	
5	b		(2a)	b	b1	b1		D3-	TX+		TX-	TX-	
6	e	b	(2b)		b2	b2	RX-	D2-	RX-			RX-	
7								D4+		RX+			X
8								D4-		RX-			X

15.4.3.8 - Nachfolger für den RJ45-Stecker

15.4.3.8.1 - GG45



Abbildung 269: GG45 (Quelle KSI)

Für die Anwendung in einer CAT7-Installation ist der RJ45-Stecker nicht mehr geeignet.

Beim RJ45-Stecker sind die Pins zu nah beieinander und verursachen ein zu großes Nebensprechen.

Eine wichtige Vorgabe bei der Entwicklung eines Nachfolgers war die Rückwärts-Kompatibilität zum bisher verwendeten RJ45-Stecker.

Die Firma NEXANS fand mit der GG45-Stecker-Buchse-Kombination eine abwärtskompatible Lösung. GG steht für GigaGate. Der Name GG lies sich allerdings nicht schützen. Deshalb schlossen sich die Hersteller NEXANS, Kerpen und TKM zur GG45-Allianz zusammen um den GG45 als Namen zu schützen.

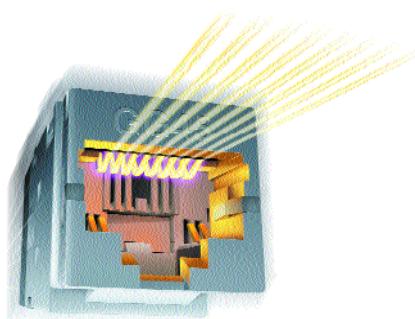


Abbildung 270: GG45 im CAT 5 und 6-Modus (Quelle: LANmark)

Die GG-45-Buchse besitzt nicht nur die 8 Pins an der Oberseite sondern noch zusätzlich jeweils 2 Pins links und rechts neben der Aussparung für den Verriegelungshebel. Der Stecker hat an der Stirnseite eine zusätzliche Nase mit der er in der Buchse einen Federschalter betätigt, um zwischen den Modi (CAT 5,6 und CAT7) umzuschalten.

Mit dem Umschalter werden die beiden inneren Kontaktpaare der oberen 8 Pins auf den Buchsenschirm geschaltet. Damit liegen die noch verfügbaren 4 Paare so weit auseinander, dass die erforderlichen Werte für das Übersprechen erreicht werden.

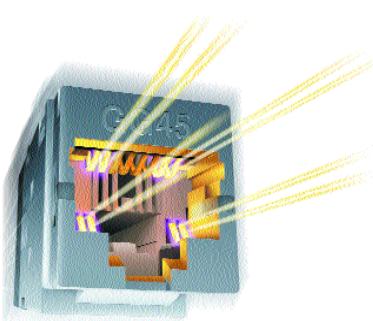


Abbildung 271: GG45 im CAT7 Modus (Quelle: LANmark)

Die Channel-Werte bis 1.000MHz werden nach der neuen Klasse F gemäß ISO/IEC Amendment 1 erfüllt. Damit werden die Anforderungen, die über 10GBaseT hinausgehen erfüllt.

Diese Lösung bietet bereits die Möglichkeit PoE (Plus) nach IEEE 802.3at, mit der doppelten Leistung von 30W über 4 Paare, zu realisieren.

Weitere Informationen über: www.gg45-alliance.org

Die erforderliche Messtechnik wird z. B. Von der Firma Ideal Industries (Zusammenschluss von Waveteck, Wandel & Goltermann, TCC und Acterna) in Form des Lantec 7 bereitgestellt.

15.4.3.8.2 - TERA-Stecker

Ein weiterer Aspirant auf den Stecker-Standard bei 10GBase-T ist der TERA-Stecker der Firma Siemon. Dieser Stecker ist für Multimedia-Anwendungen konzipiert. Bei ihm sind die Paare einzeln patchbar.



Abbildung 272: TERA-Stecker (Quelle Fa. Siemon)

Stecker erfüllt die Anforderungen für die Klasse FA und die Norm ISO/IEC 15018 (Generic Cabling for Homes).

Die als Anhang zum ISO/IEC-Standard 11801 geschaffene Klasse FA ist für eine obere Grenzfrequenz von 1.000 MHz spezifiziert und soll die kommende Generation von Daten-Applikationen oberhalb von 10GBASE-T ebenso unterstützen, sowie sämtliche Kabelfernseh-Frequenzen.

Um die Voraussetzungen für die künftigen Klasse FA Parameter zu bieten, heben die in IEC 61076-3-104, Ed. 2.0 enthaltenen Steckverbinder-Spezifikationen die obere Grenzfrequenz symmetrischer Twisted-Pair-Steckverbinder von 600 MHz (bei CAT 7) auf nunmehr 1.000 MHz an.

Leider ist der Stecker nicht rückwärts kompatibel wie der GG45-Stecker. Damit muss an eine bestehende/vorhandene RJ45-Verkabelung mit TERA/RJ-Patchleitungen angeschlossen werden.

Weitere Informationen gibt es bei: www.siemon.com/de

15.4.4 - RJ21 TELCO -Stecker

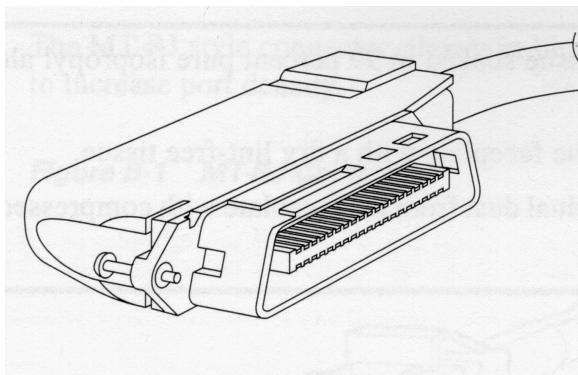


Abbildung 273 – RJ21-Stecker (TELCO-Stecker)

Der TELCO-Stecker, wie in obiger Abbildung, wird vor allem dort verwendet, wo eine hohe Portdichte gefordert wird. Damit lassen sich z. B. auf einem CISCO Group-Switchmodul 48 Ports unterbringen. Das andere Ende der Leitung wird auf das Patchfeld geführt, wo normalerweise mit RJ45-Steckern weiter verbunden wird.

15.5 - Stecker für IBM-Verkabelungs-System (IVS)

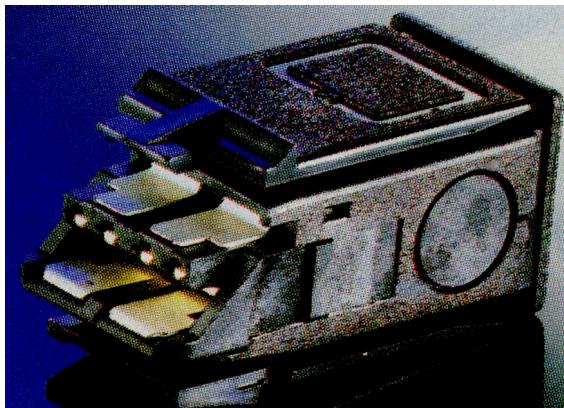


Abbildung 274 – IBM-Typ-I-Stecker für IVS

IBM hat für sein Verkabelungssystem einen eigenen Stecker entwickelt. Der so genannte TYP-I – Stecker. Er wurde für Twisted Pair bei Ethernet und Token Ring verwendet. Der Stecker ist für Datenraten bis 100 Mbps geeignet.

16 - Strukturierte Verkabelung

16.1 - Grundlagen

Für die Verkabelung ist ein großer Normierungsaufwand getrieben worden. Besonders für die Planung und den Betrieb einer Netzwerk-Infrastruktur sind diese Grundlagen wichtig. Ein repräsentativer Ausschnitt der derzeit aktuellen Normen für die Verkabelung sind:

- **EN 50310**

Anwendung von Maßnahmen für Erdung und Potentialausgleich in Gebäuden mit Einrichtungen der Informationstechnik.

- **EN 50173**

Verkabelung die unabhängig von Diensten und Anwendungen ist.

- **EN 50174**

Ausführung und Betrieb von informationstechnischer Verkabelung unter Verwendung von symmetrischer Kupfer- und Lichtwellenleiterverkabelung.

- **EN 50346**

Informationstechnik - Installation von Verkabelung - Prüfen installierter Verkabelung.

Eine Übersicht wann, welche Norm zum tragen kommt, bietet die folgende Tabelle:

Phase				
Gebäudeplanung	Verkabelungsentwurf	Planung	Realisierung	Betrieb
EN 50310 5.2: Gemeinsame Potentialausgleichsanlage (CBN) in einem Netzwerk 6.3: AC-Verteilung und Anschluss des Schutzleiters	EN 50173-1 4: Topologien 5: Leistungsvermögen der Übertragungsstrecken 7: Anforderungen an Kabel 8: Anforderungen an Verbindungseinheit	EN 50174-1 4: Betrachtungen zu Festlegungen 5: Qualitätssicherung 7: Verwaltung der Verkabelung	EN 50174-1 6: Dokumentation 7: Verwaltung der Verkabelung 8: Instandsetzung und Instandhaltung	EN 50174-1 5: Qualitätssicherung 7: Verwaltung der Verkabelung 8: Instandsetzung und Instandhaltung
		und EN 50174-2	und EN 50174-2	
		und EN 50174-3	und EN 50174-3	
		und für Potentialausgleich EN 50310	und für Potentialausgleich EN 50310	
			und EN 50346	

16.2 - EN 50173

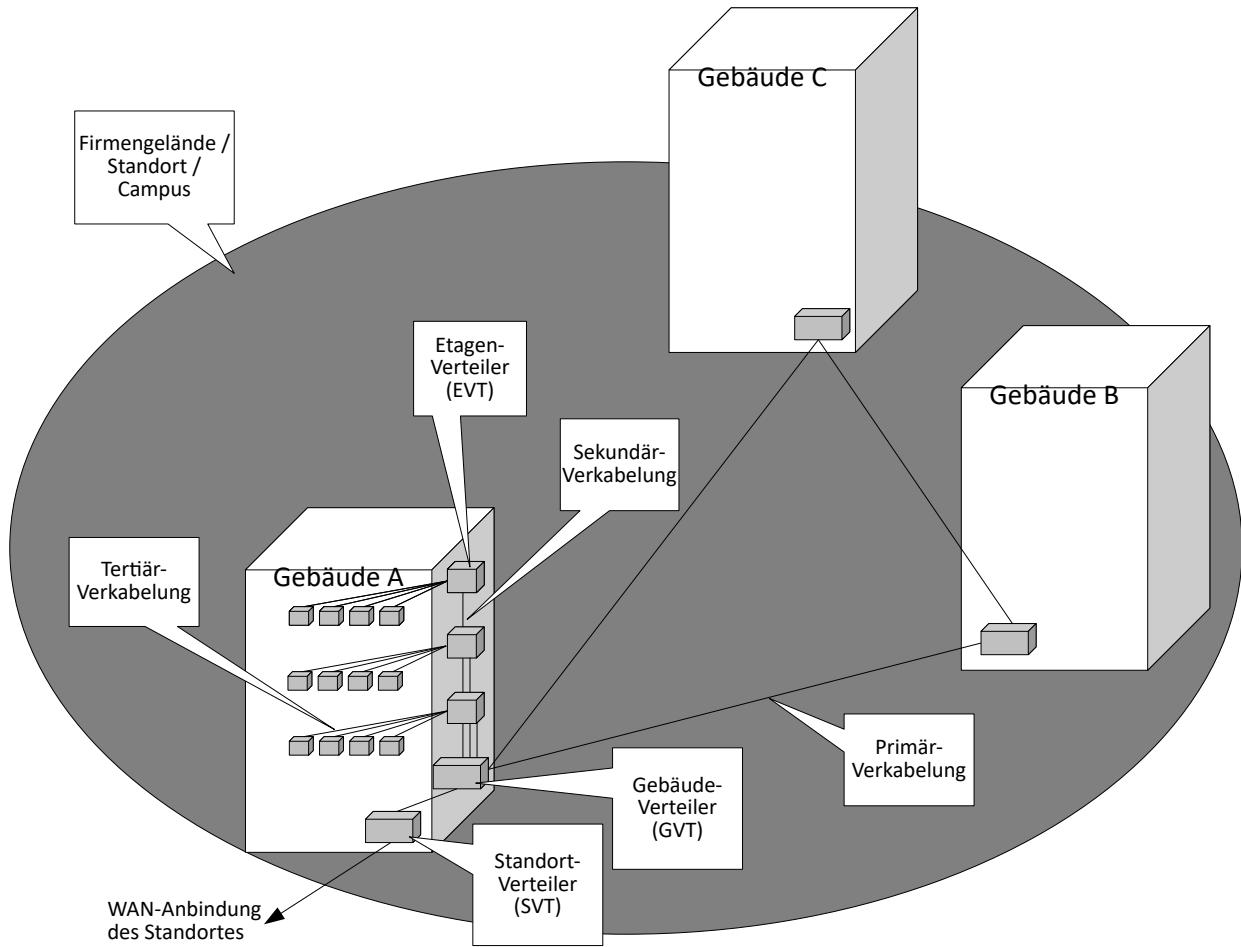


Abbildung 275: Strukturierte Verkabelung

Früher wurden für unterschiedliche Dienste unterschiedliche Verkabelungssysteme verwendet. Für eine Verkabelung, die unabhängig von Diensten und Anwendungen ist, wurde 1995 die erste Version der EN 50173 von dem Normungsgremium CENELEC/TC 215 verfasst. Diese Norm basiert auf der ISO/IEC 11801, welche weltweit Gültigkeit hat.

Für die folgenden Bereiche wurden Unternormen festgelegt:

- EN 50173-1 Allgemeine Verkabelung

Hier werden die Grundlagen der primären und sekundären Verkabelung beschrieben. Weiterhin werden die übertragungstechnisch relevanten Spezifikationen der Übertragungsstrecken-Klassen und den dazugehörigen Kategorien für Kabel, Verbindungen (Stecker) sowie Anschlussleitungen für Endgeräte. Um unterschiedliche Umgebungsbedingungen abbilden zu können wurden die MICE-Klassen eingeführt. Dabei werden die folgenden Begriffe festgelegt

- ◆ Topologie
- ◆ Leistungsvermögen der Übertragungsstrecke
- ◆ Anforderungen an Kabel
- ◆ Anforderungen an Verbindungstechnik

Strukturierte Verkabelung

EN 50173-2 Bürogebäude

Hier werden die Festlegungen des tertiären Bereichs sowie die Anforderungen an den so genannten informationstechnischen Anschluss am Arbeitsplatz beschrieben.

EN 50173-3 Industriell genutzte Standorte

Hier sind die Anforderungen, die durch Automationssysteme an eine Verkabelung gestellt werden, beschrieben.

EN 50173-4 Wohnungen

Hier werden anwendungsneutrale Kommunikationskabelanlagen in Ein- und Mehrfamilienhäusern beschrieben. Darunter fallen auch Arztpraxen und Kanzleien. In Wohnungen treten vielfältige Ausprägungen von Netzen auf.

- Informations- und Kommunikationstechnik (IuK)

- Rundfunk und Kommunikationstechnik (RuK)

- Steuerung, Regelung und Kommunikation in Gebäuden (SRKG)

Im Gegensatz zur sternförmigen Topologie-Struktur von IuK- und RuK-Netzanwendungen kann bei einer SRKG-Netzanwendung eine andere Topologie-Ausprägung wie z. B. Eine Bustopologie auftreten. Dem trägt die Norm im Abschnitt 5 mit einer eigenen Verkabelungsstruktur (im Teilsystem der Versorgungsbereichsverkabelung) Rechnung. SRKG-Netzanwendungen sind auch in der DIN EN 50090 festgelegt.

Dieser Bereich schließt auch kleine Büroumgebungen, wie sie z. B. An kleinen Außenstellen auftreten können ein.

EN 50173-5 Rechenzentren

Hier wird den Planern und Betreibern von Rechenzentren eine strukturierte Verkabelung vorgegeben.

Vor allem die speziellen Anforderungen durch hohe Leitungs- und Nutzer-Anzahl werden hier zusammen mit redundanter Netzausführung festgelegt um möglichst geringe Unterbrechungen des laufenden Betriebs zu ermöglichen.

Im November 2002 wurde die erste Korrektur der EN 50173-1 vorgenommen. Diese wird mit EN 50173-1:2002 bezeichnet. Bei dieser Korrektur wurden Teile, die in den Teilen 2 – 5 gleich auftraten, im Teil 1 zusammengefasst. Deshalb ist ein Teilbereich 2 – 5 immer zusammen mit Teil 1 anzuwenden. Im Jahr 2007 wurde die EN 50173-1 nochmals überarbeitet und lautet jetzt EN 50173-1:2007. Die EN 50173 wurde mittlerweile in die für Deutschland gültigen DIN-Normen übernommen und trägt jetzt deshalb die Bezeichnung DIN EN 50173.

16.2.1 - Topologie

Der Begriff Topologie wird unter unterschiedlichen Gesichtspunkten verwendet.

- ➊ Logische Topologie. Hier ist die Funktionsweise eines Netzwerks entscheidend. Es gibt zum Beispiel Bus-Topologien oder Ring-Topologien.
- ➋ Verkabelungstopologie. Hier ist zu beachten mit welchen Komponenten die Netzwerke aufgebaut werden.
- ➌ Logische Struktur eines Netzwerkes. So ist z. B. die Aufteilung in verschiedene kleinere logische Netzwerke einer Übersicht zuträglich. Dies wird näher bei den IP-Netzwerken betrachtet.

16.2.1.1 - Logische Topologie

Bei der Realisierung von Netzwerken wurden von unterschiedlichen Herstellern unterschiedliche Realisierungen angeboten. So hat IBM z. B. lange Zeit den Token Ring favorisiert.

Netzwerk-Protokoll	Logische Topologie	Verkabelungstopologie
Token Ring	Ring	Ring, Stern
High Speed Token Ring	Ring	Ring, Stern
FDDI	Ring	Ring, Stern
Ethernet (10 Mbps)	Bus	Bus, Stern
Fast Ethernet (100 Mbps)	Bus, Punkt zu Punkt	Stern
Gigabit Ethernet (1000 Mbps)	Bus, Punkt zu Punkt	Stern
ATM	Virtual Path / Channel	Ring, Stern

16.2.1.2 - Verkabelungstopologie

Dieser Bereich wird oft auch unter dem Begriff der strukturierten Verkabelung beschrieben. Unter strukturierter Verkabelung, wird eine Aufteilung der Netzwerkphysik verstanden. Dabei wird die Verkabelung in verschiedene Bereiche, je nachdem an welchem Ort die Verkabelung betrachtet wird, unterteilt. Grundlage der strukturierten Verkabelung ist eine Stern-Struktur da sie sich auf alle gängigen Realisierungen anwenden lässt. Siehe hierzu auch die obige Tabelle.

Es wird in:

- ➊ Gelände zwischen Gebäuden (Standortverkabelung)
- ➋ Verkabelung der Stockwerke (Gebäudeverkabelung)
- ➌ Verkabelung innerhalb eines Stockwerks (Etagenverkabelung)

unterschieden.

Die Primärverkabelung dient zur Verkabelung der einzelnen Gebäude auf einem Firmengelände (Aus den Zeiten in den nur Universitäten vernetzt waren, stammt der Ausdruck Campus).

Die Sekundärverkabelung dient zur Verkabelung der einzelnen Etagen miteinander.

Die Verkabelung auf einer Etage wird Tertiärverkabelung genannt.

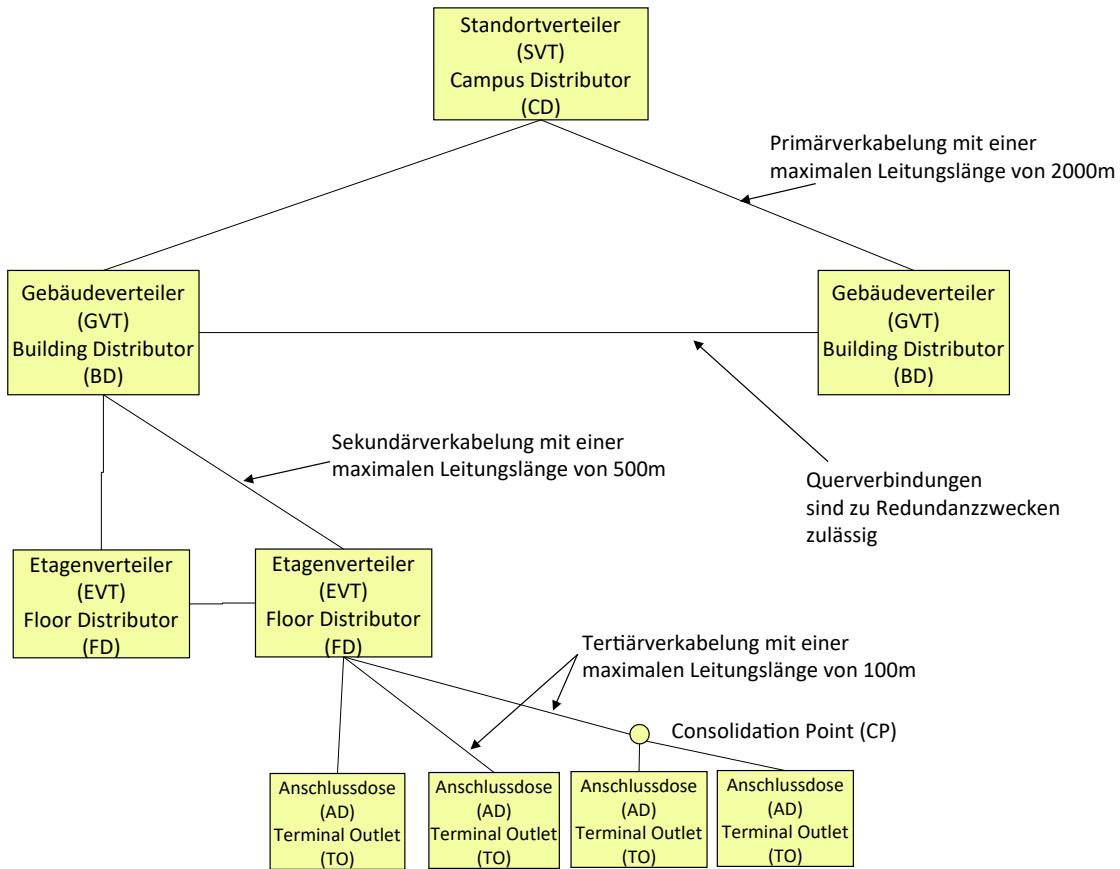


Abbildung 276: Hierarchische Verkabelungsstruktur

Damit ergibt sich die folgende hierarchisch geordnete Baum-Struktur.

Die Primär-, sowie die Sekundär-Verkabelung wird heute mit Lichtwellenleitern realisiert. Die Tertiär-Verkabelung auf der Etage wird mit einer Kupferverkabelung realisiert. Die Tertiär-Verkabelung mit einer maximalen Gesamtlänge von 100 m zerfällt in 2 Teile. Dem Permanent Link mit 90m und den beiden Patch-Leitungen von jeweils 5 m. In der obigen Abbildung sind nur die Teile des Permanent-Links abgebildet.

Es gibt für Anbindungen mit hohen Performance-Ansprüchen auch die Möglichkeit die Tertiär-Verkabelung mit LWL zu realisieren. Lange Zeit wurde dies unter der Marketing-Bezeichnung „Fiber to the Desk“ an besonders liquide Kunden verkauft. Dies führt allerdings zu einer erheblichen Verteuerung, auch bei den anzuschließenden Geräten da diese normalerweise nur eine Kupfer-Schnittstelle haben. Nachdem allerdings Gigabit-Ethernet auch auf Kupferbasis zu bekommen ist gibt es kaum mehr ein Argument - abgesehen von Potential- und Störungsproblemen - für den Einsatz von LWL für die Tertiär-Verkabelung.

16.2.2 - Leistungsvermögen der Übertragungsstrecke

Die Anforderungen an das Leistungsvermögen einer Übertragungsstrecke sind im Kapitel Leitungsmessungen beschrieben.

16.2.3 - Anforderungen an Leitungen und Verbinder

Die Anforderungen an Leitungen sind im Kapitel Leitungsmessungen beschrieben. Die Verbinder sind im Kapitel Steckverbindungen beschrieben.

16.3 - Backbone

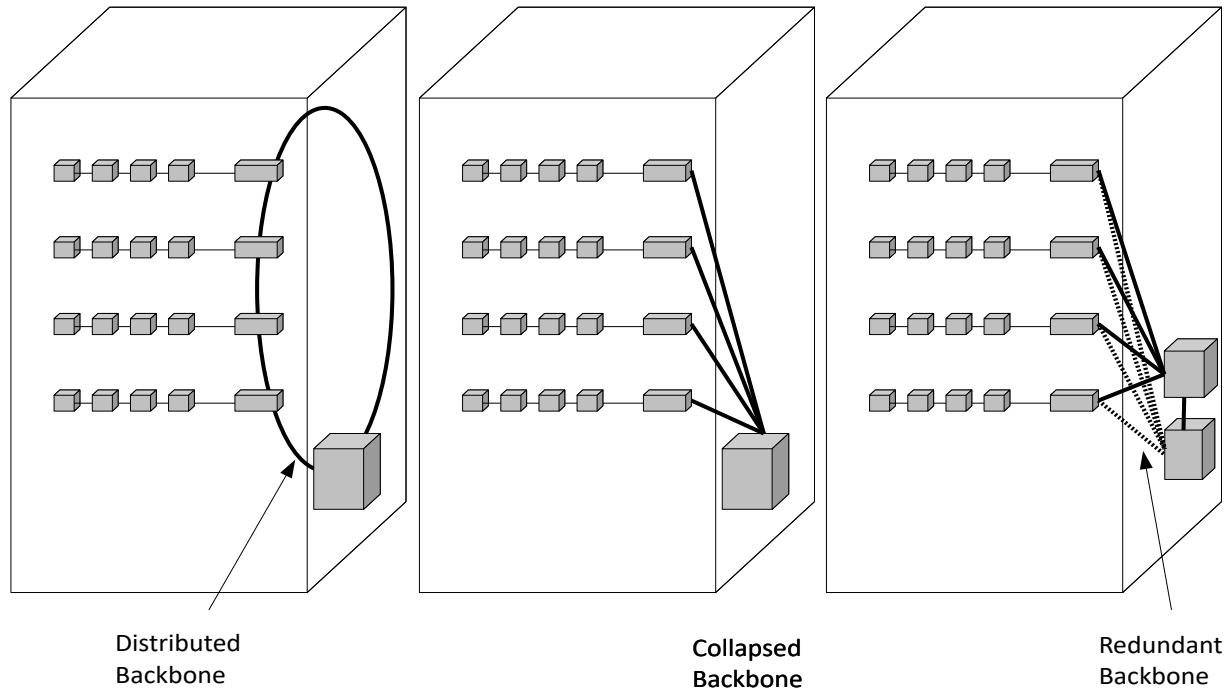


Abbildung 277 – Backbone

Es gibt verschiedene Strukturen von Backbones (deutsch: Rückgrat)

16.3.1 - Distributed Backbone

(deutsch: Verteilter Backbone) als FDDI-Ring oder (Fast-)Ethernet-Netz mit vermaschter Ausführung. Hierbei sind redundante Strukturen möglich.

16.3.2 - Collapsed Backbone

Dies bedeutet nicht, dass das Netzwerk zusammengebrochen ist, sondern dass sich das Backbone auf die Backplane des zentralen Netzwerkgerätes reduziert hat.

Allerdings hat diese Netzwerkstruktur auch einen gravierenden Nachteil. Ein Collapsed Backbone stellt einen „Single-Point-Of-Failure“ (deutsch: zentrale/einzelne Fehlerquelle die alles lahm legen kann) dar. Dies lässt sich am besten als zentrale Fehlerquelle übersetzen, da ein Ausfall dieses Gerätes das gesamte Netz außer Betrieb nimmt. Deshalb ist bei solchen Netzwerkstrukturen dafür Sorge zu tragen, dass noch ein Ersatzgerät im Fehlerfall die Funktionen aufnehmen kann. Dies erhöht die Kosten für die Netzwerkgeräte und deren Wartung.

17 - PoE (Power over Ethernet)

17.1 - Einleitung

Nach jahrelangen Debatten konnte im August 2003 IEEE den Standard IEEE-802.3af veröffentlichen, der die Stromversorgung von Endgeräten über die Ethernet-Schnittstelle festlegte. Es wird dabei Power over Ethernet (PoE) festgelegt. Damit können die bislang proprietären Lösungen verschiedenen Hersteller abgelöst werden. Der Standard gilt für Datenübertragungsraten von 10 Mbps bis 1000 Mbps.

17.2 - Stromversorgung

Die Versorgungsspannung beträgt 48 Volt (minimal 44 Volt bis maximal 57 Volt). Damit ist zum einen eine Berührung der offenen RJ45-Steckerkontakte eines Menschen ungefährlich und zum anderen bleibt die Verlustleistung in den Twisted-Pair-Leitungen gering. Der Strom wird auf maximal 350 Milliampere begrenzt. Damit kann in Kabeltrassen die Temperatur in Grenzen gehalten werden. Dies ergibt eine maximale Speiseleistung von 15,4 Watt. Bei der zulässigen Kabellänge von maximal 100 Metern bleibt für ein Endgerät 13 Watt übrig.

17.3 - Geräte

Mit 13 Watt Leistung, die zur Verfügung steht ist die Auswahl an Geräten, die für Power over Ethernet in Frage kommen, begrenzt. Typischerweise ist PoE für folgende Geräte interessant:

- WLAN-Accesspoints
- Überwachungskameras
- IP-Telefone

Im Standard sind die beteiligten Geräte folgendermaßen festgelegt:

- Verbraucher

Das mit Strom versorgte Gerät wird im Standard mit PD (Powered Device; deutsch: mit Strom versorgtes Gerät) bezeichnet.

- Stromversorger

Ist ein Gerät, das die Versorgungsspannung liefern kann. Es handelt sich hierbei um das so genannte PSE (Power Sourcing Equipment; deutsch: Stromversorgungsausrüstung)

17.4 - Erkennung der PoE-Endgeräte

Die PSE dürfen die Spannungsversorgung erst anlegen wenn sie erkannt haben, dass ein PoE-fähiges Endgerät (PE) angeschlossen ist. Dazu legen sie eine definierte Leerlaufspannung von 30 Volt mit einem auf 5 mA begrenzten Strom an die entsprechenden Ports. Misst die Testschaltung einen Innenwiderstand von 19 – 26,5 kΩ und eine Kapazität bis maximal 10 µF, dann wird die PSE die Stromversorgung aktivieren.

17.5 - Mögliche Konfigurationen

Da mit unterschiedlicher Verkabelungstechnik die neuen PoE-fähige Endgeräte betrieben werden dürfen, hat der Standard 3 unterschiedliche Möglichkeiten definiert, um Endgeräte mit PoE zu versorgen:

- Endspan-Versorgung mit Phantomspeisung
- Endspan-Versorgung mit Verwendung der Spare-Pairs (Ersatzpaare)
- Midspan-Versorgung

Die Endgeräte müssen zwei unterschiedliche Übertragungsmöglichkeiten berücksichtigen, wenn sie standardkonform sein wollen. Sowohl die Speisung über die Datenpaare, als auch die Speisung über die freien Ersatzpaare ist möglich.

17.5.1 - Endspan-Versorgung mit Phantomspeisung

Bei der Phantomspeisung werden die Datenpaare für die Stromversorgung mit genutzt. Dies ist vor allem dann erforderlich, wenn nur zwei Adernpaare zur Verfügung stehen.

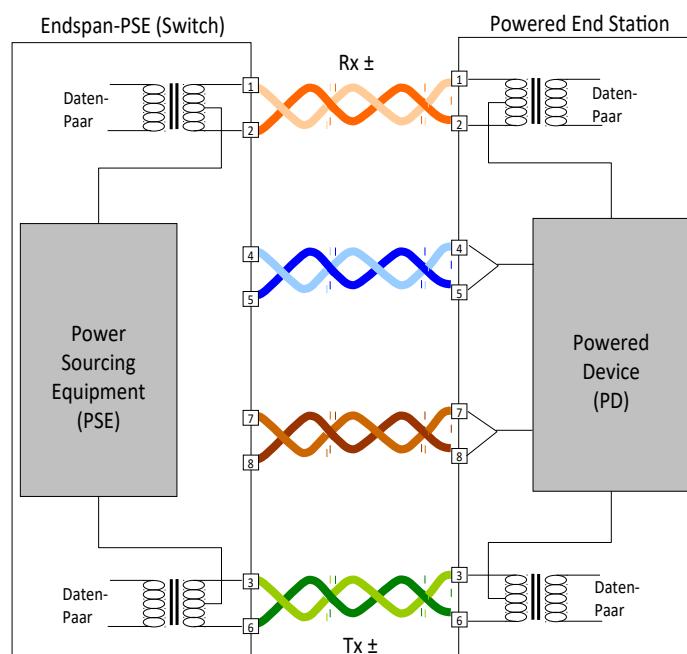


Abbildung 278: PoE-Endspan-Phantomspeisung

17.5.2 - Endspan-Versorgung über die freien Adernpaare

Bei einer Verkabelung bei der alle 4 Adernpaare zur Verfügung stehen, werden die beiden ungenutzten Adernpaare zur Stromversorgung genutzt.

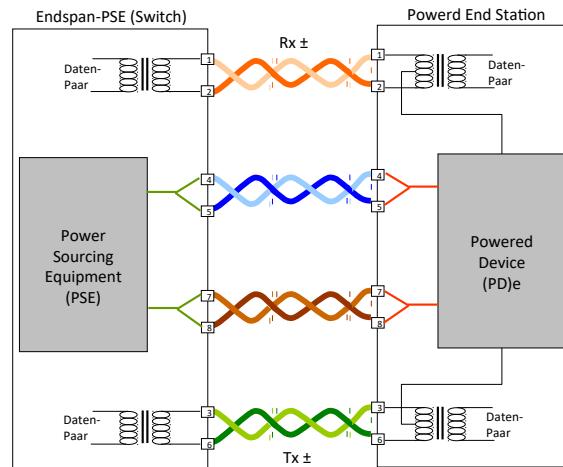


Abbildung 279: PoE-Endspan-Spare-Pairs

17.5.3 - Midspan-Versorgung

Kann der Switch, an dem das PoE-fähige Endgerät angeschlossen ist die Stromversorgung nicht selbst ermöglichen, gibt es Geräte um die Stromversorgung in einer zwischengeschalteten Einspeisung zu ermöglichen.

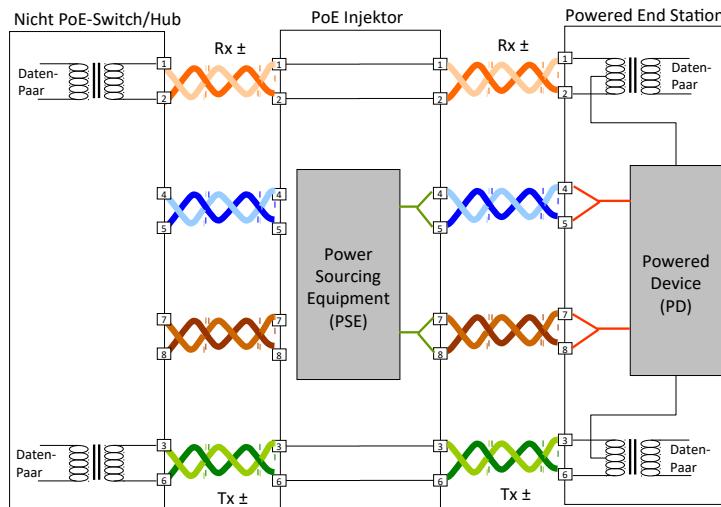


Abbildung 280: PoE-Midspan

17.6 - Management

Die Stromversorgung über Ethernet bietet die Möglichkeit die Versorgung der Endgeräte über ein Netzwerk-Management zu steuern. Hierzu sind die entsprechenden MIB-Variablen im Standard definiert worden. Dadurch hat ein Administrator die Möglichkeit, von seiner Administrationskonsole aus die Geräte zurückzusetzen, einz- oder auszuschalten.

17.7 - PoE-Leistungsklassen

Um die zu übertragende Leistungen einzuschätzen wurden Klassen definiert.

Klasse	Verwendung	Strom	Max. Speiseleistung (PSE)	Max. Entnahmleistung (PE)
0	default	0-5 mA	15,4W	0,44 – 12,95 W
1	optional	8-13mA	4,0W	0,44 – 3,84 W
2	optional	16-21mA	7,0W	3,84 – 6,49 W
3	optional	25-31mA	15,4W	6,49 – 12,95 W
4	reserviert	35-45mA	15,4W	reserviert

17.8 - Pinbelegung

Für unterschiedliche Topologien sind die Pinbelegungen wie folgt:

RJ45-Pin	Farbcode nach EIA/TIA 568B	100Base-TX	802.3af Phantom		802.3af Spare	100Base-T4/1000Base-T	ISDN
			MDIX	MDI			
1	orange gestreift	RX+	RX+, V-	TX+, V+	RX+	TX-D1+	-
2	orange	RX-	RX-, V-	TX-, V+	RX-	TX-D1-	-
3	grün gestreift	TX+	TX+, V+	RX+, V-	TX+	RX D2+	Tx+
4	grün	-	-	-	V+	BI D3+	Tx-
5	blau gestreift	-	-	-	V+	BI D3-	Rx-
6	blau	TX-	TX-, V+	RX-, V-	TX-	RX D2-	Rx+
7	braun gestreift	-	-		V-	BI D4+	-
8	braun	-	-		V-	BI D4-	-

Der Standard wurde mehrfach verbessert und hat diverse Erweiterungen bekommen. Die maximale Kabellänge bleibt dabei bei 100m.

Standard	Ausgangsspannung in V [DC]	Storm in mA [DC]	Adernpaare	Leistung PSE (Versorgung)	Leistung PD (Endgerät)
802.3af (2003) CAT3 max 20 Ω pro Paar PD-Typ: 1	36 – 57	350	2	15,4	12,95
802.3at (2009) CAT5 max 12,5 Ω pro Paar PD-Typ: 1 und 2	42,5 - 57	600	2	30	25,5
802.3bt (2018) CAT5 max 12,5 Ω pro Paar bei 2PPoE max 6,25 Ω pro Paar bei 4PPoE PD-Typ: 1, 2, 3 und 4	42,5 – 57	2 * 960	2 (2PPoE) oder 4 (4PPoE)	45 60 75 90	40 51 62 71

18 - MAN / WAN

18.1 - Grundlagen

18.2 - PDH

Die PDH (Plesiochrone Digitale Hierarchie) stellt ein synchrones Zeitmultiplex-System dar. Sie überträgt also Signale aus verschiedenen Quellen über einen gemeinsamen Kanal. Dabei sind die Bitraten der einzelnen Kanäle/Leitungen nicht exakt gleich, sondern nur annäherungsweise (plesios kommt aus dem Griechischen und bedeutet nahe). 1972 wurden die Bitraten für die PDH von der CCITT festgelegt. Dabei sind die Bitraten in den Regionen unterschiedlich festgelegt worden. In der folgenden Tabelle sind die Bitraten in kbit/s angegeben.

Hierarchiestufe	Nordamerika		Europa		Japan	Transatlantik
0		64		64	64	64
1	DS1	1544	E1	2048	1544	2048
2	DS2	6312	E2	8048	6312	6312
3	DS3	44736	E3	34368	32064	44736
4	DS4	274176	E4	139264	97728	139264
5			E5	564992		

Der Aufbau eines E1-Rahmens ist folgender. Die Bits eines jeden Kanals werden hintereinander übertragen. Die Kanäle 0 und 16 stehen nicht für den Datentransport zur Verfügung. Im Kanal 0 wird abwechselnd ein Rahmen-Kennwort (Synchronisation / Fehlerprüfinformation) und ein Rahmen-Meldewort (für Fehlermanagement) übertragen. Der Kanal 16 beinhaltet Signalisierungsinformationen.

32 Kanäle mit je 8 Bit in 125µs																															
0	1	2	3	4	5	6	7	8	9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Zur Leitungscodierung wird der HDB3-Code verwendet. Als Übertragungsmedien stehen Koaxialkabel mit einem Wellenwiderstand von 75Ω , sowie eine verdrillte Zweidrahtleitung mit 120Ω zur Verfügung. Der Sender hat Spannungspegel von $\pm 2,37V$.

Rahmen einer höheren Stufe En werden durch Digitalsignalmultiplexer zusammengesetzt. Dazu werden 4 Rahmen der Stufe En -1 zusammengefasst. Da die einzelnen Rahmen aus unterschiedlichen Teilnetzen kommen können, kann die Bitrate unterschiedlich sein. Zum Ausgleich der Unterschiede wird mit Stopfbits aufgefüllt. Dazu benötigen die Multiplexer Pufferspeicher um die einzelnen Rahmen aufzubereiten, bis sie in den neuen Multiplexrahmen passen.

Beim Positiv-Stopfverfahren wird der Pufferspeicher schneller gelesen als beschrieben. Je nach Füllstand des Pufferspeichers wird das Lesen an bestimmten Bitpositionen im Rahmen (Stopfstellen) unterbrochen und ein Stopfbit übertragen. Der Demultiplexer kann durch Stopfinformationsbits erkennen, ob an den möglichen Stopfstellen Stopfbits oder Nutzbits übertragen wurden. Die Stopfbits können dann vom Demultiplexer wieder entfernt werden.

Beim Negativ-Stopfverfahren wird der Pufferspeicher langsamer gelesen als gefüllt. Je nach Füllstand werden anstelle von Stopfbits Informationsbits eingesetzt. Der Demultiplexer wird über die Stopfinformationsbits darüber informiert. Beim Positiv-Null-Negativ-Stopfverfahren sind im Rahmen sowohl positive als auch negative Stopfstellen enthalten. Dieses Verfahren wird bei SDH verwendet.

18.3 - SDH

Die SDH (Synchronous Digital Hierarchie) ist eine synchrone Multiplex-Übertragungstechnik für Glasfasern und Richtfunkstrecken. SDH ist der primäre Standard für Netze im WAN-Bereich. SDH ist von der ITU-T standardisiert und wird vom SONET-Standard (Synchronous Optical Network) abgeleitet. Entwickelt wurde er von AT&T und Bellcore. SDH eignet sich für die Datenübertragung von B-ISDN (Breitband-ISDN), sowie auch für den transparenten Transport von ATM-Zellen.

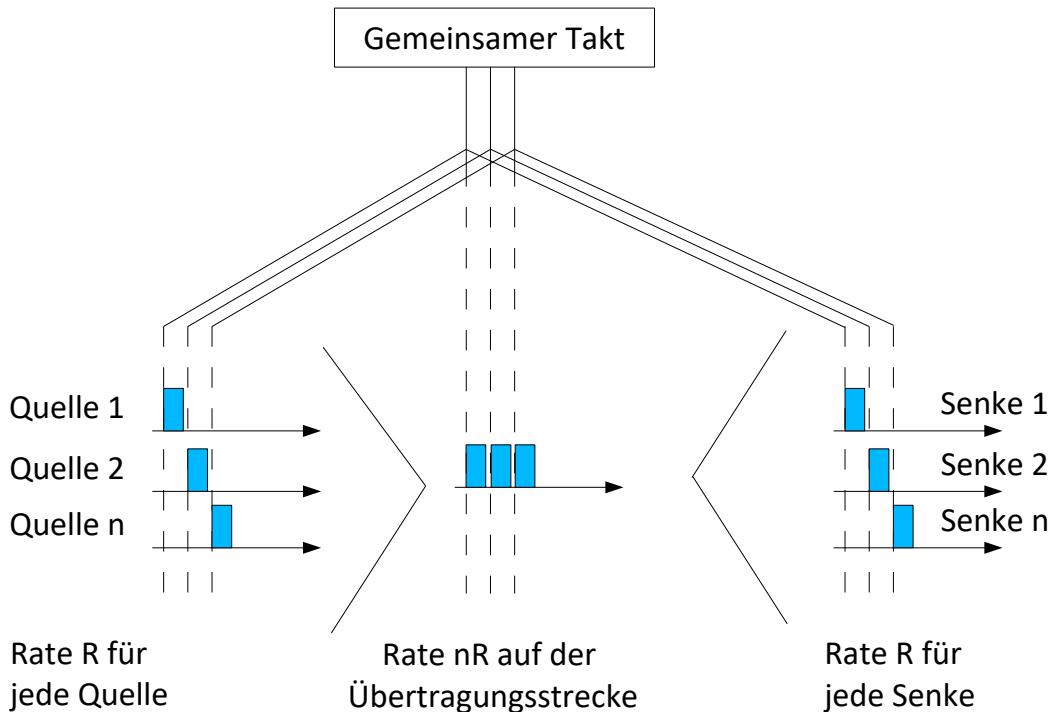


Abbildung 281: SDH

SDH stellt ein synchrones Zeit-Multiplex-Verfahren dar. SDH ist auf die optimale Ausnutzung der Übertragungskapazität von Glasfasern ausgerichtet. Die einzelnen Takte sind strikt synchron und stehen zueinander in einem ganzzahligen Verhältnis. Byteströme aus n Quellen mit der Rate R werden per synchronem Multiplex zu einem Bytestrom der Rate nR zusammengefasst.

Hierarchiestufe SDH	Bitrate in Mbit/s	Hierarchiestufe SONET	Signalbezeichnung SONET
-	51,84	STS-1	OC-1
STM-1	155,52	STS-3	OC-3
STM-2	297,36		
STM-3	466,56	STS-9	OC-9
STM-4	622,08	STS-12	OC-12
STM-6	933,12	STS-18	OC-18
STM-8	1244,16	STS-24	OC-24
	1866,24	STS-36	OC-36
STM-16	2488,32	STS-48	OC-48
STM-32	4976,64	STS-96	OC-96
STM-64	9953,28	STS-192	OC-192

Ein SDH-Rahmen hat das folgende Aussehen:

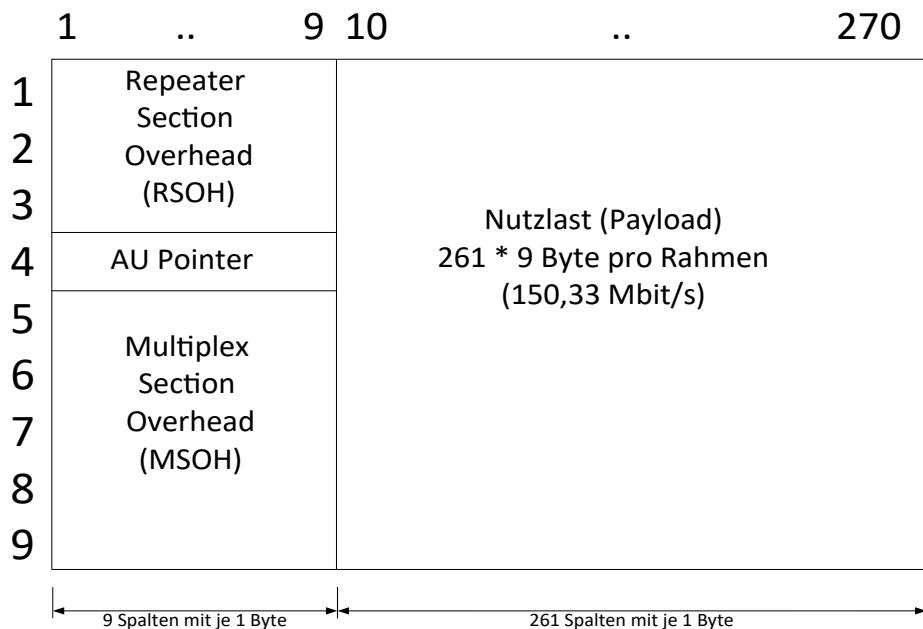


Abbildung 282SDH-Rahmen

18.4 - MAN

Ein Metropolitan Area Networks (MAN; deutsch: Metronetz) ist für Ausdehnungen, etwa einer Großstadt, bis zu 100km konzipiert. Beispiele hierfür sind das Netzwerk für Kabelfernsehen oder das neue kabellose Stadtnetz nach IEEE-802.16 (WiMAX).

18.4.1 - DQDB

Der Distributed Queue Dual Bus ist ein MAN-Konzept das mit zwei gegenläufigen parallelen Bussen funktioniert. Stationen, die Daten senden wollen, erhalten über eine verteilte Warteschlange das Zugriffsrecht auf den Bus und können dann Zellen konstanter Länge übertragen. Der Zellaufbau ist der gleiche wie bei ATM, was den Transport von DQDB über ATM einfach macht.

Ein Slotgenerator erzeugt freie Rahmen mit einer Dauer von 125µs.

Es gibt zwei unterschiedliche Slots:

- PA-Slots (Pre Arbitrated; deutsch: vorverhandelt) für isochronen Verkehr.
- QA-Slots (Queued Arbitrated Access) für asynchronen Verkehr.

Die Rahmen enthalten einen Header von 5 Byte und einen Nutzdaten-Anteil von 48Byte.

Die Rahmen wandern in Richtung Abschluss an allen Stationen vorbei.

Eine Station greift über ihre AU (Access Unit) auf den Bus zu.

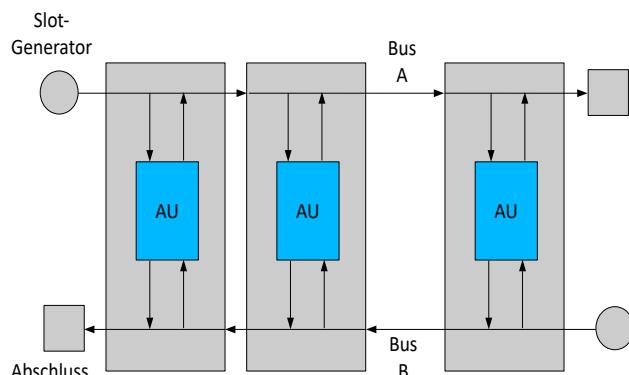


Abbildung 283: DQDB

Auf DQDB wird der Dienst SMDS (Switched Multi-Megabit/Metropolitan Data Service. In Europa auch CBDS Connectionless Broadband Data Service) als ausschließlich asynchroner Dienst angeboten. Die Deutsche Telekom bietet SMDS seit 1994 unter der Bezeichnung DATEX-M an. Die Datenrate beträgt 34 Mbit/s. Die Zugangskanäle haben Datenraten von 64 kBit/s und 25 MBit/s

18.5 - WAN

Wide Area Networks (WAN; deutsch: Weitverkehrsnetze)) haben eine Ausdehnung zwischen 10 km und 1000 km. Damit erstreckt sich ein WAN über ein sehr großes Gebiet, etwa ein Land oder gar einen Kontinent und hat potentiell eine große Teilnehmerzahl.

Die meisten WANs bestehen aus zahlreichen Übertragungsleitungen, die jeweils ein Routerpaar miteinander verbinden. Es kann vorkommen, dass die Router nicht direkt miteinander kommunizieren können. Dann sind weitere Router zwischengeschaltet. Die Pakete werden auf den Routern jedes mal zwischengespeichert und bearbeitet, bevor sie weitergesendet werden können. Gibt es aus Redundanzgründen mehrere Wege von der Quelle zum Ziel kann ein Router jedes Mal, wenn er ein Paket verarbeitet, aufgrund einer Routing-Tabelle entscheiden, welchen Weg das Paket bis zum Ziel nehmen soll.

Ein Verbindungsnetz das auf diesem Prinzip basiert, nennt man auch Speichervermittlungsnetz (Store-and-Forward-Net) oder Paketvermittlungsnetz. Fast alle WANs (mit Ausnahme von Satelliten-Verbindungen) enthalten Speichervermittlungsnetze.

Sind die Pakete klein und haben sie alle die gleiche Größe werden sie auch Zellen genannt. (z. B. bei ATM sind alle Zellen 53 Byte groß)

18.5.1 - X.25

1976 wurde X.25 von der CCITT (heute ITU-T) standardisiert. Mit X.25 wird die Schnittstelle zwischen Endgerät und dem Netz mit seinem Anschaltgerät beschrieben. Die Datenraten sind zwischen 300 bit/s und 64 kbit/s. Seit 1992 sind auch 2 Mbit/s möglich.

Es wurde für die Verwendung von schlechten analogen Übertragungsstrecken mit hohen Bitfehlerraten entwickelt. X.25 ist flächendeckend weltweit verfügbar. Damit steht es in direkter Konkurrenz zu Frame Relay.

Die Endgeräte werden als DCE (Datenendeinrichtung) oder DTE (Data Terminal Equipment) bezeichnet.

Die Anschaltgeräte werden mit DÜE (Datenübertragungseinrichtung) oder DCE (Data Circuit Terminating Equipment) bezeichnet.

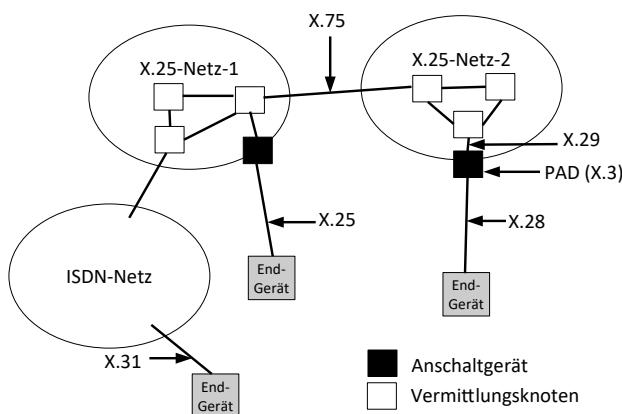


Abbildung 284: Paketvermittelnde Datennetze

über die X.75-Schnittstelle miteinander verbunden.

Paketierende Endgeräte werden direkt über die X.25-Schnittstelle mit dem DCE an das Netz angeschlossen.

Nicht paketierende Endgeräte werden mit einer X.28-Schnittstelle mit einem PAD (Packet Assembler/Disassembler) an das Netz über die X.29-Schnittstelle angeschlossen. Der PAD ist in X.3 beschrieben.

Ein DTE kann auch über die X.31-Schnittstelle und ISDN auf das paketvermittelnde Netz zugreifen.

Die unterschiedlichen Netzbetreiber werden

18.5.2 - Frame-Relay

Dieses Verfahren wurde 1984 von dem CCITT (heute ITU-T) eingeführt. Bei diesem Verfahren werden Rahmen variabler Länge aus mehreren Verbindungen im asynchronen (statistischen) Zeitmultiplex über eine Leitung übertragen. Jede Verbindung erhält eine Mindest-Übertragungsrate (CIR = Committed Information Rate) die jedoch überschritten werden kann wenn Leitungskapazität frei ist. Frame Relay erlaubt den Transport einer Vielzahl von Protokollen höherer Schichten.

Die Datenrate in Frame Relay reicht von 56 bzw. 64 kbit/s in ganzzahligen Vielfachen bis 1,544 Mbit/s bzw. 2,048 Mbit/s.

Frame Relay kann als abgemagerte X.25-Variante verstanden werden.

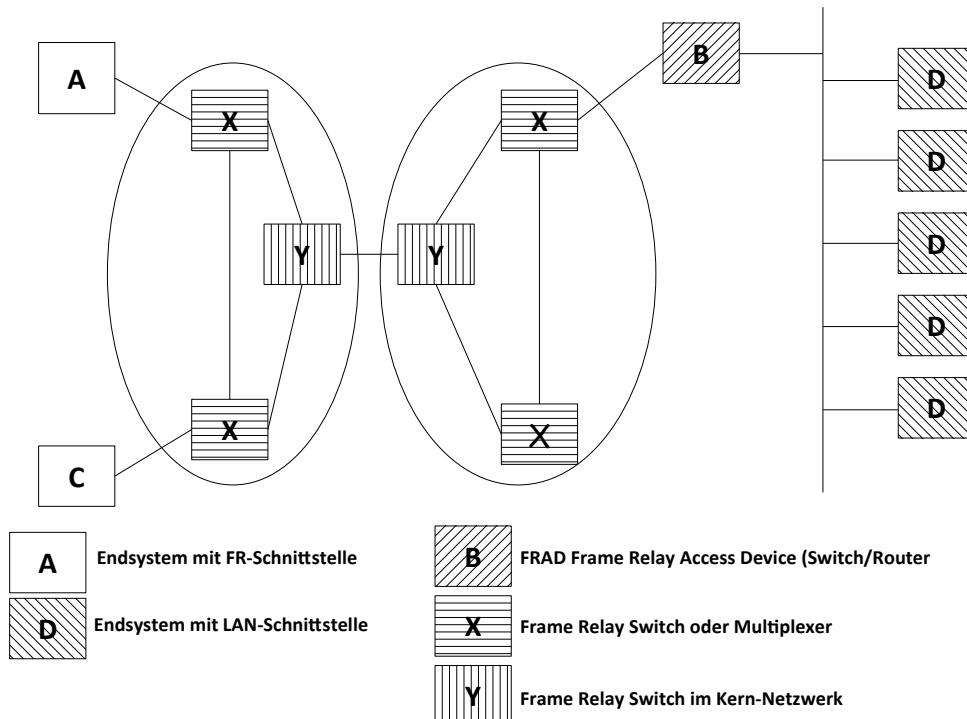


Abbildung 285: Frame Relay Netz-Aufbau

18.5.3 - ISDN

Integrated Services Digital Network integriert verschiedene Dienste wie Sprach-, Daten- und Bildkommunikation in einem Netz.

ISDN stellt dem Anwender Kanäle mit je 63kbit/s zur Verfügung und nutzt dabei Übertragungsstrecken der PDH (Plesiochrone digitale Hierarchie)

B-ISDN (Breitband-ISDN) stellt dem Anwender 155 Mbit/s, unter Nutzung von Übertragungsstrecken der SDH (Synchrone digitale Hierarchie), zur Verfügung.

Für die Datenübertragung stehen zwei unterschiedliche Kanäle zur Verfügung:

- B-Kanal (Bearer Channel) für Nutzdaten
- D-Kanal (Data Channel) für die Signalisierung

Die Telefongesellschaften bieten zwei unterschiedliche Anschlusstypen an:

- BA (Basisanschluss) BRI (Basic Rate Interface), BRA (Basic Rate Access) oder S₀-Anschluss
 - ◆ 1 D-Kanal mit 16 kbps
 - ◆ 2 B-Kanäle mit 64 kbps

Hier können Telefon, Fax oder PC's angeschlossen werden.
- PMX (Primärmultiplex-Anschluss) PRI (Primary Rate Interface), PRA (Primary Rate Access) oder S_{2M}-Anschluss
 - ◆ 1 Signalkanal mit 64 kbps
 - ◆ 30 Datenkanäle mit 64 kbps

Verwendung findet dieser Anschlusstyp in Firmen zur Anbindung verschiedener LANS oder Telefonnetze größerer Unternehmen

18.5.3.1 - ISDN-Dienste

Zusätzlich zur Integration von Daten und Bildübertragung in das Telefonnetz werden viele Dienste ermöglicht.

Diese Dienste sind teilweise gesondert zu beantragen und zu bezahlen:

- Automatischer Rückruf bei besetzt
- Übermittlung der Tarifeinheiten
- Verbindung weiter vermitteln
- Anrufweiterschaltung bei besetzt
- Verzögerte Anrufweiterschaltung
- Direkte Ruf-Weiterschaltung
- Anzeige der Rufnummer von A bei B-Teilnehmer
- Unterdrückung der Anzeige der Rufnummer des Anruflenden
- Übermittlung der Zielrufnummer bei Rufumleitung an den Rufenden
- Konferenzschaltung bis zu 10 Teilnehmer
- Geschlossene Benutzergruppen
- Anklopfen bei belegter Leitung
- Durchwahl (bei Verwendung von TK-Anlagen kann bis zum Endteilnehmer durchgewählt werden)
- Halten einer Verbindung
- Identifizieren böswilliger Anrufer
- Mehrfach-Rufnummern (MSN = Multiple Subscriber Number)
- Anrufweiterschaltung von Nebenstellenanlagen
- Subadressierung (Zusätzliche Informationen werden beim Verbindungsaufbau mitgegeben)
- Umstecken am Bus (Bei aktiver Verbindung kann an einer anderen S₀-Dose weiter telefoniert werden)
- Parken einer Verbindung
- Reverse Charging (R-Gespräch)
-

18.5.3.2 - ISDN-Schnittstellen

Innerhalb von ISDN sind folgende Schnittstellen definiert worden.

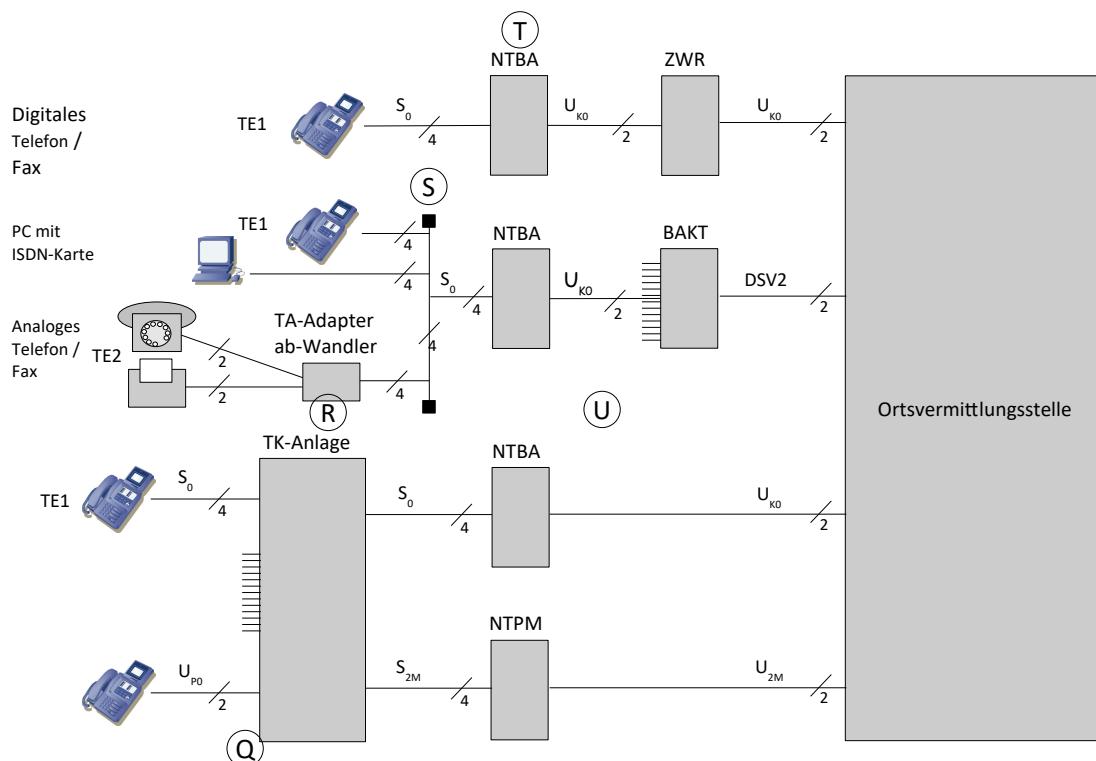


Abbildung 286: ISDN-Schnittstellen

TE = Terminal-Equipment

TE1 = ISDN-fähiges Endgerät

TE2 = Nicht ISDN-fähiges Endgerät

BAKT= Basisanschluß-Konzentrator

ZWR = Zwischenregenerator

NTBA = Network Termination Basic Access

NTPM = Network Termination Primary Multiplex

Die Endgeräte (TE) werden in ISDN-fähige (TE2) und nicht ISDN-fähige Geräte(TE1) unterschieden. Dies eröffnet die Möglichkeit alte analoge Endgeräte weiterhin zu betreiben. Dazu ist zwischen das analoge Endgerät und dem S₀-Bus ein TA-Adapter (a/b-Wandler) einzubauen. Allerdings sind dann die zusätzlichen Dienste, die ISDN bietet nicht, oder nur teilweise nutzbar.

Für die unterschiedlichen Schnittstellen hat man folgende Bezugspunkte eingeführt:

- Q = Referenzpunkt für die Verbindung von TK-Anlagen
- R = Damit ist ein Terminaladapter (a/b-Wandler) gemeint
- S = Hier wird der S₀-Bus beschrieben
- T = Diese Schnittstelle stellt die Trennlinie zwischen Telekom und privatem Haushalt in Deutschland dar.
- U = Hier sind unterschiedliche internationale Standards gültig.
- V = dies ist die Ortsvermittlungsstelle / Endvermittlungsstelle

Im NTBA können Prüfschleifen zur Ermittlung von Bitfehlerraten und einem ordnungsgemäßen Abschluss geschaltet werden.

Die T-Schnittstelle im NTBA kann auch so aufgefasst werden, dass der NTBA in zwei NT's (NT1 und NT2) aufgeteilt wird. Dies hätte z. B. eine Reihenfolge R – (TA) - S - (NT2) - T - (NT1) - U zur Folge.

18.5.3.3 - ISDN-S₀-Basisanschluss

Die Endeinrichtungen können wahlweise mit Strom- oder Spannungseinspeisung senden. D. h. jeder Sender regelt den eingespeisten Strom oder die eingespeiste Spannung in Abhängigkeit seiner Ausgangsspannung. Dadurch ist gewährleistet, dass die Spannung an jedem Senderausgang innerhalb gewisser Toleranzen bleibt, auch wenn mehrere Endeinrichtungen einen Impuls senden.

Die Senderausgänge und die Empfängereingänge sind immer hochohmig.

ISDN-Telefone brauchen keine eigene Stromversorgung. Sie können mit der Stromversorgung des NTBA betrieben werden. Da ein ISDN-Telefon (ohne Netzversorgung) im Normalbetrieb eine Leistungsaufnahme von max. 1 W hat, ein NTBA jedoch nur max. 4 W liefert, sind 4 Telefone an einem S₀-Bus zulässig. Weitere Geräte müssen eine eigene Stromversorgung haben.

Der S₀-Bus ist in 3 Ausprägungen möglich:

- Kurzer passiver Bus
- Verlängerter passiver Bus
- Punkt-zu-Punkt-Verbindung

Jedes Endgerät ist mit einer bis zu 10 m langen Anschlussleitung an die Anschlussdose anzuschließen.

Bei einer Punkt-zu-Punkt-Verbindung ist eine maximal 25m lange Anschlussleitung mit max. 6 dB Gesamtdämpfung erlaubt.

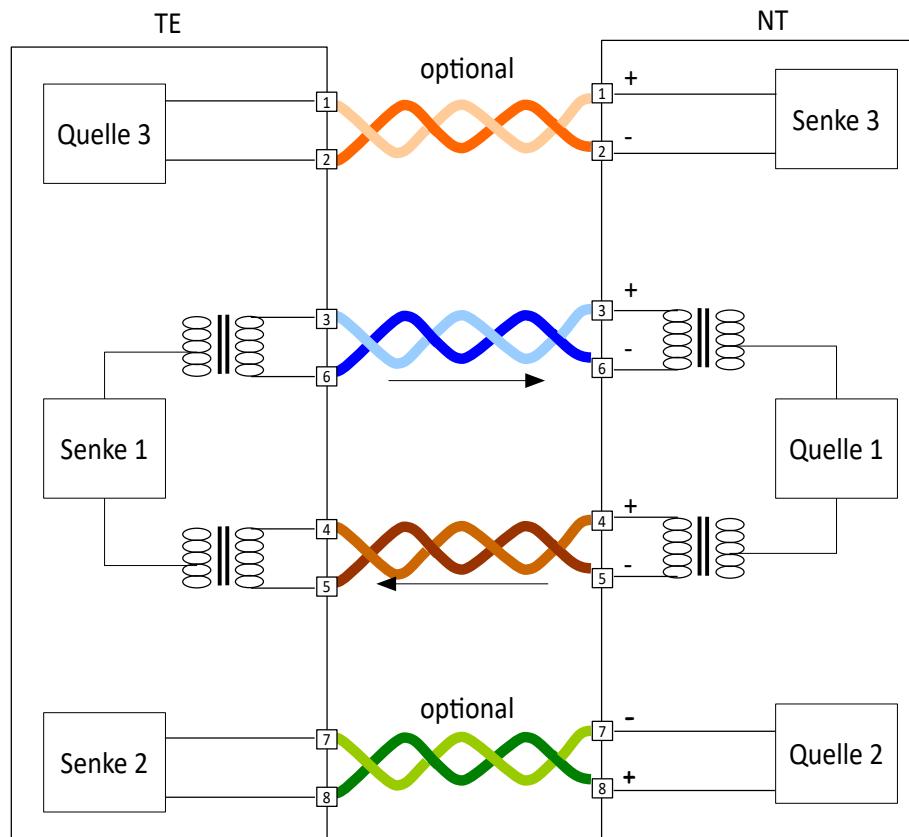


Abbildung 287: S₀-Bus-Aufbau

18.5.3.4 - Kurzer Passiver Bus

Bei diesem Bus können die Endgeräte an jeder beliebigen Stelle angeschlossen werden. Maximal sind 12 Anschlussdosen möglich. Es dürfen maximal 8 Endgeräte gleichzeitig angeschlossen sein. 4 Geräte können für den Dienst X.31 genutzt werden. Bei X.31 können 9,6 kbit/s über den D-Kanal übertragen werden.

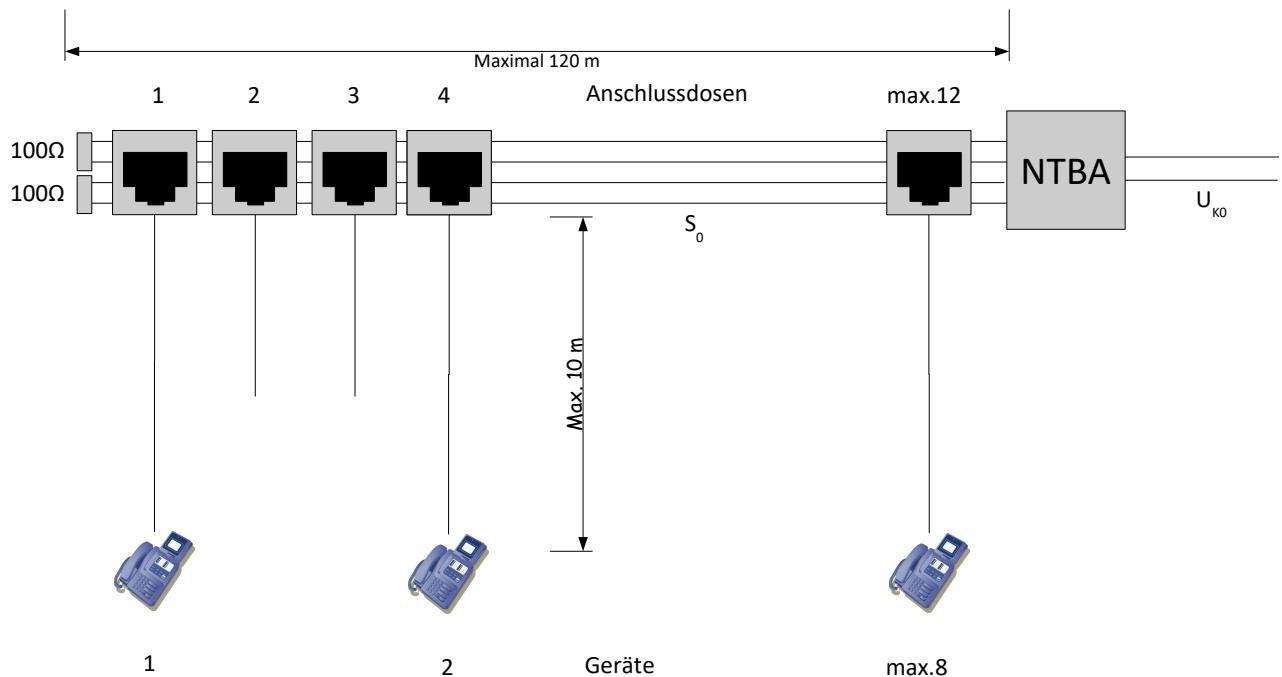


Abbildung 288: So-Bus (kurz)

18.5.3.5 - Erweiterter Passiver Bus

Bei diesem Bus können die Endgeräte an jeder beliebigen Stelle angeschlossen werden. Maximal sind 8 Anschlussdosen möglich. Es dürfen maximal 4 Endgeräte gleichzeitig angeschlossen sein. Die erste Dose darf maximal 50 m vom Abschlusswiderstand entfernt sein. Auf den letzten 30-50 Metern dürfen maximal 8 Anschlussdosen installiert sein. 4 Geräte können für den Dienst X.31 genutzt werden.

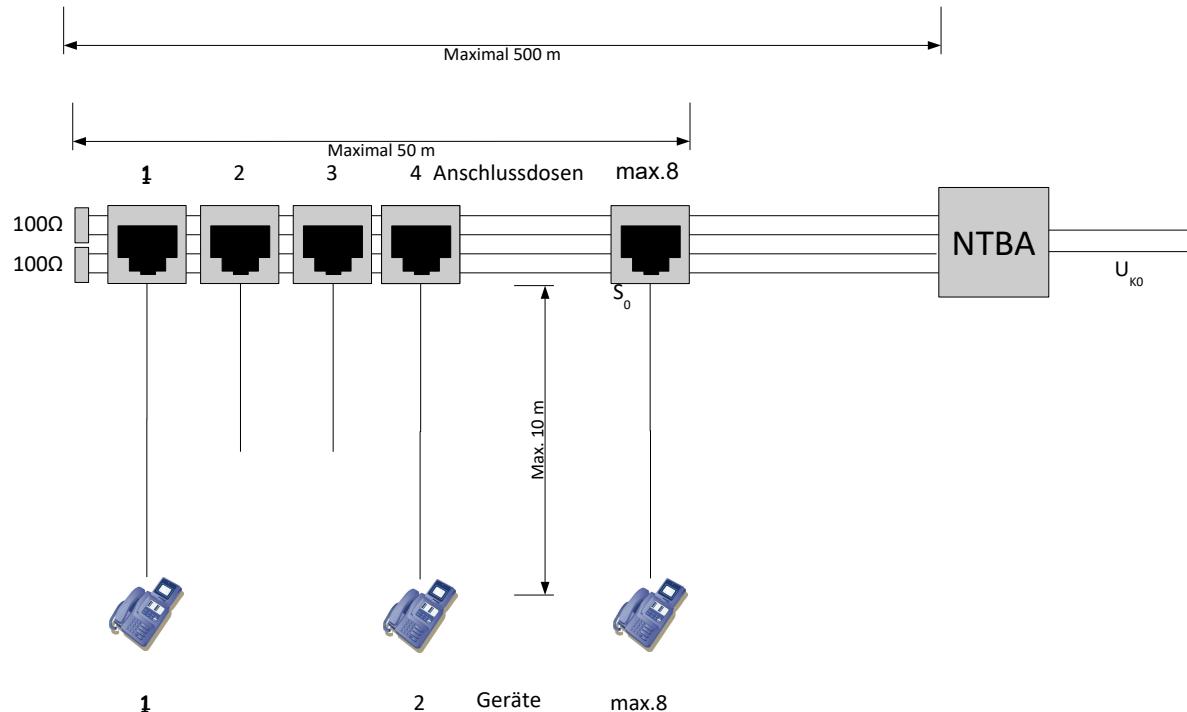


Abbildung 289: SO-Bus (erweitert)

18.5.3.6 - Punkt-zu-Punkt-Verbindung

Ist nur ein Endgerät an den NTBA angeschlossen, spricht man von einer Punkt-zu-Punkt-Verbindung. Diese muss beim Netzbetreiber extra bestellt werden. Im allgemeinen wird eine TK-Anlage so angeschlossen.

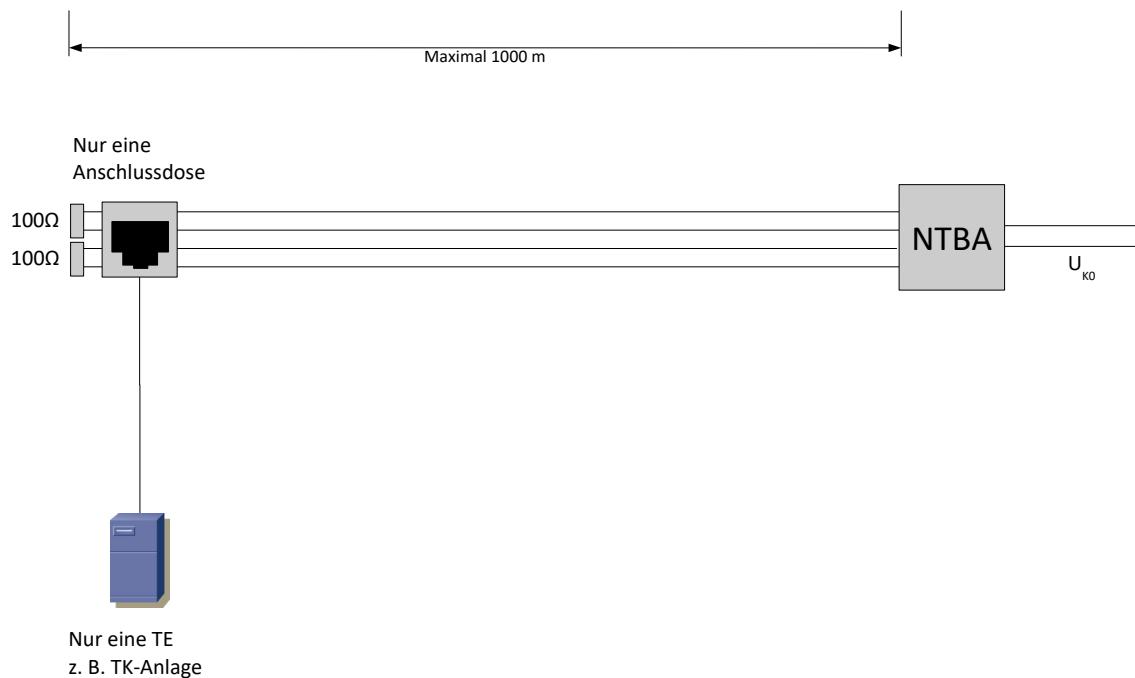


Abbildung 290: SO-Bus (Punkt zu Punkt)

18.5.3.7 - Externer und interner S₀-Bus

Es gibt TK-Anlagen, die an den externen S₀-Bus der vom NTBA gespeist wird angeschlossen werden. Sobald diese TK-Anlage wiederum einen weiteren, internen S₀-Bus bedient, können an diese TK-Anlage wiederum ISDN-Telefone angeschlossen werden. Solange über den internen S₀-Bus kommuniziert wird fallen keine externen Kosten an. Erst wenn über die TK-Anlage nach außen telefoniert wird, fallen Kosten an.

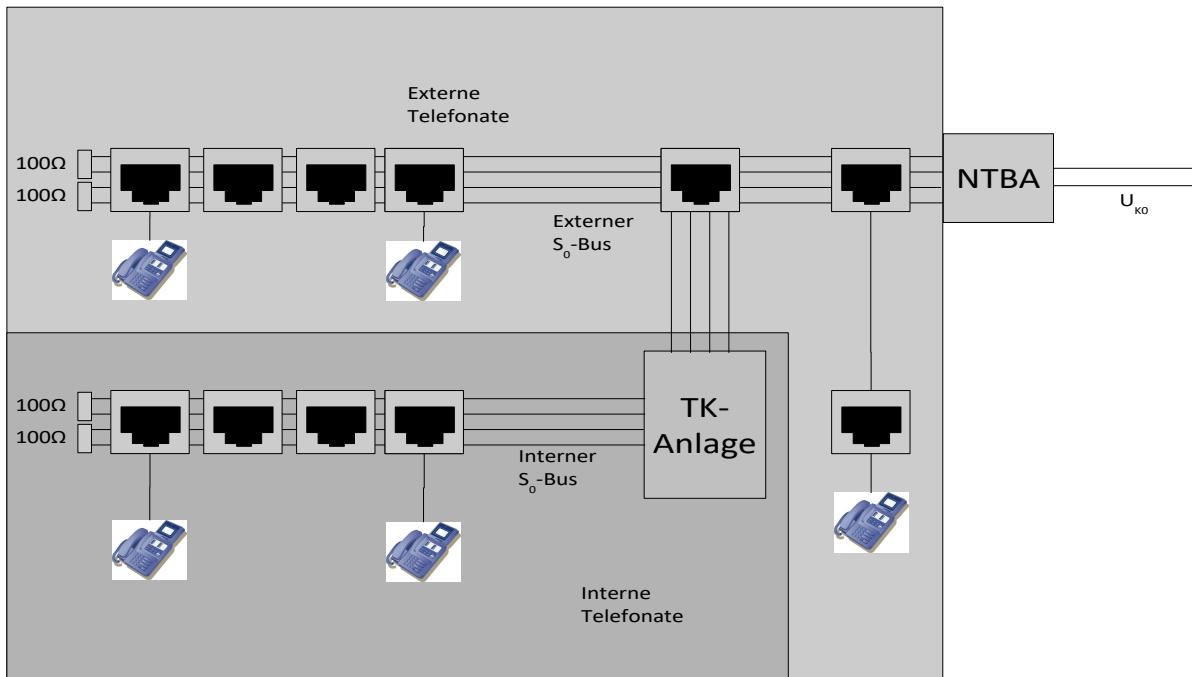


Abbildung 291: interner / externer S₀-Bus

Die Anzahl der Endgeräte am internen Bus ist von der TK-Anlage abhängig.

Die TK-Anlagen haben teilweise den Vorteil der integrierten a/b-Wandler.
Damit lassen sich an der TK-Anlage alte analoge Endgeräte weiter betreiben.

18.5.3.8 - S₀-Rahmenaufbau

Alle Teilsignale (Signalisierung Nutzkanäle und Steuerinformationen) sind im Zeit-Multiplex zusammengefasst. Das D-Bit ist das Rahmen-Synchronisationsbit. Innerhalb eines S₀-Rahmens werden für jeden B-Kanal 2 * 8 Bit übertragen.

Leitungssignal: 192 kbit/s

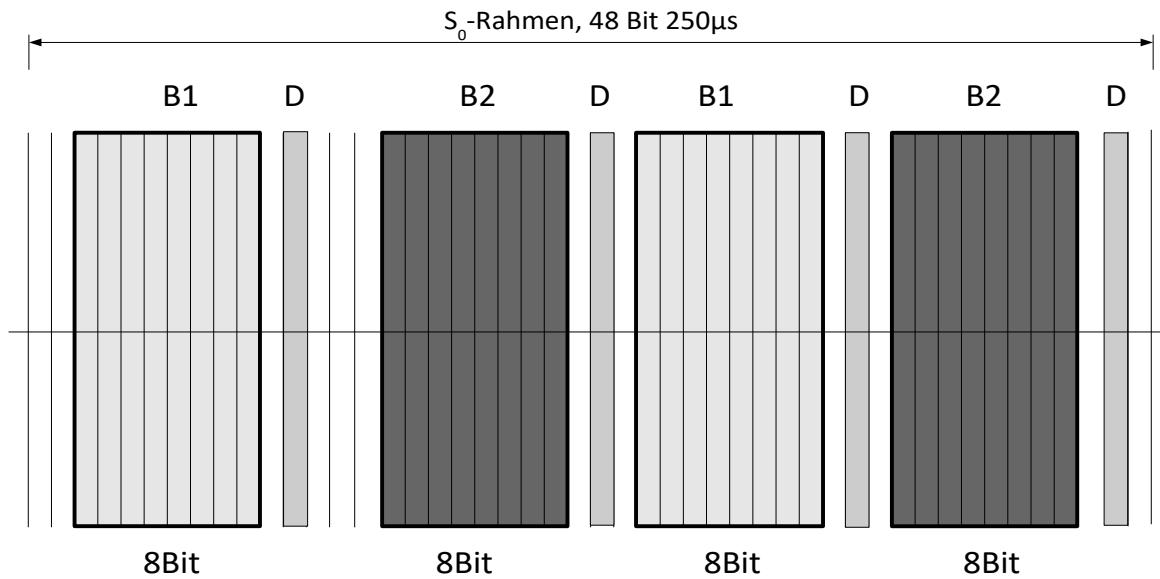


Abbildung 292: S₀-Rahmenaufbau

Es wird ein modifizierter AMI-Code mit 100% Impulsbreite verwendet.

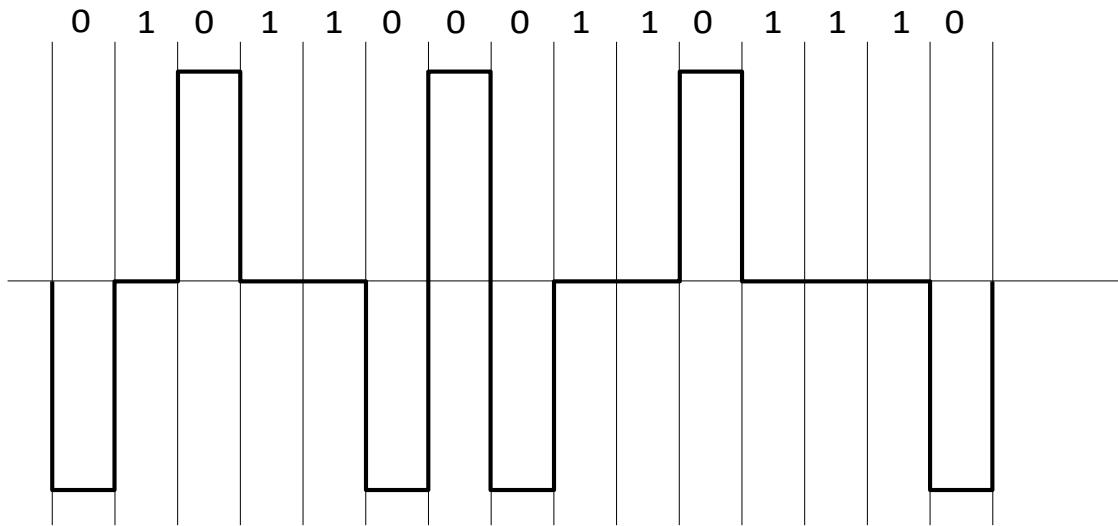


Abbildung 293: Modifizierter AMI-Code

Dieser Code macht die Kollisionserkennung und somit die verwendeten Zugriffsprozeduren möglich.

In Sende- und Empfangsrichtung werden alle Steuer und Nutzsignale im Zeitmultiplex zu einem Rahmen mit 48 Bit zusammengefasst. Dieser Rahmen wird 4000 mal in der Sekunde übertragen. Daraus ergibt sich die Bitrate von 192 kbit/s.

Der Rahmen TE->NT ist um 2 Bit gegenüber dem Rahmen NT->TE verzögert.

18.5.3.9 - Kollisionserkennung

In den Nutzkanälen sendet jeweils nur eine Endeinrichtung zur Zeit. Dies wird durch die Vermittlungsstelle sichergestellt. Sie teilt über den Signalisierungskanal (D-Kanal) jedem der beiden Nutzkanäle nur eine Endeinrichtung zu. Da es sich um einen Bus handelt ist durch eine Zugangsprozedur sichergestellt, dass die Endgeräte sich nicht gegenseitig stören wenn sie auf den Signalisierungskanal zugreifen. Dazu wird der Echo-Kanal (E-Bits) NT->TE verwendet. Der NT spiegelt die von TE->NT empfangenen D-Bits zurück. Jede Endeinrichtung hört auf diesen Kanal und kann daraus diverse Informationen ableiten.

Eine Endeinrichtung sendet nur dann im D-Kanal, wenn eine bestimmte Anzahl von aufeinander folgenden logischen Einsen (Nullpegel) im Echo-Kanal erkannt wurde. Die Anzahl der Bits ist abhängig von der Übertragung. Im Normalfall wird vor dem Aussenden von Signalisierungsinformationen acht Einsen abgewartet. Hat eine Endeinrichtung einen Rahmen erfolgreich ausgesendet wartet sie neun aufeinander folgenden Einsen ab. Dadurch haben alle Endeinrichtungen die Möglichkeit auf den Bus zuzugreifen. Paketdaten, die über den D-Kanal gesendet werden sollen, werden mit einer niedrigen Priorität gesendet. Deshalb wartet die Endeinrichtung 10 Einsen ab bevor sie ihre Daten über den D-Kanal sendet. Durch die niedrige Priorität der Daten auf dem D-Kanal ist sichergestellt, dass die Signalisierungsinformationen bevorzugt behandelt werden.

Das Sicherungsprotokoll (Schicht2) sorgt dafür, dass acht aufeinander folgende Einsen (Ruhesignal) in den Informationsblöcken nicht vorkommen.

Während des Sendens prüft jede Endeinrichtung, durch Vergleich des ausgesendeten Signalisierungs-bits, mit den gespiegelten E-Bits, ob noch andere Endeinrichtungen aktiv auf den D-Kanal zugreifen. Aufgrund der elektrischen Festlegungen setzen sich Stationen die eine logische Null senden (Impuls) gegen Stationen die eine logische Eins (Nullpegel) senden durch. Endeinrichtungen die eine logische Eins gesendet haben und auf dem Echokanal eine logische Null empfangen, erkennen eine Kollision und hören mit dem Senden sofort auf.

Das Sicherungsprotokoll gewährleistet, dass sich Informationsrahmen von zwei verschiedenen Endeinrichtungen, auch bei gleichem logischen Inhalt, unterscheiden.

Endeinrichtungen, die eine Kollision erkennen, warten bis der D-Kanal wieder frei ist und senden anschließend den Informationsrahmen erneut.

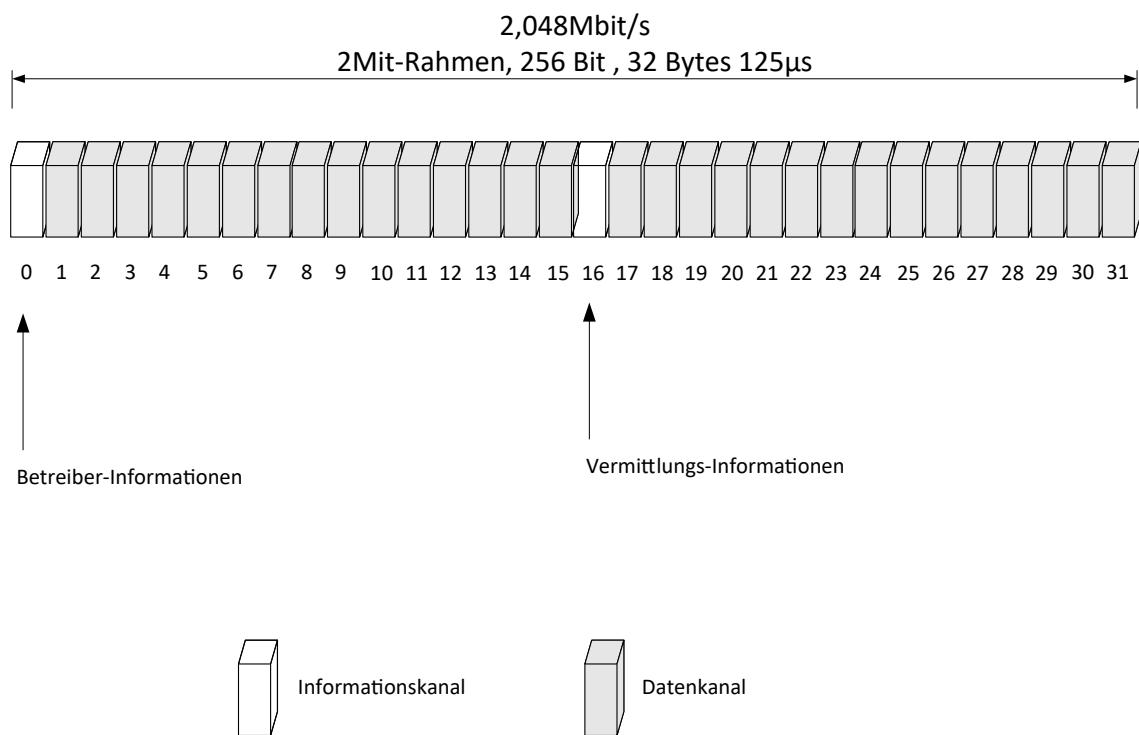
18.5.3.10 - ISDN-S_{2M}-Primary Rate Interface

Abbildung 294: S2M-Rahmen

Die Nettobitrate beträgt im strukturierten Betrieb 1,920Mbit/s. Dies entspricht 30 Kanälen anstelle von 32 Kanälen mit jeweils 64 kbit/s. Zwei Kanäle werden zur Übermittlung von Steuerungs-Informationen belegt (Kanal 0 und 16).

Durch Bündelung (Bonding) können mehrere Datenkanäle zu einem Kanal größerer Bandbreite zusammen gefasst werden.

18.5.4 - xDSL

DSL (Digital Subscriber Line; deutsch: digitale Teilnehmer-Anschlussleitung) bietet gegenüber ISDN eine höhere Datenrate obwohl die selben Kupfer-Doppeladern verwendet werden. Das x steht für unterschiedliche Varianten:

18.5.4.1 - ADSL

Asymmetric DSL. In diesem Zusammenhang bedeutet asymmetrisch, dass die Download-Seite eine höhere Datenrate als die Upload-Verbindung hat.

Bei diesem Verfahren ist ein ungestörter Telefondienst auf der selben Leitung auch dann noch möglich wenn das DSL-Modem ausfällt. Dies wird durch den Splitter ermöglicht, der den Frequenzbereich des POTS (Plain Old Telephone Service) durch einen Frequenzfilter, auf eine separate Telefonschnittstelle führt.

18.5.4.2 - HDSL

HDSL (High Bit Rate DSL) ist die älteste Variante mit einer symmetrischen Übertragung. Bei diesem Verfahren ist nur der Datentransport vorgesehen.

18.5.4.3 - SDSL

Die Symmetric DSL wird auch als Single Pair DSL bezeichnet. Es wird nur ein Adernpaar benötigt, dafür ist jedoch die Leistung eingeschränkt.

18.5.4.4 - UADSL

Universal ADSL ist eine ADSL-Variante die ohne die aufwändigen Splitter auskommt.

18.5.4.5 - VDSL

Very High Bit Rate DSL bietet sehr große Bitraten über kurze Distanzen. Es ist ein asymmetrischer sowie ein symmetrischer Betrieb möglich.

18.5.4.6 - Vergleich der unterschiedlichen DSL-Varianten

Beider Beurteilung der Varianten ist zu beachten, dass die Datenraten und die Distanz umgekehrt proportional zueinander stehen.

	ADSL	HDSL	SDSL	VDSL
Bedeutung	Asymetric DSL	High Data Rate DSL	Symmetric DSL	Very High Data Rate DSL
Datenrate Upstream	16-640 kbit/s	1,544 bzw. 2,048 Mbit/s	1,544 bzw. 2,048 Mbit/s	1,5 – 2,3 Mbit/s
Datenrate Downstream	64 kbit/s - 8,192 Mbit/s	1,544 bzw. 2,048 Mbit/s	1,544 bzw. 2,048 Mbit/s	13 – 52 Mbit/s
Leitungslänge	2,7 – 5,5 km	3 - 4 km	2 – 3 km	0,3 – 1,5 km
Aderpaare	1	2 bei 1,544Mbit/s 3 bei 2,048Mbit/s	1	1
Belegte Bandbreite	ca. 1MHz	ca. 240 kHz	ca. 240 kHz	ca. 30 MHz
Telefon- Übertragung möglich ?	Analog	Nein	Analog	Analog und ISDN

18.5.4.7 - Übertragung von POTS / Uplink / Downlink

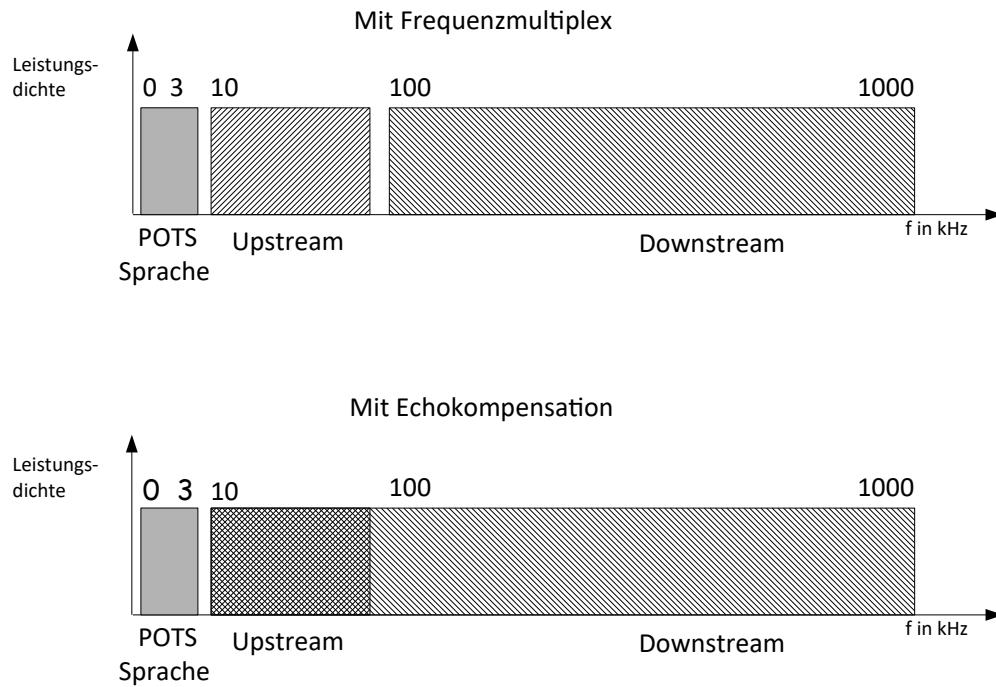


Abbildung 295: DSL-Frequenzbereiche

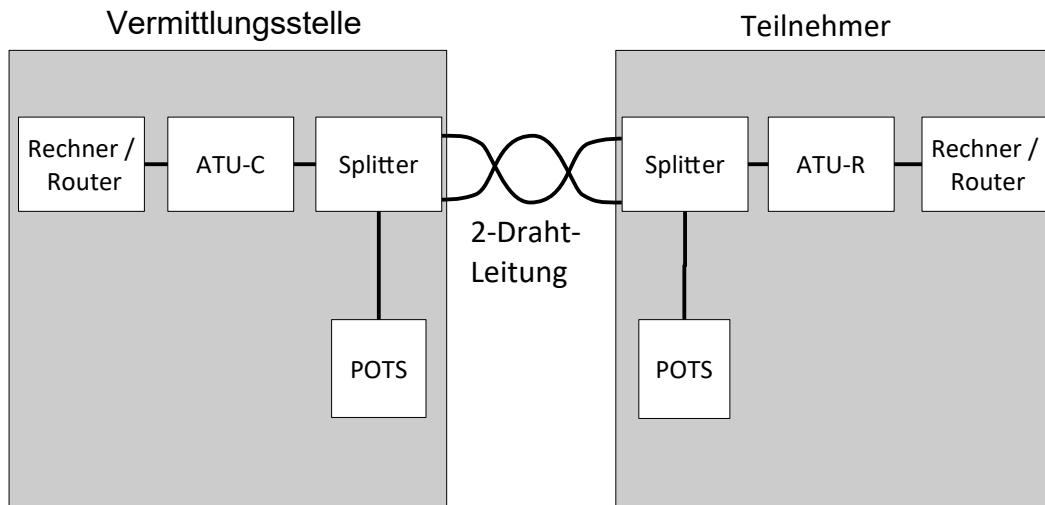
Auf xDSL-Anschlüssen wird eine Vollduplex-Verbindung gewünscht. Dazu kann, wie bei den Modems Modulation, Echounterdrückung oder Frequenz-Multiplex eingesetzt werden. Da parallel dazu noch eine Sprachübertragung (POTS = Plain Old Telephone Service) gewünscht ist, wird Frequenz-Multiplex mit oder ohne Echounterdrückung eingesetzt.

Bei ADSL wird eine Modulation ähnlich wie bei V.34 verwendet. Dabei ist die Abtastrate jedoch 4000 Baud anstelle 2400 Baud. Die Leitungsqualität wird kontinuierlich überwacht und die Datenübertragungsrate dementsprechend angepasst. Bei ADSL werden 256 Kanäle mit je 4 kHz Bandbreite verwendet.

18.5.4.8 - ADSL-Aufbau

Der Aufbau einer ADSL-Verbindung benötigt einen Splitter und ein Modem.

Der Splitter ist ein Frequenzfilter der den Telefondienst bzw. ISDN abtrennt. Damit bleibt dieser Dienst auch bei Ausfall des Modems verfügbar. Früher wurde das Modem von der Telekom zur Verfügung gestellt. Mittlerweile ist das Modem zu bezahlen. Aus diesem Grund gibt es Hersteller die das Modem in einem ADSL-Router bereits integriert haben.



ATU = ADSL Terminal Unit (ADSL-Modem)

C: Central Office; R: Remote

POTS = Plain Old Telephone Service bzw. ISDN

Abbildung 296ADSL-Aufbau

18.5.5 - MPLS

18.5.5.1 - Einführung

Das Multi Protocol Label Switching (MPLS) ist in den RFCs 3031 (MPLS Architecture) und 3032 (Label Stack Encoding) beschrieben. Für MPLS-VPNs gibt es noch die RFCs 2541 und 2917.

Routinglisten wurden von den Routern, als MPLS entwickelt wurde, noch mit Software, also mit der CPU nach dem Prinzip des Longest-Prefix-Matching von IP-Adressen durchsucht, was bei langen Routinglisten wesentlich rechenintensiver und damit zeitaufwändiger ist. Die ursprüngliche Intension von MPLS war die Router beim IP-Forwarding also dem Routen, zu entlasten.

Anstelle von aufwändigem Suchen in großen Routinglisten wurde in die Pakete ein Label mit einer Länge von 32 Bit vor dem IP-Header integriert. Damit kann die Wege-Entscheidung wesentlich schneller erfolgen.

Mittlerweile können Routinglisten mit ASICs, also mit Hardware, untersucht werden, was den Geschwindigkeitsvorteil von MPLS relativiert. MPLS bietet jedoch noch weitere Funktionen, die einen Einsatz sinnvoll erscheinen lassen.

18.5.5.2 - Funktionsweise

MPLS ermöglicht die verbindungsorientierte Kommunikation über verbindungslose Netzwerke und wird oft mit ATM oder Frame Relay verglichen, da auf einer mehrfach genutzten Infrastruktur getrennte logische Pfade etabliert werden können. MPLS wird auch als Layer-2.5-Protokoll bezeichnet, da es einerseits auf Layer-2 aufsetzt, jedoch Layer-3-Dienste wie IP benötigt. Im Falle von MPLS können die Router parallel auch noch andere Protokolle, für weitere Verbindungen, bearbeiten. Bei ATM oder Frame Relay werden die Geräte ausschließlich für ATM oder Frame Relay genutzt.

Sobald ein IP-Paket eine MPLS-Domäne erreicht wird es zunächst klassifiziert. Dabei wird es einer Forwarding Equivalence Class (FEC) zugeordnet. FECs sind ein abstraktes Konzept zur Beschreibung von Mengen von Paketen. Jede FEC wird auf die gleiche weise bei der Weiterleitung behandelt. Eine FEC kann unterschiedliche Kriterien beschreiben. Hierbei sind Quell- und Ziel-IP-Adressen, TOS des folgenden IP-Headers, Paketgröße oder Portnummern höherer Schichten wie TCP oder UDP denkbar.

Damit repräsentiert das Label die FEC. Da es mehrere unterschiedliche FECs geben kann, können die FECs, und damit die Labels, gestackt werden. Bei der Paketbearbeitung im Router wird immer nur das vorderste Label bearbeitet, bis die das Paket den FEC-Gültigkeitsbereich verlässt. Dann wird das vorderste Label gelöscht und das nächste Label verwendet. Dies geht so lange bis das letzte Label (gekennzeichnet mit dem Bottom-Of-Stack-Bit =1) erreicht ist. Beim Verlassen des letzten FEC-Gültigkeitsbereichs wird auch die MPLS-Domäne verlassen. Während des Transports eines MPLS-Pakets wird immer nur das vorderste Label vom Router bearbeitet. Dabei tauscht er das Label aus und gibt das Paket an den zuständigen Nachbarn weiter.

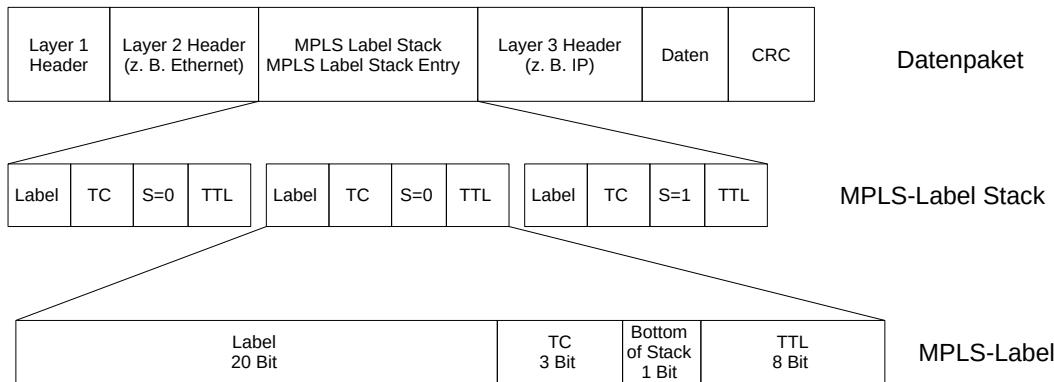


Abbildung 297: MPLS-Tag

MPLS fügt an den Grenzen der MPLS-Domäne, an den so genannten AS-Boundary-Routern den MPLS-Label-Stack ein (Push-Operation), bzw. entfernt ihn wieder (Pop-Operation). Der Label-Stack wird auch Shim-Header (dt. Zwischenlegescheibe) genannt, was ein Hinweis auf die Kürze des Labels mit 32 Bit ist.

Bedeutung der MPLS-Header-Felder:

- Das 20 Bit große Label kennzeichnet den LSP (Label Switched Path) und gilt jeweils nur für eine Weiterleitung, also zwischen 2 Routern.
- Das TC-Feld (Traffic-Class) wird im RFC5462 beschrieben. Damit kann es mittels einer Differentiated Services Information zur Sicherstellung einer Dienstgüte verwendet werden.
- Das Bottom-of-Stack-Bit wird dazu verwendet um auf weitere Labels hinzuweisen bzw. das letzte Label (mit 1) zu kennzeichnen.
- Die 8 Bit des TTL-Feldes (Time-To-Live) ermöglichen, dass 255 MPLS-Router eine Weiterleitung vornehmen. Danach wird das Paket verworfen. Das TTL-Feld eines enkapsulierten IP-Headers wird hierbei nicht beeinflusst.

Vor der Bearbeitung der Pakete müssen die LSPs (Label Switched Path) definiert werden. Die Festlegung kann manuell, halbautomatisch oder vollautomatisch erfolgen. Für die automatisierte LSP-Erstellung verwendet MPLS ein IGP-Routingprotokoll wie OSPF oder IS-IS. Bei der automatisierten Festlegung hat der Administrator keine Möglichkeit mehr einen Pfadoptimierung vorzunehmen. Er muss sich auf das Ergebnis des IGP verlassen.

Der Anfangsknoten eines LSPs ist der Ingress-Router, der Endknoten wird als Egress-Router bezeichnet. Sie werden auch als Label-Edge-Router (LER) bezeichnet. Die Router innerhalb der MPLS-ADomäne werden als LSR (Label Switched Router) bezeichnet.

Die Bedeutung der Label, also die Signalisierung, wurden von den Routern über das Label Distribution Protocol (LDP) einschließlich der Erweiterung CR-LDP ausgehandelt. RSVP-TE (Resource Reservation Protocol) wird beim Traffic-Engineering verwendet.

Darüber bekommt jeder Router eine Label-Tabelle, anhand der er die Weiterleitung der Pakete vornehmen kann. In der Tabelle wird für jedes Eingangslabel ein Ausgangslabel zugeordnet. Dies bedeutet, dass ein zentraler Steuerungsmechanismus nicht notwendig ist.

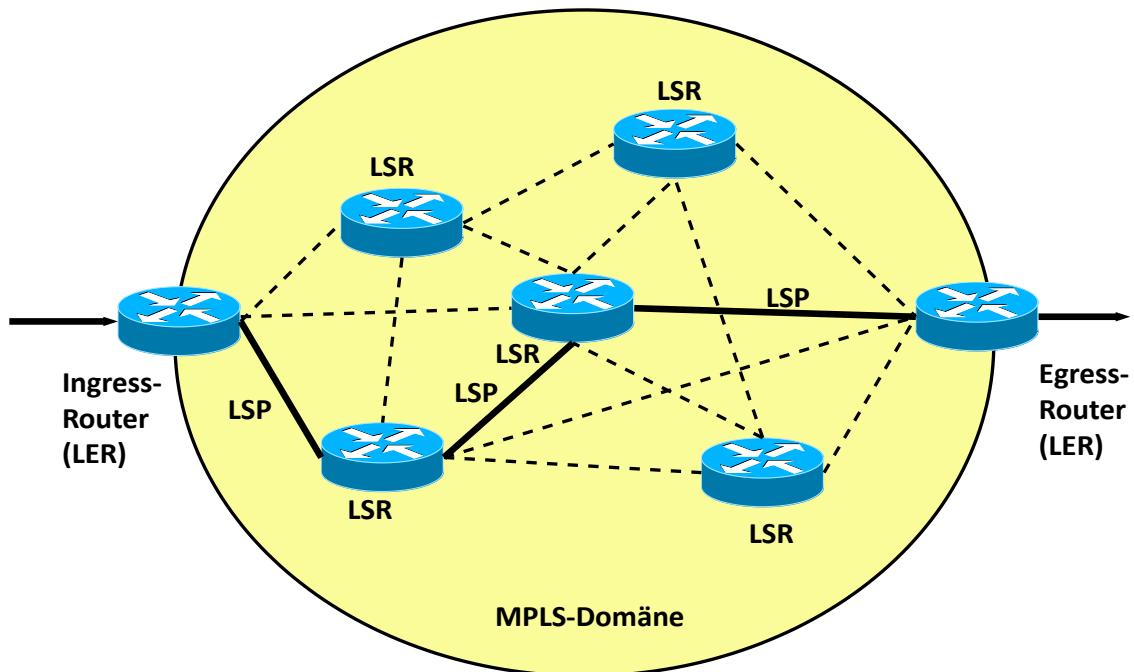


Abbildung 298: MPLS-Domäne

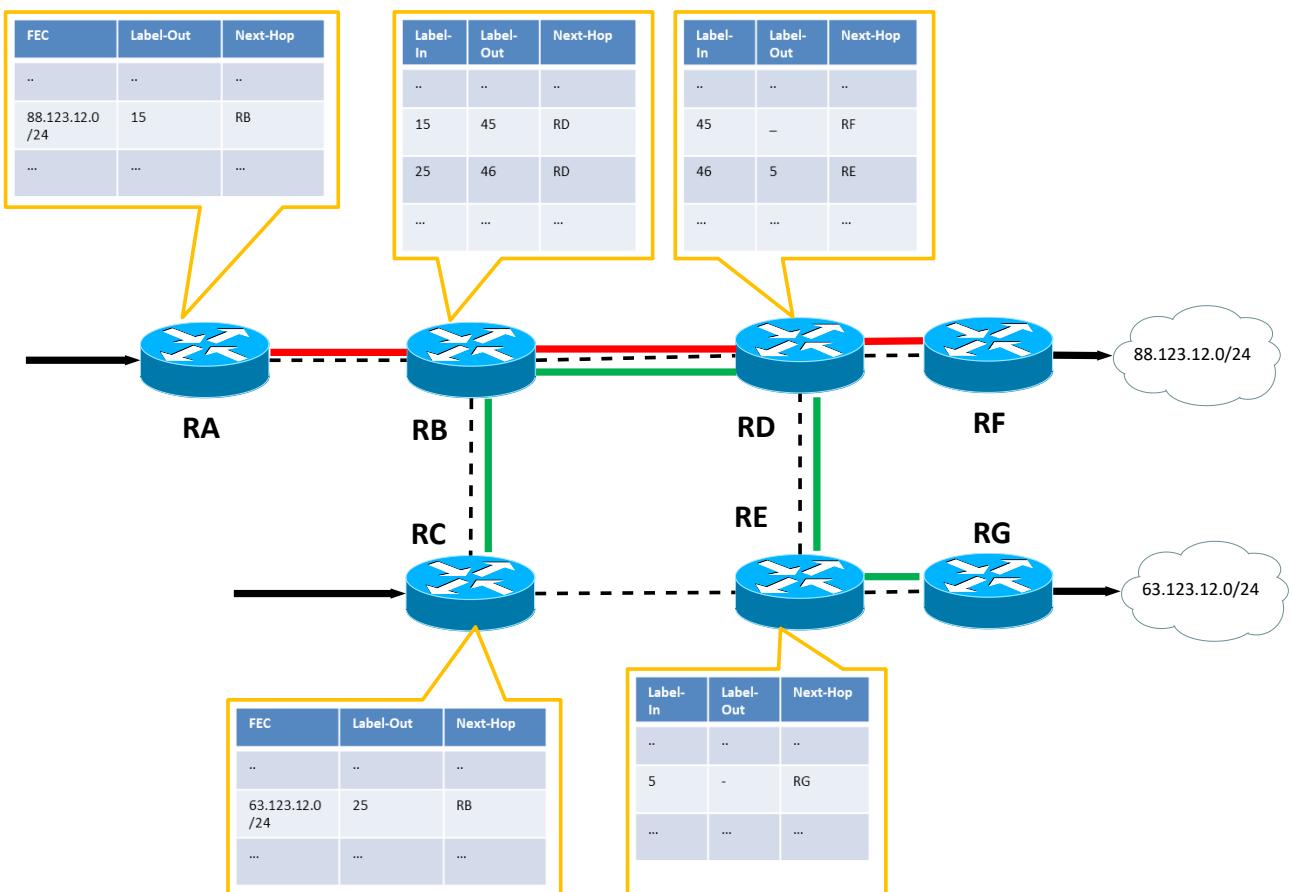


Abbildung 299: Paketweiterleitung unter MPLS

LSPs sind unidirektional. Das bedeutet, dass es für den Hinweg einen anderen Weg, als für den Rückweg geben kann. Die Weiterleitung von Paketen in den Routern, die so genannte Swap-Operation, erfolgt auf Layer-2 (Label-Swapping, also Austauschen/Ändern von Labeln) statt auf Layer-3 und ist damit schneller. Dabei wird das Label als Index in der Label-Tabelle verwendet, was den eigentlichen Geschwindigkeitsvorteil gegenüber einem Routing ausmacht. In der Tabelle wird auf die Forwarding-Information oder ein weiteres Label gezeigt. Wird auf ein weiteres Label gezeigt, wird das Label im Header ausgetauscht. (Swap-Operation)

Bei den LSPs kann bereits am vorletzten Router (PHP-Router) das MPLS-Label entfernt werden. Dieser Vorgang wird Penultimate Hop Popping (PHP) genannt. Da der PHP-Router den Weg zum Egress-Router kennt, kann er das MPLS-Label entfernen und damit die Pop-Operation ausführen. Der Egress-Router muss dann das Paket nur noch weiter leiten.

Neben der Paketbehandlung sind noch weitere Funktionen zugesagt, diese können in die MPLS-Services unterteilt werden.

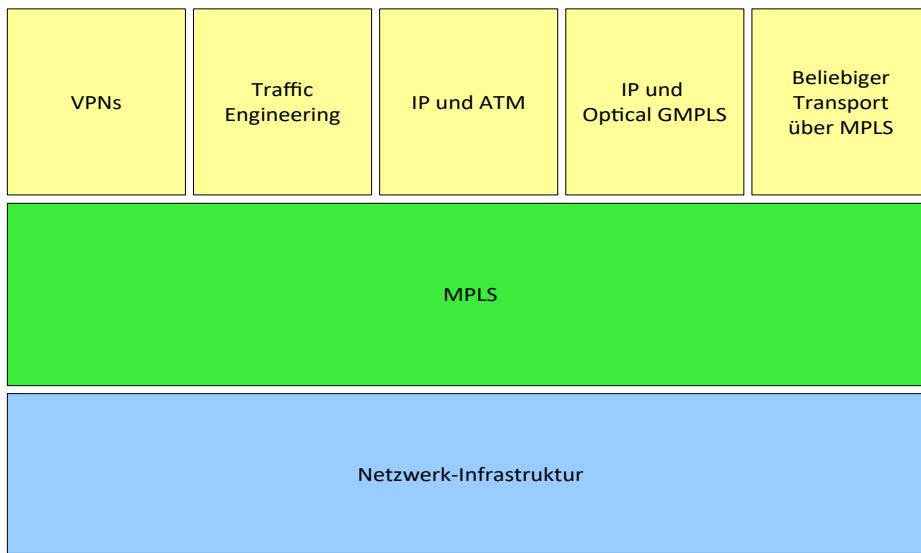


Abbildung 300: MPLS-Dienste

MPLS kann auf unterschiedlichen Infrastrukturen aufgesetzt werden. Es ist sowohl Ethernet als auch ATM und Frame Relay möglich. Die VPN-Funktionalität soll hier im Folgenden beschrieben werden.

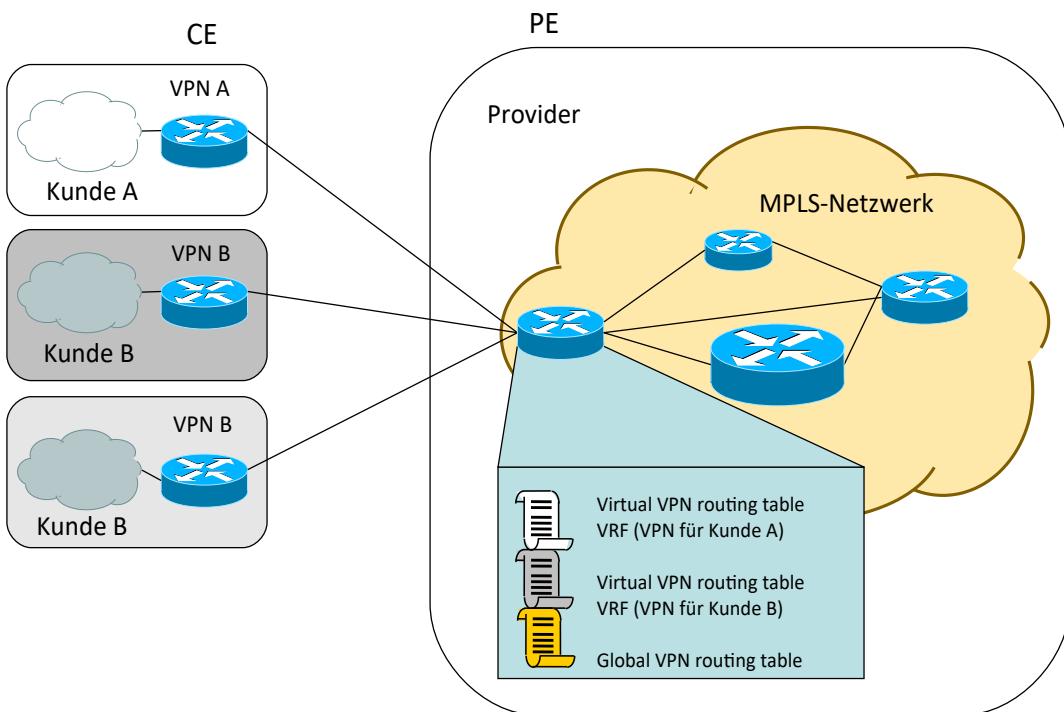


Abbildung 301: MPLS-Übersicht

Zunächst wird in Provider-Netz und Kunden-Netz unterschieden.

Die Anbindung auf der Providerseite wird mittels eines Provider Edge Device (PE) durchgeführt. Die PEs ermitteln im Vorfeld der Datenübertragung die Routen im Netzwerk. Trifft ein Paket von der Kundenseite her ein, wird ein Label eingefügt. Im Provider-Netzwerk wird von den Label Switched Routern (LSR) anhand des Labels und nicht aufwändig mittels einer Routingtabelle entschieden wie weiter geleitet werden soll.

Ein PE hat für die MPLS-Funktionalität eine „Globale Routingtabelle“. Für jeden Kunden gibt es noch weitere Tabellen, die so genannten Virtual Routing and Forwarding Instances (VRFs). Mit diesen Tabellen werden die Kunden-VPNs veraltet. Da für jeden Kunden eine eigenen VRF geführt wird ist es sogar möglich, dass unterschiedlichen Kunden den gleichen IP-Addressraum nutzen.

Die PEs tauschen sich über die angebundenen Kunden aus. Dabei werden die dem jeweiligen Kunden zugeordneten Präfixes (also die Kunden-Netze) mitgeteilt. Dazu verwenden die PEs das Multiprotocol BGP (MP-BGP). Es handelt sich hierbei um eine Erweiterung des Border Gateway Protocol (BGP). Die propagierte Information lautet: Über mich (PE) kann mit folgendem Label dieses oder jenes Präfix (Netz) von diesem oder jenem Kunden erreicht werden. Es sind natürlich mehrere VPNs für einen Kunden möglich.

Im Kunden-Netzwerk ist keine Funktionalität bezüglich MPLS sichtbar. Auf der Kundenseite wird für die Anbindung ein Customer Edge Device verwendet. (CE)

18.5.5.3 - VPN-Funktion

Im PE wird jedem Kunden-Netz, mithilfe eines Route Distinguisher , ein Label zugeordnet.

Das Triple, bestehend aus dem Route Distinguisher, Netz-Präfix und dem zugehörigen Label wird über MP-BGP propagiert.

Damit weiß jeder PE, welches Kunden-Netz von welchem PE erreicht werden kann und welches Label hierfür zu verwenden ist.

Sobald ein PE von einem CE ein Paket erhält, wird es um mindestens zwei Labels erweitert.

19 - Netzwerk-Komponenten

19.1 - Einleitung

Für die unterschiedlichsten Einsatzzwecke wurden Geräte entwickelt deren Eigenschaften im Folgenden beschrieben sind. Oft wurden neue Entwicklungen vorangetrieben um Probleme, die durch immer größer werdende Netzwerke entstehen, zu beheben. Deshalb werden an dieser Stelle zuerst die Prämissen, unter denen die Geräte entwickelt werden, genannt.

Bei der Datenübertragung sind viele Randbedingungen wichtig:

- ➊ Dämpfungsprobleme, die letztendlich Längenprobleme erzeugen können.
- ➋ Begrenzung der Anzahl der Teilnehmer auf einem Netzsegment.
- ➌ Räumliche Trennung
- ➍ Logische Trennung
- ➎ Lastprobleme
- ➏ Antwortzeiten
- ➐ Kollisionen
- ➑ Sicherheit
- ➒ Management

Für jedes dieser Probleme gibt es ein Heilmittel. Je nach Problem werden die Komponenten eingesetzt. Im Folgenden wird von den Geräten zur Problembehebung die Rede sein.

19.2 - Repeater



19.2.1 - Einleitung

Ein Repeater (grob übersetzt: Wiederholer) ist nichts anderes als ein dummer Verstärker. Mit ihm kann ein durch Dämpfung abgeschwächtes Signal aufgefrischt und dadurch ein Netzwerk-Segment verlängert werden. Er besitzt keine Intelligenz.



Bei 100MB-Netzen gibt es zwischenzeitlich verschiedene Klassen:

Klasse	Bedeutung
I	Entspricht einem Media-Konverter. Es können unterschiedliche Medien miteinander verbunden werden. Z. B. kann 100Base-Tx mit 100Base-Fx verbunden werden. Ist somit langsamer als Repeater der Klasse II. Deshalb darf nur ein Repeater der Klasse I in einem abgeschlossenen Netz-Segment vorhanden sein!
II	Diese Repeater verbinden immer nur Ports mit dem gleichen Medium.

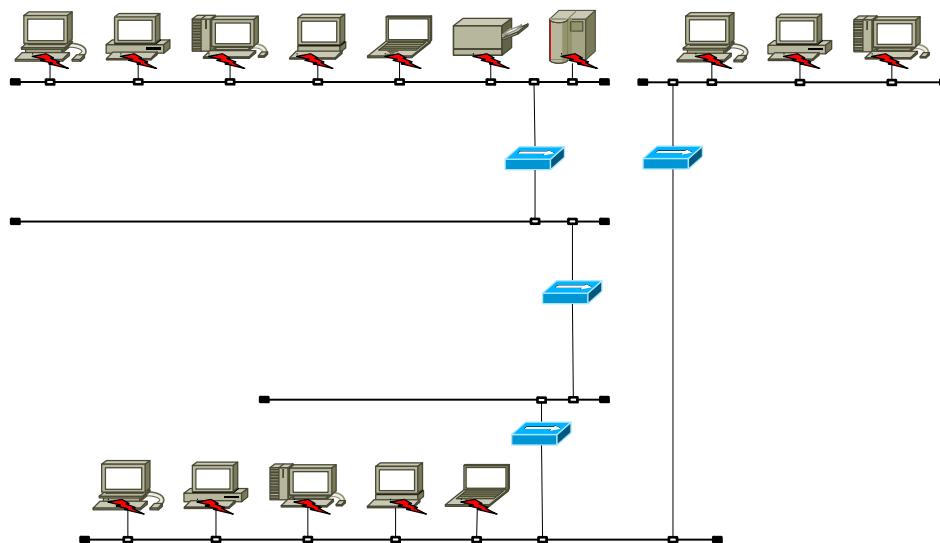


Abbildung 302 : Störung im Repeater-Netz

In einem mit Repeatern aufgebauten Netzwerk werden sämtliche Daten überall hin transportiert. Dies bedeutet aber auch, dass alle Kollisionen auf allen Netz-Segmenten auftreten können. Bei einem Netzwerk mit vielen Teilnehmern kann dies zu Problemen führen. Damit die Kollisionen auf kleinere Bereich eingeschränkt werden, sind die Repeaters durch Brücken oder Switches zu ersetzen. (Siehe nächste Kapitel)

19.2.2 - Ausprägungen von Repeatern

Es gibt 2 Ausprägungen von Repeatern, die je nach Verwendungszweck unterschieden werden.

19.2.2.1 - Local Repeater

Diese Repeater dienen nur zur Auffrischung des Signals. Damit können 2 Kupfer-LAN-Segmente miteinander verbunden werden.

19.2.2.2 - Remote Repeater

Diese Repeater dienen dazu größere Distanzen (bis maximal 1000m) zu überbrücken. Damit können 2 Kupfer-LAN-Segmente mit einer FOIRL (Fibler Optic Inter Repeater Link) Verbindung zusammen geschaltet werden.

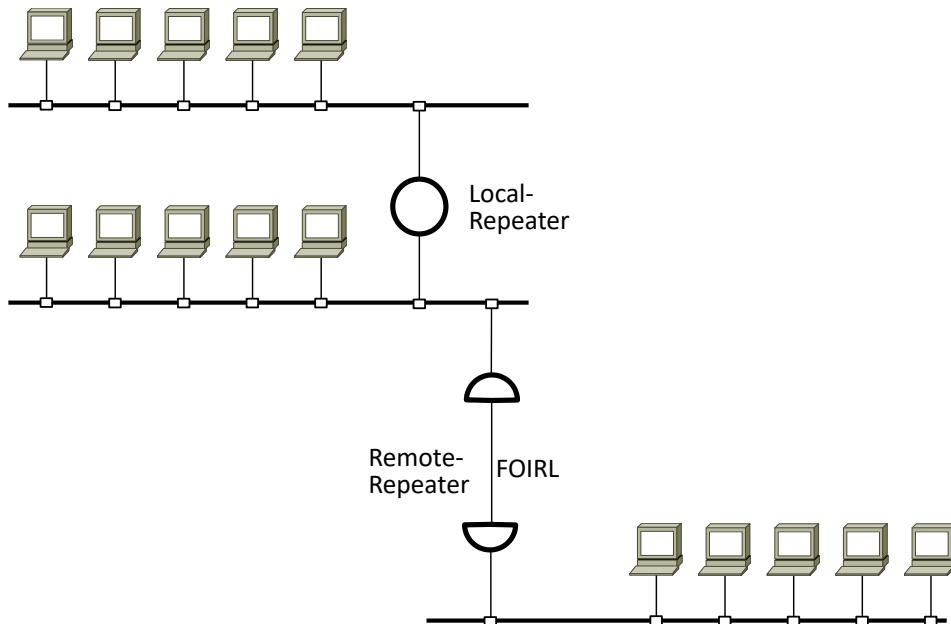


Abbildung 303: Local- und Remote-Repeater

19.2.3 - Repeater-Regeln für 10 Mbps

Max. 5 Segmente

Max. 4 Repeater zwischen zwei Endgeräten

Max. 3 gleichzeitig genutzte Segmente (an 3 Segmenten dürfen gleichzeitig Stationen betrieben werden)



19.2.4 - Repeater-Regeln für 100 Mbps

Max. 4 Segmente

Max. 3 Repeater zwischen zwei Endgeräten

Max. 2 gleichzeitig genutzte Segmente (an 2 Segmenten dürfen gleichzeitig Stationen betrieben werden)



19.2.5 - Sicherheitsmechanismen

Mittlerweile wurde auch den Repeatern ein gewisses Maß an Intelligenz eingebaut. Diese Intelligenz beschäftigt sich nicht mit den Rahmen, sondern mit den Problemen auf der Ebene 1.

19.2.5.1 - Auto Partitioning

Ausblenden / Stilllegen von Ports, auf denen eine Kollisionsanzahl pro Sekunde überschritten wird

19.2.5.2 - Scrambling

Bei dieser Funktion, die eigentlich den Switches vorbehalten ist, wird folgendermaßen vorgegangen:

- ➊ Repeater lernt alle MAC-Adressen an allen Ports.
- ➋ Nur Ports, die von Unicasts betroffen sind, werden mit Daten versorgt. Alle anderen erhalten Einsen. Somit kann sichergestellt werden, dass nur der berechtigte Empfänger und sonst niemand die Daten empfangen kann.

19.2.6 - Repeater im ISO-RM

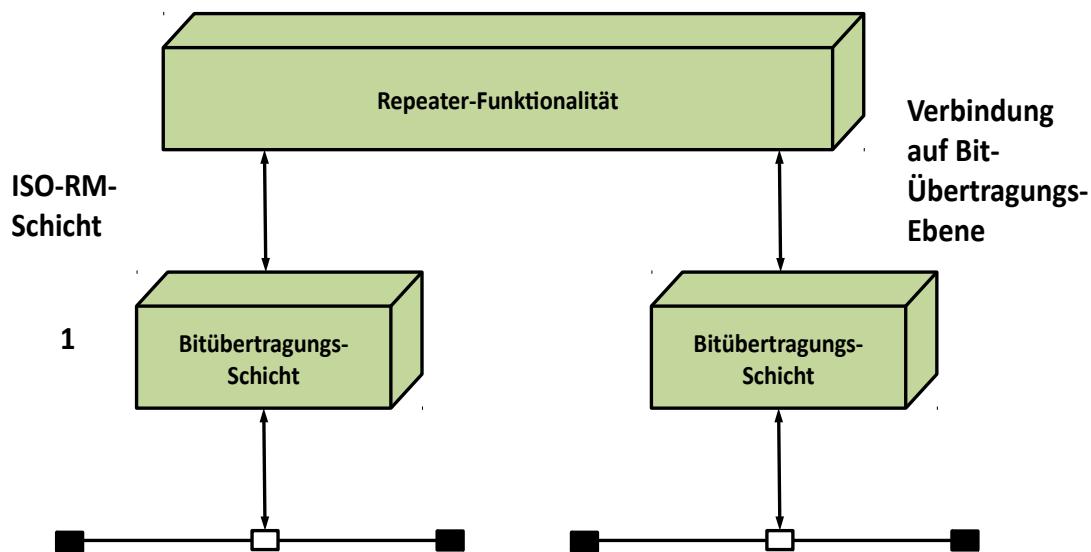


Abbildung 304 : Repeater im ISO-RM

19.2.7 - Repeater-Bauformen

19.2.7.1 - Sternkoppler

Sind im Sinne des ISO-RM Repeater. Allerdings gibt es Bauformen mit etwas Eigen-Intelligenz. So können z. B. Ports mit Kollisionen abgeschaltet werden. (siehe auch Auto Partitioning)

19.2.7.2 - Hub

Hubs zählen zu den Repeatern. Sie fassen einen Bus zu einem Punkt zusammen.

Der Name Hub kommt aus dem Englischen und bedeutet Radnabe. Stellt man sich einen Hub als zentralen Knotenpunkt sternförmig zulaufender Netzwerk-Leitungen vor, sieht er von oben aus wie eine Radnabe.

19.2.7.3 - Media-Konverter

Entspricht einem Repeater der Klasse I (bei 100Mbps). Es darf in einem abgeschlossenen Netzsegment immer nur ein Repeater der Klasse I sein!

Es sind 2 Repeater der Klasse II zulässig.

19.2.7.4 - Switching Hub

Entspricht einer Mischung aus Switch und Hub. Dabei werden mehrere Hub-Ports zu Gruppen zusammen geschaltet. Innerhalb dieser Portgruppen werden die Ports wie in einem Hub behandelt.

Die einzelnen Gruppen werden allerdings geswitcht. Dies findet auch in einem Group-Switch-Modul (etwa bei einem Cisco Catalyst 5000) statt. Eine weitere Bezeichnung für diesen Gerätetyp ist Dual-Speed-Hub. Ein Hub kann, da er funktional nur ein Repeater ist, nicht gleichzeitig zwei unterschiedliche Geschwindigkeiten bearbeiten. Dazu werden Pufferspeicher benötigt, die nur von Switches oder Router bereitgestellt werden.

19.2.8 - Probleme in Netzwerken, bei denen ein Repeater hilfreich ist

- ➊ Bei Längenrestriktionen kann durch den Einsatz eines Repeaters das Netzsegment verlängert werden. Hierbei sind allerdings die Repeater-Regeln einzuhalten!
- ➋ Durch Stilllegen eines Ports kann bei managbaren Repeatern mit Sicherheitsproblemen umgegangen werden.
- ➌ Mit intelligenten Repeatern kann ein Netzwerk gemanagt werden.

19.3 - Brücken (engl. Bridges)



19.3.1 - Allgemeines

Brücken arbeiten im Sinne des ISO-RM auf Ebene 2 (MAC-Ebene). Sie teilen ein Netzsegment in zwei oder mehrere Subsegmente auf. Auf Ebene 3 arbeiten Brücken transparent. Sie haben somit z. B. auf das IP-Protokoll keine Auswirkung. (Die Netzteilnehmer aller Subsegmente befinden sich im gleichen IP-Netz. Damit ist der Netzwerk-Teil der IP-Adresse für alle in allen Subnetzen gleich!)



Die Aufteilung in Subnetze geschieht dadurch, dass die Brücken nur dann einen Rahmen weiterleiten, wenn er ein Ziel in einem anderen Subsegment hat. Um die Entscheidung für das Weiterleiten oder Wegwerfen (Forwarding-Decision) zu treffen, bauen die Brücken sich eine Tabelle auf. Diese Tabellen enthalten die MAC-Adressen der Geräte, die an einem Port angebunden sind. Um diese Tabellen aufzubauen, hören die Brücken den Netzverkehr auf jedem Port ab. Damit alle Rahmen mitgelesen werden müssen die Ports im Promiscuous Mode betrieben werden. Es werden die Sender- und Empfänger-MAC-Adressen aller Rahmen mit gelesen und in der Tabelle vermerkt.

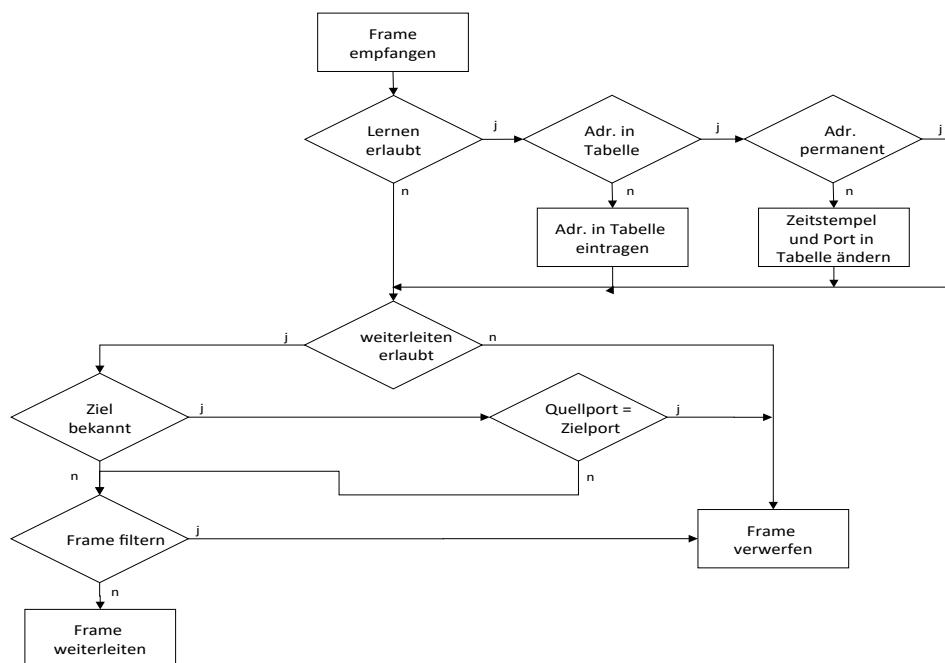


Abbildung 305 : Rahmen-Bearbeitung in Brücken

Erkennt nun eine Brücke, dass ein Sender im gleichen Subsegment (am selben Port) wie der Empfänger ist, braucht die Brücke den Rahmen nicht mehr in das Empfänger-Subsegment transferieren. Dadurch entsteht in den anderen Subsegmenten kein Datenverkehr! Damit könnten in dieser Zeit in den anderen Subsegmenten weitere Rahmen übertragen werden, ohne dass sich die Rahmen durch eine Kollision beeinflussen. Erkennt eine Brücke allerdings, dass Sender und Empfänger in verschiedenen Subsegmenten sind, wird der Rahmen vom Subnetz des Senders in das Subnetz des Empfängers übertragen.

Dies geht allerdings nur bei Unicasts (Ein Sender und ein Empfänger). Multicasts (ein Sender und viele Empfänger) und Broadcasts (ein Sender und alle empfangen) müssen von einer Brücke immer übertragen werden. Ausnahmen bilden hier z. B. Rahmen für die Flow-Control-Funktion (siehe Kapitel Ethernet).

Im Allgemeinen brauchen Brücken für ihre Grundfunktionen keine Parametrierung. Sie können in einem Selbstlernmodus die MAC-Adressen der Subnetze in Tabellen sofort nach dem Einschalten speichern. Dies benötigt jedoch erst einmal Zeit. In dieser Zeit werden die Pakete noch nicht weitergeleitet! (Diese Wartezeit ist oft abschaltbar)



Brücken weisen im Gegensatz zu Repeatern eine gewisse Intelligenz auf. Sie werden mit RISC- oder CISC-Prozessoren realisiert, was für die Erledigung der Aufgaben auch nötig ist. Am Anfang waren Brücken nichts anderes als ein Rechner mit zwei Schnittstellenkarten (NICs) und etwas Software.

19.3.2 - Probleme in Netzwerken, bei denen eine Brücke hilfreich ist

- Längenbegrenzung von Netzwerken

Je nach verwendeter Topologie sind die Netzsegmente in ihrer Länge begrenzt. Z. B. bei 10Base2 185 m.

Bei einer Aufteilung eines Netzwerkes durch eine Brücke in zwei Subnetze, steht in beiden Subnetzen wieder die gesamte Längenausdehnung (Entsprechend den definierten Standards) zur Verfügung. Hier bei 10Base2 sind es 370 m.

- Begrenzung der Stations-Anzahl

In einem Netzsegment ist die Anzahl der möglichen Teilnehmer begrenzt, z. B. 30 in einem 10Base2-Netzsegment.

Bei einer Aufteilung eines Netzwerkes durch eine Brücke in zwei Subnetze steht in beiden Subnetzen wieder die gesamte Stations-Anzahl zur Verfügung. Hier bei 10Base2 sind es 60.

- Ausbreitung fehlerhafter Pakete

Erkennt eine Brücke auf einem Netzsegment ein fehlerhaftes Paket, wird es nicht auf das andere Netzsegment übertragen. Genauso werden auch Kollisionen auf ein Subnetz begrenzt.

- Große Netzlast innerhalb eines Netzsegments

Da nicht alle Rahmen von einer Bridge übertragen werden, ist die Netzlast in den einzelnen Subnetzen geringer. Dies ist je nach Verkehrsart (Unicasts, Multicasts und Broadcasts) jedoch nur bedingt wirksam.

Netzwerk-Komponenten

Darüber hinaus können in Brücken Filter parametriert werden. Damit können Rahmen, je nach gesetztem Filter, transportiert oder verworfen werden. Es kann auf folgende Rahmenteile gefiltert werden:

- Dedizierte Ziel-MAC-Adresse
- Dedizierte Quell-MAC-Adresse
- Eine Broadcast-Adresse
- Ein Typfeld
- Eine Maske

Die Filterung kann :

- positiv (nur parametrierte Rahmen werden transportiert) als auch
- negativ (alle parametrisierten Rahmen werden verworfen) parametriert werden.

Maximale Brückenanzahl

Nach IEEE-802.1d ist die max. Brückenanzahl 7. (Max. Hold-Time ist ca. 1 Sec. -> Es sollte keine Datenübertragung länger als 7 Sec. dauern)

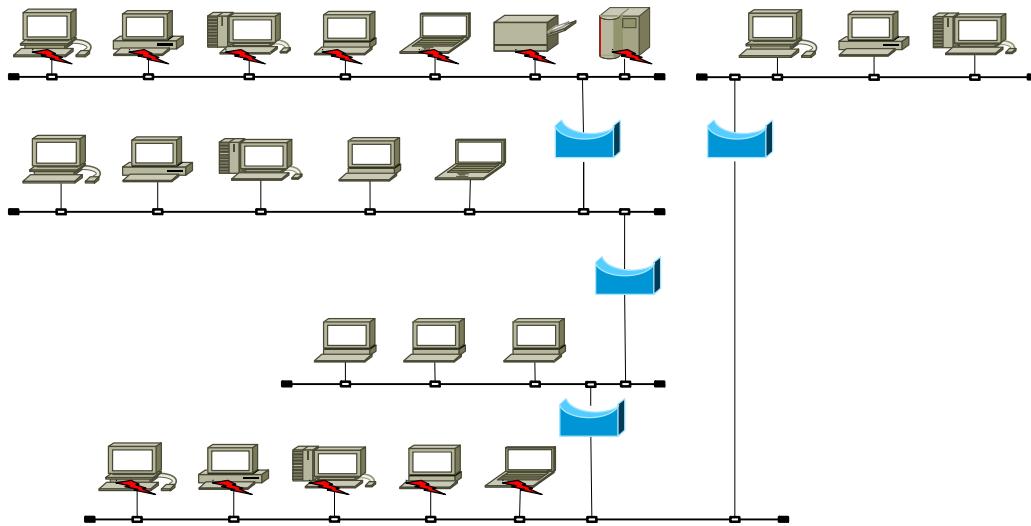


Abbildung 306 : Brücken im Netzwerk

Kollisionen auf einem Netzwerksegment beeinflussen weitere Netzwerksegmente nicht, da eine Brücke die Kollision als Fehler erkennt und deshalb nicht weiterleitet. Die Kollisions-Domäne bleibt damit auf das Subsegment begrenzt in dem die Kollision auftritt. Genauso werden fehlerhafte Rahmen (z. B. mit CRC-Fehler) nicht weiter geleitet.

19.3.3 - Brücke im ISO-RM

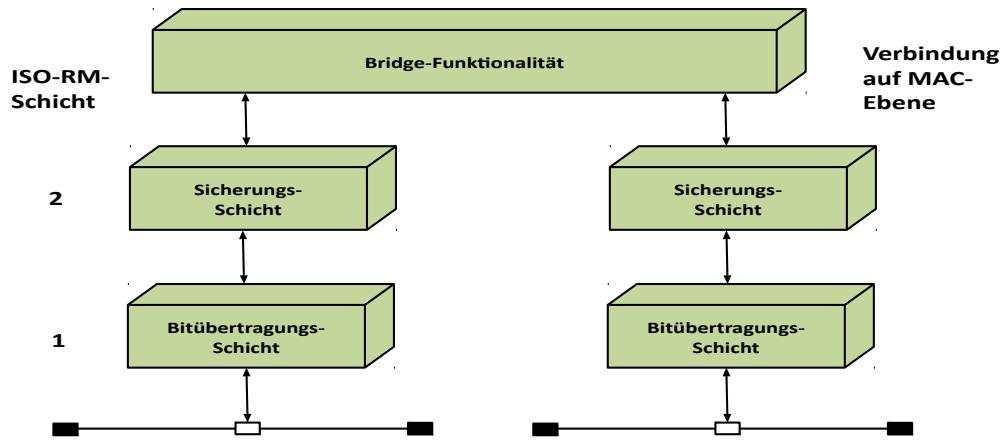


Abbildung 307 : Brücken im ISO-RM

19.3.4 - Brückentypen

19.3.4.1 - Lokale Brücken

Eine lokale Brücke hat typischerweise zwei Ports, mit denen sie zwei Subnetze miteinander verbindet. Dies können sowohl Subnetze gleichen Typs (Ethernet Ethernet) als auch unterschiedlichen Typs (Ethernet Token Ring) sein.

19.3.4.2 - Remote-Brücken

Remote-Brücken verbinden typischerweise Subnetze über Weitverkehrsstrecken. Oft sind sie reine Backbone-Verbindungen ohne eine Anbindung von Endgeräten. Sie treten mindestens paarweise auf, können jedoch auch zu dritt oder zu viert auftreten.

An den Enden einer Weitverkehrsstrecke ist dann immer eine Remote-Brücke installiert, was ihnen auch den Namen Half-Bridge eingebracht hat.

Typische Vertreter haben einen LAN-Port und einen X21-Port sowie, zu Redundanzzwecken, einen ISDN-Port.

Bei Remote-Brücken ist die Pufferkapazität wichtig, um die verschiedenen Geschwindigkeiten ausgleichen zu können.

19.3.4.3 - Multiport-Brücken

Hierbei handelt es sich schlicht um Brücken mit mehr als 2 Ports. Sie entstanden aus den Remote-Brücken und haben sich mit 4 bis etwa 20 Ports auch bei LANs etabliert.

19.3.5 - Adressbuchverwaltung

19.3.5.1 - Dynamisches Adressbuch

Die MAC-Adressen werden während der Bearbeitung im Selbstlernmodus in einem dynamischen Adressbuch vermerkt. Die Einträge werden nach einem Aging-Mechanismus wieder aus dem Adressbuch entfernt. Typische Zeiten sind hierbei 5 Minuten (Cisco). Dies ist evtl. auch die Zeit, die ein Notebook bei einem Switchport-Wechsel warten muss um wieder erreichbar sein.

19.3.5.2 - Statisches Adressbuch

Für Adressen, die nicht dem Alterungsmechanismus unterliegen sollen, besteht die Möglichkeit von manuellen statischen Einträgen. Diese Einträge bleiben auch über einen Neustart der Brücke erhalten.

19.3.6 - Redundanz und Zyklendifreiheit

Damit in einem Netzwerk eine Brücke nicht zu einem Single-Point-Of-Failure wird, ist es möglich, in einem Netzwerk mehrere Wege von A nach B aufzubauen. Allerdings darf nur ein Weg von A nach B aktiv sein. Alle weiteren Wege müssen deaktiviert sein. Es ist schnell erkennbar, was bei mehreren möglichen Wegen im Fall eines Broadcasts passiert. Da ein Broadcast von einer Brücke weiterzuleiten ist, werden alle Brücken den Broadcast an allen Ports an alle Netzwerkteilnehmer weiterleiten. Dadurch senden alle Brücken den Broadcast an alle weiter. Dies bedeutet, dass ein Broadcast durch die verschiedenen Subnetze durch die Brücken in kürzester Zeit vervielfacht wird. Das führt unter Umständen dazu, dass ein Netz innerhalb einer Sekunde unbrauchbar wird.

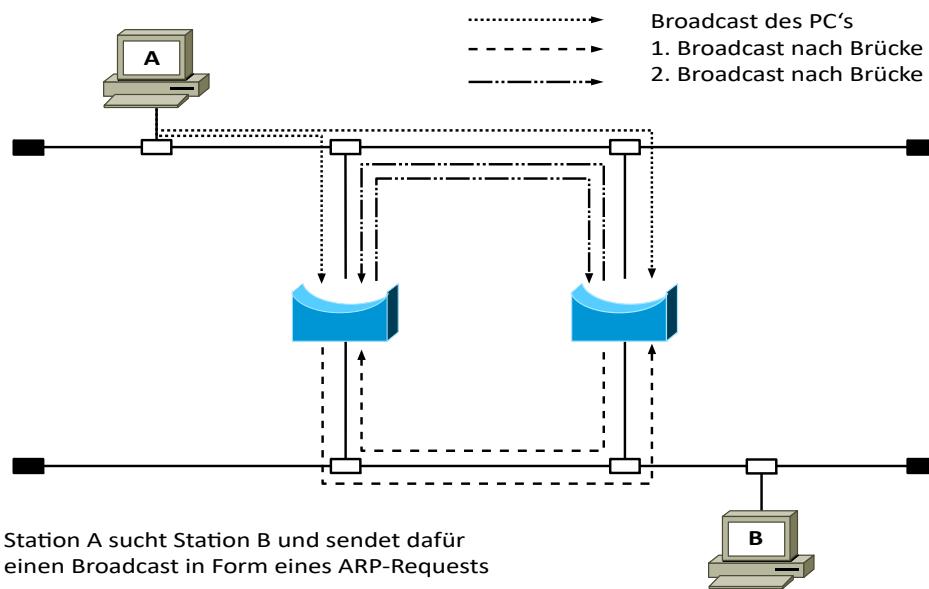


Abbildung 308 : Brücken-Schleifen

19.3.7 - Spanning-Tree-Algorithmus

Ein automatisierter Weg, die Zyklendifreiheit bei transparenten Brücken herzustellen, ist der Spanning-Tree-Algorithmus (SPT). Er wurde in den 1980er Jahren von Radia Perlman (damals bei Digital Equipment) entwickelt. Der SPT ist im Standard IEEE- 802.1d festgelegt.

Da für eine sinnvolle Abarbeitung des SPT Einstellungen durch den Administrator erforderlich sind, können, vor allem in großen Netzwerken, nur Geräte mit Management-Schnittstelle eingesetzt werden. Switches ohne Management-Schnittstelle beherrschen den SPT entweder nicht.

Der SPT gilt sowohl für Brücken als auch für Switches, da beide Gerätetypen auf der gleichen Ebene im OSI-RM arbeiten und deshalb den SPT abhandeln müssen.

19.3.7.1 - Grundlagen

Die Brücken unterhalten sich während ihrer Initialisierungs-Phase miteinander. Dazu bedienen sich die Brücken eines Rahmens, das Configuration-BPDU (Configuration Bridge Protocol Data Unit) genannt wird. Es ist auch als Hallo-Paket bekannt.

Nach Durchlauf des Algorithmus werden Ports, die eine Schleife erzeugen würden, blockiert. Erreicht wird dies durch den Aufbau einer hierarchischen Baum-Struktur, in dem es dann für alle Geräte immer nur einen Weg gibt, Daten zu einem beliebigen Kommunikationspartner zu senden.

Für den SPT sind einige Festlegungen notwendig:

- Jede Brücke hat eine eigene **MAC-Adresse** für das Management.
- Jede Brücke bekommt eine eindeutige **Brücken-ID**. Sie besteht aus einer 2 Byte langen Brücken-Priorität und der 6 Byte langen MAC-Adresse des Switches. Die Priorität ist vom Hersteller auf den Default-Wert 32786 (also die Mitte des möglichen Wertebereichs) gesetzt worden. Kleinere Werte ergeben eine höhere Priorität. Der Wert kann vom Administrator über das Brücken-Management geändert werden, um gezielt eine Root-Brücke festzulegen.

2 Bytes Priorität (Default 32786)	6 Bytes MAC-Adresse
Brücke-ID / Switch-ID	
- Jeder Brücken-Port bekommt innerhalb einer Brücke eine **Port-ID** sie besteht aus einer Port-Priorität und der Portnummer. Die Port-Priorität ist per Default auf 100 gesetzt. Für die Portnummer werden alle Ports der Brücke durchnummieriert. Über die Port-Priorität kann der Administrator priorisieren.
- Jede Verbindung zu einem anderen Switch hat aufgrund ihrer maximal möglichen Datenrate proportionale Kosten. Für jeden Port werden während des SPT die Kosten bis zur Root-Brücke ermittelt. Die Summe aller Verbindungen ergibt die **Pfadkosten** bis zur Root-Brücke. Um Verbindungen zu priorisieren kann der Administrator die Pfadkosten beeinflussen.
- Zum Versenden der **BPDUs** werden Multicast-Adressen verwendet. Somit kann eine Brücke über eine Multicast-Adresse angesprochen werden. Die nach IEEE 802.1D festgelegte Multicast-Adresse lautet 01-80-C2-00-00-00. Diese Adresse wird nur von Brücken und Switches für die Bearbeitung des SPT verwendet.

19.3.7.2 - Ablauf des Spanning-Tree-Algorithmus

Anhand der Brücken-ID wird zuerst die Root-Bridge festgelegt. Es ist die Brücke mit der höchsten Priorität, die sich aus dem eingegebenen Prioritätswert und der eindeutigen Brücken-Adresse ergibt.

Danach entscheidet jede Brücke, welcher ihrer Ports die geringsten Pfadkosten zur Root-Bridge hat und macht diesen Port zum Root-Port. Er ist die kostengünstigste Anschlussmöglichkeit zur Root-Brücke.

Die Pfadkosten zur Root-Bridge (Root-Path-Cost = Wurzel-Pfad-Kosten) errechnen sich aus der Summe aller Einzelpfad-Kosten, die auf dem Weg zur Root-Bridge (auf dem Root-Path = Wurzel-Pfad), auch über mehrere Brücken hinweg, entstehen.

Gibt es mehrere Pfade an unterschiedlichen Ports, die alle die gleichen Kosten aufweisen, dann wird der Port mit der höchsten Priorität (kleinster Wert) genommen.

Gibt es durch eine schlechte Parametrierung mehrere Ports mit der gleichen Priorität, gewinnt der Port mit der niedrigsten Port-ID.

Zuletzt wird für jedes LAN-Segment eine Designierte Brücke bzw. in dieser Brücke ein Designierter Port festgelegt, der die kostengünstigste Verbindung zur Root-Bridge darstellt. Erfüllen mehrere Brücken die Voraussetzungen um Designierte Brücke bzw. Designierter Port zu werden, wird die Entscheidung anhand der gesetzten Priorität oder Brückenadresse bzw. fortlaufenden Portnummer getroffen (die niedrigste Port-ID gewinnt).

Nun werden folgende Ports aktiviert (Forwarding State):

- Root-Port
- Ports, die LANs verbinden für welche die Brücke die Designierte Brücke ist

Alle anderen Ports werden deaktiviert. (Blocking State). Diese Ports decken die Backup-Funktionalität ab und können jederzeit aktiviert werden. Es werden nur noch BPDUs auf diesen Ports übertragen, um sicher zu stellen, dass die Verbindung physikalisch besteht und evtl. genutzt werden könnte!



19.3.7.3 - Beispiel für einen Spanning-Tree-Algorithmus-Durchlauf

Im folgenden Beispiel werden Switches verwendet. Der SPT-Ablauf ist für Brücken gleich. Netzwerk vor dem Ablauf des Spanning Tree Algorithmus.

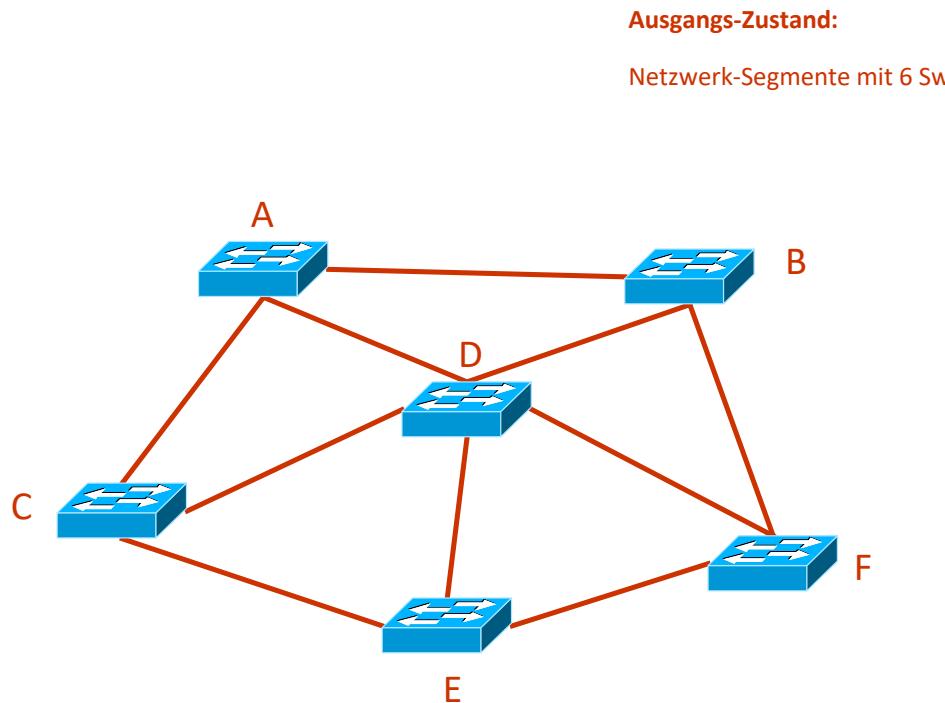


Abbildung 309 : Spanning-Tree-Ablauf 1

In der obigen Abbildung ist der Ausgangszustand eines redundanten Netzwerks dargestellt.

An dieser Stelle wird noch keine Aussage über die Topologien zwischen den Switches gemacht. Die Verbindungen zwischen den Switches sind als LAN-Segmente zu verstehen. Damit ist gemeint, dass es sich um eine 1:1-Verbindung zwischen den Switches, oder ein ganzes Bussystem handeln kann.

Netzwerk-Komponenten

Für den Aufbau einer hierarchischen Struktur muss ein Kopf oder zentraler Punkt definiert werden. Dafür wird die Brücken-ID verwendet. Dies ist eine Kombination aus Brückenpriorität und MAC-Adresse. (Bridge-ID = Bridge-Priority (2Byte) und der MAC-Adresse (6 Byte)).

Da die MAC-Adresse vom Hersteller fest vergeben sein sollte, kann der Administrator nur die Brückenpriorität ändern. Dies geschieht indem er einer Bridge eine höhere Priorität einräumt als allen anderen. In der folgenden Abbildung ist dies die Bridge A.

Die Default-Einstellung für die Priorität ist 32768. Damit liegt der Wert in der Mitte des möglichen Wertebereichs von 0 bis 65535. Soll nun die Priorität erhöht werden ist der Prioritätswert zu verkleinern. (z. B. auf 1000)

Hat der Administrator keine Root Bridge festgelegt, dann haben alle Brücken die gleiche Priorität.

Damit nun trotzdem die Systeme einen Häuptling wählen können wird die hoffentlich eindeutige MAC-Adresse verwendet. Es ist also immer möglich eine Root-Bridge zu ermitteln.

Ermitteln des Root-Switches

Um eine hierarchische Struktur zu ermitteln, ist zuerst die Root-Brücke zu ermitteln.
Die Brücke/Switch mit der höchsten Priorität wird Root-Bridge/Switch.
In diesem Fall Switch A

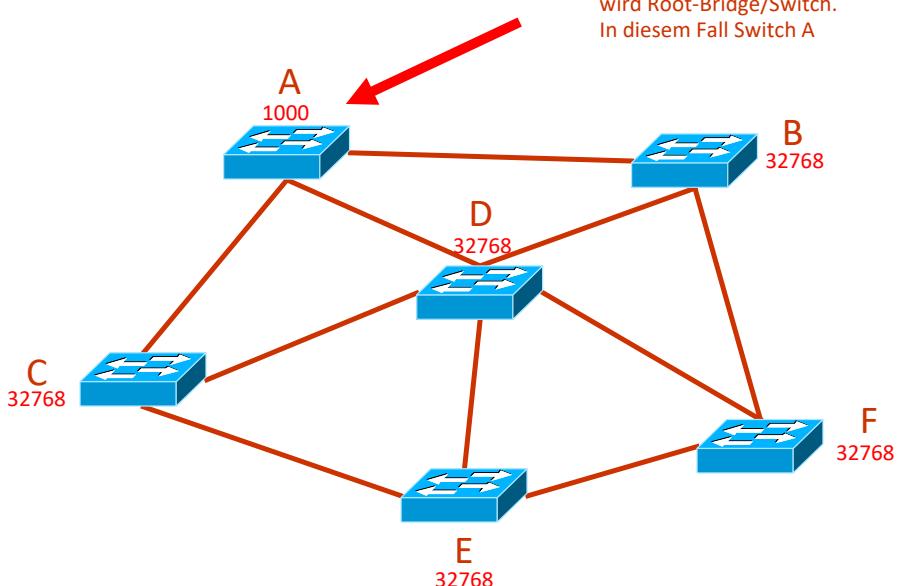


Abbildung 310 : Spanning-Tree-Ablauf 2

An dieser Stelle wird klar, dass nicht administrierte Netzwerke zwar funktionieren jedoch bei Weitem nicht optimal arbeiten. Der Großteil des Datenverkehrs wird über den Root-Switch erfolgen. Deshalb sollte der Administrator mit Bedacht einen performanten Switch zum Root-Switch konfigurieren. Wird z. B. ein nicht performanter Switch zum Root-Switch, ist als Konsequenz die gesamte Performance des LANs suboptimal.

Nachdem die Root-Bridge bestimmt ist, werden die Pfadkosten von jeder Brücke zur Root Bridge bestimmt. Die Ermittlung der Pfadkosten über mehrere Brücken hinweg wird für eine Einzelverbindung folgendermaßen errechnet:

$$\text{Pfadkosten} = 1000 / \text{Bandbreite [in Mbps]}$$

Dabei ist ausschlaggebend, welche Topologie zwischen den Brücken besteht. Hier kommen die verschiedenen möglichen Topologien ins Spiel.

Schnelle Topologien, wie z. B. 1000Base-T, haben niedrige Pfadkosten. Langsame Topologien, wie ISDN, haben hohe Pfadkosten. Die folgende Abbildung zeigt die Verteilung bei den jetzt angenommenen Topologien.

Verbindung	Topologie	Kosten
A - B	ISDN	15626
A - C	10Mbps	100
A - D	ISDN	15626
C - D	ISDN	15626
B - D	100Mbps	10
B - F	10Mbps	100
C - E	ISDN	15626
E - F	ISDN	15626
D - E	10Mbps	100
D - F	ISDN	15626

Netzwerk-Komponenten

Pfadkosten = 1000/Bandbreitein [Mbps]

1	= 1000 Mbps Ethernet
10	= 100Mbps Ethernet
100	= 10Mbps Ethernet
250	= 4Mbps Token-Ring
15625	= 64k (ISDN)

Wegeermittlung

Nach dem Festlegen der Root-Bridge werden die Wege ermittelt.

Zuerst müssen alle Switches/Brücken den günstigsten Weg zur Root-Bridge ermitteln

Dazu werden die Pfadkosten (proportional zur Bandbreite) ermittelt

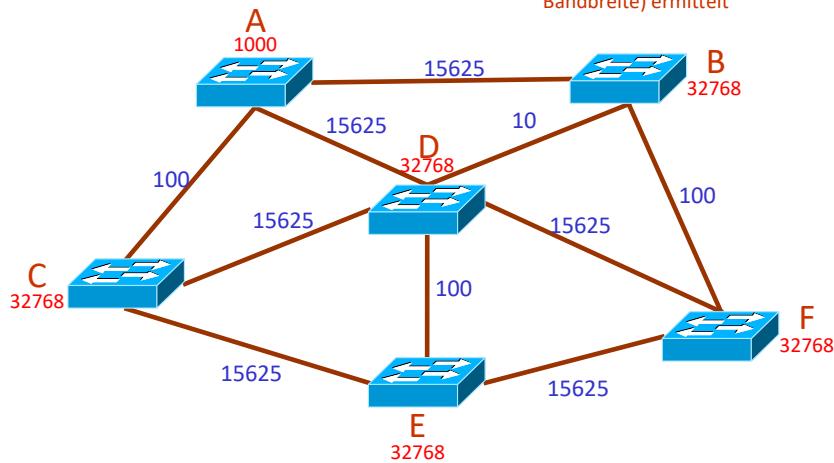


Abbildung 311 : Spanning-Tree-Ablauf 3

Nun kann es vorkommen, dass der Weg zur Root Bridge redundant und dann auch noch von den Kosten her gleich ist. In der obigen Abbildung ist dieses Dilemma am Beispiel des Switches E dargestellt. Der Weg zum Root-Switch, über den Switch C, ist genauso teuer wie der Weg über den Switch D.

Für die einzelnen Brücken ergeben sich nun die folgenden besten Pfadkosten bis zum Root-Switch.

Brücke	Kosten zur Root-Brücke	Bemerkungen
A	0	A ist Root-Brücke
B	15625	
C	100	
D	15625	
E	2 * 15725	2 gleiche Wege zur Root-Brücke
F	15725	

Deshalb wird ein zusätzliches Entscheidungskriterium benötigt. Man verwendet hierzu die Port-ID.

Jeder Port hat eine ID. Die niedrigste Port-ID wird verwendet.

Die Port-ID setzt sich, wie bei der Root-Bridge, aus einer Port-Priorität (kann vom Administrator geändert

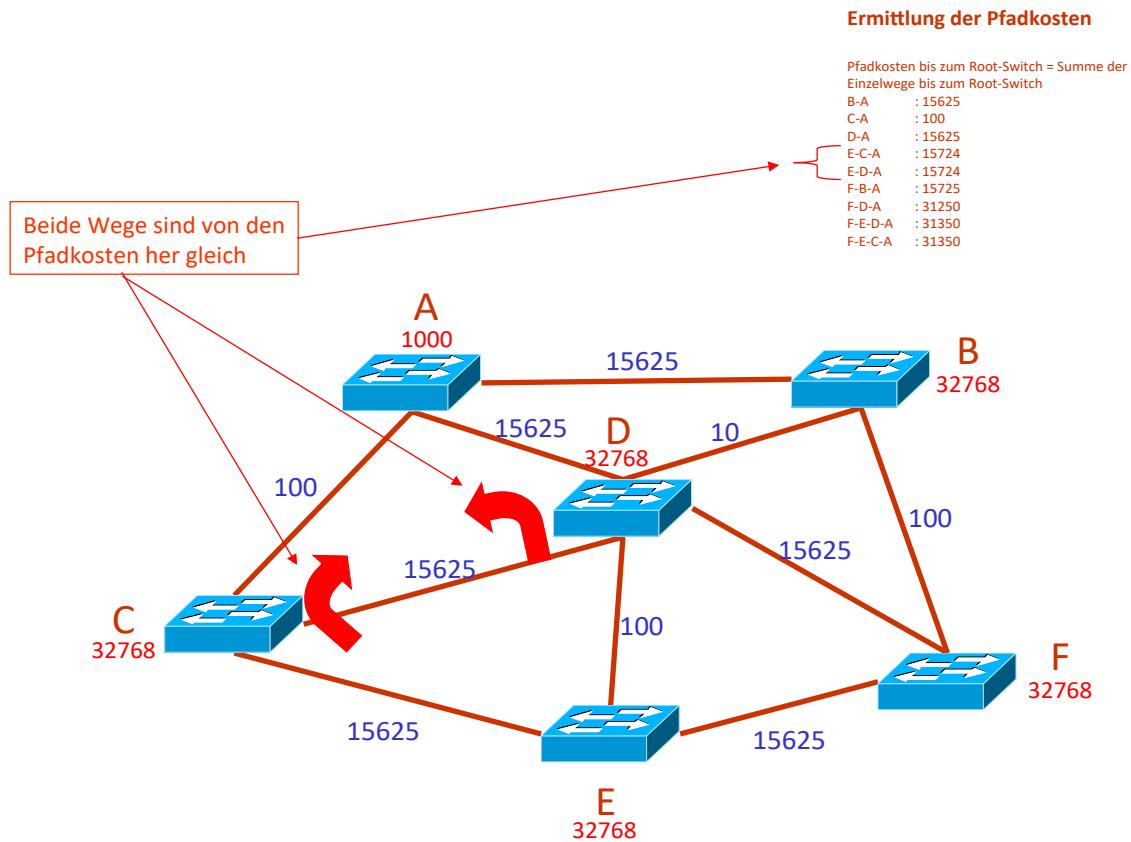


Abbildung 312 : Spanning-Tree-Ablauf 4

werden. Der Defaultwert steht normalerweise auf 100) und der auf der Bridge geführten Portnummer.

In der folgenden Abbildung hat der Weg zum Switch D die Port-ID 100-1. Der Weg zum Switch C hat die Port-ID 100-3. Damit wird der Weg zum Root-Switch über den Switch D gewählt.

Netzwerk-Komponenten

Die niedrigere Port-ID wird bevorzugt.

Daraus folgt für den Switch E der Pfad: E-D-A

Entscheidung bei gleichen Pfadkosten:

Bei gleichen Pfadkosten entscheidet die PortID

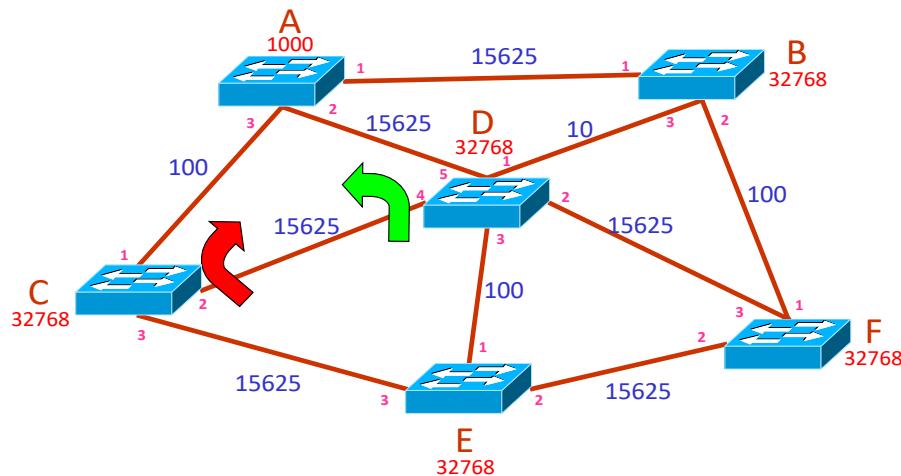


Abbildung 313 : Spanning-Tree-Ablauf 5

Für jeden Switch kann nun ein Root-Port (RP) definiert werden. (Dies ist der Port, der zum Root-Switch führt)

Jedes Netzwerk, das sich zwischen zwei Switches befindet, legt einen Designated Port (DP) fest, der die nächste Verbindung zum Root-Switch herstellt.

Dabei gelten die Verbindungen zwischen den Switches als Netzwerke mit beliebiger Topologie (1:2, Bus, ...). Alle anderen Ports werden zunächst nicht benötigt. Deshalb werden sie in den Blocking-Status geschaltet. Um zu erkennen, ob die benachbarten Switches noch funktionieren, werden auch über Ports, die sich im Blocking-Modus befinden, BPDUs ausgetauscht.

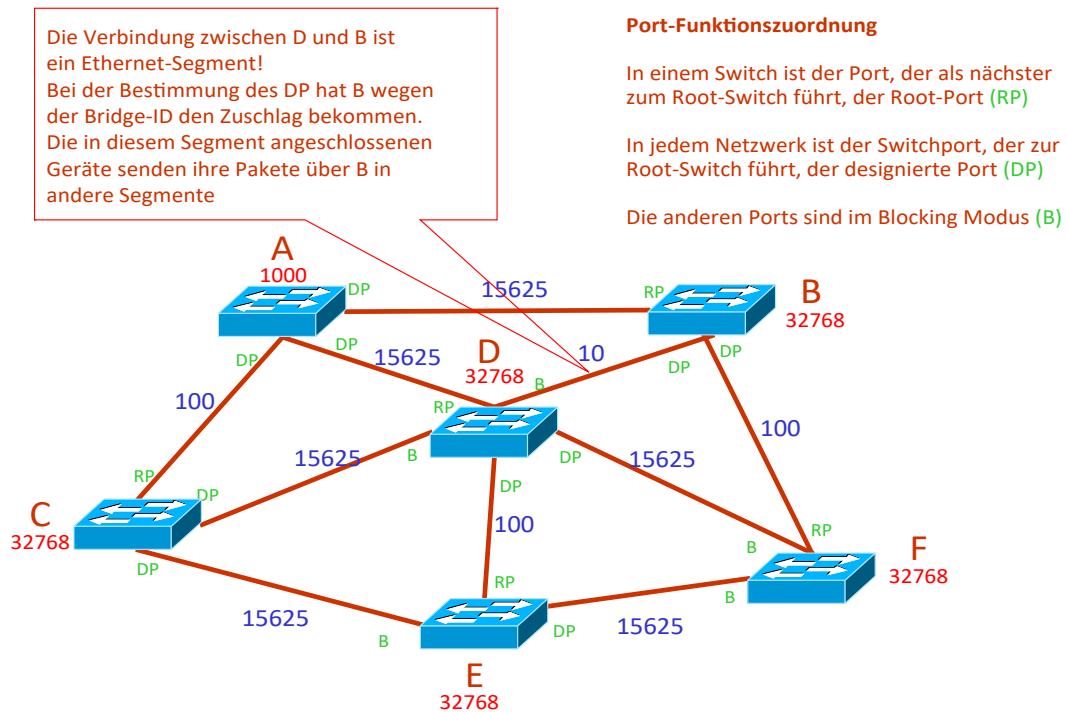


Abbildung 314: Spanning-Tree-Ablauf 6

In der obigen Abbildung wird noch ein Sonderfall beschrieben. Die Verbindung zwischen Switch B und D ist ein 100Mbps-Ethernet. Für jede Verbindung ist ein Designated Port festzulegen. Die Pfadkosten zum Root-Switch sind von Switch-B und Switch-D gleich.

Sind die Pfadkosten bei beiden Möglichkeiten gleich, entscheidet die MAC-Adresse des Switches. Hier gewinnt wieder das Gerät mit der kleinsten MAC-Adresse. In diesem Fall ist es der Switch B.

Ergebnis:

Damit ergibt sich nach dem Ablauf des Spanning-Tree-Algorithmus dieser Aufbau

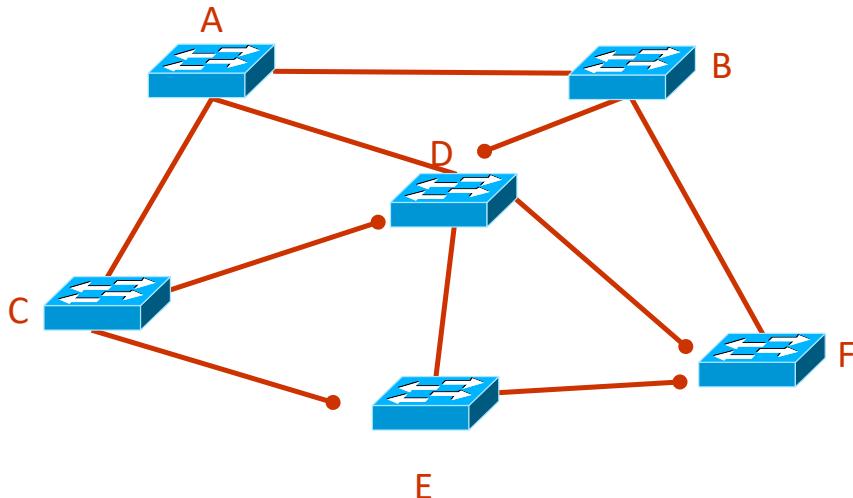


Abbildung 315 : Spanning-Tree-Ablauf 7

Das Ergebnis ist eine Baum-Struktur. Von überall aus kann man bis auf die Root-Bridge Daten übertragen.

Auch über die nicht genutzten Wege (Ports im Blocking-Status) werden die so genannten BPDUs gesendet. Damit können die Switches jederzeit erkennen, ob der Partner auf der anderen Seite noch verfügbar ist und die Verbindung im Bedarfsfall bei einem neuerlichen Durchlauf des Spanning-Tree-Algorithmus nutzen.

Fällt die BPDU 10 Mal hintereinander aus wird der Spanning-Tree neu organisiert.
Dies bedeutet, dass die Neuorganisation des Spanning-Tree bis zu einer Minute dauern kann.

Wird ein Gerät an einen Switchport angeschlossen, dann werden die Daten nicht sofort über den Port transportiert. Zuerst muss ein Switch überprüfen, ob ein normales Endgerät oder ein Switch angeschlossen wurde, denn dann ist evtl. ein neuerlicher Spanning-Tree-Durchlauf notwendig.

Dieser Vorgang ist auch bei einem administrativen Ein-/Ausschalten eines Ports relevant.

Verschiedene Hersteller geben dem Administrator die Möglichkeit, den Listening- und den Learning-Modus zu überspringen. Die folgende Abbildung zeigt, wie CISCO mit der Portfast-Einstellung eine Möglichkeit bietet, die Zeit, bis die Pakete weitergeleitet werden, auf etwa 4 – 20 Sekunden (je nach Gerät) zu verkürzen.

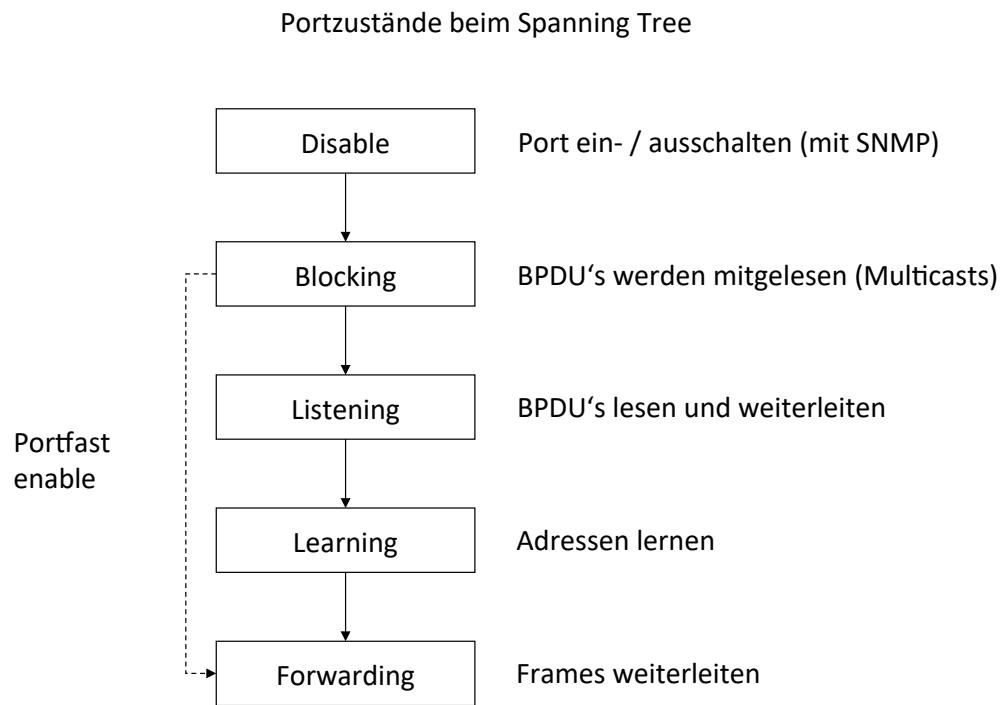


Abbildung 316 : Spanning-Tree – Port-Zustände

19.3.8 - Rapid Reconfiguration Spanning Tree (RSTP) und Multiple Spanning Tree (MSTP)

Beim Spanning-Tree gibt es mittlerweile zwar keine Fragen zur Funktionalität. Dies geht auch zwischen unterschiedlichen Hersteller ganz gut. Allerdings ist die Zeit, die ein Spanning-Tree zur Neubildung, nach dem Ausfall einer Verbindung oder eines Geräts, doch für manche Applikation zu lange. Die BPDU muss 10 Mal ausgefallen sein, bevor ein Spanning-Tree neu aufgebaut wird. Das liegt an der über Timer organisierten Struktur des Verfahrens.

Zudem sind die Leitungen welche im Blocking-Status betrieben werden totes Kapital da sie nicht genutzt werden können.

Deshalb wurde 2002 der Standard IEEE-802.1t festgelegt. Jeder Hersteller, der behauptet sein Gerät arbeitet mit dem Spanning-Tree-Verfahren, muss mit diesem neuen Standard arbeiten.

Er arbeitet anstelle einer timerbasierten Vorgehensweise mit Events. Ein Switch kann ja bereits bei dem Event Link-Down bereit davon ausgehen, dass der Spanning Tree neu zu organisieren ist.

Bei der Festlegung des neuen Standards wurde Wert darauf gelegt, dass der neue Standard zum alten abwärts kompatibel ist. Nachdem der Spanning Tree aufgespannt ist, kann eigentlich nicht gesagt werden ob er nach dem alten oder dem neuen Standard errichtet wurde.

19.3.8.1 - Aufbau des RSTP

19.3.8.1.1 - Root Bridge

Wie beim STP ist zuerst die Root Bridge zu ermitteln. Das Verfahren ist das gleiche. Also wird nach Bridge-Priorität oder, bei gleichen Prioritäten, nach der MAC-Adresse entschieden. Wobei auch hier die kleinsten Werte die größte Priorität haben.

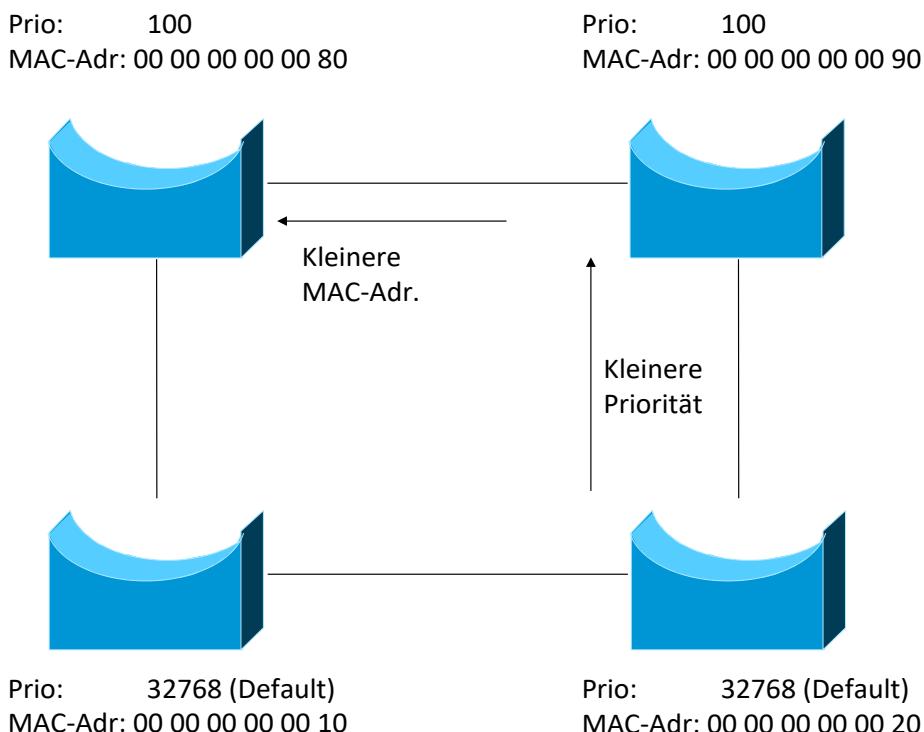


Abbildung 317 : RSTP-Root-Ermittlung

19.3.8.1.2 - Designated Bridge

Ist die Root-Bridge gefunden wird die Designated Bridge ermittelt. Ist ein LAN-Segment über mehrere Bridges mit der Root Bridge erreichbar, muss eine ausgewählt werden um den Weg zur Root Bridge herzustellen. Hierbei entscheiden die Pfadkosten zur Root Bridge. Die Bridge mit den niedrigsten Pfadkosten wird zur Designated Bridge (Fall 1). Sind die Pfadkosten bei zwei Bridges gleich entscheidet die Port-Prioritäten der angeschlossenen Bridges (Fall 2). Sollten die Prioritäten ebenfalls gleich sein, entscheidet die Port-ID (Fall 3). Ist auch hier wieder ein Gleichstand wird als letztes Mittel zur Regelung die MAC-Adresse der Bridges verwendet (Fall 4). Hier zeigt sich, dass die Überlegungen des Administrators bei der Einrichtung eines RSTP nicht nur die Default-Werte zulassen. Um einen sinnvollen Spanning Tree aufzubauen ist einiges an Konfigurationsarbeit von Nöten.

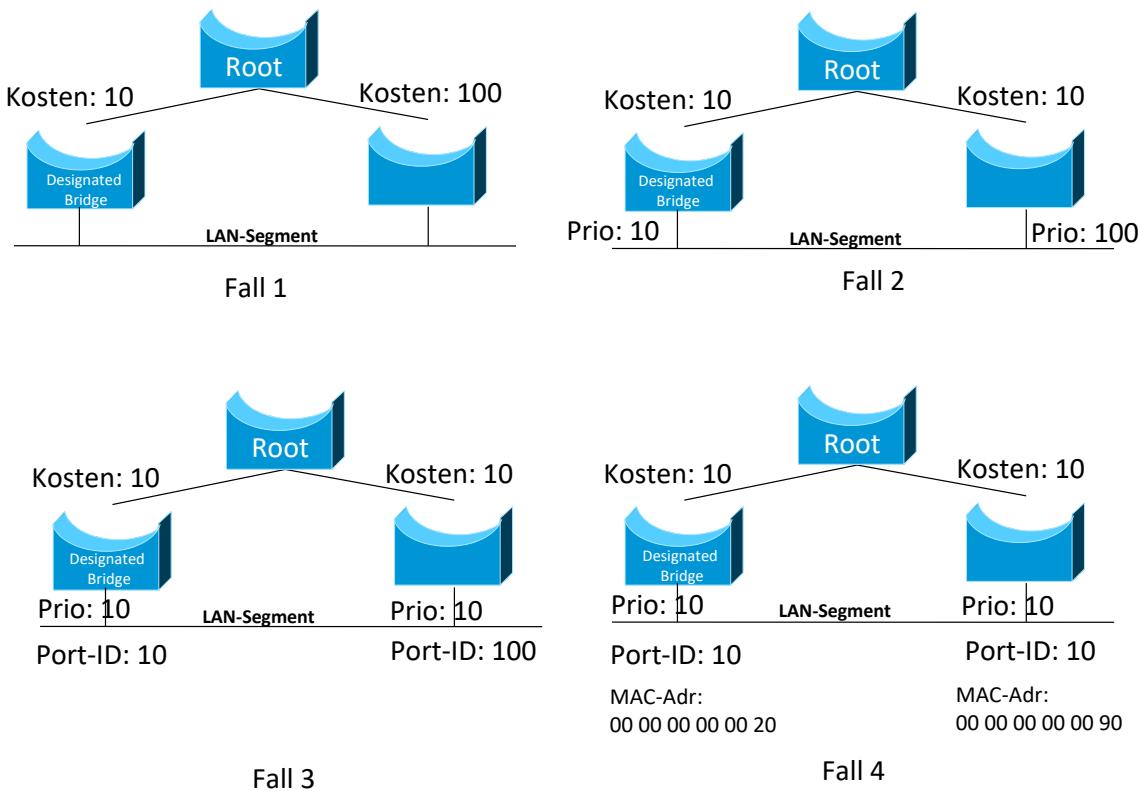


Abbildung 318 : RSTP-Designated-Bridge-Ermittlung

19.3.8.1.3 - Ports

Waren beim klassischen STP (IEEE-802.1d) die Portrollen nur für die Nomenklatur so bekommen beim RSTP (IEEE 802.1t) die Portrollen eine tragende Bedeutung.

19.3.8.1.4 - Root Port

Der Root Port ist der Port eines Switches der zum Root Switch hin (upstream) aktiv, also im FORWARDING-Modus ist. Da auf einem Switch nur ein Root Port zulässig ist, muss hier evtl. ein Auswahlverfahren stattfinden. Dabei werden, wie beim Designated Port folgende Kriterien verglichen bis ein eindeutiger Root Port ermittelt ist:

1. Kosten zum Root
2. Port Priorität
3. Port ID

Die MAC-Adresse braucht nicht mehr herangezogen werden, da auf einem Switch die Ports alle durchnummert sind.

19.3.8.1.5 - Designated Port

Der Designated Port ist der Port der downstream (also vom Root Switch weg) bestimmt werden. Es ist der Port der zur Designated Bridge gehört.

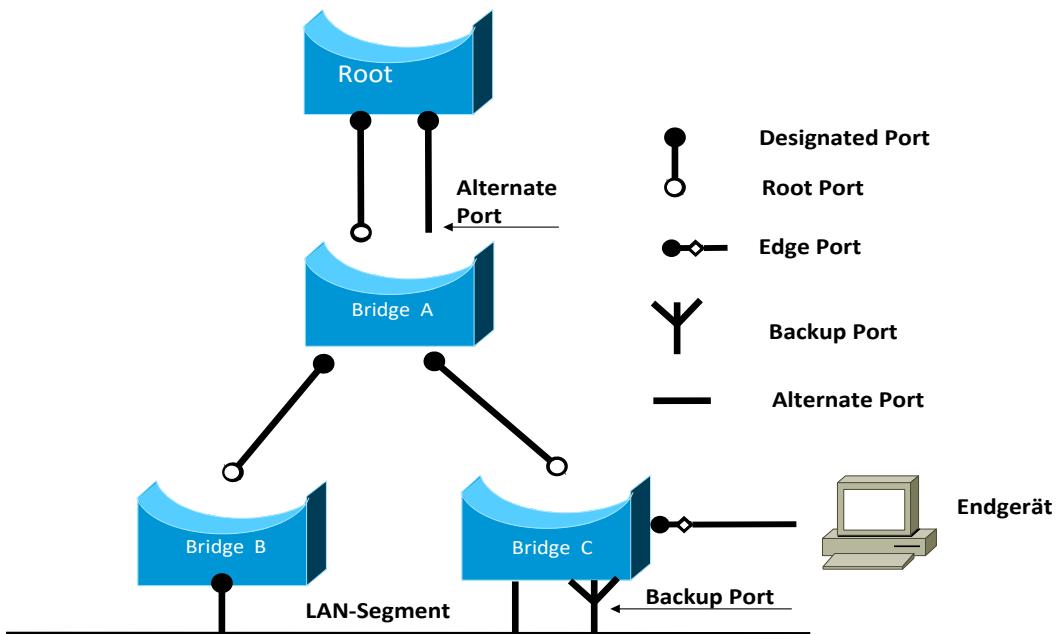


Abbildung 319 : RSTP Root- / Designated- / Edge-Port

19.3.8.1.6 - Edge Port

Der Edge Port ist ein Port an dem kein Switch mehr angebunden ist. Dies bedeutet, dass an diesem Port keinerlei Bridging-Funktionalität mehr hängt und damit der RSTP nicht durchgeführt werden muss.

19.3.8.1.7 - Alternate Port

Der Alternate Port ist ein Port der einen Weg zum Root Port weist jedoch aufgrund des Auswahlverfahrens nicht zum Root Port wurde.

19.3.8.1.8 - Backup Port

Der Backup Port ist ein Port der wie ein Designated Port arbeiten könnte, jedoch aufgrund des Auswahlverfahrens nicht zum Designated Port wurde.

19.3.8.2 - RSTP Port Modi

Im Vergleich zum STP ist beim RSTP der Listening Modus weggefallen. Aus dem Blocking Mode ist der Discarding Mode geworden.

19.3.8.2.1 - Discarding Mode

Der ehemalige Blocking Mode leitet nur noch BPDUs weiter oder empfängt diese. Deshalb ist er entweder ein Alternate- oder ein Backup Port. Ein solcher Port ist nicht disabled. Für diesen Port ist keine Bridge-Tabelle zu führen da keine Daten weitergeleitet werden.

19.3.8.2.2 - Learning Mode

Dieser Modus hat die Tätigkeiten des Listening Modus übernommen. In diesem Modus werden BPDUs gesendet und empfangen jedoch werden noch keine Daten-Rahmen verarbeitet. Dieser Modus ist nur noch aus Kompatibilitätsgründen vorhanden.

19.3.8.2.3 - Forwarding Mode

Dieser Modus funktioniert wie beim STP. Es werden Daten-Rahmen sowie BPDUs weitergeleitet.

In der folgenden Tabelle sind die Portstati und die Portrollen aus dem STP denen aus dem RSTP gegenübergestellt.

Port Status			
STP	RSTP	Active Topologie	Port Role
Disable	Discarding	Excluded	Disabled
Blocking	Discarding	Excluded	Alternate / Backup
Listening	Discarding	Included	Root, Designated, Edge
Learning	Learning	Included	Root, Designated
Forwarding	Forwarding	Included	Root, Designated, Edge

Netzwerk-Komponenten

Der Standard IEEE-802.1w hat für die Darstellung der Port-Zustände und Rollen folgenden Vorschlag.

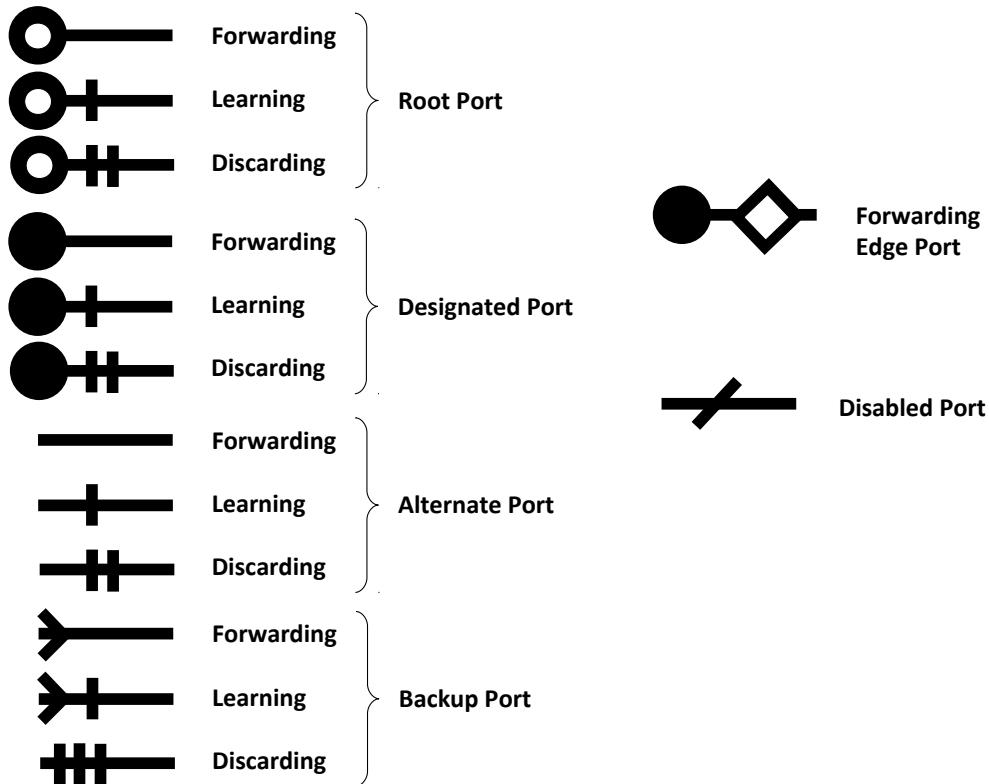


Abbildung 320 : IEEE-802.1w

Für den RSTP ist noch eine Anmerkung relevant bevor der Aufbau eines RSTP erläutert werden kann. Es gibt im neuen Standard die Möglichkeit Punkt-zu-Punkt-Verbindungen zu definieren. Damit weiß der Algorithmus, dass an einem Port kein CSMA/CD auftreten kann. Dies ist durch zwei möglichen Port-Einstellungen möglich:

- Es handelt sich um einen aggregierten Link
- Der Port arbeitet im Full Duplex Mode

19.3.8.3 - RSTP-Regeln

19.3.8.3.1 - RSTP-Regel 0

Ein Port kann unmittelbar sofort in den Discarding Mode versetzt werden.

19.3.8.3.2 - RSTP-Regel 1

Der einzige Port eines LAN-Segments kann unmittelbar sofort nach Aktivierung in den Forwarding Mode versetzt werden. Da es keine weiteren Möglichkeiten für dieses LAN-Segment gibt eine Verbindung zum Root Switch zu erhalten kann kein Loop entstehen. Deshalb sind alle Ports eines Switches per Default als Edge-Port konfiguriert. Jeder Edge Port sendet BPDUs damit ein neu angeschlossenen Switch erkennen kann, dass er mit einem Switch verbunden wurde. Sobald ein Switch keine BPDUs an einem Port empfängt kann er davon ausgehen, dass kein weiterer Switch an diesem Port angeschlossen ist und deshalb wird er ihn in den Forwarding Modus schalten.

19.3.8.3.3 - RSTP-Regel 2

Hat ein Root Port oder ein Designated Port seine Rolle lange genug kann er in den Forwarding Mode wechseln. Es ist das Forwarding Delay abzuwarten bevor die Daten-Rahmen übertragen werden dürfen. Dabei ist der Listening Modus entfallen.

19.3.8.3.4 - RSTP-Regel 3

War der Spanning Tree zuvor lange genug stabil, darf ein Alternate Port sofort zum Root Port werden und in den Forwarding Modus wechseln. Diese Regel wird auch Rapid Transition genannt. Dies bedeutet, dass ein Switch sich auch dann wenn der Spanning Tree stabil ist, den zweitbesten Weg berechnen muss.

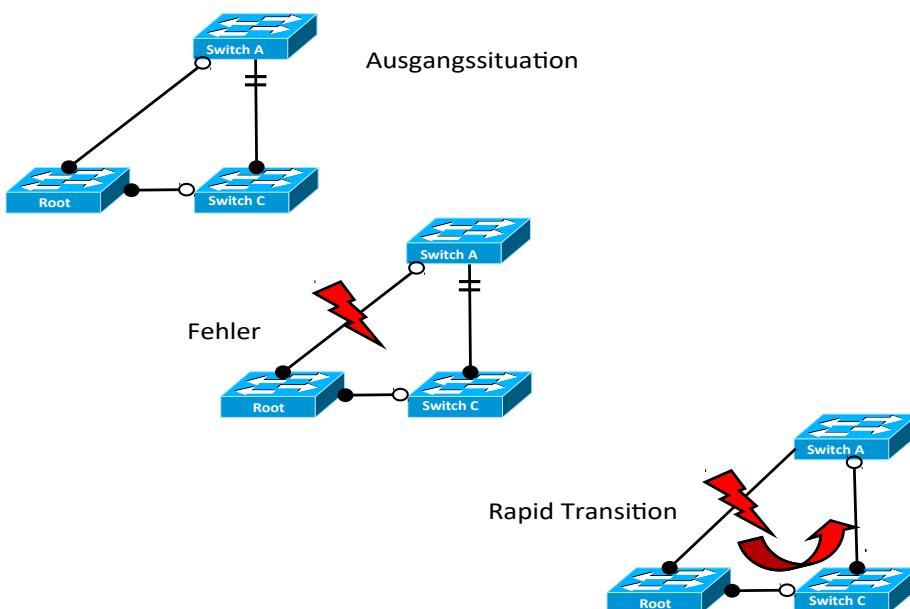


Abbildung 321 : RSTP Rapid Transition

19.3.8.3.5 - RSTP-Regel 4

Ein Designated Port einer Punkt-zu-Punkt-Verbindung darf in den Forwarding Modus wechseln, sobald sein Nachbar-Switch dies genehmigt hat. Dafür werden 2 Nachrichten (Request und Reply) definiert, die von den Switches dann ausgetauscht werden.

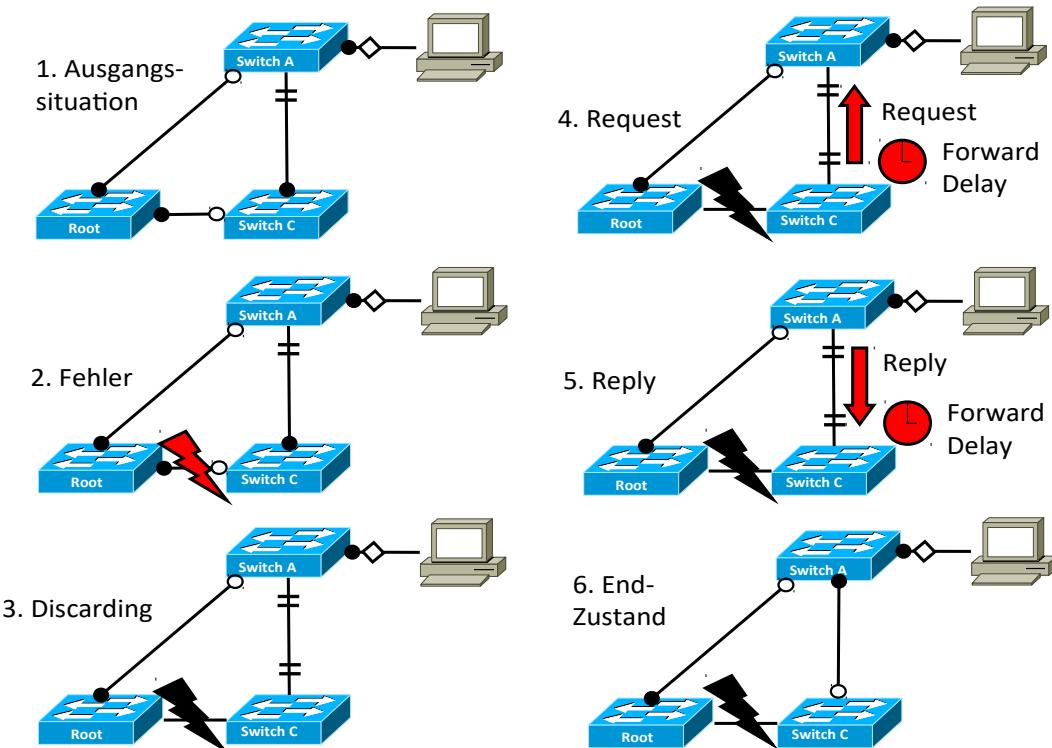


Abbildung 322 : RSTP Request und Reply

Im Fehlerfall schaltet der Switch C zuerst seinen Designated Port zum Switch A in den Discarding Mode. Danach sendet er einen Request an den Switch A. Zusätzlich wird ein Timer auf Switch C aufgezogen. Damit ist die Abwärtskompatibilität zum STP gewährleistet. Switch A schaltet seinen bisher im Discarding Mode befindlichen Port auf Designated, sendet ein Reply und schaltet den Port in den Forwarding Modus. Sobald vom Switch A eine Antwort (Reply) kommt kann der Switch C den Port zum Root Port machen und in den Forwarding Modus schalten.

19.3.9 - Topologie Change

Beim STP war es so, dass jede Änderung in der Topologie dazu führte, dass alle Switches ihre Bridging Tables wegwarfen und neu aufbauen mussten. Moderne Switches sind in der Lage ihre Bridging Tables portbezogen zu verwalten. Damit kann versucht werden nur die umkonfigurierten Ports mit neuen Bridging Tables zu versorgen. Diese Funktion ist optional. Es bleibt jedem Switch überlassen alle Bridging Tables zu verwerfen.

19.3.9.1 - Versand der TC-Meldung (Topologie Change)

Die Meldung wurde früher nur upstream in Richtung Root von allen Switches weitergeleitet und nicht bearbeitet. Erst wenn die Meldung vom Root als TC-Meldung kam wurde sie beachtet und der Erhalt bestätigt. Beim RSTP wird die Meldung bereits auf dem Weg zum Root beachtet, jedoch nicht mehr bestätigt. Um den Empfang sicher zu stellen wird die Meldung beim RSTP doppelt versendet.

19.3.9.2 - Verarbeitung der TCN-Meldung

Die Regelung lautet nun folgendermaßen.

1. Einträge, die sich auf wegfallende Ports (discarding oder disabled) beziehen werden gelöscht.
2. Löschen der Einträge aller Ports eines Switches, bei dem ein Alternate Port zu Root oder Designated Port wurde.
3. Ein Switch löscht alle Einträge seiner Routing Table, es sei denn Regel 4 oder Regel 5 finden Anwendung.
4. Für Edge Ports ändert sich niemals etwas, solange die Edge Port bleiben.
5. Für einen Port, auf dem eine TC-Meldung empfangen wird, bleibt die Bridge Table erhalten.
6. Wird ein Alternate Port zum Root Port, so kann der Alternate Port alle Adressen übernehmen, die zuvor dem Root Port zugeordnet waren.
7. Systeme, bei denen sich etwas ändert, senden TC-Meldungen auf dem Root und allen Designated Ports aus.
8. Empfangenen TC-Meldungen werden auf dem Root und allen Designated Ports weitergeleitet.

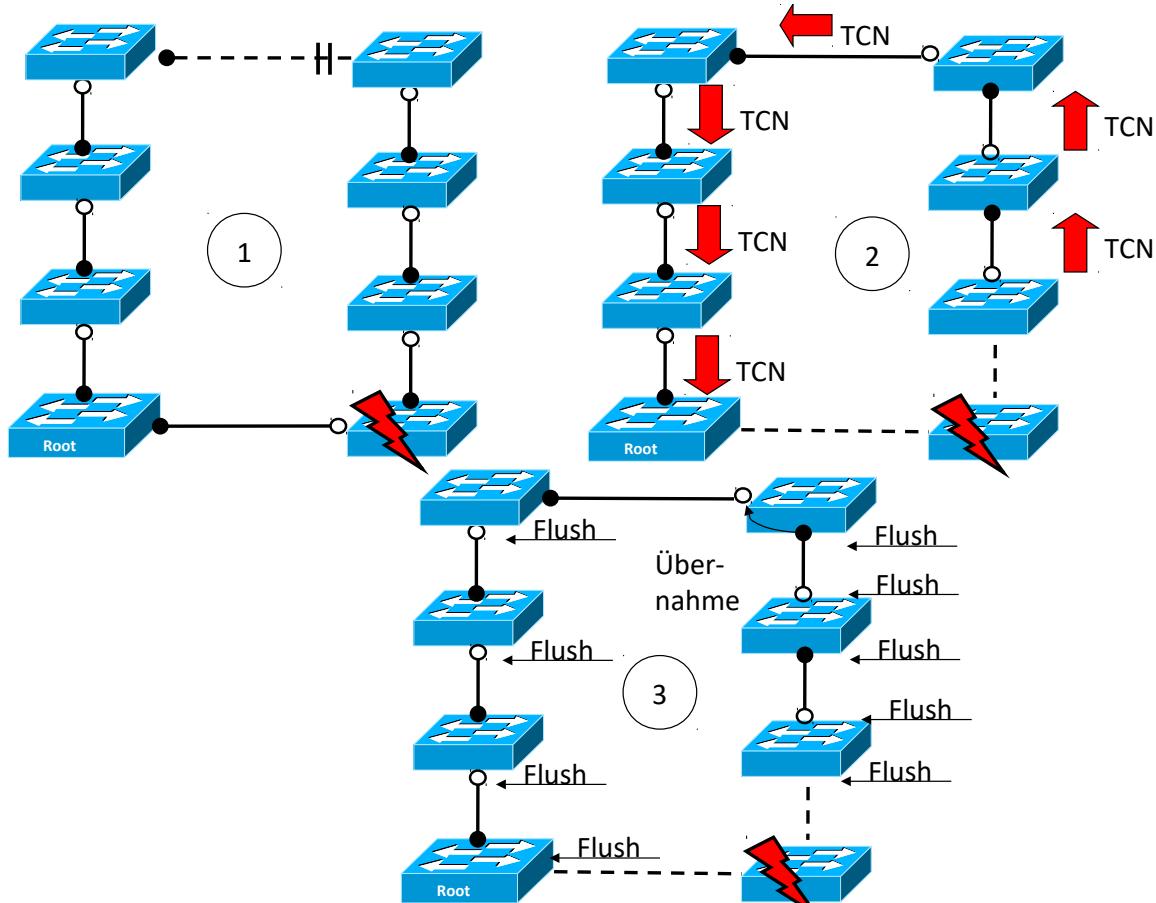


Abbildung 323 : RSTP Verarbeitung der TCN-Meldungen

So schön wie der RSTP jetzt aussieht; es ist nicht alles Gold was glänzt. Auch hier gibt es Probleme. Allerdings hängen die mit der Geschwindigkeit des RSTP zusammen. Während des Respanning (Neuaufbau) des RSTP kann es zu Rahmen-Verdopplungen kommen. Allerdings ist das bei modernen Protokollen (z. B. TCP/IP) eher irrelevant.

Ein weiteres Problem kann dann schon mehr Ärger verursachen. Es handelt sich hierbei um ein Vertauschen der Rahmen-Reihenfolgen. TCP/IP hat hier wiederum keine Probleme. Allerdings gibt es noch Protokolle wie LAT, LLC2 oder NetBEUI die hier Probleme haben. Bei Verwendung solcher Protokolle sollte der RSTP besser im Compatilble Mode betrieben werden.

Quelle für RSTP: Netzwerk Insider Dezember 2002

Source-Routing-Brücken

Obwohl Source-Routing-Brücken (SRB) auch für FDDI und CSMA/CD möglich wäre, ist es nur für den Token-Ring implementiert.

Um mit transparenten Brücken (welche mit Spanning Tree arbeiten) zusammenarbeiten zu können, wurde ein neuer Brücken-Typ entwickelt. Die Arbeitsweise wird mit Source Routing Transparent Bridging (SRT) bezeichnet.

Beim Source-Route-Bridging hält nicht die Brücke die Information zur Wege-Wahl, sondern die sendende Station. Dadurch können die Brücken einfacher hergestellt werden. Allerdings muss die Information in den einzelnen Endgeräten in Tabellenform vorgehalten werden. Damit brauchen keine großen Adresstabellen in Brücken gehalten werden, sondern nur kleine Adresstabellen mit den einzelnen Partnern der Stationen. Allerdings müssen die Stationen für die Tabellen, in einem Route-Discovery-Prozess die Partner und die Wege dorthin erst einmal lernen.

Zusätzlich muss in jedem Rahmen die Routing-Information mitgegeben werden. Da das Routing-Informationsfeld von seiner Länge her fest ist, sind maximal 13 Brücken zwischen zwei Endgeräten zulässig. Bei IBM sind maximal 7 Brücken zwischen zwei Endgeräten zulässig. (Über 7 Brücken musst Du gehen. Maffei lässt Grüßen.)

19.4 - Switches



19.4.1 - Allgemeines

Switches entsprechen ihrer ursprünglichen Funktionalität nach Multiport-Brücken. Allerdings haben Brücken Prozessoren, um die Wegewahl der Pakete durchzuführen. Bei Switches ist die Wegewahl in ASIC's (Application Specific Integrated Circuit), also in Hardware, realisiert. Neuerdings werden die ASICs durch FPGA (Field Programmable Gate Array) ersetzt, denn diese bieten die Möglichkeit, die Firmware per Update auf einen neueren Stand zu bringen.



19.4.2 - Merkmale

Switches unterscheiden sich im allgemeinen durch

- ➊ Managebarkeit (ja/nein)
- ➋ Portanzahl
- ➌ Unterstützte Protokolle (Ethernet, Fibre-Channel (FC),...)
- ➍ Anzahl unterstützter VLANS
- ➎ Performance (Geschwindigkeit, Durchsatz)
- ➏ Interner Aufbau

19.4.3 - Switching-Verfahren bezogen auf den Datenweitertransport

19.4.3.1 - Cut-Through

Das Paket wird so wie es am Eingangs-Port eintrifft an den Ausgangs-Port geleitet und weiter transportiert, sobald die Empfänger-MAC-Adresse bekannt ist. Dies ist das schnellste, jedoch unsicherste Verfahren, da keine Prüfsummenberechnung (CRC-Check) möglich ist. Dadurch können sich fehlerhafte Pakete evtl. fortpflanzen.

19.4.3.2 - Cut-Through (Collision-Free)

Es werden die ersten 64 Byte gespeichert und gelesen. Tritt bis dahin keine Kollision auf, wird das Paket auf den Ausgangs-Port geleitet und weiter transportiert.

Dieses Verfahren ist ein Kompromiss zwischen Geschwindigkeit und Sicherheit.

19.4.3.3 - Store-And-Forward

Es wird erst das gesamte Paket gespeichert und überprüft (z. B. auf CRC-Error). Ist die Prüfsumme in Ordnung wird der Frame weiter geleitet. Ist die Prüfsumme nicht in Ordnung wird der Frame kommentarlos verworfen. Dies ist das langsamste, jedoch sicherste Verfahren, da die Bearbeitung der Prüfsumme Zeit benötigt.

19.4.4 - Kommunikationsarten

Je nachdem, wie viele Empfänger ein Sender adressieren kann, werden unterschiedliche Kommunikationsarten unterschieden.

- | | |
|-------------|--|
| ➊ Unicast | Dabei sendet ein Sender an einen Empfänger |
| ➋ Multicast | Hier sendet ein Sender an eine Gruppe von Empfängern |
| ➌ Broadcast | Wie beim Rundfunk, sendet ein Sender an alle Empfänger |
| ➍ Anycasts | Ein Sender sendet an den nächsten Empfänger einer Gruppe. (Nur auf Ebene3 möglich) |

Multicasts und Broadcasts werden vom Eingangsport an alle Ausgangsports übertragen. Als Ausnahme hiervon, ist hier der Port zu sehen, an dem der Frame empfangen wurde.

Ist die Empfänger-MAC-Adresse noch nicht bekannt, muss hier auch an alle Ports (mit Ausnahme des Eingangsparts) weiter geleitet werden (Unknown Unicast Flooding).

19.4.5 - Layer2-Switches

19.4.5.1 - Beispiel

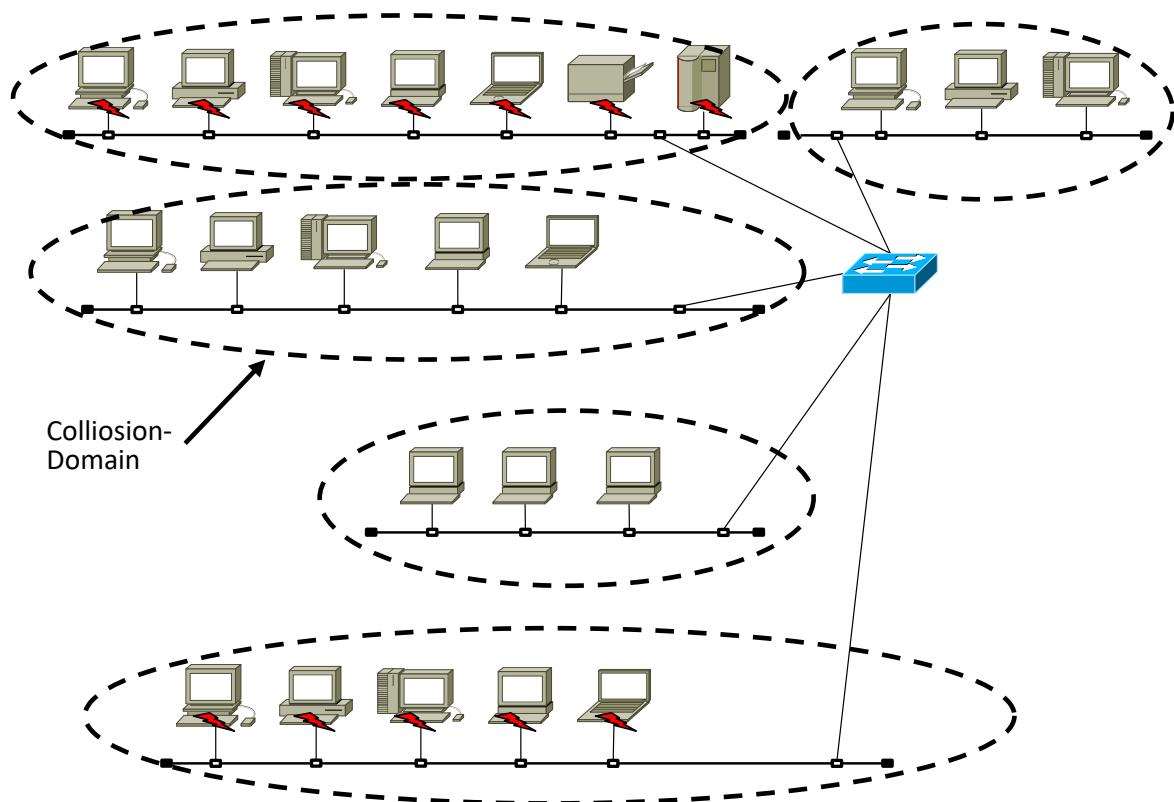


Abbildung 324 : Layer-2-Switch im Netzwerk

Ein Layer-2-Switch funktioniert wie eine Multiport-Bridge. Er begrenzt die Kollisionen auf einen Port. Damit begrenzt er Collision-Domains. Die Bussysteme in Abbildung 324 sind einzelne Collision-Domains.

In der Literatur werden diese Domains auch als Mikrosegmente bezeichnet. Alle Mikrosegmente zusammen bilden ein Segment. Das entspricht einer Broadcast Domain. Ein von einem Gerät gesendeter Broadcast wird also von einem Layer-2-Switch auf alle Mikrosegmente verteilt und an jedes Endgerät gesendet.

Innerhalb des Segments können sich alle Geräte direkt ansprechen.

Sollen Geräte in anderen Segmenten(Netzwerken) angesprochen werden müssen Frames über einen Router gesendet werden, können also nicht direkt adressiert werden.

19.4.5.2 - Layer-2-Switch im ISO-RM

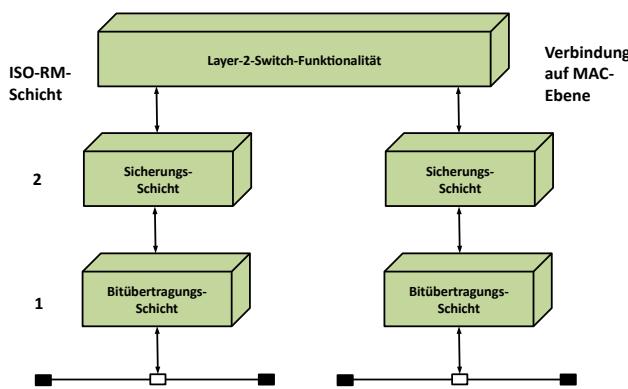


Abbildung 325 : Layer-2-Switch im ISO-RM

19.4.6 - Layer-3-Switches

Hierbei handelt es sich um einen Switch, der in sich einen Router integriert hat. Dies ist sehr hilfreich bei geswitchten VLANs (Virtual Local Area Network). Die VLANs müssen mit einem Router voneinander getrennt bzw. miteinander verbunden werden. Dieser Router war früher als externes Gerät angeschlossen. Durch die Möglichkeit einen Router in ein Switchgehäuse zu integrieren, kann als Verbindung zwischen Switch und Router, die Backplane des Switches genutzt werden. Diese ist im Normalfall wesentlich leistungsfähiger als die Anbindung eines externen Routers.

19.4.6.1 - Beispiel

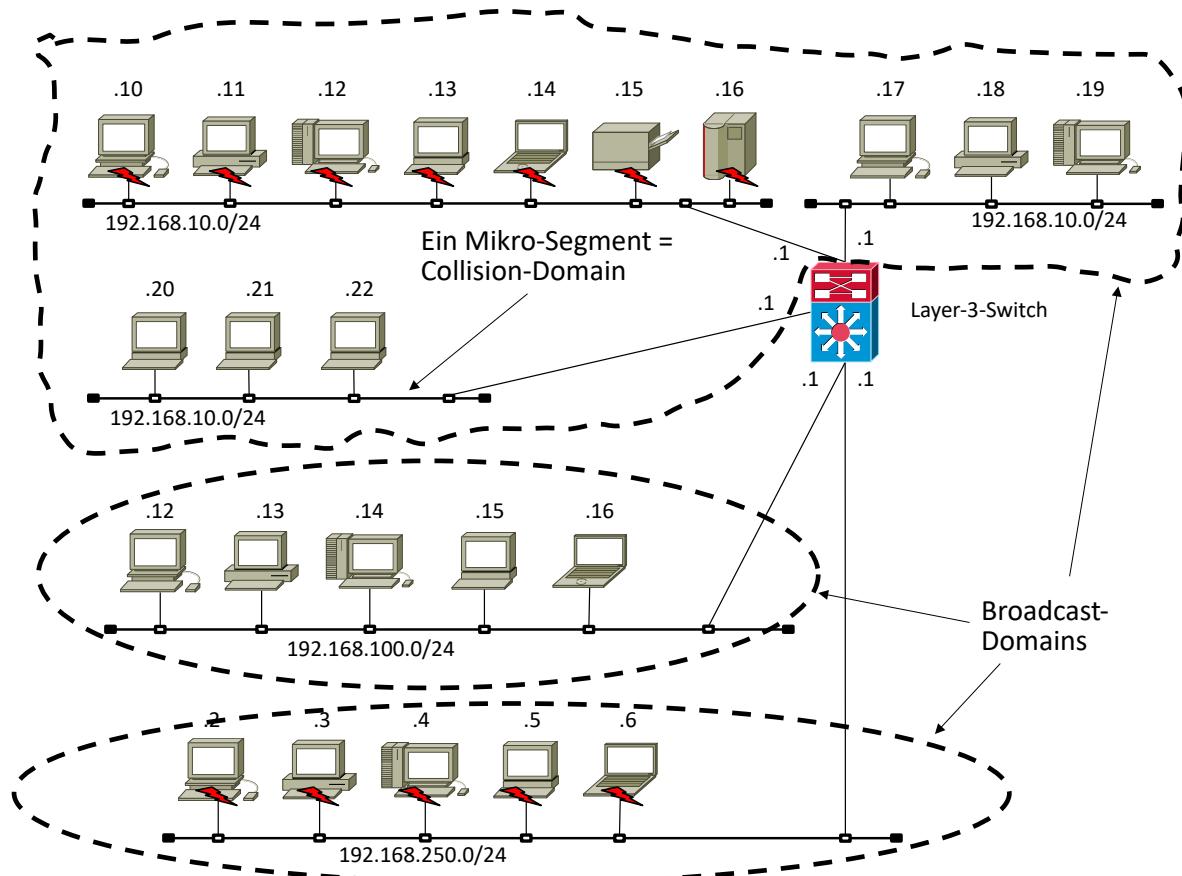


Abbildung 326 : Layer-3-Switch im Netzwerk

Kollisionen werden auf ein Mikro-Segment begrenzt. Mehrere Mikro-Segmente können zu einem Segment zusammengefasst werden. Ein Segment kann ein VLAN und somit eine Broadcast-Domain sein. Broadcasts werden deshalb auf alle (Mikro-)Segmente des gleichen Netzwerks weiter geleitet. Im obigen Bild hat das Netzwerk 192.168.10.0/24 drei Segmente!

19.4.6.2 - Layer-3-Switch im ISO-RM

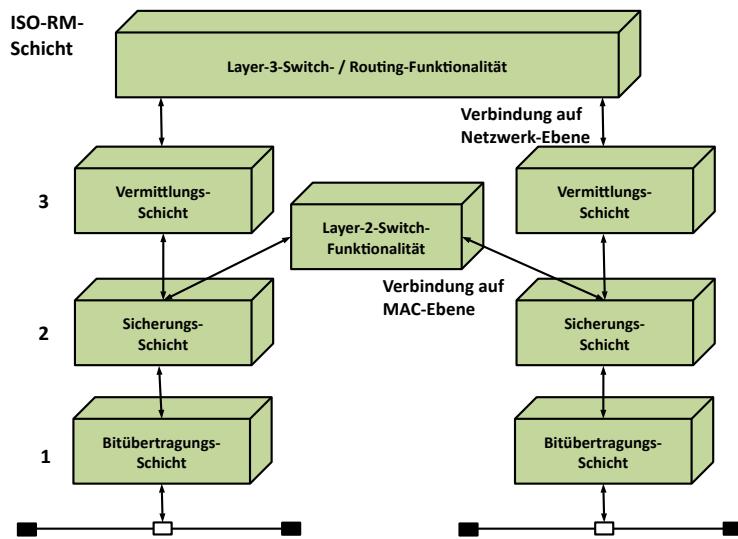


Abbildung 327 : Layer-3-Switch im ISO-RM

19.4.7 - Layer2-Layer3-Switching-Methoden

Verfahren	
Layer-3-Switching	Überall routen
Layer-3-Cut-Through-Switching	Einmal routen danach switchen
Layer-2/3-Switching	Switchen wo möglich Routen wo unumgänglich
Layer-2-Switching	Überall switchen

19.4.8 - Layer-4-Switch

QoS (Quality of Service; deutsch: Dienst-Qualität) ist, wie der Name bereits sagt, einem Dienst zugeordnet. Um QoS zu ermöglichen, muss der Dienst definiert bzw. erkannt werden können. Dies ist auf Ebene 1-3 nicht möglich. Erst auf Ebene 4 kann aufgrund des verwendeten Ports entschieden werden, welcher Dienst gerade im aktuellen Telegramm übertragen wird. Erst auf Ebene 4 kann anhand der Ports erkannt werden, welche Applikationen die Verbindung nutzen. Erst hier kann erkannt werden, ob Videodaten, Filetransfer oder Voice over IP (VoIP) (Telefongespräche über IP) übertragen werden. Dienste wie VoIP oder Videodaten reagieren empfindlich auf Bandbreiten-Engpässe. Es muss sichergestellt sein, dass immer genügend Bandbreite zur Verfügung steht.

Wie in der folgenden Abbildung dargestellt, kann ein Layer-4-Switch Kommunikations-Beziehungen mittels Quell- und Ziel-IP-Adresse, DS-Byte und Protokollfeld im IP-Header, sowie Quell- und Zielport des TCP-Headers unterscheiden.

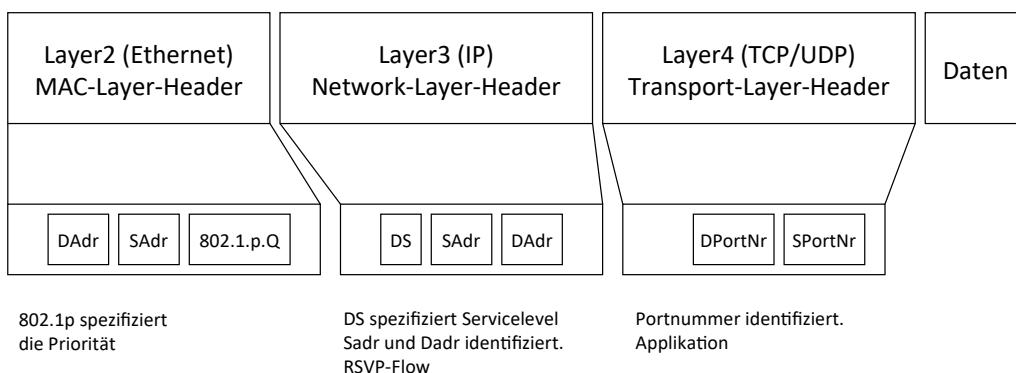


Abbildung 328 : Layer-4-Switching

Da erst ein Switch mit seiner ASIC-Switch-Technologie einen Datenfluss mit „Wire Speed“, also ohne Verzögerungszeiten, übertragen kann, ist hier erstmals die Möglichkeit geschaffen, Applikationen mit großem definierten Bandbreitenbedarf zu bedienen. Mit dem Lightweight Flow Accounting Protocol (LFAP RFC2124) steht den Layer-4-Switches auch eine Möglichkeit des Accounting zur Verfügung. Damit kann eine Abrechnung auf Basis der übertragenen Daten vorgenommen werden.

19.4.9 - Aufbau von größeren Netzwerken mit Switches

Heutzutage gibt es in den Netzwerken keine Repeater oder Hubs mehr, denn ihnen haftet der Makel des Half-Duplex-Mode an und damit auch das Thema Kollisionen. Netze werden mit Switches aufgebaut denn damit ist jede Verbindung, ob von Switch zu Switch, oder von Switch zu Endgerät, immer einen 1-zu-1-Verbindung und damit eine eigenen Collision-Domain. Somit kann ein Full-Duplex-Mode - also auch die doppelte Bandbreite - angewandt werden und es gibt keine Kollisionen mehr. Das erreicht ein Switch dadurch, dass hinter jeder Schnittstelle ein Datenpuffer realisiert ist, in dem die Daten zwischengespeichert werden, bevor sie weiter geleitet werden. So kann jedem verbundenen Gerät suggeriert werden, es gäbe nur die beiden Geräte, die miteinander verbunden sind.

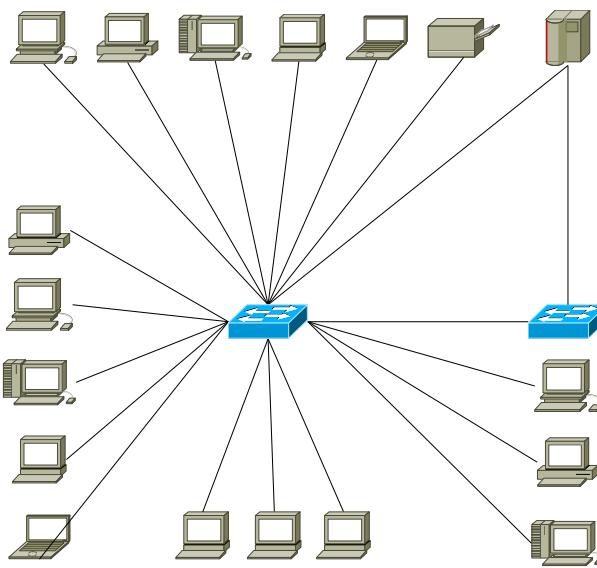


Abbildung 329: 1 zu 1 - Verbindungen bei Switches

rechten Seite definiert werden. Dabei werden Core- Aggregations- und Access-Switches im Rechenzentrum untergebracht.

Die Verbindung zwischen Applikationen und Endgerät wird als North to South-Verbindung bezeichnet.

Es ist zu Redundanzzwecken auch möglich, ein Endgerät über zwei oder mehrere Schnittstellen, an ein Netzwerk anzubinden. Dabei ist dann immer nur einer von zwei Switchen aktiv.

In großen klassischen Installationen wird wie in Abbildung 330 auf der linken Seite ein dreistufiges Konzept verfolgt. Dabei werden die Endgeräte an die Access-Layer angeschlossen. Die Aggregation Layer dient zur Zusammenfassung von Gruppen. Die Core-Layer fasst im Rechenzentrum dann alle Verbindungen zu den Endgeräten zusammen.

Dabei können bei einem Layer-3-Switch auch unterschiedliche VLANs definiert und miteinander verbunden werden. Core-Layer und Aggregation-Layer sind normalerweise zu Redundanzzwecken mindestens doppelt ausgelegt. Hier können auch weitere Verbindungen über Kreuz die Ausfallsicherheit erhöhen.

Da die Server normalerweise nicht bei den Endgeräten in der Fläche stehen, kann eine weitere Aggregations- und Access-Layer wie in Abbildung 330 auf der

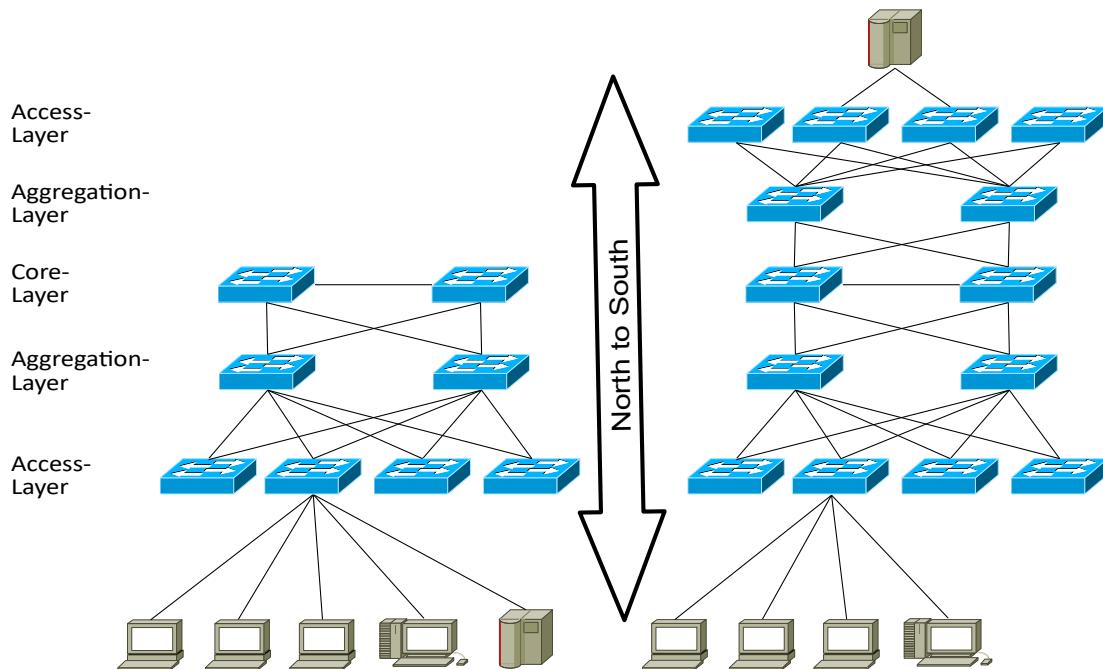


Abbildung 330: Klassische 3stufige Hierarchie

Netzwerk-Komponenten

Die klassische Hierarchiestruktur mit drei oder fünf Switch-Ebenen hat den Nachteil, dass die Daten viele Switches passieren müssen um an ihr Ziel zu gelangen. Bei der moderneren Leaf-Spine-Architektur wird die Anzahl der zu passierenden Switches reduziert und die Redundanz erhöht. Allerdings setzt diese Architektur eine voll vermaschte Netzinfrastruktur voraus. Die Verbindungen zwischen den Servern und dem Storage wird East to West-Traffic genannt

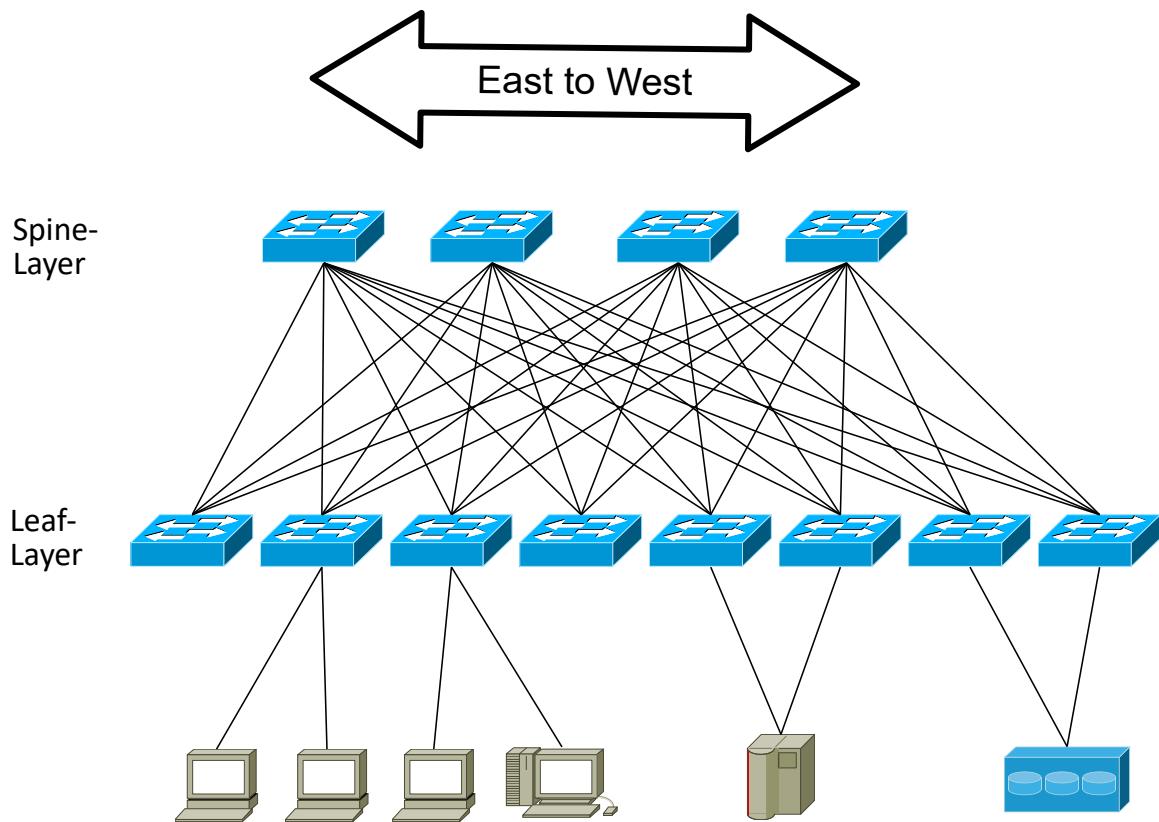


Abbildung 331: Leaf-Spine-Architektur

Switches unterscheiden sich in ihrer Bauform je nach Verwendungszweck. Während bei Core-Switches meist Glasfaser-Ports vorhanden sind um die hohen Datenraten transportieren zu können sind bei den Access-Switches Kupferports in der Mehrzahl anzutreffen, da die Endgeräte wie Drucker PCs oder Notebooks auch nur Kupferports bereitstellen.

Bei den Ethernet-Ports ist der RJ45-Anschluss in der Mehrzahl anzutreffen. Im Industriellen Umfeld werden auch M8- oder M12-Anschlüsse verwendet.

Bei den Glasfaseranschlüssen hat sich eine Vielzahl von steckbaren Transceivern entwickelt die unterschiedliche Datenraten zur Verfügung stellen können.

Tabelle 36: Switch Glasfasermodule

Bezeichnung	Bedeutung	Datenrate
GBIC	Gigabit Interface Converter	1 Gbps
SFP	Small Formfactor Pluggable	1 Gbps
SFP+	Small Formfactor Pluggable +	10 Gbps
SFP28	Small Formfactor Pluggable	25 Gbps
QSFP	Quad Small Form Factor Pluggable	40 Gbps
QSFP+	Quad Small Form Factor Pluggable	40 Gbps
QSFP28	Quad Small Form Factor Pluggable	100 Gbps
OSFP	Octal Small Form Factor Pluggable	400 Gbps
QSFP-DD	Quad Small Form Factor Pluggable Double Density	800 Gbps

Die Bezeichnungen Quad(SFP) = 4 oder Octal(SFP) = 8, geben einen Hinweis auf die Anzahl der Lanes (Datenströme), die in einem Stecker untergebracht werden können.

19.4.10 - Management

Ein weiteres Merkmal von Switches ist die Möglichkeit Konfiguriert zu werden. Switches bieten eine Vielzahl von Funktionen, die konfiguriert werden können. Das wird durch die so genannten Managebaren Switches ermöglicht. Dazu haben sie eine Management-Schnittstelle. Das war früher ein serieller Port, heutzutage ist das eine USB-Schnittstelle. Weiterhin können diese Switches auch über das Netzwerk selbst gewartet werden. Dazu gibt es entweder eine WEB-Schnittstelle oder eine Command-Line-Interface (CLI).

19.4.11 - Stackports

Sobald bei einem Switch alle Ports mit Geräten belegt sind, erhebt sich die Frage, wie der Switch erweitert werden kann. Dazu bieten einige Hersteller Switches an, die einen Stackport haben. Darüber können bis zu 8 Switches zu einer großen Verwaltungseinheit mit einer Kapazität von 1Tbps zusammengeschaltet werden und wie ein großer Switch verwaltet werden.

Dabei wird ein Switch mittels einer Priorität zum Master. Der Master beinhaltet die Management- und Control-Ebene. Wurde Keiner Priorität seitens des Administrators vergeben, wird der Switch zum Master der die kürzeste Startzeit hat. Sind mehrere Switches gleich schnell entscheidet die kleinste MAC-Adresse wer Master wird. Beim Master-Ausfall übernimmt ein bisher passives Mitglied des Stacks die Master-Rolle.

19.4.12 - Backplane

Die Backplane, die alle Linecards (Portmodule) miteinander verbindet gibt es in aktiver oder auch passiver Ausprägung. Sie sollte die maximalen bidirektionalen Datenraten transportieren können (Line-Rate-Forwarding / Noch-Blocking-Architecture).

19.4.13 - Priorisierung

Frames (Layer-2-Switch) oder Pakete(Layer3-Switch) können je nach zu transportierenden Daten priorisiert oder verzögert werden. Dazu müssen die Daten klassifiziert werden. Auf Ebene 2 läuft das im Protokoll IEEE802.1q durch das einfügen /entfernen von VLAN-Tags ab. Die Tags können eine Prioritäts-Information beinhalten. Mittlerweile wird die Priorisierung auf Ebene 3 abgehandelt. Dazu wird DSCP (Differentiated Services Codepoint) verwendet, wofür im IP-Header 6 Bits reserviert sind.

19.5 - Router



19.5.1 - Allgemeines

Router arbeiten auf ISO-RM-Ebene 3 (Netzwerk-Schicht) und verbinden somit zwei Netzwerke miteinander. Broadcasts werden auf ISO-RM-Ebene 2 abgehandelt und werden von Routern somit nicht weitergeleitet. Kollisionen werden auf ISO-RM-Ebene 1 abgehandelt und werden von Routern ebenfalls nicht weitergeleitet. Somit begrenzen Router sowohl Broadcast- als auch Kollisions-Domänen. Siehe auch Abbildung 332 : Router verbinden Netzwerke.

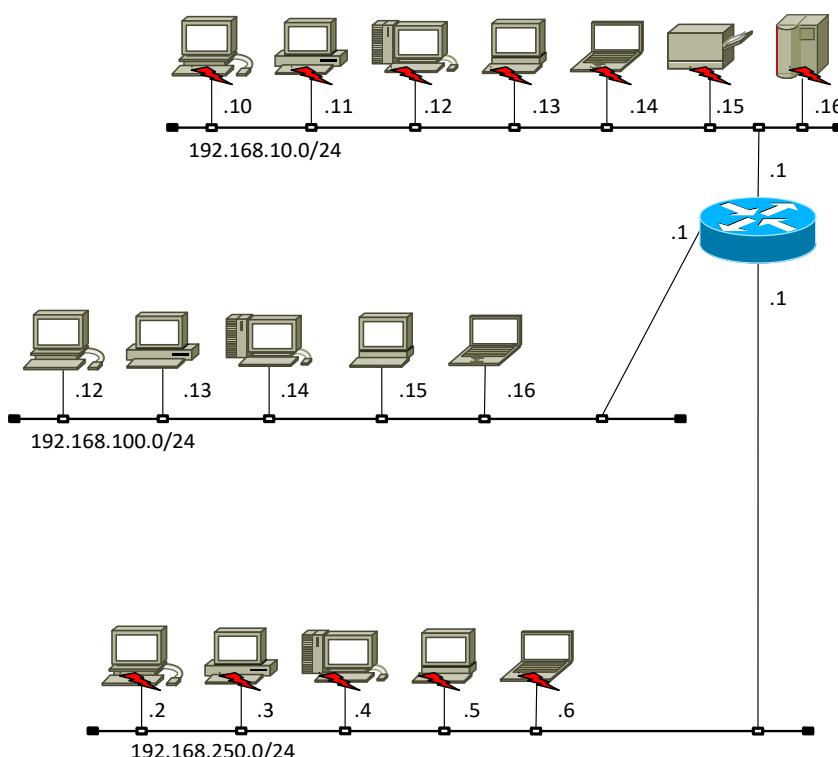


Abbildung 332 : Router verbinden Netzwerke

Die oben beschriebenen Zusammenhänge machen Router zum Mittel der Wahl, bei zu hoher Broadcast-Last. Durch geschicktes aufteilen eines Netzwerks, kann die Beeinflussung durch Broadcasts reduziert werden.

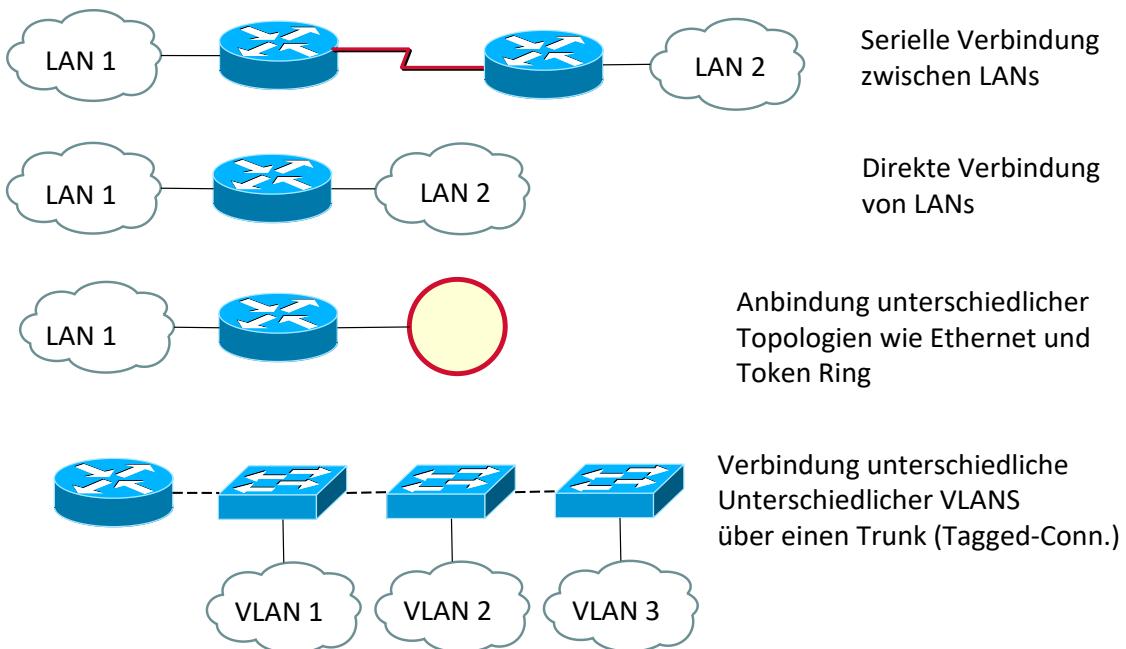


Abbildung 333 : Router-Anschlussmöglichkeiten

Router werden in verschiedenen Netztopologien angetroffen.

In Abbildung 333 : Router-Anschlussmöglichkeiten sind 4 mögliche Strukturen dargestellt.

- Verbinden von 2 Ethernet-Segmenten über eine serielle Verbindung wie z. B. ISDN.
- Direkte Verbindung von 2 Ethernet-Segmenten.
- Verbinden von unterschiedlichen Topologien wie z. B. Ethernet und Token Ring.
- Routing in VLAN's. Hier wird der Router über eine Trunk-Verbindung angeschlossen. Es ist somit nur einen Ethernet-Schnittstelle notwendig. Die unterschiedlichen Netzwerke werden über Subinterfaces definiert.



Router können noch weitere Funktionen beinhalten. So ist z. B. Eine Firewall in vielen Routern im SOHO-Bereich anzutreffen.



Ist ein Router für eine Anbindung des Firmen-Ethernet an verschiedene Topologien wie ISDN oder analoge Leitung zuständig, spricht man auch von einem ACCESS-Server.

19.5.2 - Router im ISO-RM

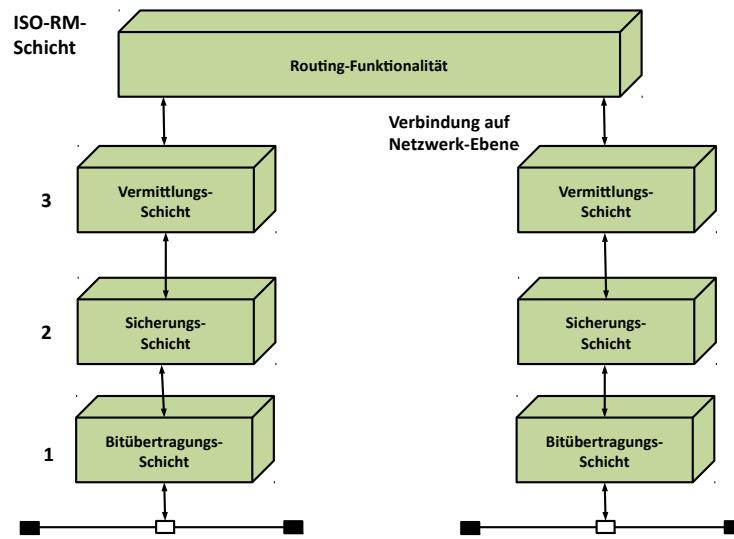


Abbildung 334 : Router im ISO-RM

Die obige Abbildung zeigt, dass die Arbeit eines Routers mit den Informationen der Ebene 3 abgehandelt wird. Hier sind IP- sowie IPX-Adressen die Informationen, welche für die Weitervermittlung von Paketen herangezogen werden.

19.5.3 - Protokolle im Zusammenspiel mit Routern

Es gibt sowohl routebare Protokolle, als auch Routingprotokolle. Beide werden oft miteinander verwechselt.

Bei den routebaren Protokollen handelt es sich um Protokolle, die von Routern weitergeleitet werden können.

Bei den Routingprotokollen handelt es sich um die Protokolle, welche die Router untereinander zur Abwicklung ihres Routing-Auftrages benützen. Hiermit werden Informationen, wie z. B. Routingtabellen, dynamisch ausgetauscht. Damit können die Router auf Veränderungen der Netzwerk-Struktur, wie z. B. den Ausfall eines Routers, reagieren.



20 - Routingprotokolle

BGP (Border Gateway Protocol)

HSRP (Hot Standby Router Protocol)

IGRP/EIGRP (Enhanced Interior Gateway Routing Protocol)

OSPF (Open Shortest Path First)

RIP (Routing Information Protocol)

21 - Routbare Protokolle

IP (Internet Protocol)

IPX (Internet Paket Exchange)

OSI (Open Systems Interconnection)

Apple Talk (Kommunikation zwischen Apple-Rechnern)

22 - Nicht routbare Protokolle

NetBIOS, NetBEUI und LAT sind nicht routbare Protokolle, da sie auf Ebene 3 keine Informationen für die Vermittlung zur Verfügung stellen

22.1.1 - Funktionsweise von Routern

Router verbinden Netzwerke oder auch direkt Netzwerkteilnehmer miteinander. Dazu müssen sie die Verbindungswege zu den angeschlossenen Netzteilnehmern kennen. Die Verwaltung wird in sogenannten Routing-Tabellen gespeichert. Genau genommen kennen Router entweder die Wege zu den erreichbaren Netzwerken (Net-Route-Eintrag) oder den Weg zu einem bestimmten Netzteilnehmer. Dann spricht man von einem Host-Route-Eintrag in der Routing-Tabelle. Im jeweiligen Netzwerk kennen die Router dann die Teilnehmer.

Erhält ein Router ein Paket, sieht er sich die Empfänger-IP-Adresse an und arbeitet nach folgendem Ablaufschema:

- Ist die Empfänger-IP-Adresse in einem Netzwerk, an das der Router selbst angeschlossen ist? Falls ja, wird das Paket direkt an den Netzteilnehmer gesendet.
- Ist die Empfänger-IP-Adresse in einem über einen weiteren Router erreichbaren Netzwerk (Kenne ich jemanden, der diese Adresse kennt)?
Falls ja, wird das Paket an den Router gesandt, der das Paket weiter routen kann.
- Ist die Empfänger-IP-Adresse mir nicht bekannt und kenne ich auch niemanden, der das Netzwerk für den Empfänger kennt?
Falls der Router ein Default-Gateway hat, wird er das Paket dorthin senden. Vielleicht weiß dieser Router einen Weg.
Fehlt der Default-Gateway-Eintrag, dann wird der Router ein ICMP-Paket an den Sender dieses Pakets senden. Siehe ICMP-Meldungen (Destination unreachable; deutsch Empfänger nicht erreichbar)

Router haben mindestens zwei Schnittstellen zu verschiedenen Netzwerken (Ausnahme Router in VLAN's; diese können über eine Trunk-Verbindung angeschlossen werden. Das ist zwar nur eine Schnittstellenkarte, jedoch werden darüber mehrere logische Netzwerke abgehandelt.)

Router halten ihre Routing-Informationen in so genannten Routing-Tables. Darin sind die Ziele hinterlegt, die über die verschiedenen Anschlüsse erreicht werden können. Diese Tabellen können entweder von Hand parametrierte Einträge enthalten (Statische Routing-Einträge) oder aus Mitteilungen von anderen Routern automatisch erstellt werden (Dynamische Routing-Einträge). Die automatisiert ablaufenden Mitteilungen werden über spezielle Routingprotokolle, wie z. B. RIP, OSPF usw. abgehandelt. Automatisiert erstellte Einträge in der Routing-Tabelle unterliegen einem Aging-Mechanismus. Das bedeutet, dass die dynamisch erstellten Einträge nur eine bestimmte Lebens- / Gültigkeitsdauer haben. Statische Einträge unterliegen keinem Alterungsmechanismus.



Der Weg zu einem Netzwerk kann durch mehrere Einträge beschrieben sein. So ist zum Beispiel der Eintrag einer „Default Route“ ein Weg, der für alle anderen Wege auch passen könnte. Anhand der Subnetmask für ein Zielnetz weiß ein Router allerdings, wie groß der Netzwerk-Adressteil ist, den er zu betrachten hat. Da ein Router bei einer Wegeentscheidung im schlimmsten Fall die gesamte Routingtabelle durchgehen muss, kann es mehrere mögliche Wege geben. Bei mehreren Wegen wird der Tabellen-Treffer ausgewählt, der den längsten Adressteil hat (longest Match; deutsch: längste Übereinstimmung in der Subnetmask). Die Routen sind in einer Routingtabelle nach Subnetmask-Länge sortiert angeordnet. Der Router fängt immer an der Stelle mit der längsten Subnetmask an und überprüft die Einträge in Richtung kürzerer Subnetmasken. Sobald er einen passenden Eintrag findet, nimmt er diesen, da er nur noch Einträge mit kürzeren Subnetmasken finden kann.

Damit fällt die Default-Route bei allen beschriebenen Routen heraus. Die Default-Route hat die Subnet-Mask 0.0.0.0. (immer die Route mit dem kürzesten Match). Die Default-Route ist somit immer der letzte Eintrag, den ein Router bei seiner Routing-Entscheidung untersucht und auch nimmt.

22.1.2 - Beispiele von Pakettransporten in verschiedenen Netzwerken

Ausgangssituation :

3 Netzwerke, davon 2 C-Klasse-Netze (195.212.31.0 und 195.212.21.0) und ein A-Klasse-Netzwerk (11.0.0.0). Zu beachten ist, dass jedes Gerät nur ein Default-Gateway kennt!

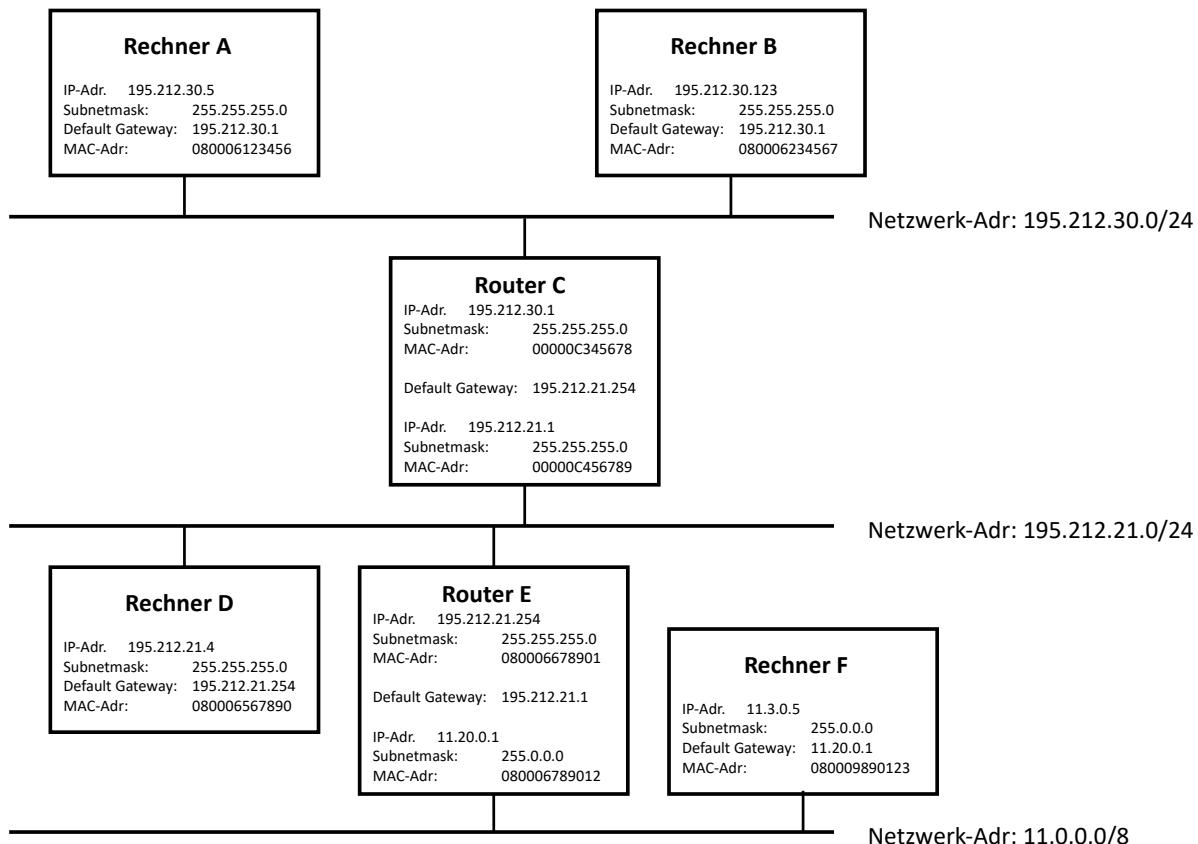


Abbildung 335 : Routing-Beispiel

Beispiel-1:

Rechner A will ein Paket an Rechner B senden.

Mit seiner Subnet-Mask ermittelt Rechner A, dass Rechner B im selben Netzwerk liegt. Deshalb kann Rechner A das Paket direkt an den Rechner B senden.

Rechner A ermittelt die MAC-Adresse von Rechner B (falls er sie noch nicht in seinem ARP-Cache kennt) und sendet das Telegramm an Rechner B.

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006234567	0800006123456	0x800	195.212.30.123	195.212.30.5

Beispiel-2:

Rechner A will ein Paket an Rechner D senden.

Mit seiner Subnet-Mask ermittelt Rechner A, dass Rechner D nicht im selben Netzwerk liegt. Deshalb sendet Rechner A sein Paket an sein Default-Gateway. In diesem Fall ist das Router C. Rechner A ermittelt die MAC-Adresse von Router C (falls er sie noch nicht in seinem ARP-Cache kennt) und sendet das Telegramm an Router C.

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
00000C345678	0800006123456	0x800	195.212.21.4	195.212.30.5

Router C sieht in seiner Routingtabelle nach und findet das Netzwerk für den Rechner D. Das Paket wird daraufhin von Router C an Rechner D gesandt. Dabei wird das Paket umgebaut. Die Empfänger-MAC-Adresse für das Ziel wird eingetragen. Der Router trägt seine eigene MAC-Adresse als Quell-MAC-Adresse ein. Die IP-Adressen bleiben erhalten!



Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006567890	00000C456789	0x800	195.212.21.4	195.212.30.5

In diesem Beispiel wird zum ersten Mal klar, dass die IP-Adressen nie umgebaut werden. Nur die MAC-Adressen werden vom Router umgebaut.

Beispiel-3:

Rechner A will ein Paket an Rechner F senden.

Mit seiner Subnet-Mask ermittelt Rechner A, dass Rechner F nicht im selben Netzwerk liegt.

Deshalb sendet A sein Paket an sein Default-Gateway. In diesem Fall ist das Router C.

Rechner A ermittelt die MAC-Adresse von Router C (falls er sie noch nicht in seinem ARP-Cache kennt) und sendet das Paket an Router C.

Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
00000C345678	0800006123456	0x800	11.3.0.5	195.212.30.5

Router C schlägt die Empfänger-IP-Adresse in seiner Routing-Tabelle nach und findet das Netzwerk für den Rechner F. Allerdings hängt Rechner F nicht in einem Netzwerk, an das Router C direkt angeschlossen ist. Router C weiß nur, dass Router E weiß, wie das Paket weiterzuleiten ist, denn er hat als Empfänger für solche Pakete den Router E in seiner Routing-Tabelle eingetragen. Deshalb sendet Router C das Paket an Router E. Dazu baut er die MAC-Adressen um. Die IP-Adressen bleiben erhalten!



Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080006678901	00000C456789	0x800	11.3.0.5	195.212.30.5

Router E hat den Rechner F in einem ihm angeschlossenen Netzwerk parametriert. Somit kann Router E das Paket an seinen Empfänger senden. Dazu werden die MAC-Adressen abermals umgebaut. Auch hier bleiben die IP-Adressen erhalten!



Ziel-MAC-Adr.	Quell-MAC-Adr.	Telegrammtyp (z.B. IP)	Ziel-IP-Adr.	Quell-IP-Adr.	Rest
080009890123	080006789012	0x800	11.3.0.5	195.212.30.5

Damit erhält die HP-Workstation ein Paket.

Auch in diesem Beispiel zeigt sich, dass die IP-Adressen nie umgebaut werden. Nur die MAC-Adressen werden vom Router, wenn notwendig auch mehrfach, umgebaut.

22.2 - Gateways

22.2.1 - Allgemeines

Gateways arbeiten auf den ISO-RM-Schichten 4 bis 7. Damit können Netzwerke miteinander verbunden werden, in denen unterschiedliche Protokolle verwendet werden. So können Rechner, die unterschiedliche Protokolle verwenden, miteinander kommunizieren.

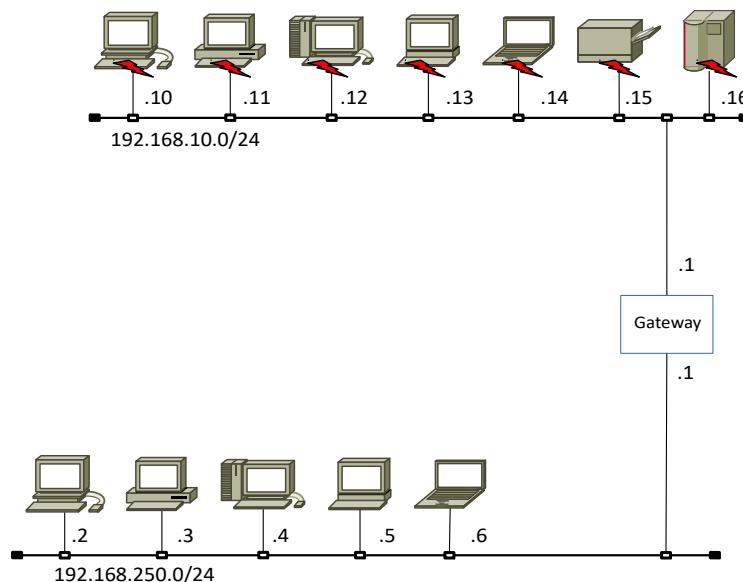


Abbildung 336 : Ein Gateway verbindet Netze unterschiedlicher Protokolle

Ein Gateway verbindet verschiedene Netzwerke mit unterschiedlichen Protokollen. Kollisionen und Broadcasts bleiben auf ein Segment begrenzt.

22.2.2 - Gateways im ISO-RM

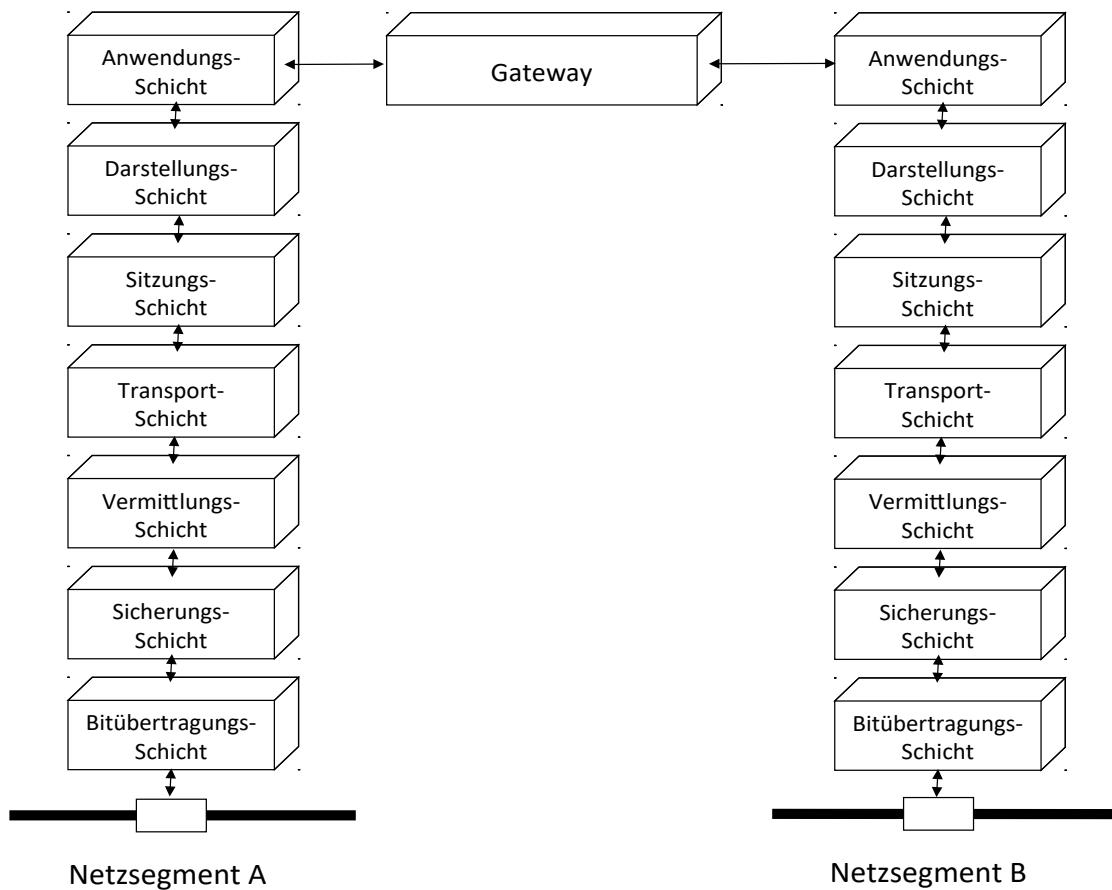


Abbildung 337 : Gateway im ISO-RM

Da Gateways Netzwerke auf Ebene 7 miteinander verbinden, müssen die Pakete vollständig auseinander genommen und danach in einer anderen Struktur wieder zusammengesetzt werden. In diesem Fall arbeiten Gateways als Protokoll-Umsetzer. Gateways werden auch bei den Firewalls eingesetzt. Siehe hierzu auch Application Level Gateways (ALGs)

22.2.3 - Mischformen von Netzwerkgeräten

Mittlerweile gibt es bei den Netzwerkgeräten unterschiedliche Ausprägungen. Einerseits wurden bei vielen Herstellern zusätzliche Funktionalitäten zu den Geräten hinzugefügt (Z. B. Layer-3-Switches) und andererseits beinhalteten einige Geräte die Funktionalität von anderen Gerätegruppen (Z. B. Switching Hubs). Es empfiehlt sich hier bei den einzelnen Herstellern zu hinterfragen, was mit den Funktionserweiterungen gemeint ist.



22.3 - Collision-Domain / Broadcast-Domain

Eine Collisiondomain (Kollisions-Bereich) ist der Netzwerkbereich, der von einer Kollision betroffen ist. Da eine Kollision auf der ISO-RM-Ebene 1 stattfindet, wird sie von Repeatern weitergeleitet und von Brücken, Switches oder Routern nicht weitergeleitet.

Eine Broadcastdomain (Broadcast-Bereich) ist der Netzwerkbereich, der von einem Broadcast erreicht wird. Da ein Broadcast auf der ISO-RM-Ebene 2 oder 3 stattfindet, wird er von Repeatern, Brücken und Switches weitergeleitet, jedoch von Routern nicht weitergeleitet.

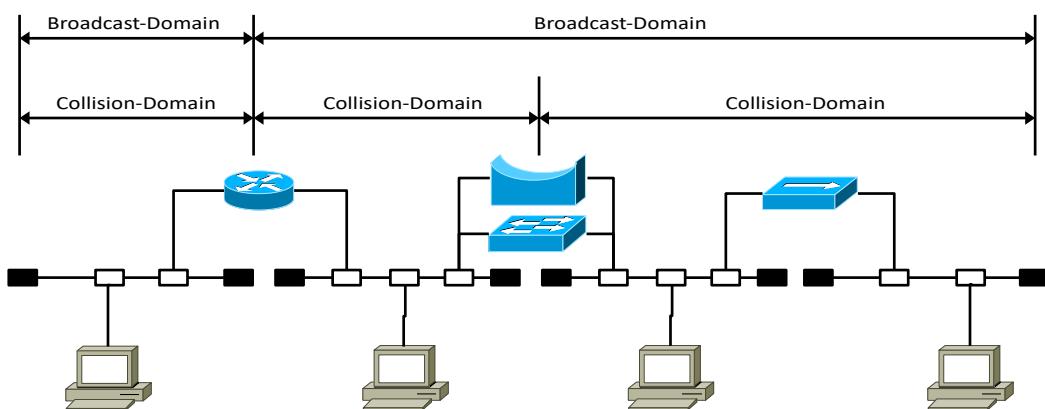


Abbildung 338 : Collision/Broadcast-Domain

23 - Protokoll-Funktionen

Damit Protokolle funktionieren sind eine Reihe von Voraussetzungen zu erfüllen die im Folgenden beschrieben sind.

23.1 - Vermittlung

Hierbei wird festgelegt wie die unterschiedlichen Kommunikationspartner eine Verbindung aufbauen. Es geht hierbei um die Verbindung von Kommunikationsteilnehmern auch über Teilnetzwerke hinweg. Im Laufe der Zeit wurden unterschiedliche Methoden entwickelt.

- ➊ Leitungsvermittlung
- ➋ Speichervermittlung
- ➌ Paketvermittlung

23.1.1 - Verbindungsorientierte Übertragung

Eine verbindungsorientierte Übertragung hat folgende Eigenschaften:

- ➊ Nutzung eines virtuellen Kanals
- ➋ Der Kanal ist vor dem Datenaustausch aufzubauen
- ➌ Datenzuordnung über die Kanalnummer. Die Kanalnummer wird beim Verbindungsaufbau vergeben.

23.1.2 - Verbindungslose Übertragung

Es ist auch eine Datenübertragung ohne einen vorher durchgeföhrten Verbindungsaufbau denkbar. Dabei gelten folgende Eigenschaften:

- ➊ Datentransport über mitgegebene Adress-Informationen
- ➋ Kein Verbindungsaufbau und kein Verbindungsabbau.

23.1.3 - Leitungsvermittlung

Hierbei wird jeder Kommunikations-Teilnehmer über einen dedizierten Verbindungssatz mit dem Kommunikationspartner verbunden. Dies war in den Anfängen der Telefonie der Fall als die Verbindungen manuell durch das Fräulein vom Amt hergestellt wurden.

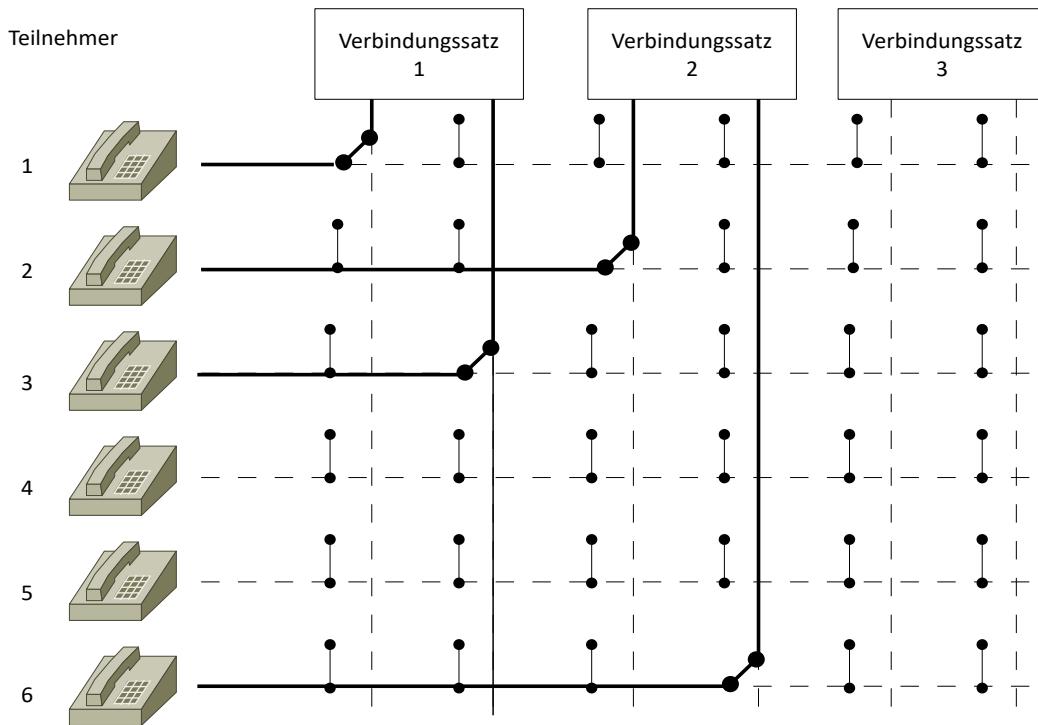


Abbildung 339 : Leitungsvermittlung

Eigenschaften

- ➊ Laufzeit = Signallaufzeit + Verbindungs-Aufbauzeit
- ➋ Teuer
- ➌ Ineffizient

23.1.4 - Speichervermittlung

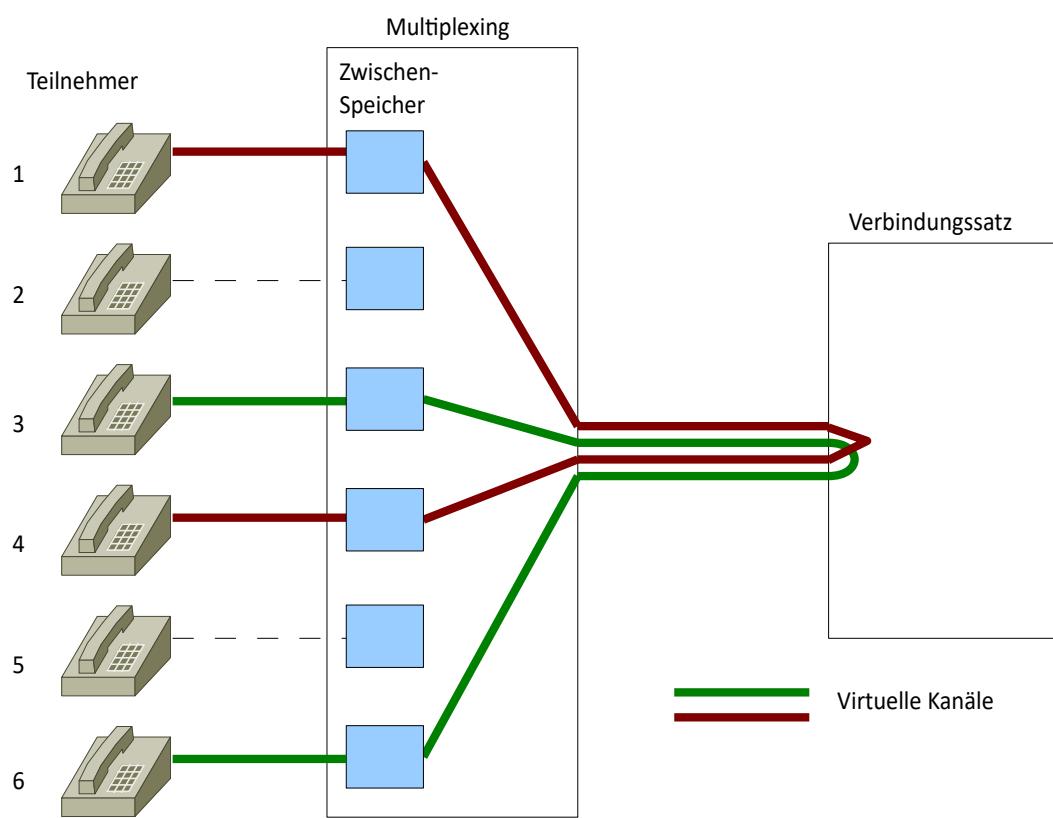


Abbildung 340 : Speichervermittlung

Eigenschaften

- ➊ Eine physikalische Ende-zu-Ende Verbindung fehlt.
- ➋ Die Kanalnummern werden beim Verbindungsaufbau vergeben.
- ➌ Es gilt: Laufzeit = Signallaufzeit + Summe der Speicherzeiten.

23.1.5 - Paketvermittlung

Werden Nachrichten in einzelne Pakete gestückelt transportiert, dann spricht man von Paketvermittlung. Dadurch kann der Zwischenspeicher für die Vermittlungssysteme klein gehalten werden.

23.2 - Signalisierung

Für den Verbindungsaufbau und den Verbindungsabbau werden Steuersignale benötigt. Die Übertragung von Steuersignalen wird in zwei Bereiche unterteilt:

- ➊ Teilnehmer-Signalisierung
- ➋ Netz-Signalisierung

Beide Bereiche zusammen werden Ende-zu-Ende-Signalisierung genannt.

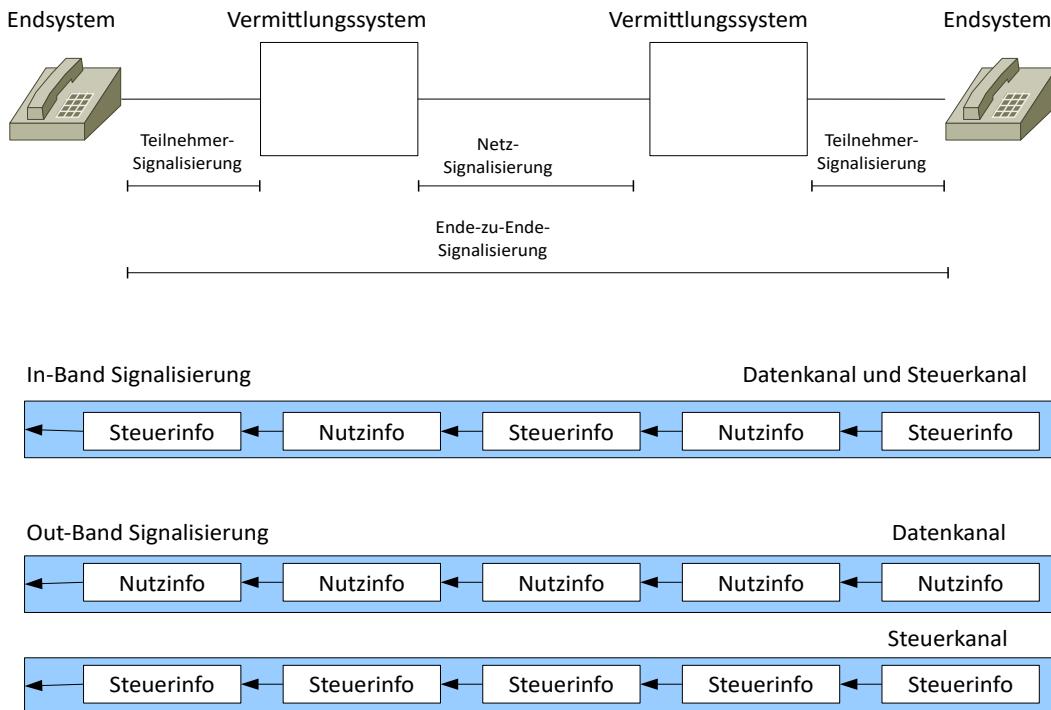


Abbildung 341 : Signalisierung

Die Übertragung der Steuersignale kann entweder im gleichen Kanal wie die Übertragung der Nutzdaten (In-Band Signalisierung) vorgenommen werden oder in einem getrennten Steuerkanal (Out-Band Signalisierung).

23.3 - Multiplexing

Um mehrere Kanäle auf einen Kanal zusammen zu fassen gibt es verschiedene Möglichkeiten:

- ➊ Raum-Multiplex Räumlich getrennte Weiterleitung -> Mehrere Leitungen
- ➋ Frequenz-Multiplex Frequenz-Umsetzung erforderlich
- ➌ Zeit-Multiplex Plesiochrone und synchrone digitale Hierarchie
- ➍ Wellenlängen-Multiplex Optische Übertragungstechnik
- ➎ Code-Multiplex Spread Spektrum z. B. bei WLAN Fehlerbehandlung

Eine Fehlerbehandlung findet in fast allen Schichten des ISO-RM statt. Je früher, also in den unteren Schichten, desto besser oder einfacher ist die Fehlerbehandlung.

23.3.1 - Fehlerarten

Fehler können als Einzelfehler oder als Burst-Fehler (mehrere Fehler hintereinander) auftreten.

23.3.2 - Fehler-Erkennung und -Korrektur

Für eine Erkennung von Fehler kommen unterschiedliche Verfahren zum Einsatz:

- ➊ Parity
- ➋ CRC
- ➌ FEC
- ➍ Quittungen

23.4 - Flusskontrolle

Eine Flusskontrolle wird auf unterschiedlichen Ebenen des ISO-RM eingesetzt. Eine Flusskontrolle ist immer dann notwendig, wo eine Datenquelle schneller sendet als der Empfänger die ankommenden Daten verarbeiten kann. Es kann auch vorkommen, dass bei einem Datentransport über mehrere Netzwerke hinweg ein Transitnetzwerk einen langsamen Datendurchsatz hat. Auch hier muss der Sender gebremst werden.

Um die Datenübertragung über solche Strecken hinweg zu optimieren wird die übertragende Information in mehrere kleine Stücke, die so genannten Pakete, zerlegt. Dieser Vorgang wird Fragmentierung genannt. Das

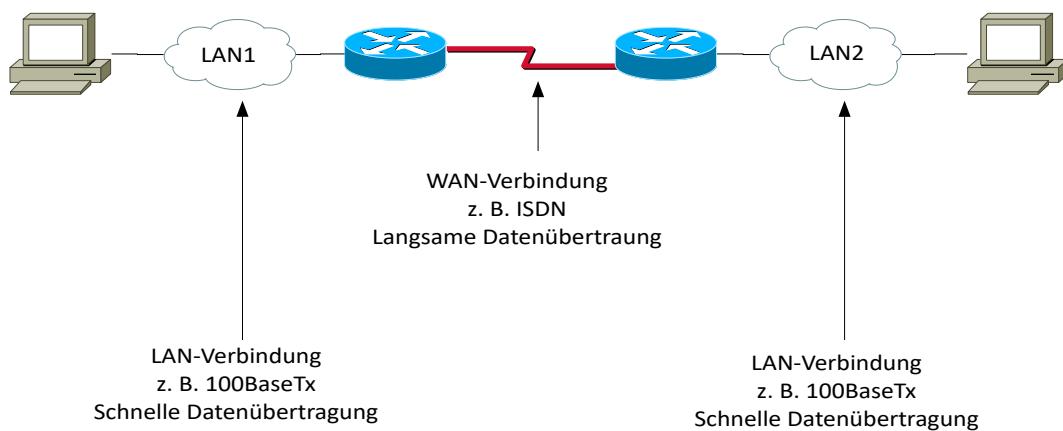


Abbildung 342 : Flusskontrolle

Zusammenfügen der einzelnen Pakete in die zusammenhängende Information auf der Empfängerseite nennt man Reassemblierung.

Protokoll-Funktionen

Die Gründe dafür sind:

- ➊ Je länger ein Datenpaket ist , desto größer ist die Wahrscheinlichkeit, dass ein Bitfehler auftritt und das gesamte Paket wiederholt werden muss.
- ➋ Multiplexing soll möglich sein damit mehrere Kommunikationsbeziehungen über den gleichen Weg bedient werden können.
- ➌ Der Empfänger hat nur eine begrenzte Empfangspuffer-Größe

Realisiert wird dies durch folgende Techniken:

- ➊ Sliding Window
- ➋ Automatic Repeat Request
- ➌ Stop and Wait
- ➍ Go back N
- ➎ ARQ (Selective Reject Automatic Repeat Request)

23.4.1 - Übertragungswiederholung

Jedes Paket das auf der Empfängerseite richtig verarbeitet wurde, wird zurückgesendet. Ist auf der Sendeseite das gesendete Paket identisch mit dem eingetroffenen Quittungspaket, kann das nächste Paket gesendet werden. Besteht keine Übereinstimmung zwischen dem gesendeten Paket und dem Quittungspaket wird das gesendete Paket nochmals wiederholt. Ein Nachteil dieser Übertragungsform ist, dass zum einen die Datenleitung nicht optimal ausgelastet wird da vor jeder weiteren Übertragung eines Pakets erst die Quittung eintreffen muss. Zum anderen wird das gesamte Paket nochmals übertragen.

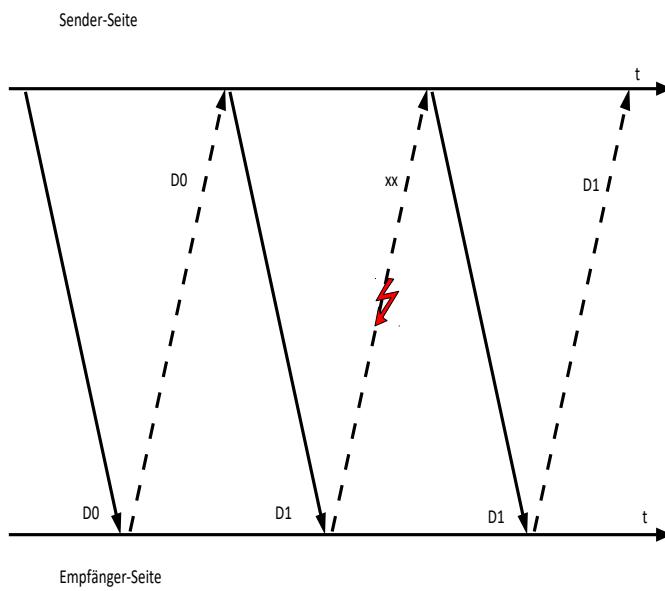


Abbildung 343 : Übertragungswiederholung

Wird auf der Empfängerseite das Paket nicht oder fehlerhaft empfangen kann keine Quittung zurückgesendet werden. Damit fehlt die Quittung auf der Sendeseite. Damit die Datenübertragung an dieser Stelle nicht stecken bleibt wird auf der Empfängerseite nach dem Senden eines Paketes ein Timer aufgezogen. Trifft die Quittung ein bevor der Timer abgelaufen ist, kann der Timer gelöscht werden. Läuft der Timer jedoch ab wird ein Timeout signalisiert und das Paket muss wieder holt werden.

23.4.1.1 - Stop and Wait

Eine Optimierung der Übertragungswiederholung ist das Stop and Wait Verfahren. Dabei wird anstelle des gesamten empfangenen Datenpakets vom Empfänger nur ein kurzes Quittungspaket (ACK = Acknowledge) an den Empfänger zurückgesendet.

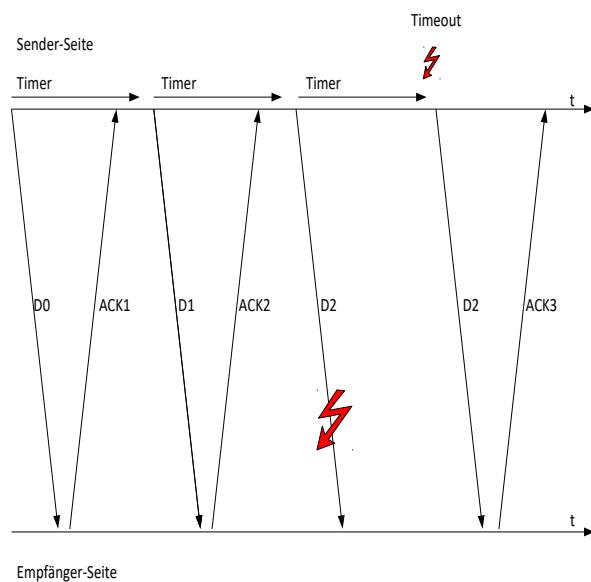


Abbildung 344 : Stop and Wait

Allerdings wird auch hier die vorhandene Kanalkapazität nicht optimal ausgenutzt.

23.4.1.2 - Sliding Window

Bei dieser Fenstertechnik geht man davon aus, dass mehrere Pakete gesendet werden können bevor sie zu quittieren sind. Der Sender hat beim Empfänger einen so genannten Kredit. Der Kredit ist ein Zähler der auf der Sendeseite verwaltet wird. Dieses Verfahren setzt voraus, dass auf der Sender- und der Empfängerseite die zu übertragenden Daten zwischengespeichert werden. Jedes gesendete Paket dekrementiert beim Sender den Kredit um den Wert 1. Jede empfangene Quittung inkrementiert den Kredit-Wert um mindestens eins (bei Sammelquittungen kann der Kredit um mehr als den Wert 1 inkrementiert werden). Beim Sliding Window geht man von einem kontinuierlichen Datenstrom aus der in einzelne durchnummelierte Pakete unterteilt ist. Die Fenstergröße, also der Kredit, wird beim Verbindungsauflauf von beiden Kommunikationspartner festgelegt. Damit ist klar, dass dieses Verfahren nur bei einem verbindungsorientierten Verfahren Anwendung finden kann. Die Fenstergröße ist von folgenden Parametern abhängig:

- Durchsatz
- Verzögerungszeit
- Rahmengröße
- Fehlerwahrscheinlichkeit

Im folgenden Beispiel steht der Kredit bei Beginn der Datenübertragung auf 3. Damit kann der Sender 3 Pakete senden bevor er auf eine Quittung warten muss.

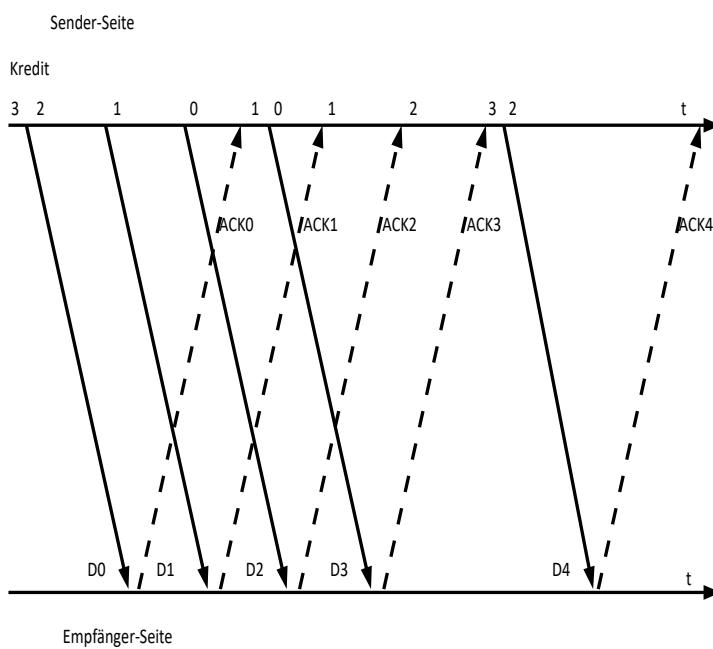


Abbildung 345 : Fenstertechnik

Der Sender sendet die Pakete D0, D1 und D2. Mit dem Senden eines jeden Paketes wird der Kredit um den Wert 1 dekrementiert. Nachdem die ersten 3 Pakete gesendet wurden ist der Kredit auf 0 und damit darf der Sender keine weitere Pakete mehr senden. Nachdem der Sender die Quittung für das erste Paket (ACK0) empfangen hat wird der Kredit um den Wert 1 erhöht. Damit darf der Sender wiederum ein Paket senden. Nach dem Senden des Pakets D3 ist der Kredit wiederum auf den Wert 0 gesunken und der Sender muss warten. Nun treffen in schneller Folge die Quittungen (ACK1, ACK2 und ACK3) beim Sender ein. Damit ist der Kredit wieder auf den Wert 3 angestiegen. Der Sender sendet nun das Paket D4.

Ein schneller Empfänger kann die ankommenden Pakete schnell verarbeiten. Er wird die Quittungen also auch schnell zurück senden.

Ein langsamer Empfänger braucht für die Verarbeitung mehr Zeit und wird deshalb die Quittungen später senden.

Mit dieser Technik kann einerseits die Leitung besser ausgenutzt werden und andererseits die Leistungsfähigkeit des Empfängers die Sende-Geschwindigkeit (Pakete pro Zeiteinheit) des Senders steuern.

Eine weitere Optimierung ist das Zusammenfassen von Quittungen in einer Sammelquittung. Wenn z. B. nur jedes 5. Paket zu Quittieren ist kann Netzlast eingespart werden.

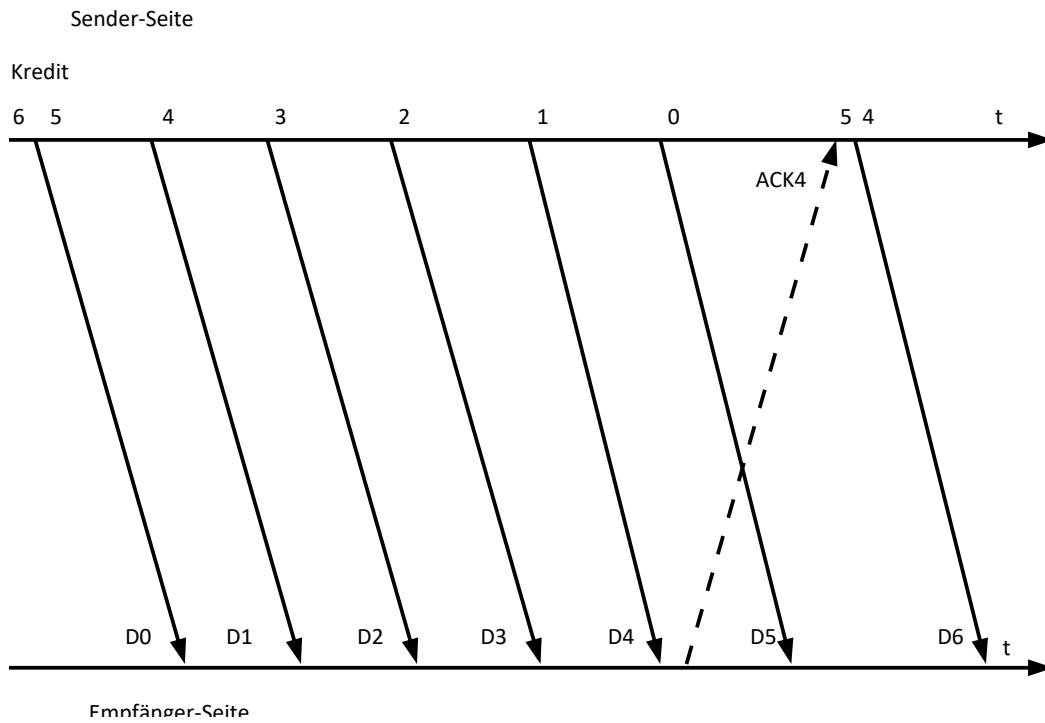


Abbildung 346 : Zusammenfassung von Quittungen

Hierbei wird schnell klar, dass der Sender alle nicht quittierten Pakete zwischenspeichern muss. Im obigen Beispiel wird jeder 5. Rahmen quittiert.

Die so genannte Fenstergröße (Window Size) ist 6. Nach dem Senden von 6 Paketen ist der Kredit erschöpft. Der Sender muss warten. Der Empfang von ACK4 bedeutet, dass die Rahmen D0 – D4 quittiert wurden. Nachdem Empfang der Quittung ACK4 können wieder 5 Pakete gesendet werden.

Eine weitere Optimierung ist, dass eine Quittung an ein Paket angehängt werden kann das der Empfänger an den Sender sendet. Dieses Verfahren wird Piggybacking-Verfahren genannt und wird z. B. bei TCP eingesetzt.

23.4.2 - Fehlerbehandlung bei der Fenstertechnik

Bleiben beim Empfänger Quittungen aus oder kommen beim Empfänger defekte Pakete an kann mit unterschiedlichen Mitteln reagiert werden.

23.4.2.1 - Go back n

Sobald ein Paket gesendet wurde wird ein Timer gesetzt und angestoßen. Trifft keine Quittung ein dann erzeugt der Timer einen Timeout. Sobald ein Timeout signalisiert wird werden alle Timer zurückgesetzt und ab dem Paket mit der vermissten Quittung werden alle Pakete nochmals gesendet.

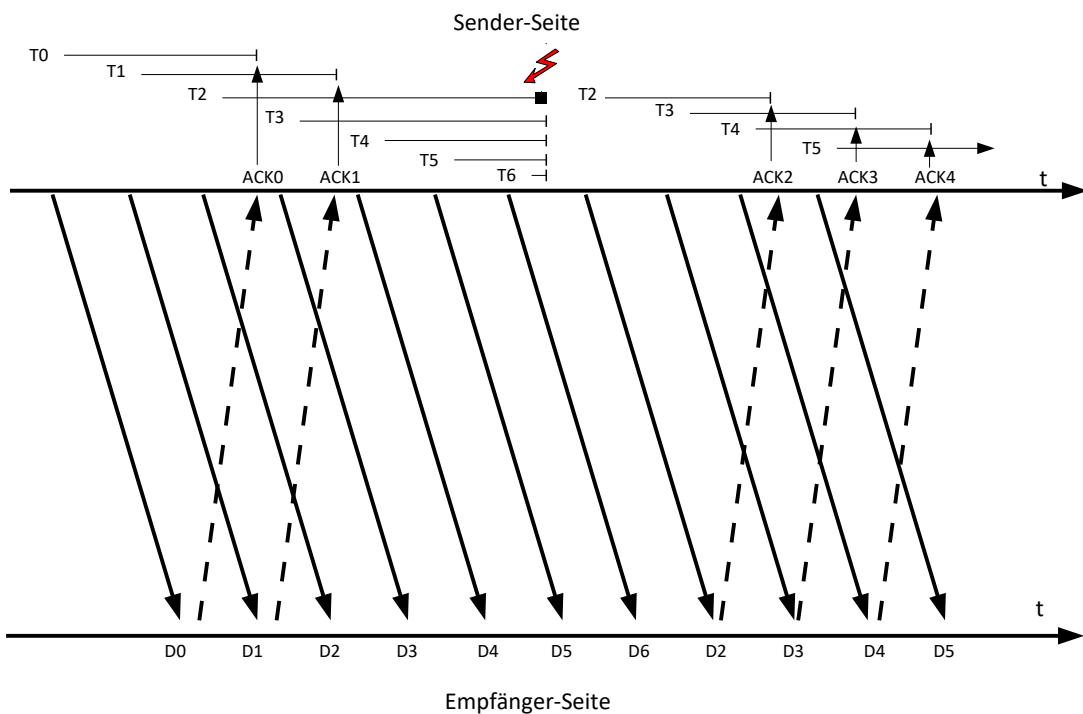


Abbildung 347 : Go back n

Im obigen Beispiel werden die Timer T0 und T1 durch die beiden Quittungen ACK0 und ACK1 rechtzeitig zurückgesetzt. Der Timer T2 läuft ab und erzeugt einen Timeout. Die Timer T3 - T6 werden darauf hin zurückgesetzt. Ab dem Paket D2 werden nochmals alle Pakete gesendet.

Je nach Timer-Einstellung kann es vorkommen, dass viele Pakete zu wiederholen sind obwohl sie bereits korrekt auf der Empfängerseite angekommen, jedoch noch nicht quittiert sind.

23.4.2.2 - Selective Repeat

Beim Selective Repeat wird für jedes gesendete Paket ein Timer aufgezogen. Läuft ein Timer ab, erzeugt der zugehörige Timeout nur ein erneutes Senden des unquittierten Paketes.

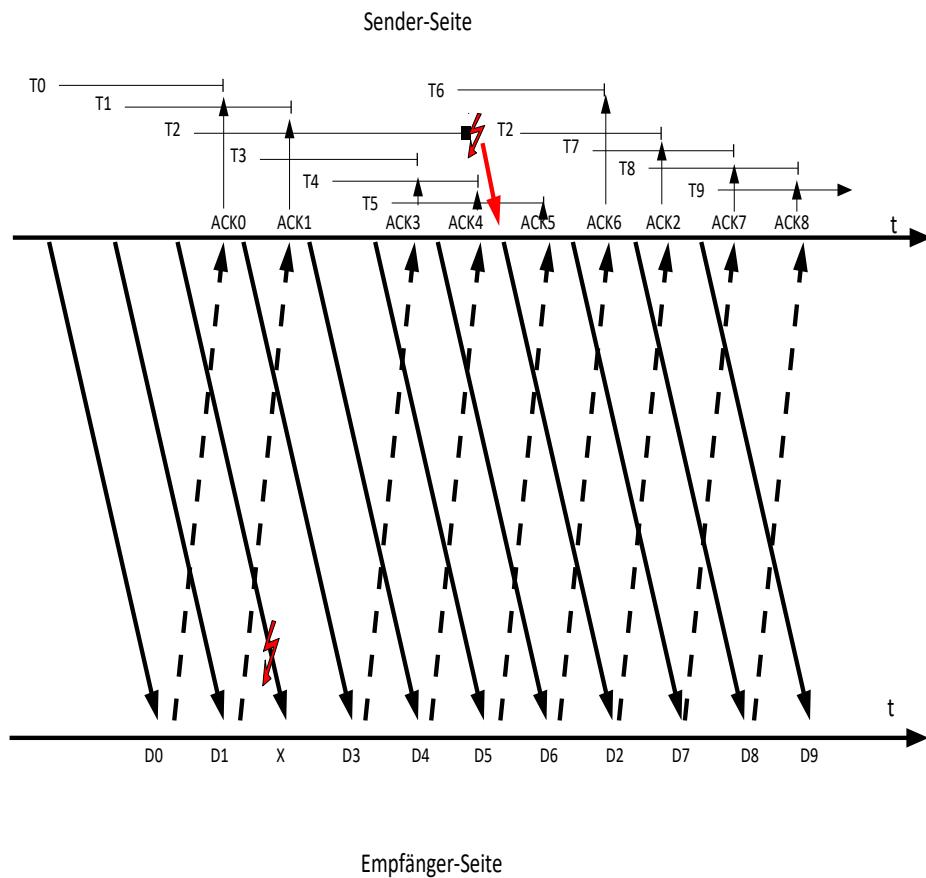


Abbildung 348 : Selective Repeat

Im obigen Beispiel kommt das Paket D2 nicht beim Empfänger an. Dieser sendet deshalb auch keine Quittung an den Sender zurück. Beim Sender läuft deshalb der Timer T2 ab. Der zugehörige Timeout bewirkt, dass das Paket D2 nochmals gesendet wird.

Diese Vorgehensweise nutzt den Übertragungskanal besser aus da nur das fehlerhafte Paket wiederholt wird. Dies wird durch eine intelligenter und deshalb aufwändigere Paketverwaltung auf beiden Seiten erkauft.

23.4.2.3 - Selective Reject ARQ

Die Fehlerbehandlung ist der vom Selective Repeat ähnlich. Es sind alle Pakete bis zur lückenlosen Quittungssequenz zwischengespeichert. Bei dieser Fehlerbehandlung besteht die Möglichkeit, dass der Empfänger eine negative Quittung (NACK) an den Sender zurück sendet. Der Empfänger kann damit auf ausgebliebene oder fehlerhafte Pakete reagieren. Um ausgebliebene Pakete zu erkennen, ist eine Paketverwaltung mit Sequenznummern notwendig. Bleibt ein Paket aus hat das nächste Paket die nächst höhere Sequenznummer.

23.5 - Zusammenfassung

Leitungsvermittlung vs. Paketvermittlung

Bei der klassischen Kommunikation hat der Teilnehmer das Gefühl, dass die Verbindung nur für ihn alleine reserviert und geschaltet wurde. Er hat das Gefühl eines exklusiven Kanals. In Wahrheit wird die Verbindung, falls keine Ressourcen mehr frei sind, mit einem Besetztzeichen abgewiesen.

Bei der Paketvermittlung wird die zu übertragende Information in kleine Teile zerlegt und getrennt voneinander auf die Reise gesendet. Durch die Adressinformation im Header findet das Paket seinen Weg zum Ziel selbst. Somit können sich viele Informationsströme einen Kanal teilen. Jedes Paket wird in den Vermittlungsknoten getrennt für sich behandelt und erfährt dort eine andere Verzögerung. In einem Paketnetz können mehr als die Summe der Spitzenwerte der angeschlossenen Quellen übertragen werden, da statistisch nicht alle Quellen gleichzeitig mit ihrem Maximum senden. Es reicht ein statistisches Mittel zur Verfügung zu stellen. Man kann also so viele Quellen zulassen, wie die Summe ihrer mittleren Verkehre nicht die Transportkapazität überschreitet.

Im Paketbetrieb gibt 3 unterschiedliche Verfahren:

- ➊ Synchroner Transfermodus
Wird z. B. bei PCM30 realisiert. Dort wird als elementare Einheit ein Zeitschlitz durch ein Oktett repräsentiert. Die Verbindung ist dadurch festgelegt, dass immer der gleiche Zeitschlitz in jedem Rahmen verwendet wird.
- ➋ Paket-Transfer-Mode
Dieser Mode wird beim Paketvermittlungssystem X.25 bearbeitet. Die Pakellänge ist innerhalb eines festgelegten Rahmens variabel. Die Verbindung wird durch die Quell- und Ziel-Informationen im Header repräsentiert.
- ➌ Asynchroner Transfer-Mode
Hier handelt es sich um eine Sonderform bei der die Pakete eine feste Länge haben. Man spricht hier auch nicht von Paketen sondern von Zellen. Vom synchronen Transfer-Mode wurde der Zelltakt übernommen und vom Paket-Transfermode die Header.

Elementare Einheit: Zeitschlitz im Rahmen / Verbindung: fester Zeitschlitz in jedem Rahmen

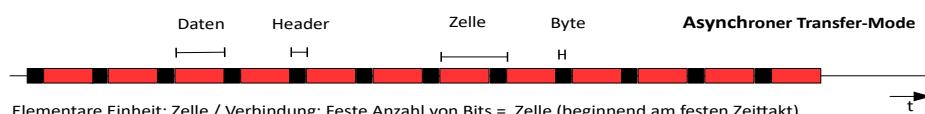
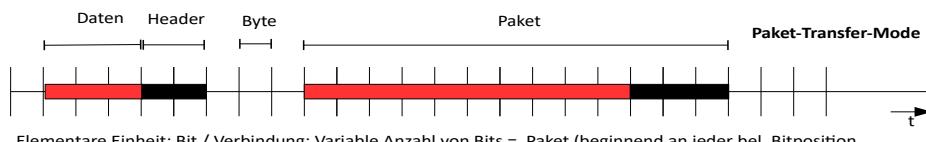
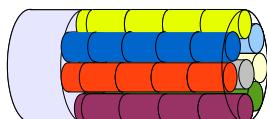
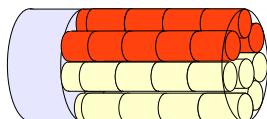


Abbildung 349: Transfermodi

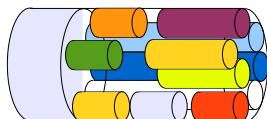
In der folgende Abbildung sind die Verhältnisse nochmals mit Röhren dargestellt, die einer Übertragungskapazität entsprechen.



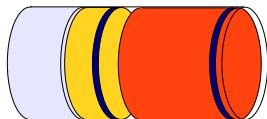
Synchroner Transfermodus
Leitungsvermittlung
Zeitschlitz



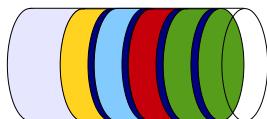
Multirate Circuit Switching
Leitungsvermittlung
Zeitschlitz
Kanalbündelung



Fast Circuit Switching
Leitungsvermittlung
Freigabe nach Nutzung / Schneller Wiederaufbau



Packet-Transfer-Mode
Paketvermittlung (Zielinformation im Header)
Unterschiedlich große Pakete



Asynchroner-Transfer-Mode
Zellvermittlung (Zielinformation im Header)
Alle Zellen haben die gleich Größe

Abbildung 350: Kommunikationsprinzipien

	Leitungsvermittelt	Paketvermittelt
Verbindungsorientiert	PSTN / ISDN	X.25 Frame Relay ATM
Verbindungslos	Keine Anwendung	IP

24 - Protokolle

24.1 - Übersicht

In Anlehnung an das DARPA-RM und das ISO-RM ist in der folgenden Abbildung, eine Übersicht der Protokolle mit einer Zuordnung zu den entsprechenden Ebenen der Referenzmodelle dargestellt.

DARPA-Layer		ISO-Layer									
4 Prozess/Anwendung	Daten-Übertragung	Electronic-Mail	Terminal-Emulation	Daten-Übertragung	Client-Server	Netzwerk-Verwaltung	7 Anwendung				
	File-Transfer-Protocol (FTP) RFC 959	Simple-Mail-Transfer-Protocol (SMTP) RFC 821	TELNET RFC 854	Trivial-File-Transfer-Protocol (TFTP) RFC 783	SUN Network-File-Systems-Prot. (NFS) RFC 1014, 1057, 1094	Simple-Network-Management-Protocol (SNMP) RFC 1157	6 Presentation				
3 Host-to-Host	Transmission-Control-Protocol (TCP) RFC 793			User-Datagram-Protocol (UDP) RFC 768			5 Session				
2 Internet	Address-Resolution-Protokoll ARP RFC 826 RARP RFC 903	Internet-Protokoll (IP) RFC 791		Internet-Control-Message-Protokoll (ICMP) RFC 792		3 Network					
1 Netzwerk-Schnittstelle	Netzwerkschnittstellenkarten Ethernet, StarLAN, Token-Ring, ARCNET RFC 894, 1042, 1201					2 Data-Link					
	Übertragungsmedium Twisted Pair, Koax, Fiberglas, drahtlose Medien					1 Physical					

Abbildung 351 : Protokoll-Übersicht

Zu beachten ist hierbei die unterschiedliche Aufteilung in Ebenen beim DARPA-Modell im Vergleich zum ISO-Referenzmodell.

24.2 - Einführung

Die Protokolle auf Ebene 1 und 2 werden in der Hardware der Netzwerkkarte (NIC = Network Interface Controller) realisiert.

24.3 - Aufbau eines Rahmens auf der Leitung

In der folgenden Abbildung wird auf den Aufbau der Daten, die über eine Leitung transportiert werden eingegangen.

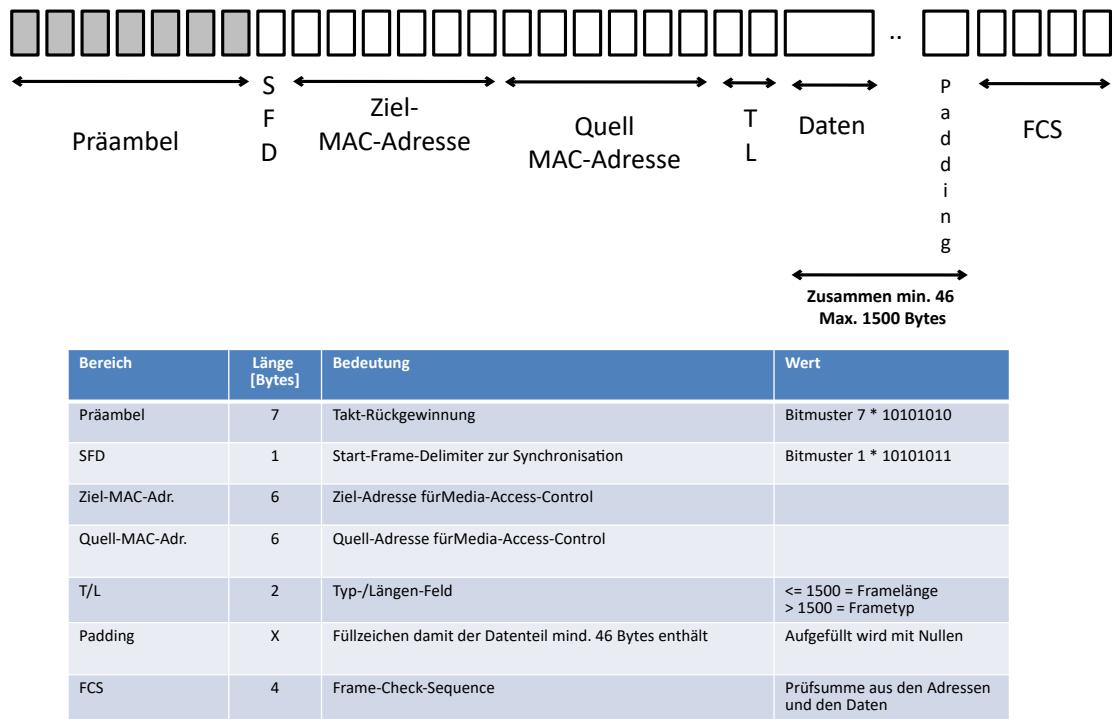


Abbildung 352 : Aufbau eines Rahmens auf der Leitung

Vor allem die Bitmuster der Präambelfelder sind hier interessant.

Bis auf die Daten werden alle Informationen von der Netzwerkkarte erzeugt und bearbeitet.

24.4 - Ethernet Protokolle

Im Folgenden wird auf die Unterschiede der derzeit üblichen 4 Frame-Formate eingegangen.

Die Adressierung erfolgt hier in der kanonischen Form. Dies bedeutet, dass das niedrigwertigste Bit eines Bytes auf der Leitung als erstes übertragen wird (LSB = Least Significant Bit). Bei der nicht kanonischen Adressierung wird das höchstwertigste Bit zuerst übertragen (MSB = Most Significant Bit). (Siehe hierzu FDDI und Token Ring)

Am Anfang eines jeden Frames müssen sich die Netzwerkkarten auf den Frame synchronisieren. Dazu wird die Präambel benutzt. Hier wird ein 10101010...-Bitmuster auf die Datenleitung gelegt.

Bis auf IEEE802.3 werden 8 Präambel-Bytes genutzt. IEEE802.3 hat 7 Präambel-Bytes und ein Start-Frame-Delimiter-Byte. Damit sind es auch wieder 8 Bytes für den Header der Ebene 1.

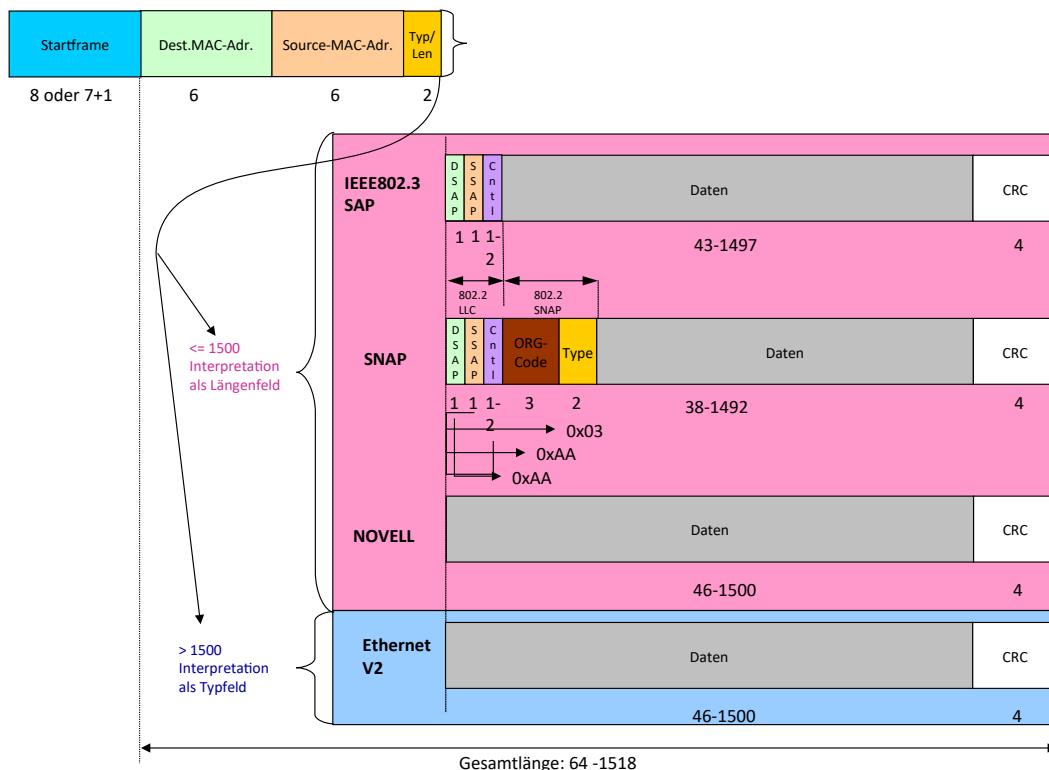


Abbildung 353 : Ethernet-Formate

Die nächsten 2 Felder sind bei allen Formaten gleich. Hierbei handelt es sich um die Ziel- und die Quell-MAC-Adresse. Das nächste Feld ist das Typ- oder Längenfeld. Je nach Wert dieses 2 Byte wird das Feld als Typ- oder Längenangabe interpretiert. Ist der Wert kleiner oder gleich 1500, handelt es sich um eine Längenangabe. Ist der Wert größer als 1500, handelt es sich um eine Typ-Angabe. Die möglichen Typen sind im RFC 1700 beschrieben. In der obigen Abbildung sind die unterschiedlichen verfügbaren Datenfeldgrößen auffallend. Ausgehend von 1518 Byte für die Frame-Gesamtlänge stehen je nach verwendetem Protokoll zwischen 1492 und 1500 Byte zur Verfügung.

24.4.1 - NOVELL

Ethernet 802.3 wurde vor der Normierung durch IEEE von Novell veröffentlicht.

Es wurde von Novell als Standard-Frame für IPX/SPX verwendet. Direkt auf diesen Frame kann nur IPX/SPX gebunden werden!

Alle anderen Protokolle brauchen Erweiterungen im Header, um funktionieren zu können!

24.4.2 - IEEE-802.3

Bei der Normierung von IEEE wurde der Vorschlag von Novell modifiziert. Bei den Präambel-Bytes wurde das letzte Byte zu einem SFD (Start-Frame-Delimiter deutsch: Startrahmenbegrenzer) umgebaut.

Das Längenfeld kann den Maximalwert 1500 aufweisen. Steht an der Stelle des Längenfeldes ein Wert > 1500 (0x5DC), dann handelt es sich um einen anderen Frametyp (Ethernet V2).

Hinter dem Längenfeld wurde der so genannte LLC-Header (Logical-Link-Control) eingeführt. Er ist in IEEE-802.2 definiert und in einem der folgenden Kapitel näher beschrieben.

Er enthält:

1 Byte DSAP(Destination-Service-Access-Point) um bei einer Verbindung zwischen zwei Rechnern mehrere Verbindungen parallel zu betreiben und damit unterschiedliche Applikationen auf einem Rechner ansprechen zu können.

1 Byte SSAP(Source-Service-Access-Point)

1-2 Byte Control

Auf diesen Frametyp lassen sich IPX/SPX und NetBEUI binden.

24.4.3 - SNAP

Da das eine Control-Byte bei der IEEE802.2-Definition nicht viele Möglichkeiten bietet, wurde der LLC-Header durch das SNAP (Subnet Access Protocol) erweitert. Hierbei wird das Control-Feld um ein 3Byte langes Organization-Code und ein 2 Byte langes Ethernet-Typ-Feld erweitert. Bei den DSAP und SSAP-Feldern ist fest 0xAA eingetragen und das Controlfeld hat den Wert 0x03. Hierauf lassen sich IPX/SPX, TCP/IP und Apple Talk Phase II binden. Diese Version wird oft dort angewendet, wo die Daten nicht über IP transportiert werden.

24.4.4 - Ethernet V2

Ethernet V2 wurde von den Firmen Digital Equipment Corp. Intel Corp. Und XEROX Corp (kurz DIX) entwickelt. Es entspricht dem ursprünglichen Vorschlag von Novell mit einer kleinen Modifikation. Anstelle des Längenfeldes ist ein Typfeld definiert. Hier sind Typ-Werte >1500 möglich (kleinere Werte bedeuten, dass es sich um den IEEE802.3-Frametyp handelt). Hierauf lassen sich IPX/SPX, TCP/IP und Apple Talk Phase I binden.

Die Interpretation des Typ-Längenfeldes als Typ weist auf die nächsthöhere Ebene hin. Hier ein paar Beispiele für Typen.

Hexadezimal-Wert	Binär-Wert	Protokoll
0800	2048	IP
0806	2054	ARP
0835	2101	Reverse-ARP
8100	33024	VLAN-Tag
8847	34887	MPLS-Unicast
8848	34888	MPLS-Multicast

24.5 - IEEE-802.2

24.5.1 - Allgemeines

Hier wird die so genannte LLC-Schicht (Logical Link Control; deutsch:logische Verbindungssteuerung) beschrieben. Die Hauptaufgabe der LLC-Schicht ist der Austausch von LLC-Frames zwischen den LLC-SAP's, den DLSAP's (Destination LSAP) und SLSAP's (Source LSAP). Diese SAP's sind als Kommunikationspuffer zu interpretieren.

24.5.2 - Typen

In der LLC-Schicht können verschiedene Verfahren des Datenaustauschs realisiert werden. Im Rahmen von IEEE802.2 sind folgende Dienst-Typen definiert:

- Verbindungsloser Dienst ohne Bestätigung Typ 1
 - Verbindungsorientierter Dienst mit Bestätigung Typ 2
 - Verbindungsloser Dienst mit Bestätigung Typ 3

24.5.3 - Dienste

Ein verbindungsloser Dienst benötigt keinen Verbindungsaufbau und keinen Verbindungsabbau. Zwischen den Kommunikationspartnern müssen keine besonderen Vereinbarungen getroffen werden. Der Sender sendet, ohne zu wissen, ob der Empfänger bereit ist, die Daten zu verarbeiten oder nicht. Dieser Dienst wird allgemein als Datagrammdienst bezeichnet. Er wird häufig bei Managementaufgaben eingesetzt.

Ein Verbindungsorientierter Dienst benötigt einen Verbindungsaufbau, bei dem diverse Parameter ausgehandelt werden können, bevor die Daten übertragen werden können. Nach der Datenübertragung ist die Verbindung zu beenden.

Mit den oben beschriebenen LLC-Typen werden 4 LLC-Betriebsklassen definiert, die in der folgenden Tabelle beschrieben sind.

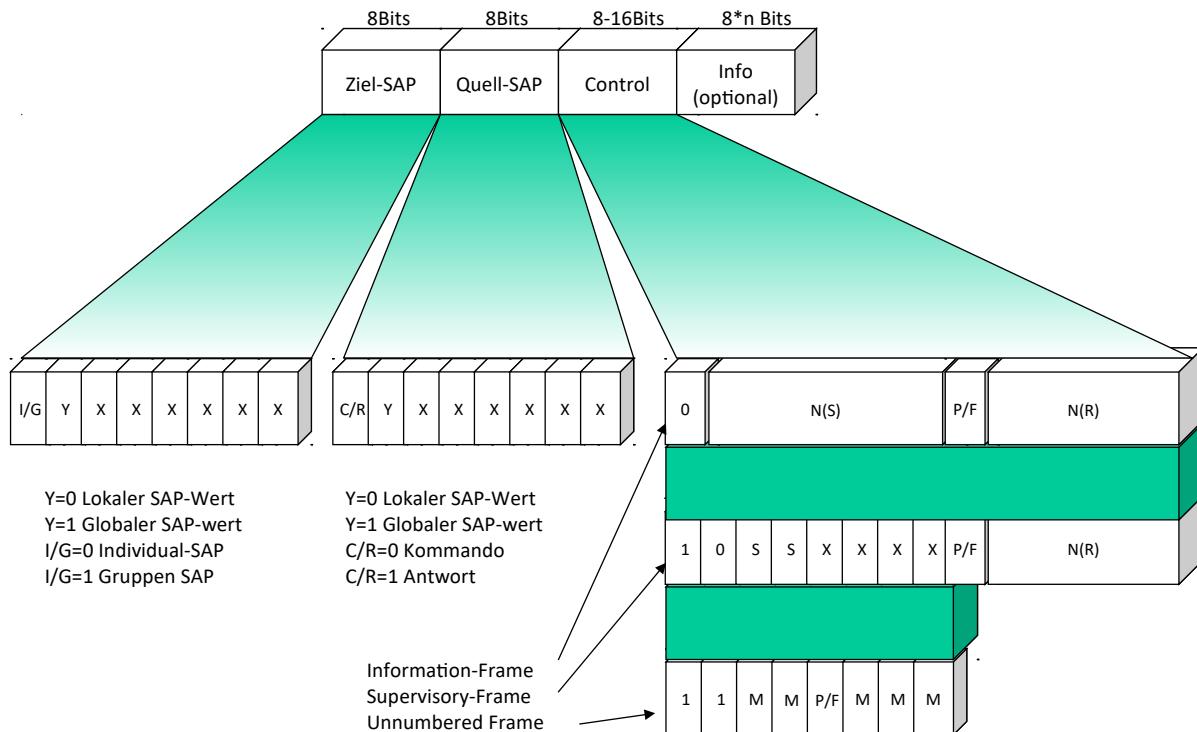
	Klasse I	Klasse II	Klasse III	Klasse IV
LLC-Typ 1	*	*	*	*
LLC-Typ 2		*		*
LLC-Typ 3			*	*

Die Betriebsklasse I unterstützt nur den LLC-Typ 1. Die Betriebsklasse IV unterstützt alle LLC-Typen.

Die LLC-Schicht realisiert somit ein LAN-Sicherungsprotokoll. Wie bei WLANs wird HDLC (High Level Data Link Control) eingesetzt, allerdings sind folgende Funktionen zusätzlich zu erbringen:

- Punkt-zu-Mehrpunkt-Verbindungen (Broadcast und Multicast)
 - verbindungslose und verbindungsorientierte Dienste
 - Multiplex-Funktion

24.5.4 - Aufbau von LLC-Frames



24.5.4.1 - I-Frames

I-Frames dienen zur Übertragung von Daten. Die Übertragung wird mit einer Sende-Folgenummer N(S) und einer Empfangs-Folgenummer N(R) kontrolliert. Die Werte können im Bereich von 1 bis 127 liegen.

24.5.4.2 - S-Frames

Die S-Frames dienen zur Signalisierung von Empfangs-Bereitschaft bzw. zur Signalisierung, dass keine Daten empfangen werden können.

Als S-Frames sind definiert:

- Receive Ready (RR) (deutsch: Empfangsbereit)
- Reject (REJ) (deutsch: Daten wurden verworfen)

- ➊ Receive Not Ready (RNR) (deutsch: Nicht Empfangsbereit)

24.5.4.3 - U-Frames

Die U-Frames dienen zur Übertragung weiterer Kontrollfunktionen. Dabei werden sie in Kommandos und Antworten unterteilt:

24.5.4.3.1 - Kommandos

- ➊ UI Unnumbered Informationen
- ➋ DISC Disconnect
- ➌ SABME Set Asynchronous Balanced Mode Extended
- ➍ XID Exchange Identifier
- ➎ TESTTest

24.5.4.3.2 - Antworten

- ➊ UA Unnumbered Acknowledgement
- ➋ DM Disconnect Mode
- ➌ FRMR Frame Reject
- ➍ AC0 Acknowledged Connectionless Information Sequence 0
- ➎ AC1 Acknowledged Connectionless Information Sequence 1
- ➏ XID Exchange Identifier
- ➐ TESTTest

24.6 - Zusammenfassung der Ethernet-Protokolle

Eine Kommunikation zwischen Stationen, welche unterschiedliche Frame-Formate einsetzen, ist nicht möglich. Allerdings können die Protokolle bei entsprechender Enkapsulierung über das gleiche Medium betrieben werden, da die Zugriffs-Mechanismen gleich sind (CSMA/CD).

Je nach verwendetem Format werden die Daten aufgebaut und übertragen. Es gibt auch Mischformen, in denen die Formate in anderen Formate eingepackt (enkapsuliert) werden.

Hierzu gibt es z. B. den RFC 1042.

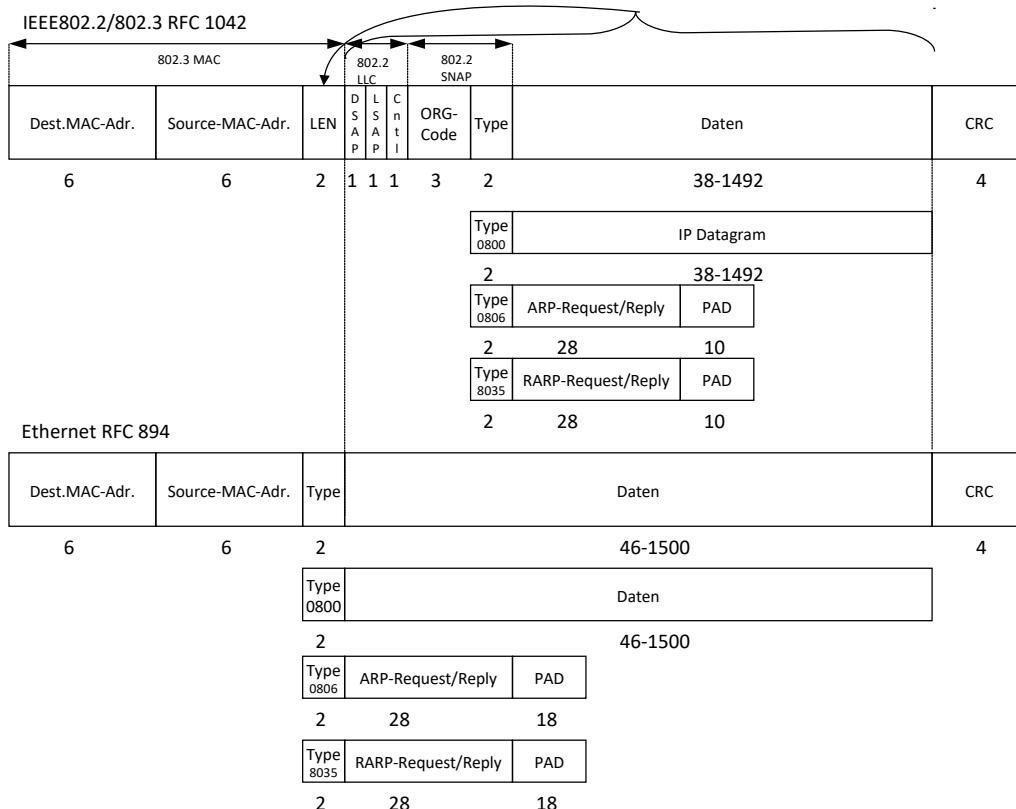


Abbildung 355 : Unterschiede-RFC894/RFC1042

Die obige Abbildung zeigt, wie Daten in das Ethernet II-Format und in das IEEE802.3-Format eingepackt werden kann.

Die Beispiele für Daten- und ARP/RARP-Übertragung zeigen die Konsequenzen. Die mögliche Rahmengröße ist bei Ethernet II maximal 1500 Bytes, beim IEEE-802.3-Format dagegen maximal 1492 Bytes.

24.7 - Mögliche Protokollbindungen

In der folgenden Abbildung soll dargestellt werden, wie die Schichten aufeinander aufbauen und wo die Unterscheidungsmerkmale in den Daten des Frames zu finden sind.

Auf der linken Seite sind die für die Verzweigung relevanten Teile im Rahmen markiert. Auf der rechten Seite sind die Protokolle den einzelnen ISO-RM-Schichten zugeordnet. Es gibt natürlich noch viel mehr Protokolle, die hier nicht aufgeführt sind. An entsprechender Stelle wird jedoch in den jeweiligen Kapiteln auf diese Struktur eingegangen. Es gibt diverse Hersteller, die zu Werbezwecken ganze Poster mit den Versuchen, eine Übersicht zu erstellen, voll pinseln.

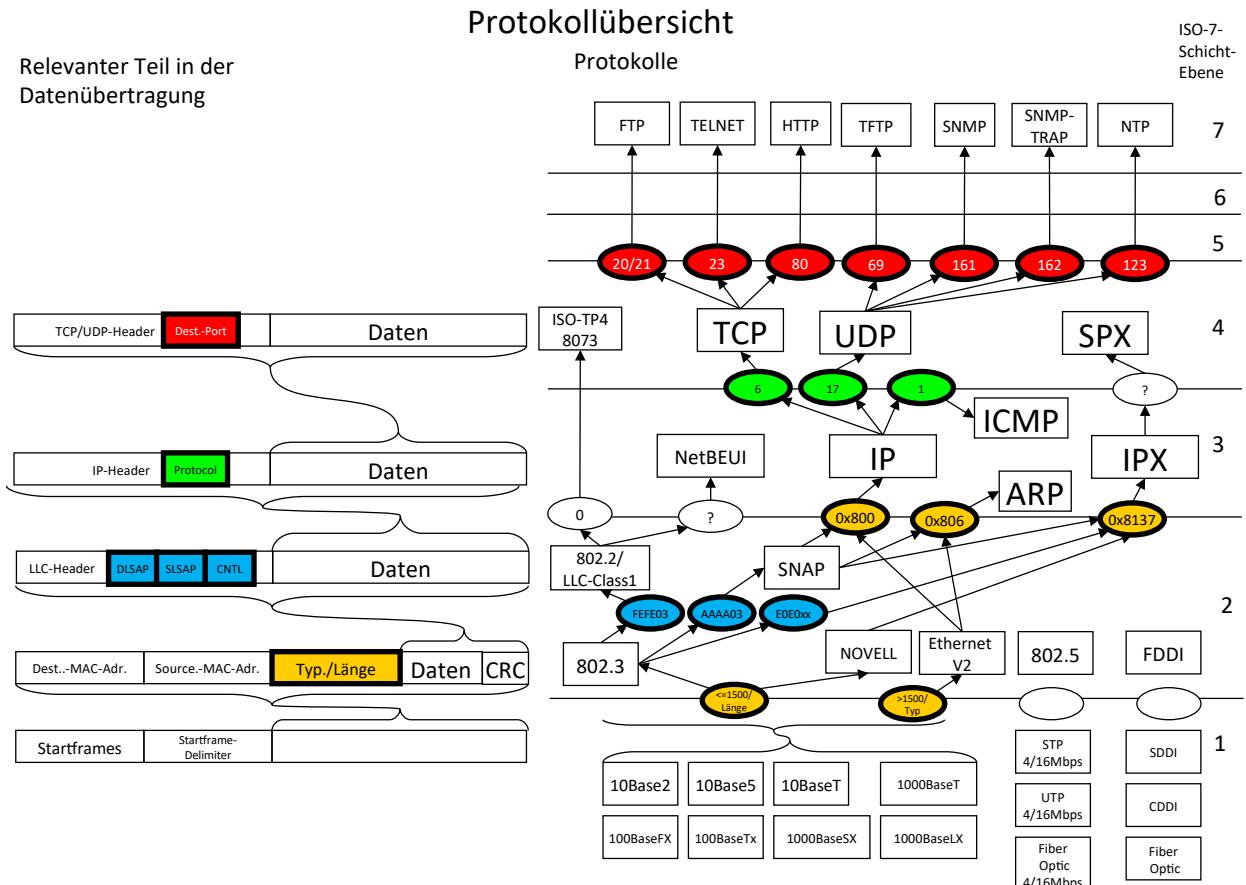


Abbildung 356 : Protokoll_Abhängigkeiten

24.8 - Token Ring

Die Adressierung erfolgt hier in der nicht kanonischen Adressierung. Dabei wird das höchstwertige Bit zuerst übertragen (MSB).

Schon der Name Token Ring deutet auf die Ringstruktur, in dem dieses LAN realisiert ist hin.

Die Datenübertragungsrate beträgt entweder 4Mbps oder 16Mbps. (100Mbps wurden standardisiert, jedoch nie realisiert)

Verwendung finden hierbei folgende Verkabelungs-Varianten:

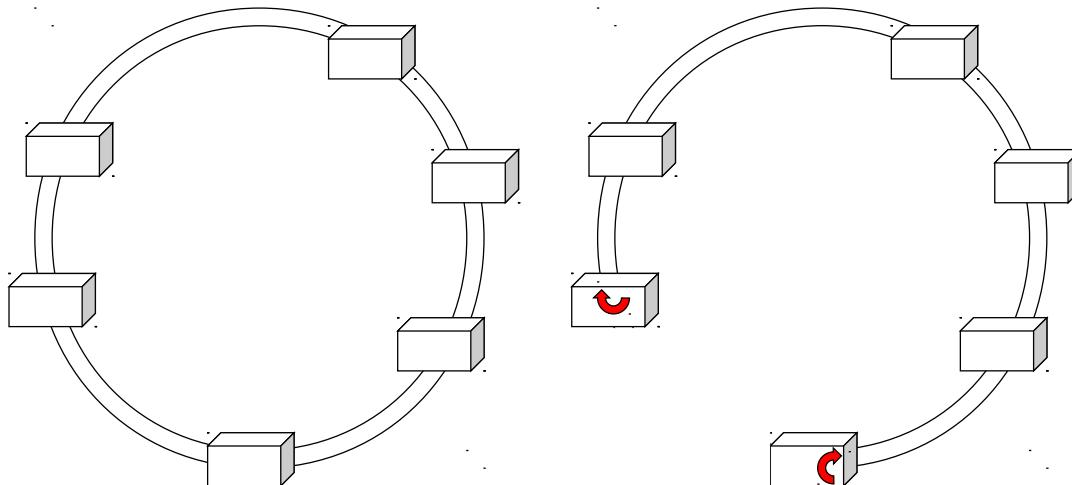
- ➊ IBM-Typ-1-Kabel (STP mit 150 Ohm) als Bestandteil des IBM-Verkabelungssystems IVM mit dem IBM Data-Connector IDC
- ➋ Multimode und Monomode LWL-Kabel mit ST-Steckern.
- ➌ CAT-5-UTP-Kabel (100 Ohm) mit RJ45-Anschluss-Technik. Hierbei sind die Pins 3 und 6 sowie 4 und 5 gepaart.
- ➍ In einer industriellen Variante werden Twisted-Pair-Leitungen mit SUB-D9Steckern oder RJ45 Steckern verwendet.

24.9 - FDDI

Die Adressierung erfolgt hier in der nicht kanonischen Adressierung. Dabei wird das höchstwertigste Bit zuerst übertragen (MSB).

FDDI wird in einer doppelten Ringstruktur realisiert. Damit steht bei Ausfall eines Rings die Möglichkeit zur Verfügung, durch einen Kurzschluss auf den zweiten Ring, die gesamte Ringstruktur wieder herzustellen. Die folgende Abbildung zeigt, wie der Ring in den Stationen an der Unterbrechung miteinander verbunden wird, um einen neuen Ring zu realisieren. Dies macht FDDI zu einer äußerst stabilen Grundlage für Backbone-Netze.

Die Datenübertragungsrate beträgt 100Mbps.



Ausfall eines Rings

Abbildung 357 : FDDI-Ring

FDDI wird mit LWL-Verkabelung aufgebaut. Verwendung findet hierbei der MIC-Stecker.

24.10 - CDDI

Die FDDI-Realisierung mit Twisted-Pair-Kabeln wurde in der CDDI-Normung festgehalten. Dabei wird die 4B/5B sowie NRZ/NRZI-Kodierung verwendet. Als Stecker wird der RJ45-Stecker verwendet.

24.11 - Unterschiede im Frame-Aufbau bei den verschiedenen Topologien

Netzwerk	Präambel	S F D	Frame Steuerung	Ziel Quell MAC- Adr.	Typ	Länge	LLC	Daten	PAD	CRC	End Begrenz.	Rahmenstat.
Eth. V2	X			X	X			X		X		
IEEE 802.3	X	X		X		X	X	X	X	X		
SNAP	X			X		X	X	X	X	X		
NOVELL	X			X		X		X	X	X		
IEEE 802.5		X		X			X	X		X	X	X
FDDI	X	X	X	X			X	X		X	X	X

24.12 - IP (v4)

Im Internet Protokoll (IP) wird eine logische Adressierung der einzelnen Netzteilnehmer im Netz über die starre Adressierung mit MAC-Adressen gelegt. Damit wird es möglich Pakete über Netzwerk-Grenzen hinweg zum Ziel-Netzwerk zu transportieren.

Derzeit wird meistens noch IP in der Version 4 verwendet. Aufgrund der Verknappung der IP-Adressen wird jedoch sukzessive auf IPv6 umgestiegen.

Das IP ist im ISO-7-Schicht-Modell auf Ebene 3 angesiedelt. Diese Schicht wird normalerweise mit Software realisiert. Dies bedeutet, dass über der Hardware-Addressierungs-Schicht eine Schicht angelegt ist, die eine Software-Addressierung ermöglicht.

Daraus folgt, dass bei Verwendung von IP einem Gerät (einer Schnittstelle) eine IP-Adresse zugeordnet wird. Dies kann manuell erfolgen, oder mittels DHCP automatisiert werden. zieht der Rechner zum Beispiel in eine andere Abteilung mit anderen Netzwerkadressen um, so kann dies leicht durch eine Parametrierung mit Software geschehen. Sollte die Netzwerkkarte kaputt gehen, kann sie einfach durch eine neue ersetzt werden. Da der Netzwerkkarte nur die MAC-Adresse fest eingebrannt ist, muss keine IP-Parametrierung mehr erfolgen. Die zur Übertragung der Daten notwendige MAC-Adresse des Ziels wird, falls sie unbekannt ist, vor der Datenübertragung etwa mit einem ARP-Request ermittelt werden.

IP ist im [RFC-791] beschrieben.

IP wurde zur ungesicherten Datenübertragung zwischen paketorientierten Rechnernetzen entwickelt.

Im IP werden zwei wichtige Funktionen des Internets abgewickelt.

- ➊ Adressierung
- ➋ Fragmentierung (Zerlegung der Datagramme in transportierbare Größen) und Reassemblierung (Zusammenbau der zerlegten Datagramme auf dem Zielsystem)

Es werden Datenpakete, die sog. Datagramme, von einer Datenquelle zu einem Datenziel übertragen. Die Datenquelle und das Datenziel werden als Hosts bezeichnet. Die Hosts werden durch Adressen (mit fester Länge von 32 Bit = 4 Byte) angesprochen. Da die Datenquelle und das Datenziel in verschiedenen Netzwerken liegen können, benötigt man Geräte, welche die Datagramme über die Netzwerk-Grenzen transportieren. Diese Geräte werden Router genannt. Sie kennen die Verbindungen (Routen) zwischen den Netzwerken und finden für die Datenpakete den Weg zum Ziel. So transportieren sie die Daten vom Quell-Netzwerk über fast beliebig viele Netzwerke hinweg zum Ziel-Netzwerk.

Die Datagramme werden nötigenfalls über mehrere Netzwerke hinweg übertragen. Da jedes Netzwerk seine eigene Topologie und somit seine eigene maximale Datagrammlänge haben kann, ist es möglich, dass ein Datagramm an einer Grenze von einem Netzwerk in ein anderes zu groß sein kann.

Hier bietet IP die Möglichkeit, das zu lange Datagramm in transportierbare Teile zu zerlegen und am Ziel wieder zusammen zu bauen (Fragmentierung und Reassemblierung)

Um die IP-Adressierung durchzuführen, benötigt die IP-Software in jedem IP-Paket eine IP-Adressinformation. Hierbei geht es um das Versenden und Weiterleiten von Paketen. Pakete, die die IP-Adressinformation nicht enthalten, können mit IP-Software nicht bearbeitet werden.

Jedes einzelne Datagramm wird als unabhängige Einheit behandelt. Abgesehen von fragmentierten Paketen, gibt keine logischen Verbindungen zwischen den einzelnen Datagrammen.

Der Dienst den die IP-Schicht liefert, wird mit 4 verschiedenen Parametern festgelegt

- TOS
- TTL
- Optionen
- Header Checksum

TOS (Type Of Service, deutsch: Art des Dienstes) wird benutzt, um die Qualität des gewünschten Dienstes zu parametrieren. (Hierbei geht es um die Festlegung von verfügbaren Bandbreiten) Der TOS wird vor allem von Gateway (Routern) benutzt, um die evtl. verschiedenen vorhandenen Wege zu beurteilen und auszuwählen. Eine Tabelle mit den Werten folgt.

TTL (Time To Live, deutsch: Lebensdauer) Funktioniert wie ein Selbstvernichtungsauslöser für Datagramme. Der TTL-Wert wird beim Senden vom IP-Stack der Datenquelle vergeben (z. B. 32). Jeder Netzknoten (Router) über den ein Datagramm hinweg transportiert wird, reduziert den TTL-Wert um 1.

Erreicht der TTL-Wert den Wert 0, ohne sein Ziel erreicht zu haben, wird das zugehörige Datagramm zerstört und der Sender mit einer ICMP-Meldung (time-to-live exceeded) darüber unterrichtet.

Somit ist ein TTL letztendlich ein hopgesteuerter Selbstvernichtungsauslöser.

Die Optionen dienen zur Steuerung von Funktionen, die in bestimmten Situationen nützlich sind. Hier werden Zeitstempel, Sicherheitsmechanismen und spezielles Routing ermöglicht.

Die Header Checksum dient zur Ermittlung, ob der Header richtig übertragen wurde. Diese Checksumme ist nur in der IP-Version 4 realisiert. In der Version 6 ist die Checksumme für den Header entfallen, da er zum CRC redundant ist.

IP macht/regelt

- keine Flusskontrolle
- keine Wiederholungen
- keine Quittungen



Erkannte Fehler (Z. B. ein nicht erreichbarer Host) werden über das Internet Control Message Protocol (ICMP) gemeldet/abgehandelt.

24.12.1 - IPv4-Adressen

Eine IP-Adresse besteht bei IPv4 aus 4 Bytes (=32Bits). Die Darstellung besteht aus vier Integer-Zahlen im Bereich 0 bis 255, die mit Punkten getrennt werden. (dotted decimal)

Ein Beispiel könnte folgendermaßen aussehen: 165.33.12.44

In der ursprünglichen Form gibt es IP-Adressen mit einem festen Netzwerk-Teil und einem festen Host-Teil. Die Aufteilung findet auf Bytegrenzen in Klassen (engl. classful) statt. Entscheidend sind die ersten (höchstwertigen) Bits im ersten Byte einer Netzwerkadresse.

Klasse	1. Byte	2. Byte	3. Byte	4. Byte	Anzahl Netze	Anzahl Hosts pro Netzwerk
A	0	7 Bit Netz- Adr.	24 Bit Host-Adr.		126	16777214
B	10	14 Bit Netz-Adr	16 Bit Host-Adr.		16382	65534
C	110	21 Bit Netz-Adr.		8 Bit Host-Adr.	2097150	254
D	1110	28 Bit - Multicast-ID				
E	1111	reserviert				

Die Bedeutung der Farben in der obigen Tabelle bei den Klassen A bis C.

Netzwerk-Teil	Host-Teil
---------------	-----------

Wie oben zu sehen ist gibt es Unicast-IPv4-Adressklassen in 3 festen Aufteilungen von Netzwerk und Host-Teil. Damit haben die unterschiedlichen Klassen Auswirkungen auf die Anzahl der möglichen Netzwerke und die Anzahl der Hosts pro Netzwerk. Mit den Adress-Klassen A bis E ergeben sich die folgenden Adress-Bereiche:

Klasse	Bereich	Subnetzmaske
A	0.0.0.0 - 127.255.255.255	255.0.0.0
B	128.0.0.0 - 191.255.255.255	255.255.0.0
C	192.0.0.0 - 223.255.255.255	255.255.255.0
D	224.0.0.0 - 239.255.255.255	
E	240.0.0.0 - 255.255.255.255	

Damit kann man bereits anhand des ersten Bytes sehen, welcher Klasse das Netzwerk zugeordnet ist. Dies gilt allerdings nur für die Classful-Bearbeitung. Für Sonderfälle gibt mehrere Adress-Bereiche:

Adress-Bereich	Bezeichnung
224.x.x.x – 239.255.255.255	Multicasts
240.x.x.x - 254.x.x.x	Experimentelle Adressen
255.x.x.x	Broadcasts

24.12.2 - Classless-inter-Domain-Routing (CIDR)

Bei den Definitionen für die Adress-Klassen kann man erkennen, dass die Unterschiede der Netzwerkgrößen bei den verschiedenen Klassen sehr groß sind. Ist man im Besitz eines A-Klasse-Netzes, dann kann man 16777213 Hosts in diesem Netzwerk adressieren. In einem Netzwerk ist dies nicht praktikabel. Auch bei einem B-Klasse-Netzwerk ist die Host-Anzahl mit 65533 immer noch nicht vernünftig.

Die Probleme in diesem Zusammenhang wurden im November 1991 von der IETF durch die Zusammenstellung der Routing and Addressing (ROAD) Group angegangen. Im Januar 1992 traf sich die Gruppe und identifizierte 3 Hauptprobleme:

- Verknappung bei den IP-Adressen der B-Klasse-Netzwerk
- Anwachsen der Routing-Tabellen im Internet
- Mögliche Verknappung des 32-Bit-IP-Adressraums

Der Lösungsvorschlag [RFC-4632] war eine Ablösung der starren Klassenaufteilung der IP-Adressen zugunsten einer klassenlosen (engl. classless) Aufteilung. Dies ergibt eine hierarchisch organisierte Aufteilung in Blöcke von IP-Adressen, welche der Internet-Topologie und der Vergabe der Pv4-Adressbereiche an die Provider folgt.

Umgesetzt wird das mit einer Ablösung der byteweisen Subnetzmaske in Dotted-decimal-Schreibweise zugunsten der bitweisen Zuordnung des Netzwerkteils. Dieser zusammenhängende Netzwerkteil wird Prefix genannt. Eigentlich ist es ein Postfix, da er der IP-Adresse nachgestellt wird.

Dabei werden die 1er-Bits des Netzwerkteil gezählt und als Dezimalzahl nach einem Schrägstrich angegeben. So entspricht /24 einer Subnetzmaske mit 24 Bits also 255.255.255.0.

Die CIDR-Schreibweise ist, wie unten dargestellt, einfacher und weniger fehleranfällig als die Dotted-decimal-Schreibweise oder die binäre Schreibweise.

Klasse	Subnetzmaske (in dottet decimal Schreibweise)	Subnetzmaske (in binärer Schreibweise)	Subnetzmaske / Präfix (in CIDR-Schreibweise)
A	255.0.0.0	11111111000000000000000000000000	/8
B	255.255.0.0	11111111111111110000000000000000	/16
C	255.255.255.0	11111111111111111111111100000000	/24

Man kann also nach wie vor mit Klassengrenzen (classful) arbeiten und trotzdem die CIDR-Schreibweise anwenden, wie in der obigen Tabelle zu sehen ist.

Protokolle

Damit ist es sowohl möglich Netzwerke künstlich zu vergrößern und dadurch die Hosts besser verwalten, als auch zusammenzufassen und damit die Routing-Tabellen in den Internet-Routern verkleinern.

Die Klassen bestehen weiterhin und man kann sie immer noch am ersten Byte erkennen, allerdings spielen sie bei der Anwendung keine Rolle mehr.

Schreibweise [/n]	Blöcke (Netzwerke) [2^n]	Adressen pro Block [2^{32-n}]	Hinweis	Schreibweise	Blöcke (Netzwerke) [2^n]	Adressen pro Block [2^{32-n}]	Hinweis
n.n.n.n/32	$2^{32} = 4294967296$	$2^0 = 1$	Host-Route	n.n.0.0/16	$2^{16} = 65536$	$2^{16} = 65536$	Legacy Class-B
n.n.n.x/31	$2^{31} = 2147483648$	$2^1 = 2$	Point-to-Point-Link	n.x.0.0/15	$2^{15} = 32768$	$2^{17} = 131072$	
n.n.n.x/30	$2^{30} = 1073741824$	$2^2 = 4$		n.x.0.0/14	$2^{14} = 16384$	$2^{18} = 262144$	
n.n.n.x/29	$2^{29} = 536870912$	$2^3 = 8$		n.x.0.0/13	$2^{13} = 8192$	$2^{19} = 524288$	
n.n.n.x/28	$2^{28} = 268435456$	$2^4 = 16$		n.x.0.0/12	$2^{12} = 4096$	$2^{20} = 1048576$	
n.n.n.x/27	$2^{27} = 134217728$	$2^5 = 32$		n.x.0.0/11	$2^{11} = 2048$	$2^{21} = 2097152$	
n.n.n.x/26	$2^{26} = 67108864$	$2^6 = 64$		n.x.0.0/10	$2^{10} = 1024$	$2^{22} = 4194304$	
n.n.n.x/25	$2^{25} = 33554432$	$2^7 = 128$		n.x.0.0/9	$2^9 = 512$	$2^{23} = 8388608$	
n.n.n.0/24	$2^{24} = 16777216$	$2^8 = 256$	Legacy Class-C	n.0.0.0/8	$2^8 = 256$	$2^{24} = 16777216$	Legacy Class-A
n.n.x.0/23	$2^{23} = 8388608$	$2^9 = 512$		x.0.0.0/7	$2^7 = 128$	$2^{25} = 33554432$	
n.n.x.0/22	$2^{22} = 4194304$	$2^{10} = 1024$		x.0.0.0/6	$2^6 = 64$	$2^{26} = 67108864$	
n.n.x.0/21	$2^{21} = 2097152$	$2^{11} = 2048$		x.0.0.0/5	$2^5 = 32$	$2^{27} = 134217728$	
n.n.x.0/20	$2^{20} = 1048576$	$2^{12} = 4096$		x.0.0.0/4	$2^4 = 16$	$2^{28} = 268435456$	
n.n.x.0/19	$2^{19} = 524288$	$2^{13} = 8192$		x.0.0.0/3	$2^3 = 8$	$2^{29} = 536870912$	
n.n.x.0/18	$2^{18} = 262144$	$2^{14} = 16384$		x.0.0.0/2	$2^2 = 4$	$2^{30} = 1073741824$	
n.n.x.0/17	$2^{17} = 131072$	$2^{15} = 32768$		x.0.0.0/1	$2^1 = 2$	$2^{31} = 2147483648$	
				0.0.0.0/0	$2^0 = 1$	$2^{32} = 4294967296$	Default-Route

n ist ein 8-Bit großer Dezimalwert.

x ist ein 1 bis 7 Bit großer Wert, der auf dem Präfix basiert.

CIDR erleichtert nicht nur die Schreibweise von Subnetzmasken sondern ist vor allem beim Routing hilfreich, wenn es darum geht den Umfang von Routing-Tabelleneinträgen klein zu halten.

Um die Vorteile beim Routing zu erkennen, soll das folgende Beispiel dienen.

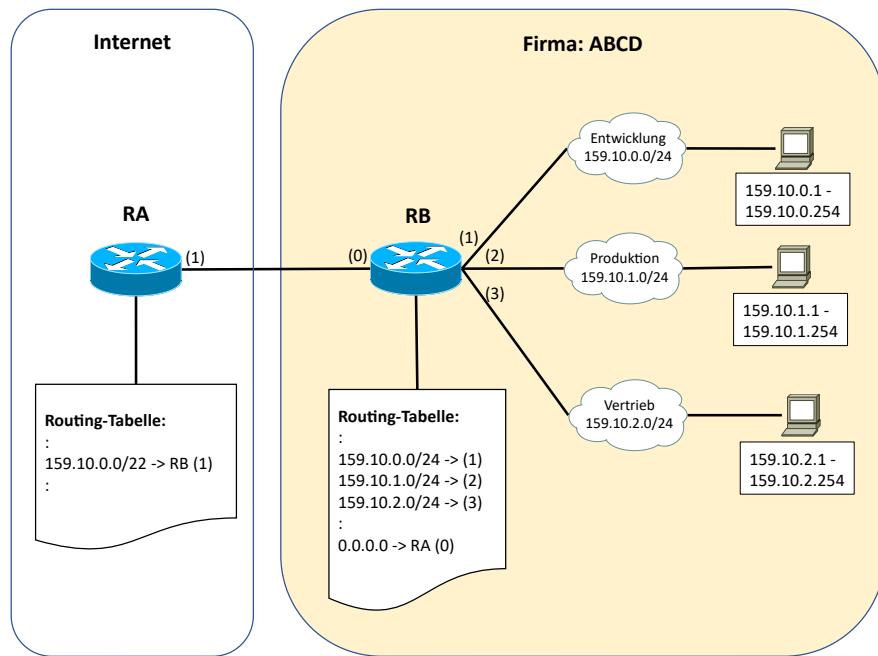


Abbildung 358: Beispiel: CIDR Teil-1

Angenommen die Firma ABCD hat von ihrem Provider den IP-Adressraum 159.10.0.0 /22 bekommen. Damit steht ihr der Adressraum 159.10.0.0 bis 159.10.3.255 zur Verfügung. Alle Geräte sollen eine im Internet gültige IP-Adresse bekommen.

Der Router RB verwaltet 3 C-Klasse-Netzwerke. Je eines für Entwicklung, Produktion und Vertrieb. Die Netzwerke sind jeweils an ein physikalisches Interface (in Klammern) direkt angeschlossen. Zusätzlich hat der Router RB eine Verbindung in das Internet über die Default-Route (0.0.0.0) und dem Interface (0).

Unter anderem hat er für jedes Netzwerk in seiner Routing-Tabelle einen Eintrag.

- ➊ 159.10.0.0 /24 → (1)
- ➋ 159.10.1.0 /24 → (2)
- ➌ 159.10.2.0 /24 → (3)
- ➍ 0.0.0.0 → RA (0)

Die Clients in den einzelnen Netzwerken können das Internet über die Default-Route des Routers RB über das Interface (0) erreichen und die Clients können im Internet vom Router RA über das Interface (1) erreicht werden.

Eigentlich müsste der Router RA im Internet die gleiche Tabelleneinträge in seiner Routing-Tabelle haben, doch Router RB propagiert nur ein Netzwerk (159.10.0.0), allerdings mit der Subnetmask /22. Damit ist der gesamte Netzwerk-Bereich von 159.10.0.0 bis 159.10.3.255 abgedeckt und der Router RA benötigt nur diesen einen Routing-Tabelleneintrag. Dieses Zusammenfassen von Einträgen in der Routing-Tabelle reduziert sowohl beim Update der Routing-Tabelle als auch beim Lookup in der Routing-Tabelle den Bearbeitungsaufwand. Weiterhin wird weniger Speicherplatz für die Routing-Tabelle benötigt.

Protokolle

Das übrig gebliebene Netzwerk (159.10.3.0/24) soll nun für die Forschungsabteilung in einer Außenstelle genutzt werden. Die Außenstelle soll über das Internet erreicht werden. Dazu wird der Router RC einerseits mit dem Interface (0) mit dem Internet verbunden und andererseits bekommt er am Interface (1) das Forschungs-Netzwerk konfiguriert. Damit wird der Router RC das Forschungsnetzwerk in das Internet propagieren.

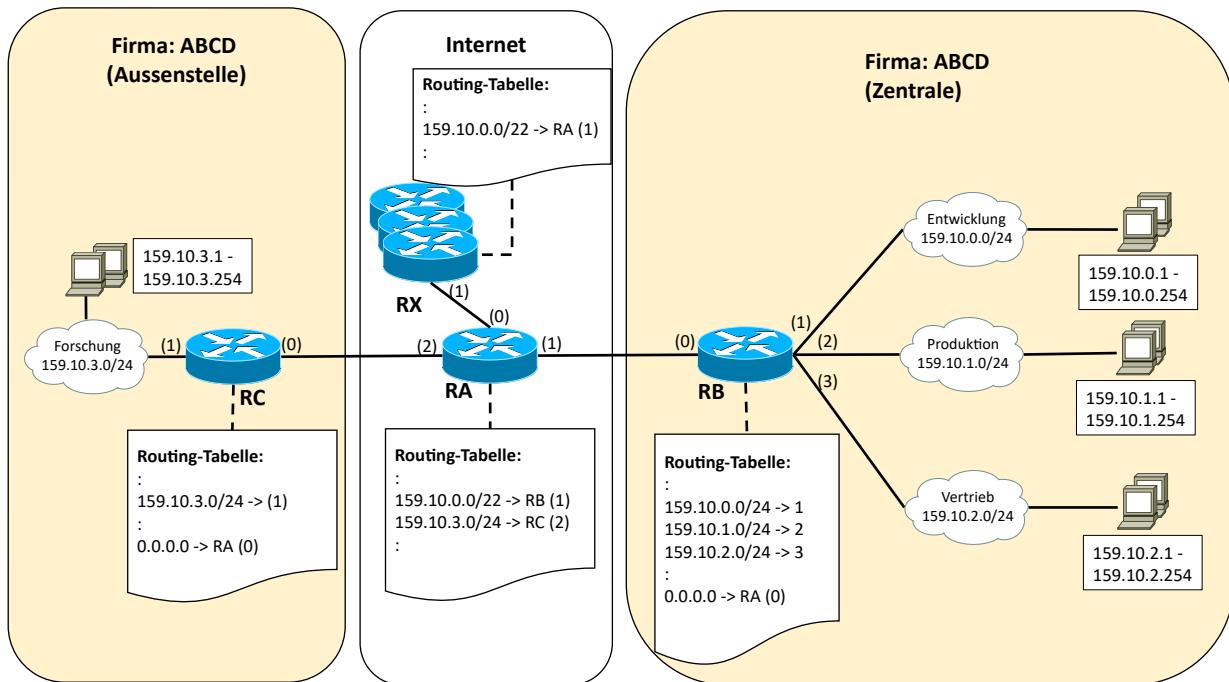


Abbildung 359: Beispiel: CIDR Teil-2

Auf diese Weise entsteht beim Router RA ein Problem in der Routing-Tabelle. Das Forschungsnetzwerk kommt als zusätzlicher Eintrag in die Routing-Tabelle.

- ➊ 159.10.0.0 /22 → RB (1)
- ➋ 159.10.3.0 /24 → RC (2)

In der Routing-Tabelle des Routers RA gibt es nun zwei überschneidende Einträge, denn 159.10.3.0 /24 ist ein Teil von 159.10.0.0 /22.

Kommt nun ein Paket für das Ziel 159.10.3.65 beim Router RA an, findet er zwei passende Einträge in seiner Routing-Tabelle. Um nun den richtigen Eintrag auszuwählen, gilt es die Regel des „Longest-Match“ anzuwenden. Das bedeutet, der Eintrag mit dem längsten passenden Netzwerk-Teil, also dem längsten Präfix, wird für die Routing-Entscheidung herangezogen. Das Paket wird darauf hin über das Interface (2) an den Router RC weiter geleitet.

Kommt ein Paket für das Ziel 159.10.1.44 beim Router RA an, kann er dafür nur einen passenden Eintrag in seiner Routing-Tabelle finden (159.10.0.0 /22) und das Paket an den Router RB weiter leiten.

Da die Provider für ganze Regionen Adressbereiche zugewiesen bekommen, können diese für das Routing im Internet entsprechend zusammengefasst werden. Dies reduziert die Routing-Tabellen erheblich. So können die beiden Routing-Tabelleneinträge im Router RA bei Routern RX (und dahinter) in anderen Internet-Regionen wiederum zu einem Netzwerk (159.10.0.0 /22) zusammen gefasst werden.

24.12.3 - Subnetting

Für die Definition des Netzwerk-Teils wird die so genannte Subnetz-Maske verwendet. Diese vordefinierten (natürlichen) Subnetz-Masken für die verschiedenen Klassen können geändert werden, um die Aufteilung der Netzwerk-Klassen „aufzuweichen“ und die Grenze zwischen Netz- und Host-Teil zu verschieben. Durch Verschieben des „1-0-Übergangs“ nach rechts in Richtung Nullen kann der Netzwerk-Teil vergrößert und der Host-Teil verkleinert werden. Damit können mehr Netze und weniger Hosts innerhalb eines Netzwerks definiert werden. Die Subnetzmasken sehen je nach Netzwerk-Klasse folgendermaßen aus.

- A-Klasse 255.v.v.v
- B-Klasse 255.255.v.v
- C-Klasse 255.255.255.v

Hierbei steht v.v.v, v.v oder v für den variablen Teil der Subnetz-Maske. Dieser teilt sich in einen Subnetting-Teil und einen Host-Teil auf.

So sieht beispielsweise ein 3-Bit-Subnetting eines B-Klasse-Netzwerks folgendermaßen aus:

nnnnnnnn.nnnnnnnn.ssshhhhh.hhhhhhhh

Wobei n für den Netzwerkteil, s für den Subnetzteil und h für den Host-Teil steht.

Der Netzwerk-Teil und der Subnetting-Teil bilden aus Host-Sicht zusammen einen Netzwerk-Teil also den Präfix.

Die Subnetmask kann damit 255.255.224.0 oder /19 sein.

Links im Netzwerk- und Subnetting-Teil stehen immer die Einsen und rechts die Nullen für den restlichen Host-Teil.

Eine Subnetz-Maske von 255.255.0.255 ist denkbar, führt allerdings nicht zu übersichtlichen Netzwerken und wird von modernen Betriebssystemen unterbunden.



Für jedes v-Byte (siehe oben) können bitweise Subnetmask-Werte anstelle der Hosts eingetragen werden.

Dual-Darstellung	Dezimal-Darstellung	Hinweis
00000000	000	Kein Subnetting
10000000	128	1-Bit-Subnetting
11000000	192	2-Bit-Subnetting
11100000	224	3-Bit-Subnetting
11110000	240	4-Bit-Subnetting
11111000	248	5-Bit-Subnetting
11111100	252	6-Bit-Subnetting
11111110	254	7-Bit-Subnetting
11111111	255	8-Bit-Subnetting

24.12.4 - Beispiel eines 3-Bit-Subnetting

IP-Netzwerk 128.89.0.0/16

das ist in ausgeschriebener Form

10000000.01011001.00000000.00000000 mit einer Subnetzmaske von

11111111.11111111.00000000.00000000

Bei der Subnetzmaske bilden die Einsen den Netzwerk-Teil (n) und die Nullen sind der Host-Teil (h).

nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh

Wird nun der 1-0-Übergang in der Subnetzmaske um drei Bits nach rechts verschoben ergibt sich

11111111.11111111.**111**00000.00000000

nnnnnnnn.nnnnnnnn.ssshhhhh.hhhhhhhh

Damit hat sich zwischen Netzwerk- und Host-Teil ein Subnetz-Teil (s) eingeschoben.

Damit ergibt sich der folgende Zustand.

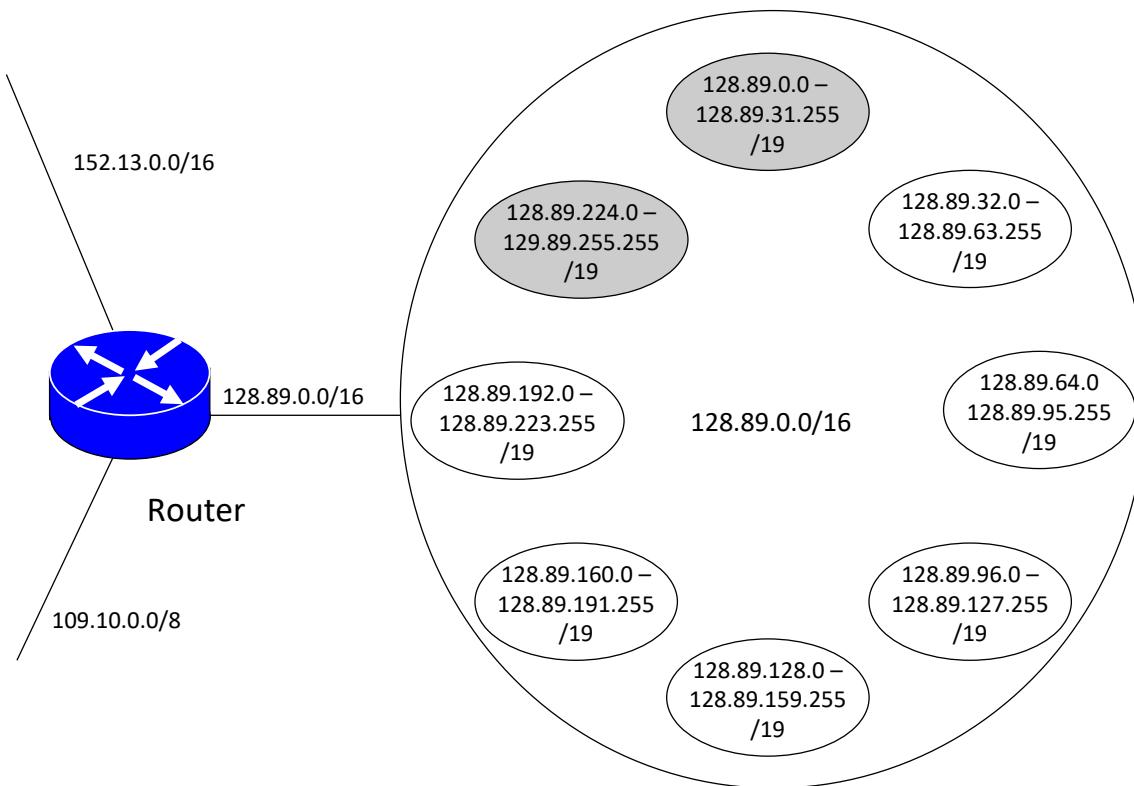


Abbildung 360 : Beispiel für Subnetting

Die 3 Bit für die Unterteilung des Netzwerks ermöglichen 8 Subnetze. Das erste und das letzte Subnetz ist nicht nutzbar, denn das erste Subnetz beschreibt das gesamte Netzwerk und das letzte Subnetz bildet die Broadcast-Adresse für das Netzwerk.

So wird auch die ehemalige Host-Adresse 128.89.64.0 zu einer Netzwerk-Adresse!

Der Ausschluss des ersten und des letzten IP-Subnetzes, wie im RFC 950 beschrieben, bedeutet eine unnötige Verschwendungen von Adressbereichen.

Um den ersten und letzten Adressbereich trotzdem zu nutzen bieten diverse Hersteller die Möglichkeit der Verwendung der „All-Ones“ und „All-Zeros“-Subnetze einzuschalten. Diese Eigenschaft ist im RFC 1878 beschrieben.

24.12.5 - Subnet-Arithmetik in einem C-Klasse-Netzwerk

Art des Subnetz	Dezimaler Wert	Binärer Wert	Anzahl der Subnetze	Anzahl der Hosts
2 Bit	192	11000000	$2^2 = 4$ Zustände -> 2 Subnetze	$2^6 = 64$ Zustände -> 62 Hosts
3 Bit	224	11100000	$2^3 = 8$ Zustände -> 6 Subnetze	$2^5 = 32$ Zustände -> 30 Hosts
4 Bit	240	11110000	$2^4 = 16$ Zustände -> 14 Subnetze	$2^4 = 16$ Zustände -> 14 Hosts
5 Bit	248	11111000	$2^5 = 32$ Zustände -> 30 Subnetze	$2^3 = 8$ Zustände -> 6 Hosts
6 Bit	252	11111100	$2^6 = 64$ Zustände -> 62 Subnetze	$2^2 = 4$ Zustände -> 2 Hosts

Ein-Bit-Subnetting sowie 7-Bit-Subnetting sind bei C-Klasse-Netzwerken zwecklos.

Denn:

Ein-Bit-Subnetting (10000000) lässt 0 Subnetze zu.

7-Bit-Subnetting (11111110) lässt 0 Hosts zu.

Die Anzahl der Zustände bei den Subnetzen sowie bei den Hosts führt über die Formel:

$$\text{Anzahl} = \text{Anzahl der Zustände} - 2$$

zu der möglichen Anzahl der Subnetze bzw. der Hosts.

Für die Subtraktion um 2 sind folgende Zusammenhänge verantwortlich:

Bei den Host-Adressen

- ➊ Die Host-Adresse 0 wird für das Netzwerk selbst benutzt.
- ➋ Die Host-Adresse 255 (alles Einsen) ist für Broadcasts reserviert.
Jedes Subnetz hat seine eigene Broadcast –Adresse!!!!



Bei den Netzwerk-Adressen

- ➊ Die Netzwerkadresse 0 wird innerhalb eines Netzwerks benutzt, um auf das Netzwerk selbst zu verweisen. (Z.B. ist die Adresse 0.0.0.18 innerhalb eines Klasse-C-Netzwerks die Host-Adresse 18 in diesem Netzwerk ohne die Netzwerkadresse zu betrachten)
- ➋ Die Netzwerkadressen 224.0.0.0 bis 255.255.255.254 sind zu experimentellen Zwecken den Klasse-D und Klasse-E-Netzwerken sowie für Multicasts vorbehalten.



Weiteres Beispiel mit 3-Bit-Subnetting

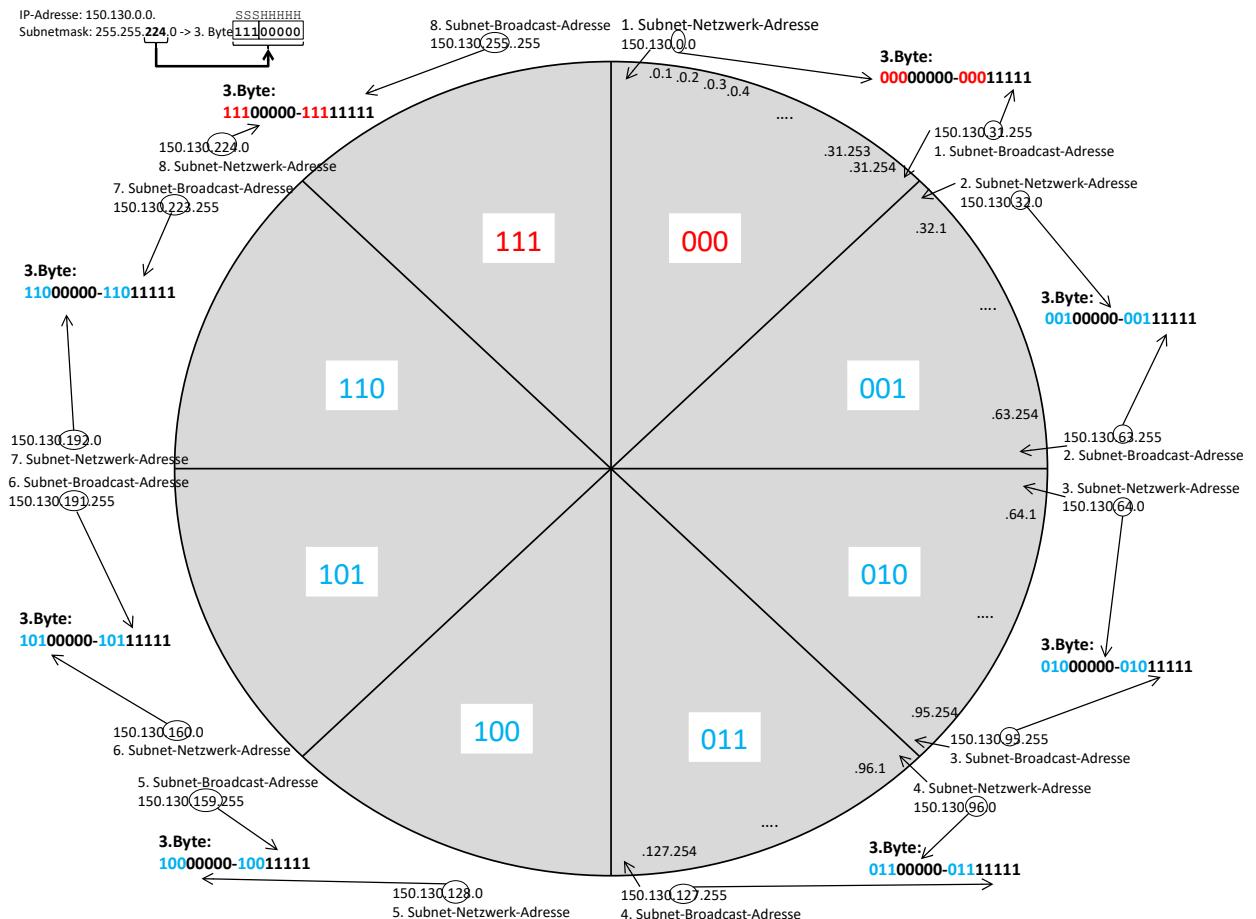


Abbildung 361 : Beispiel für Subnetting 2

Wie oben beschrieben, ist der Bereich mit den Subnetz-Werten 000 und 111 nicht für gültige Netze verwendbar!

Adressbereiche						Nicht sinnvoll da kein Subnetz übrig bleibt
1111.1110=254 7Bit=128Bereiche	1111.1100=252 6Bit=64Bereiche	1111.1000=248 5Bit=32Bereiche	1111.0000=240 4Bit=16Bereiche	1110.0000=224 3Bit=8Bereiche	1100.0000=192 2Bit=4Bereiche	1000.0000=128 1Bit=2Bereiche
0 - 1	0 - 3	0 - 7	0 - 15	0 - 31	0 - 63	0 - 127
2 - 3	4 - 7	8 - 15	16 - 31	32 - 63	64 - 127	128 - 256
4 - 5	8 - 11	16 - 23	32 - 47	64 - 95	128 - 191	
6 - 7	12 - 15	24 - 31	48 - 63	96 - 127	192 - 255	
8 - 9	16 - 19	32 - 39	64 - 79	128 - 159		
10 - 11	20 - 23	40 - 47	80 - 95	160 - 191		
12 - 13	24 - 27	48 - 55	96 - 111	192 - 223		
14 - 15	28 - 31	56 - 63	112 - 127	224 - 255		
16 - 17	32 - 35	64 - 71	128 - 143			
18 - 19	36 - 39	72 - 79	144 - 159			
20 - 21	40 - 43	80 - 87	160 - 175			
22 - 23	44 - 47	88 - 95	176 - 191			
24 - 25	48 - 51	96 - 103	192 - 207			
26 - 27	52 - 55	104 - 111	208 - 223			
28 - 29	56 - 59	112 - 119	224 - 239			
30 - 31	60 - 63	120 - 127	240 - 255			
32 - 33	64 - 67	128 - 135				
34 - 35	68 - 71	136 - 143				
36 - 37	72 - 75	144 - 151				
38 - 39	76 - 79	152 - 159				
40 - 41	80 - 83	160 - 167				
42 - 43	84 - 87	168 - 175				
44 - 45	88 - 91	176 - 183				
46 - 47	92 - 95	184 - 191				
48 - 49	96 - 99	192 - 199				
50 - 51	100 - 103	200 - 207				
52 - 53	104 - 107	208 - 215				
54 - 55	108 - 111	216 - 223				
56 - 57	112 - 115	224 - 231				
58 - 59	116 - 119	232 - 239				
60 - 61	120 - 123	240 - 247				
62 - 63	124 - 127	248 - 255				
64 - 65	128 - 131					
66 - 67	132 - 135					
68 - 69	136 - 139					
70 - 71	140 - 143					
72 - 73	144 - 147					
74 - 75	148 - 151					
76 - 77	152 - 155					
78 - 79	156 - 159					
80 - 81	160 - 163					
82 - 83	164 - 167					
84 - 85	168 - 171					
86 - 87	172 - 175					
88 - 89	176 - 179					
90 - 91	180 - 183					
92 - 93	184 - 187					
:	188 - 191					
224 - 225	192 - 195					
226 - 227	196 - 199					
228 - 229	200 - 203					
230 - 231	204 - 207					
232 - 233	208 - 211					
234 - 235	212 - 215					
236 - 237	216 - 219					
238 - 239	220 - 223					
240 - 241	224 - 227					
242 - 243	228 - 231					
244 - 245	232 - 235					
246 - 247	236 - 239					
248 - 249	240 - 243					
250 - 251	244 - 247					
252 - 253	248 - 251					
254 - 255	252 - 255					

Beispiel für 5-Bit Subnetting am Netzwerk: 141.36.48.0
mit der Subnetmask: 255.255.248.0

141.36.48.0	Netzwerk-Adresse
141.36.48.1	1. Hostadresse
141.36.48.255	255. Hostadresse
141.36.49.0	256. Hostadresse
141.36.49.1	257. Hostadresse
141.36.49.255	512. Hostadresse
141.36.50.0	513. Hostadresse
141.36.50.1	514. Hostadresse
:	:
141.36.55.254	2046. Hostadresse
141.36.55.255	Broadcast-Adresse

Protokolle**Installationshinweise**

Bei der Konfiguration eines Gerätes für IPv4 sind die folgenden Angaben zu machen:

- IP-Adresse des Hosts

Diese Adresse identifiziert den Host eindeutig innerhalb des Netzwerks.

● Subnetmask des Netzes, dessen Mitglied die Station werden soll. Damit wird der Netzwerkteil einer IP-Adresse definiert. Somit wird eingestellt, wie die eigene Adresse zu interpretieren ist. Die IP-Adresse wird erst im Zusammenhang mit der Subnetmask interpretierbar!

- Default Gateway-IP-Adresse

An diese IP-Adresse werden alle Pakete gesendet, deren Empfänger nicht im gleichen Netz liegen.

- Evtl. Broadcast-Adresse

Wird Subnetting eingesetzt, kann die Broadcast-Adresse von der Broadcast-Adresse der IP-Netzklasse abweichen. Eine Erklärung erfolgt weiter unten. Siehe auch Broadcasts.

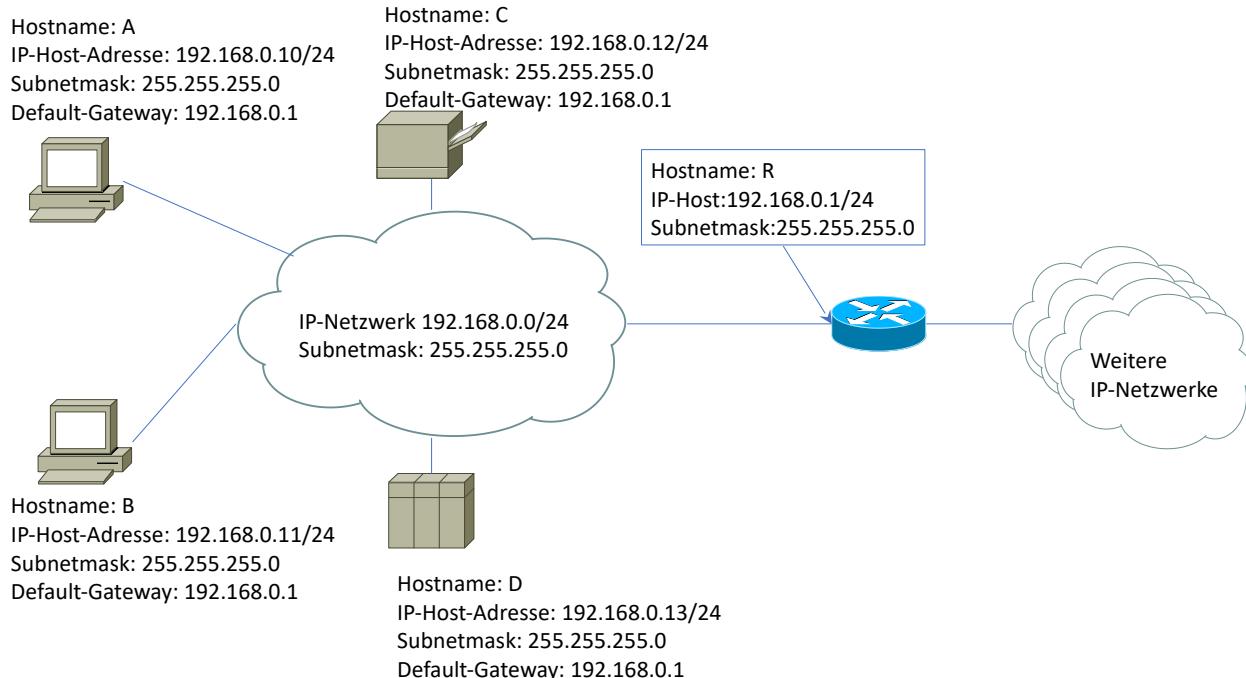


Abbildung 362: IP-Adress-Vergabe

IP-Netzwerke können wie im obigen Beispiel als Wolke oder mit einem Bus-System dargestellt werden. Dabei kann die Subnetmask voll ausgeschrieben werden (255.255.255.0) oder in der CIDR-Schreibweise mit /24 abgekürzt werden.

Damit ist die Klasse des IP-Netzwerks durch das erste Byte der Netzwerk-Adresse festgelegt (192 = C-Klasse). Ist die Adressierung classfull, so richtet sie sich auf Bytegrenzen aus. Da die Subnetmask 24 Bit entspricht, ist das in diesem Beispiel gegeben.

Die Kommunikationsteilnehmer an einem Netzwerk werden bei IPv4 als Hosts bezeichnet.

Durch die Festlegung auf ein C-Klasse-Netzwerk ist es möglich 254 Hosts in diesem Netzwerk zu adressieren. Die erste Adresse des Netzwerks kann nicht für Hosts verwendet werden, da sie das Netzwerk selbst beschreibt. Die letzte Adresse kann nicht verwendet werden, da sie für die Broadcast-Adresse (also zur Sendung eines Paketes an alle Hosts im Netzwerk des Senders) reserviert ist.

Sind mehr als die 254 Host zu adressieren, muss auf eine andere Netzwerk-Klasse (mit kleinerem Netzwerk-Anteil) ausgewichen werden (z. Klasse A oder Klasse B). Damit ändert sich dann mindestens die Subnetmask.

Für die Beschreibung eines Hosts ist mindestens seine IP-Adresse und seine Subnetmask erforderlich. Da die Subnetmask für alle Teilnehmer in einem Netzwerk gleich sein sollte, reicht es aus, die Subnetmask einmal bei der Beschreibung des Netzwerks anzugeben.

Damit kann der Host jedoch nur innerhalb des Netzwerks kommunizieren. Sobald der Host mit Hosts in anderen Ebene-3-Netzwerken kommunizieren will, benötigt er die IP-Adresse eines Gerätes, das die Pakete in weitere Netzwerke transportieren kann. Dieses Gerät wird Router genannt. In der Internet-Terminologie werden die Router Gateways genannt. Deshalb wird der Router für die Hosts eines Netzwerks auch Default-Gateway genannt, wenn mit anderen Netzwerken kommuniziert werden soll.

Die Default-Gateway-IP-Adresse wird normalerweise entweder auf den Anfang oder an das Ende des verfügbaren IP-Adress-Bandes für die Hosts gelegt.

Im obigen Fall ist die Default-Gateway-Adresse für alle Hosts, die IP-Adresse des Routers (192.168.0.1). Entfernt man alle redundanten Informationen in der obigen Abbildung kann man die erforderliche Information wie in der folgenden Abbildung darstellen.

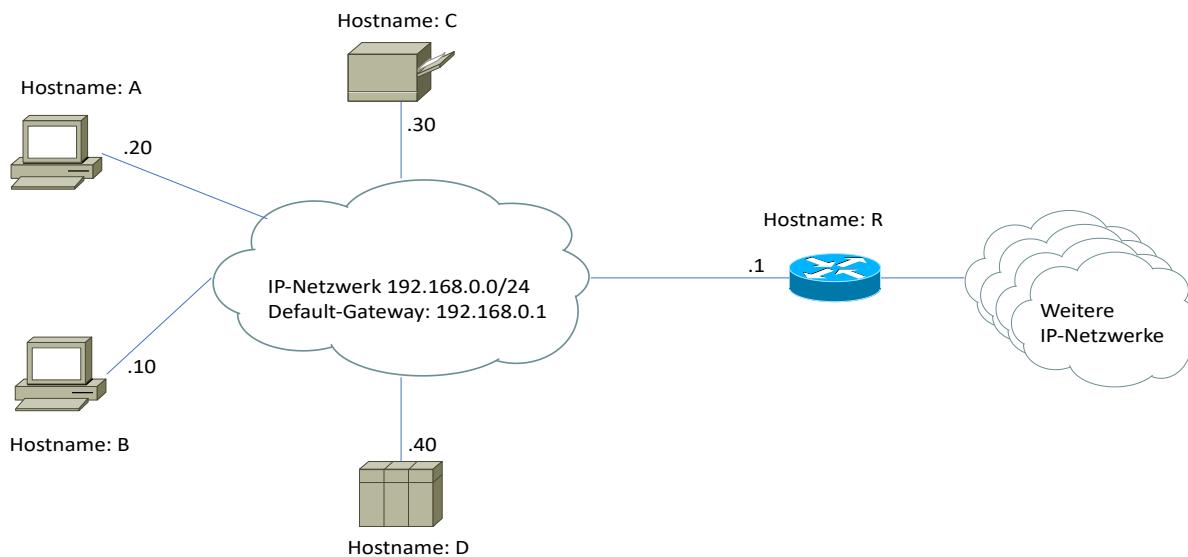


Abbildung 363: Einfachere Darstellung eines IP-Netzwerks mitsamt den Teilnehmern

Diese Informationen sind für die meisten IPv4-Netzwerke ausreichend. Da es pro Netzwerk meist auch noch weitere wichtige Zulieferer (z. B. DNS-Server, DHCP-Server, Zeit-Server,...) gibt, können diese bei der Beschreibung des Netzwerks in der Wolke mit hinterlegt werden.

In Sonderfällen kann es gewünscht sein, dass ein Teil der Hosts nur über einen bestimmten Weg (Router) in andere Netzwerke gehen soll, der andere Teil soll nur über einen anderen Weg gehen. Dafür müssen dann unterschiedliche Router (also Default-Gateways) zur Verfügung gestellt werden, die dann bei der Beschreibung der Hosts wieder anzugeben sind.

Als Erkenntnis ist daraus zu ziehen, dass eine IP-Adresse immer erst zusammen mit ihrer Subnetmask richtig in Netzwerk- und Host-Teil unterteilt werden kann. Die ausschließliche Betrachtung des Wertes des ersten Bytes ist nicht ausreichend!



24.12.6 - Interpretation der Subnetzmaske

Wozu benötigt jeder Client eine Subnetmask?

Solange es nur ein Netzwerk mit einer Netzwerkadresse gibt, wissen alle Hosts, dass ihre Kommunikationspartner im gleichen Netzwerk liegen. Dies bedeutet, dass ein Kommunikationspartner direkt angesprochen werden kann. Dazu muss ein Sender nur noch die MAC-Adresse des Empfängers kennen. Kennt er sie nicht, kann er sie mit einem ARP-Request ermitteln. Dabei fragt der Sender alle Netzteilnehmer, ob sie die zugehörige MAC-Adresse der Empfänger-IP-Adresse kennen. Ist der Empfänger im Netz vorhanden, wird er auf den ARP-Request mit einem ARP-Response antworten und seine MAC-Adresse dem Sender mitteilen. Die zurückgemeldete Zuordnung IP-Adresse zu MAC-Adresse merkt sich der Sender in einem so genannten ARP-Cache.

Damit braucht er beim nächsten Mal keinen ARP-Request zu senden, sondern er kann direkt die MAC-Adresse aus dem ARP-Cache verwenden. Damit bei einem Rechner-Umzug nicht alte IP-MAC-Adress-Zuordnungen in den ARP-Caches herumdümpeln, unterliegen sie einem Ageing-Mechanismus (deutsch: Alterungs-Mechanismus). Der sorgt dafür, dass die ARP-Cache-Einträge nach einer bestimmten Zeit gelöscht werden (ca. 20 – 30 Minuten). Manche Hersteller tun dies aufgrund ihrer Voreinstellungen erst einmal nicht z. B. Nortel-Networks (Bay)

Sobald jedoch mehrere Netzwerke über Router miteinander verbunden sind, geht das nicht mehr so einfach. Nun kann unter Umständen ein Host nicht mehr sein Paket dem Kommunikations-Partner direkt senden. Er muss sein Paket einem Router senden, der für den Weitertransport der Daten in andere Netzwerke zuständig ist.

Damit nun ein Host mit einem zweiten Host in einem anderen Netzwerk kommunizieren kann, muss er erkennen können, ob der zweite Host im gleichen Netzwerk oder in einem anderen Netzwerk liegt. Um zu erkennen, ob beide Kommunikationspartner im gleichen Netzwerk liegen, müssen zuerst die Netzwerk-Teile der beiden IP-Adressen isoliert werden.

Dazu verwendet der Sender seine eigene IP-Adresse, die IP-Adresse des Partners und seine eigene Subnetmask. Die IP-Adresse des Partners sowie die eigene IP-Adresse wird mit der eigenen Subnetmask UND-verknüpft. Das Ergebnis der beiden UND-Verknüpfungen wird miteinander verglichen.

Sind beide Ergebnisse gleich, liegt der Partner im gleichen Netz. Dies bedeutet, dass der Partner direkt mit einem IP-Paket angesprochen werden kann.

Sind beide Ergebnisse ungleich, liegt der Partner in einem anderen Netz. Dies bedeutet, dass der Partner nicht direkt mit einem IP-Paket angesprochen werden kann. Das Paket muss zu einem Router (Default Gateway) gesendet werden.

Ein beliebter Fehler beim Umzug eines Gerätes in ein Netzwerk mit einer anderen Subnet-Mask ist zu vergessen die Subnet-Mask anzupassen.



24.12.7 - Beispiel für eine Anwendung der Subnetmask

Partner-IP-Adresse 131.246.9.50

10000011 11110110 00001001 00110010

Eigene Subnetzmaske 255.255.248.0

11111111 11111111 11111000 00000000

Das Ergebnis der binären UND-Verknüpfung von Partner-IP-Adresse und eigener Subnetzmaske ist der isolierte Netzwerk-Teil der Partner-IP-Adresse

10000011 11110110 00001000 00000000

Eigene Netzadresse 131.246.8.0

10000011 11110110 00001000 00000000

Eigene Subnetzmaske 255.255.248.0

11111111 11111111 11111000 00000000

Das Ergebnis der binären UND-Verknüpfung von eigener IP-Adresse und eigener Subnetzmaske ist der isolierte Netzwerk-Teil der eigenen IP-Adresse

10000011 11110110 00001000 00000000

In diesem Beispiel ist der Netzwerk-Teil der eigenen IP-Adresse und der Netzwerkteil der Partner-IP-Adresse gleich. Damit liegen beide IP-Adressen im gleichen Subnetz. Daraus folgt, dass die Verbindung direkt in diesem Subnetz aufgebaut wird und nicht über einen Router (Default-Gateway) zu erfolgen hat.

Unicasts, Multicasts und Broadcasts

Es gibt drei unterschiedliche Anwendungsmöglichkeiten bei der Adressierung. Je nach verwendetem ersten Byte kann unterschieden werden:

Adressen	Bezeichnung	Verhalten
1.x.x.x : 223.x.x.x	Unicasts	Gehen von einem Sender an <u>einen</u> Empfänger
224.x.x.x	Multicasts	Gehen von einem Sender <u>an eine Gruppe</u> von Empfängern. So unterhalten sich z. B. Brücken miteinander
225.x.x.x : 255.x.x.x	Broadcasts	Gehen von einem Sender an alle

Unicasts

Unicasts werden von einer IP-Adresse zu einer anderen IP-Adresse gesendet. Es besteht also eine 1:1-Beziehung zwischen den Kommunikationspartnern.

24.12.7.1 - Broadcasts

Broadcasts werden, wie Multicasts, als UDP-Datagramme gesendet. Bei TCP sind nur Peer to Peer Verbindungen möglich! Es ist auch vor jedem TCP-Datenverkehr eine Verbindung aufzubauen und danach wieder abzubauen!

Um zu verstehen, was Broadcasts, Multicasts und Unicasts bedeuten, muss man sich vergegenwärtigen, dass jede Netzwerkkarte, die an ein Ethernet angeschlossen wird, ständig alle Frames auf dem Ethernet mit liest. (Zumindest der Ethernet-Header wird mit gelesen)

Alle Broadcasts, Multicasts an die eigene Gruppe und Unicasts an die eigene MAC-Adr. werden an die nächsthöhere Schicht weitergegeben. Alle anderen Frames werden von der Netzwerkkarte verworfen und nicht weiterbearbeitet.

Davon gibt es eine Ausnahme:

Wird die Netzwerkkarte in den Promiscuous Mode gesetzt, leitet sie alle Frames an die nächsthöhere Schicht weiter. Dies wird von Netzwerk-Analysesoftware wie z. B. tcpdump ausgenutzt.

Broadcasts haben den Nachteil, dass sich je nach Interface-Karte auch die CPU mit dem Frame befassen muss, da ein Interrupt erzeugt wird. Dies ist vor allem dann schlecht, wenn der Rechner den empfangenen Broadcast nur verwirft, weil er nicht für ihn ist. Somit wird CPU-Leistung unnötig verschwendet! Ein erhöhtes Broadcast-Aufkommen führt dann auch zu erhöhter CPU-Last. Dies kann im schlimmsten Fall dazu führen, dass der Rechner seiner eigentlichen Arbeit nicht mehr nachkommt, weil die CPU nur damit beschäftigt ist Broadcasts weg zu werfen. Dies entspricht einem Denial Of Service.

Das bedeutet, dass Broadcast-lastige Protokolle für alle am Netzwerk angeschlossenen Geräte eine CPU-Grundlast darstellen. Dies ist ein Grund warum IP-Netzwerke möglichst klein sein sollten. Damit werden auch die Broadcast-Domänen begrenzt.

24.12.7.1.1 - Limited Broadcast

Bei diesem Broadcast sind alle Bytes der Ziel-IP-Adresse auf 1 gesetzt. In der dotted decimal Schreibweise ist das 255.255.255.255. Dieser Broadcast wird von manchen Netzwerkteilnehmern während des Bootvorgangs verwendet, um die eigene IP-Adresse zu ermitteln. Dieser Broadcast wird nie von einem Router weitergeleitet!

24.12.7.1.2 - Net Directed Broadcast

Bei diesem Broadcast bleibt der natürliche Netzwerk-Teil erhalten und der Host-Teil wird durch Einsen ersetzt. Dieser Broadcast bezieht sich somit nur auf die Netzwerk-Klasse. Ein Router muss normalerweise einen solchen Broadcast weiterleiten. Allerdings ist eine Möglichkeit vorzusehen, das Weiterleiten auszuschalten.

Subnetze sind nicht berücksichtigt.

Beispiel: 141.73.255.255

24.12.7.1.3 - Subnet Directed Broadcast

Hier ist ein mögliches Subnetz berücksichtigt. Der Netzwerk- sowie der Subnetz-Teil bleibt erhalten. Der Host-Adress-Teil besteht aus Einsen.

Beispiel: 141.73.138.255

24.12.7.1.4 - All Subnets Directed Broadcast

Hier ist ein mögliches Subnetz nicht berücksichtigt. Nur der Netzwerk-Teil bleibt erhalten. Der Host-Adress-Teil sowie der Subnetz-Teil besteht aus Einsen. Er entspricht einem Net Directed Broadcast, falls kein Subnetting durchgeführt wird.

Beispiel: 141.73.255.255

Ein Ping auf eine Broadcast-Adresse ergibt eine Rückmeldung von allen in diesem Netzwerk befindlichen Netzwerk-Teilnehmern.

Das Ping-Kommando liefert am Ende der Ausgaben den Hinweis [DUP!]

Diese Funktion ist abhängig vom Betriebs-System.



24.12.7.2 - Multicasts

24.12.7.2.1 - Multicast-ID

Mit Multicasts kann eine bestimmte Gruppe von IP-Geräten angesprochen werden. Eine IP-Multicast-ID hat mit ihren 32 Bit immer folgendes Aussehen:

4 Bits	28 Bits
1110	Multicast Group ID

Die Schreibweise gleicht der einer IP-Adresse in dotted decimal. Somit ergibt sich der folgender Adress-Bereich:
224.0.0.0 bis 239.255.255.255

Alle Geräte, die auf eine bestimmte Multicast ID hören, werden zu einer Host-Group zusammengefasst. Diese Gruppe kann über mehrere Netzwerke hinweg aufgebaut werden. Dazu müssen die Router dazwischen das IGMP (Internet Group Message Protocol) beherrschen.

Die IANA (Internet Assigned Number Authority) verwaltet einige „well-known Multicast-ID's“. Diese werden auch „permanent host groups“ genannt.

Beispiele:

Multicast-Group-ID	Bedeutung
224.0.0.1	Alle Systeme in diesem Subnetz
224.0.0.2	Alle Router in diesem Subnetz
224.0.0.9	RIP-2
224.0.1.1	NTP (Network Time Protocol)

Die Adressen 224.0.0.0 - 224.0.0.255 werden für lokale Multicasts verwendet und somit nicht von Routern weitergeleitet. ICMP-Meldungen gibt es für Multicasts ebenfalls nicht!

24.12.7.2.2 - Umsetzung der Multicast-ID in eine MAC-Adresse

Die IANA besitzt einen MAC-Adr.-Block, der die ersten 3 Byte der MAC-Adr. festlegt:
00:00:5E

Für Multicasts wurde folgender Bereich festgelegt:
01:00:5E

Die restlichen 3 Bytes werden aus der IP-Multicast-ID gewonnen. Dazu werden die niedrigerwertigen 23 Bits der IP-Adresse verwendet. Am ersten Byte der MAC-Multicast-Adresse wird eine 0 angehängt. Daran werden die 23 Bit der IP-Multicast-ID angehängt.

Da hierbei 5 Bits der IP-Adresse nicht berücksichtigt werden, ist die MAC-Multicast-Adresse nicht eindeutig! 32 unterschiedliche Multicast-Group-IDs werden auf eine MAC-Adresse umgesetzt.



Beispiel:

224.128.64.32 (Hex: E0.80.40.20) und 224.0.64.32 (Hex: E0.00.40.20)
werden auf die MAC-Adr.: 01:00:5E:00:40:20 umgesetzt!

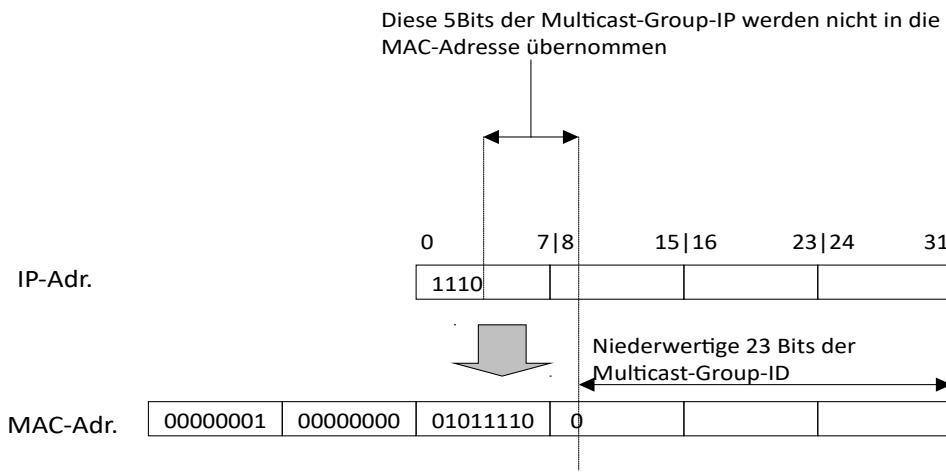


Abbildung 364 : Umsetzung der Multicast-ID in IP-Adresse

Dies bedeutet, dass bei Netzwerk-Teilnehmern, die Multicasts verarbeiten, die überlagerten Schichten die Multicasts filtern müssen!

Multicasts funktionieren auch mit mehreren Sendern (daher kommt auch der Name). Rückmeldungen sind nicht möglich. Daher kann auch TCP nicht mit Multicasts verwendet werden. Der Sender weiß nicht, wer ihm zuhört.

24.12.8 - IP-Header

Version (4Bit)	IHL (4Bit)	TOS (8 Bit)	Length (16 Bit)			
ID (16 Bit)		Flags (3Bit)	Fragment Offset (13Bit)			
TTL (8 Bit)	Protocol (8 Bit)		Checksum (16 Bit)			
Source Address (32Bit)						
Destination Address (32Bit)						
Options			Padding			

Die minimale Header-Länge beträgt 20 Bytes. Die maximale Header-Länge beträgt 60 Bytes. Die Unterschiede liegen in den möglichen Optionen.

Headerteil	Länge [in Bit]	Bedeutung
Version	4	Version des IP-Headers. Dieser Header-Aufbau bezieht sich auf die Version 4 0 = Reserviert 1-3 = nicht zugewiesen 4 = Internet-Protokoll 5 = ST Datagramm-Mode 6 = IPng 7-14 = nicht zugewiesen 15 Reserviert
IHL	4	Internet-Header-Length (wird in 32-Bit-Worten gerechnet) Die minimale Headerlänge ist 5
TOS	8	Type Of Service Bits 0-2: Priorität 111 - Network Control 110 - Internetwork Control 101 - CRITIC/ECP 100 - Flash Override 011 - Flash 010 - Immediate 001 - Priority 000 - Routine Bit 3: Minimize Delay 0 = normal Delay / 1 = low Delay

Protokolle

Headerteil	Länge [in Bit]	Bedeutung
		Bit 4: Maximize Throughput 0 = normal Throughput / 1 = High Throughput Bit 5: Maximize Reliability 0 = normal Reliability / 1 = High Reliability Bits 6: Minimize monetary cost 0 = normal cost / 1 = low cost Bit 7: Reserviert (immer 0)
Length	16	Länge des gesamten Datagramms
ID	16	Identifikation des Datagramms für das Reassemblieren von fragmentierten Datagrammen
Flags	3	Steuerflags für das Fragmentieren Bit 0: reserviert muss 0 sein Bit 1: DF (DON'T FRAGMENT) 0 = may fragment (darf fragmentiert werden) 1 = don't fragment (nicht fragmentieren) Bit 2: MF (MORE FRAGMENTS) 0 = Last Fragment 1 = More Fragments
Fragment Offset	13	Anfang/Position des Fragments im Original-Datagramm
TTL	8	Time To Live Maximale Lebensdauer des Datagramms. Bei jedem Weiterreichen eines Datagramms durch einen Router in ein weiteres Netzwerk wird der Wert um 1 reduziert. Sobald der TTL-Wert = 0 ist, wird das Datagramm verworfen und eine ICMP-Meldung erzeugt.
Protocol	8	Kennung des Protokolls der nächsthöheren Ebene (beschrieben in RFC790, siehe auch im Anhang) z. B. ICMP = 1 / IGMP=2 / TCP = 6 / UDP = 17
Checksum	16	Checksumme des Headers Ist das 16-Bit Einerkomplement der Einerkomplement-Summe aller 16 Bit Worte im Header
Source	32	Quell-IP-Adresse
Destination	32	Ziel-IP-Adresse
Options	27	Können, müssen aber nicht definiert sein
Padding	5	Füll-Bits

24.12.9 - Referenz-Netzwerke

Es gibt IP-Adress-Bereiche, die für Test-Installationen besonders geeignet sind.

Diese werden durch Router **nicht** weitergeleitet! Der RFC 1918 legt für die Klassen A, B und C Adress-Bereiche fest.

Besondere IPv4-Adressen nach RFC 3330:

Adressblock	Adressbereich	Beschreibung	CIDR
0.0.0.0/8	0.0.0.0 bis 0.255.255.255	Nicht spezifizierte IP-Adresse Aktuelles Netz (nur als Quelladresse gültig) Default-Route	RFC 3232 (ersetzt RFC 1700)
10.0.0.0/8	10.0.0.0 bis 10.255.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
127.0.0.0/8 ⁽¹⁾	127.0.0.0 bis 127.255.255.255	Localnet (Loopback-Adresse)	RFC 3330
169.254.0.0/16	169.254.0.0 bis 169.254.255.255	Zeroconf (APIPA)	RFC 3927
172.16.0.0/12	172.16.0.0 bis 172.31.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
192.0.0.0/24	192.0.0.0 bis 192.0.0.255	reserviert, aber zur Vergabe vorgesehen	
192.0.2.0/24	192.0.2.0 bis 192.0.2.255	Dokumentation und Beispielcode (<i>TEST-NET-1</i>)	RFC 5737 (ersetzt RFC 3330)
192.88.99.0/24	192.88.99.0 bis 192.88.99.255	6to4 -Anycast-Weiterleitungspräfix	RFC 3068
192.168.0.0/16	192.168.0.0 bis 192.168.255.255	Netzwerk für den privaten Gebrauch	RFC 1918
198.18.0.0/15	198.18.0.0 bis 198.19.255.255	Netz-Benchmark-Tests	RFC 2544
198.51.100.0/24	198.51.100.0 bis 198.51.100.255	Dokumentation und Beispielcode (<i>TEST-NET-2</i>)	RFC 5737
203.0.113.0/24	203.0.113.0 bis 203.0.113.255	Dokumentation und Beispielcode (<i>TEST-NET-3</i>)	RFC 5737
224.0.0.0/4	224.0.0.0 bis 239.255.255.255	Multicasts (früheres Klasse-D-Netz)	RFC 3171
240.0.0.0/4	240.0.0.0 bis 255.255.255.255	reserviert (früheres Klasse-E-Netz)	RFC 3232 (ersetzt RFC 1700)
255.255.255.255 ²⁾	255.255.255.255	Broadcast	

24.12.10 - TOS für verschiedene Applikationen

Um Protokolle, die auf IP aufsetzen zu priorisieren oder zurückzustellen wurde der TOS eingeführt.

Application	Minimize Delay	Maximize Throughput	Maximize Reliability	Minimize monetary cost	Res. Immer 0	Hex Wert
telnet, rlogin	1	0	0	0	0	0x10
FTP control data	1 0	0 1	0 0	0 0	0 0	0x10 0x08
Any bulk data	0	1	0	0	0	0x08
TFTP	1	0	0	0	0	0x10
SMTP command Phase data Phase	1 0	0 1	0 0	0 0	0 0	0x10 0x08
DNS UDP query TCP query zone transfer	1 0 0	0 0 1	0 0 0	0 0 0	0 0 0	0x10 0x00 0x08
ICMP error query	0 0	0 0	0 0	0 0	0 0	0x00 0x00
Any IGP	0	0	1	0	0	0x40
SNMP	0	0	1	0	0	0x40
BOOTP	0	0	0	0	0	0x00
NNTP	0	0	0	1	0	0x02

24.13 - Network-Address-Translation

24.13.1 - Problemstellung

Die Verwendung von nicht im Internet routebaren IP-Adressen (dies ist der Fall bei der Verwendung des RFC 1918) hat einen kleinen Nachteil, wenn man mit Netzwerkteilnehmern im Internet kommunizieren will. Die Pakete werden eben nicht weitergeleitet. Hat man ein Netzwerk wie in der folgenden Abbildung auf der linken Seite, dann können die Pakete aus dem Netzwerk 192.168.0.0 erst einmal nicht im Internet transportiert werden. Damit kann der Netzteilnehmer x mit dem Netzteilnehmer y zuerst einmal nicht kommunizieren. Damit die Kommunikation dennoch funktioniert, muss der Router A eine Umsetzung der Quell-IP-Adresse des Rechners x machen. Dieser Vorgang wird NAT (Network Address Translation; deutsch: Netzwerk-Adress-Übersetzung) genannt und wird vom Router A durchgeführt (Es kann aber auch ein spezieller NAT-Server verwendet werden).

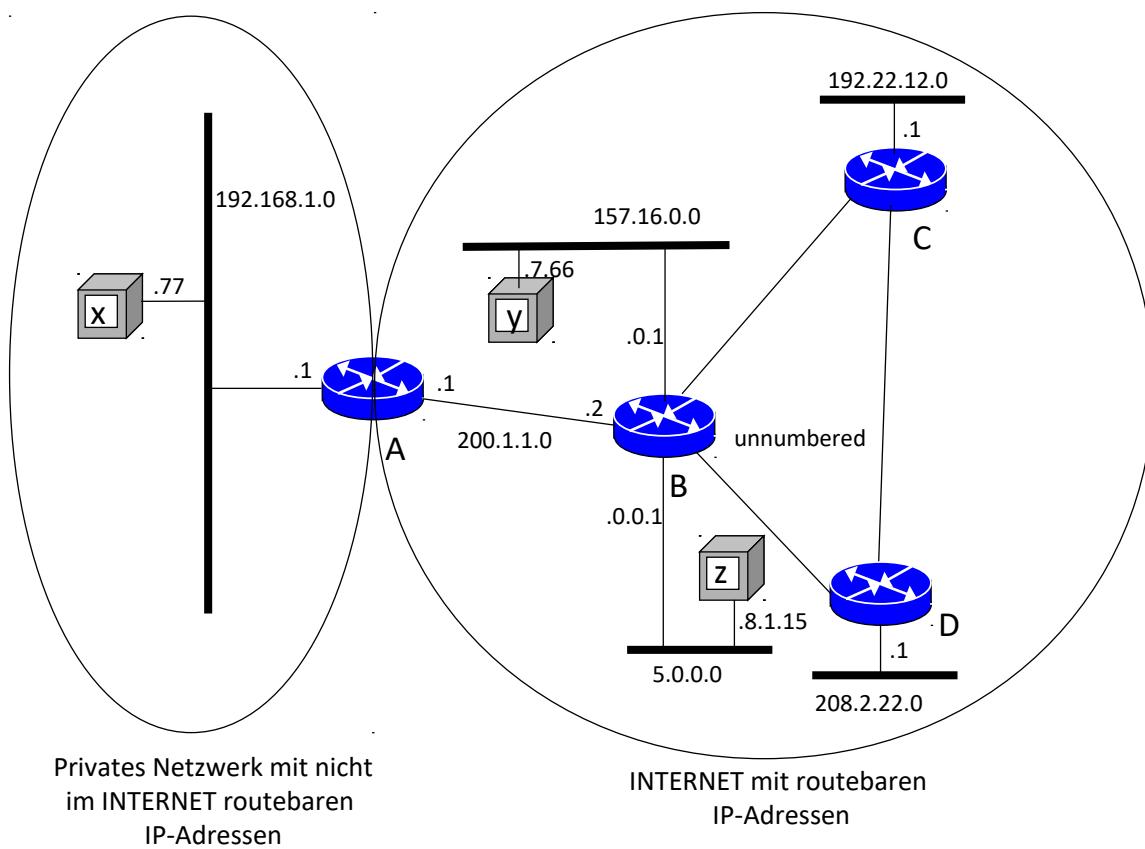


Abbildung 365 : Network-Address-Translation

NAT ist im RFC 2663 beschrieben.

24.13.2 - Vorgehensweise

Der Router verwendet dabei eine Tabelle, in der er die IP-Adresse des Rechners A und seine TCP-Port-Nummer zu einer im Internet gültigen IP-Adresse und TCP-Portnummer umsetzt. Dazu verwendet er seine eigene IP-Adresse, die er anstelle der nicht routenbaren IP-Adresse in das Paket einbaut. Zusätzlich wird der TCP-Port durch einen bei ihm freien TCP-Port ausgetauscht. Damit noch die IP- und TCP-Prüfsummen stimmen, muss er diese auch noch neu berechnen und in das Paket eintragen.

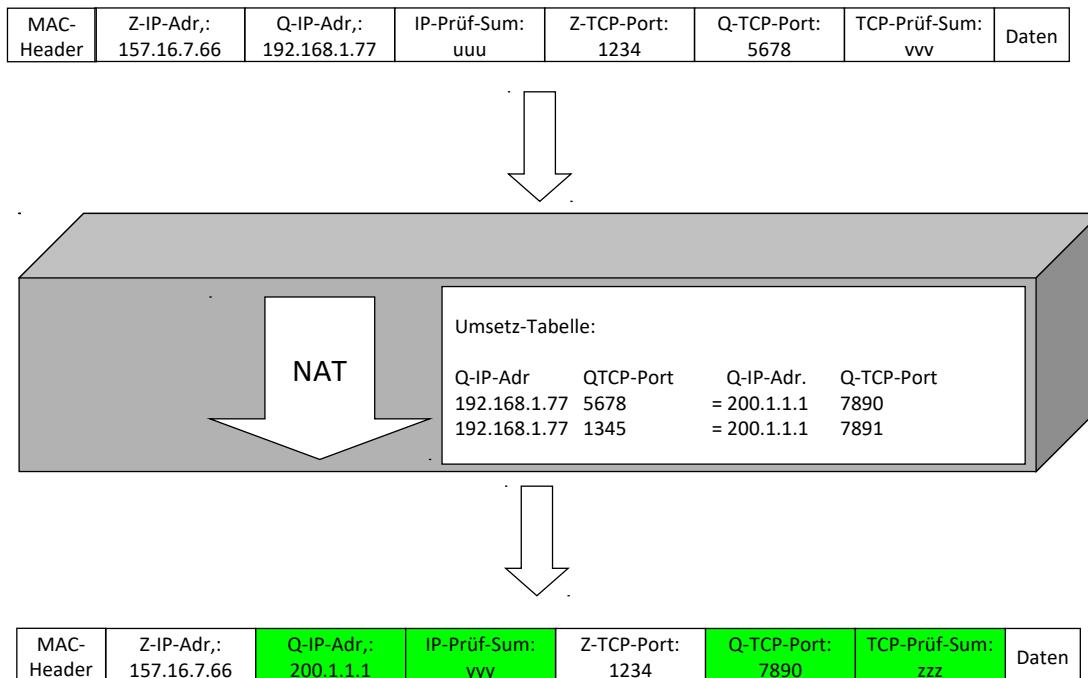


Abbildung 366 : Umsetzung der IP-Adressen bei NAT

Ein Paket, das der Rechner x dem Rechner y sendet, wird vom Router folgendermaßen umgesetzt:

24.13.2.1 - Vorteile von NAT

In der obigen Abbildung kann man außerdem noch sehen, dass ein Netzwerkeinzelne aus dem Internet immer nur die IP-Adresse des Routers A sehen kann. Alle Netzwerke und ihre Hosts hinter dem Router A sind vom Internet aus nicht zu sehen. Dies stellt einen Schutz vor Angreifern aus dem Internet dar. Was man nicht sehen kann, lässt sich nur schwer oder gar nicht angreifen.

24.13.2.2 - Nachteile von NAT

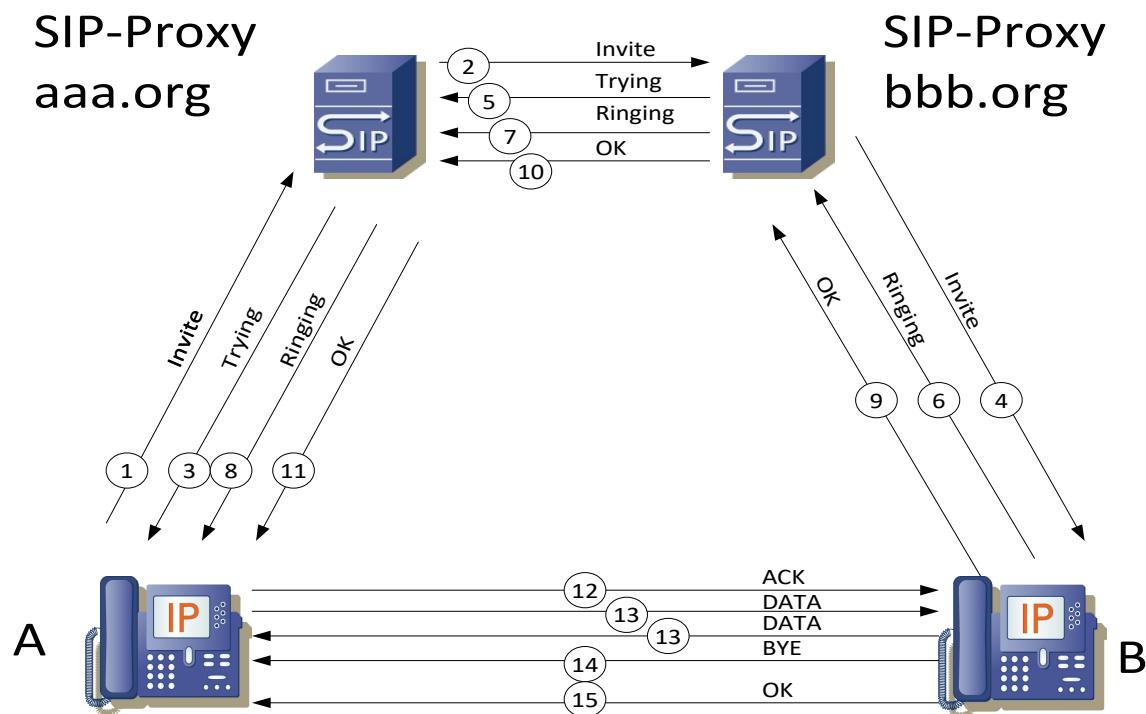
- NAT benötigt im Router Ressourcen.
- NAT behindert Protokolle zur Sicherung vor Angriffen von außen.
- Alle Dienste auf UDP-Basis haben keine Möglichkeit zur Erkennung des Verbindungsabbaus. Dadurch bleiben die Ressourcen im Router belegt.
- Eine Veränderung der IP-Adressen kann eine Änderung der TCP-Sequenznummern mit sich bringen, da die Paket-Länge in die Sequenznummerermittlung einfließt. Dies ist dann der Fall, wenn die IP-Adresse im Daten-Teil steht und ebenfalls noch umgesetzt werden muss.
Dies bedeutet wiederum ein Performance/Ressourcen-Problem.
- Eine Verwendung von IPSec ist nicht möglich. Verschlüsselung auf Ebene4 und höher (SSL und SSH) sind jedoch problemlos möglich.
- Ein Zugriff auf einen internen WEB-Server aus dem Internet macht evtl. noch keine Probleme, da der Port 80 standardmäßig verwendet werden kann. Bei verteilten X-Windows-Servern ist jedoch schnell Schluss.

Je nachdem ob nur IP-Adressen oder auch Ports umgesetzt werden wird von NAT (Network Address Translation) oder PAT / NAPT (Port Address Translation / Network and Port Address Translation) gesprochen.

24.13.3 - Formen von NAT

Bei NAT wird fast immer die Verbindung von innen nach außen aufgebaut. Ein Router kann die NAT-Tabelle dynamisch verwalten. Die Adress-Zuordnung findet erst dann statt wenn sie gebraucht wird. Diese Vorgehensweise spart Ressourcen. Es handelt sich hierbei um eine typische Client-Server-Architektur. Der Client, z. B. ein Browser baut eine Verbindung zu einem WEB-Server auf Port 80 auf.

Probleme gibt es erst, wenn aus der Client-Server- eine Peer-to-Peer-Kommunikation wird. Dies bedeutet eine Any-to-Any-Kommunikation. Dies ist z. B. bei VoIP, dargestellt am SIP-Trapez, der Fall. Hier läuft während des Gesprächs der Datenstrom von Endgerät zu Endgerät anstelle über einen Server. Zusätzlich sind die Ports nicht mehr statisch fest vergeben sondern werden erst festgelegt wenn sie benutzt werden sollen.



NAT ist aus zwei unterschiedlichen Sichtweisen zu betrachten:

- ➊ Konfiguration durch den Administrator. Für ihn stellt sich die Frage ob die NAT-Tabelle statisch oder dynamisch erstellt wird. Muss er außer den IP-Adressen auch noch die Port-Adressen betrachten?
- ➋ Der Anwendungsentwickler interessiert sich nicht für die Konfiguration der NAT-Tabelle sondern ob seine Applikation immer die selbe externe IP-Adresse oder einen ständig ändernde IP-Adresse die Basis für die Kommunikation seiner Applikation hat.

Für das Traversal-Problem haben sich mittlerweile die folgenden 4 Ausprägungen etabliert.

24.13.3.1 - Full Cone

Hierbei wird immer dieselbe interne IP-Adresse auf dieselbe externe IP-Adresse abgebildet. Die Portnummern werden deshalb auch nicht geändert.

Dies bedeutet, dass für jedes interne Gerät eine externe IP-Adresse benötigt wird. Die Frage warum nicht gleich die externe IP-Adresse verwendet wird lässt sich mit Argumenten aus dem Umfeld Sicherheit begründen. Damit ist es möglich eine Verbindung von außen nach innen zu initiieren.

Der Vorteil dieses Verfahrens liegt in der klaren Vorhersagbarkeit von IP-Adressen und Portnummern. Der Nachteil liegt in der benötigten IP-Adress-Anzahl. Sobald die interne Applikation herausgefunden hat welche IP-Adresse sie zugewiesen bekommen hat, steht einer Any-to-Any-Kommunikation nichts mehr im Wege.

e

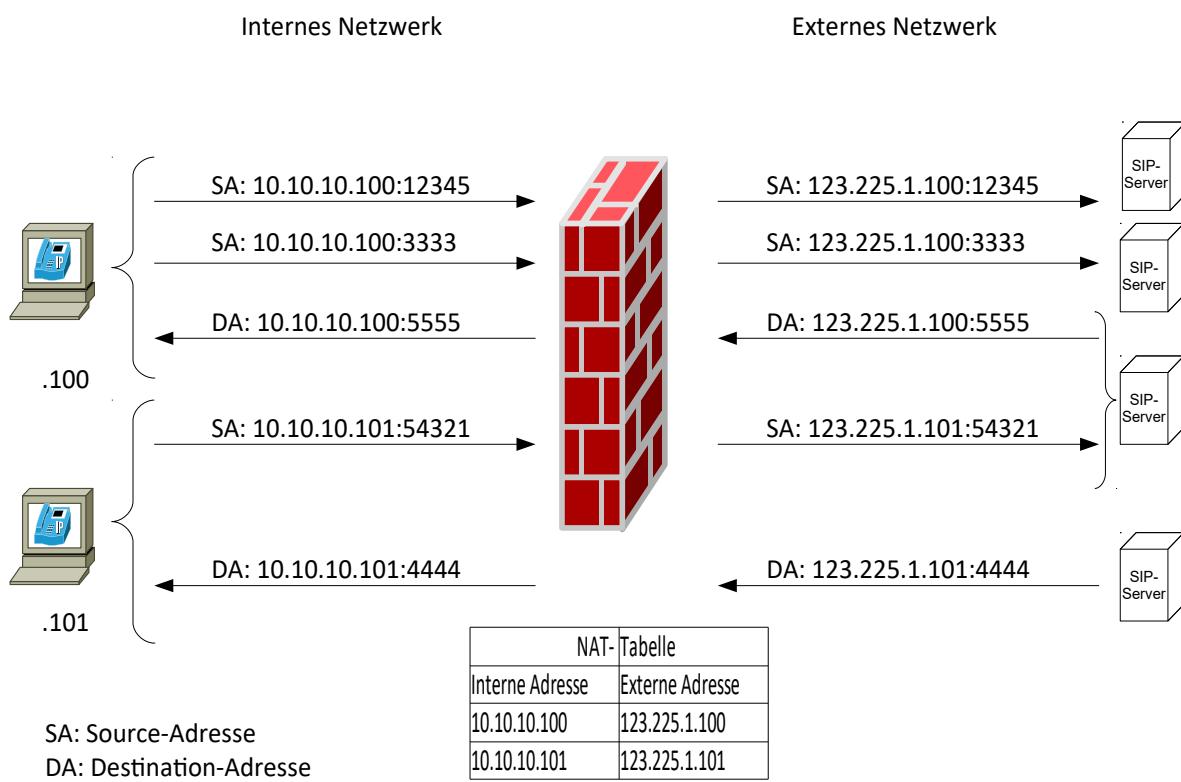


Abbildung 368 : NAT Full Cone

24.13.3.2 - Restricted Cone

Beim Restricted Cone wird, genau so wie beim Full Cone, jede innere IP-Adresse mit einer äußeren IP-Adresse sowie die innere Portnummer mit der äußeren Portnummer eindeutig verbunden. Allerdings muss die Verbindung erstmalig von innen nach außen aufgebaut worden sein. Das bedeutet, dass von außen nach innen nur eine Verbindung aufgebaut werden kann, wenn diese Verbindung bereits einmal von innen nach außen aufgebaut wurde. Ein Verbindungsauftakt von außen nach innen ist damit ausgeschlossen. Dies trägt zur Erhöhung der Sicherheit bei. Damit ist die Applikation auf einem internen Rechner immer in der Pflicht die Verbindung zuerst aufzubauen. Dies ist jedoch durch die gängigen Architekturen im Client-Server Umfeld kein Problem. Eine Client Applikation muss sich auch bei SIP an einem Server anmelden.

Der Nachteil mit den vielen notwendigen Externen IP-Adressen ist jedoch immer noch vorhanden.

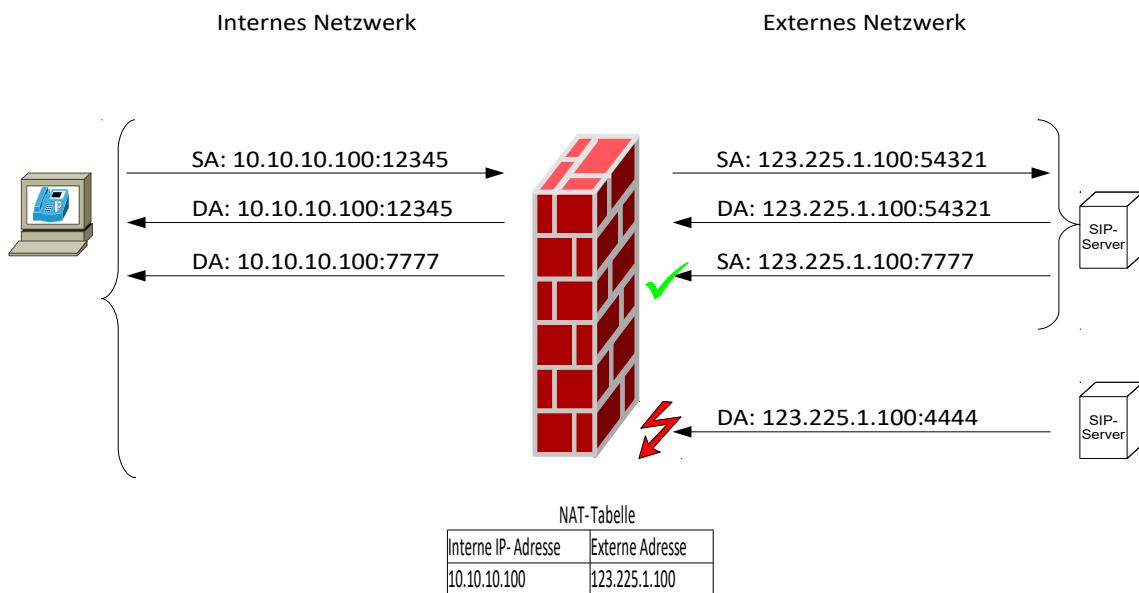


Abbildung 369 : NAT Restricted Cone

Da der untere Server aus dem externen Netzwerk noch keine Verbindung mit dem Client auf der internen Seite hatte, kann er auch keine Verbindung aufbauen.

24.13.3.3 - Port Restricted Cone

Hierbei handelt es sich um eine weitere Verschärfung des Restricted Cone. Das dynamisch erzeugte IP-Adress-Port-Pärchen ist hierbei jedoch bei zu behalten. Bei einer Änderung wird ein Verbindungsaufbau abgewiesen. Damit können nun erstmals mehrere interne IP-Adressen auf eine einzige, externe IP-Adresse gebunden werden. Damit muss sie Applikation herausfinden welche externe IP-Adresse für die Kommunikation genutzt wird. Zusätzlich muss das NAT ein Pinhole (sinngemäßes deutsch: Ausnahmeregel) in die Firewall von außen nach innen öffnen. Damit fällt einer Firewall erstmalig ein Aufgabenteil zu.

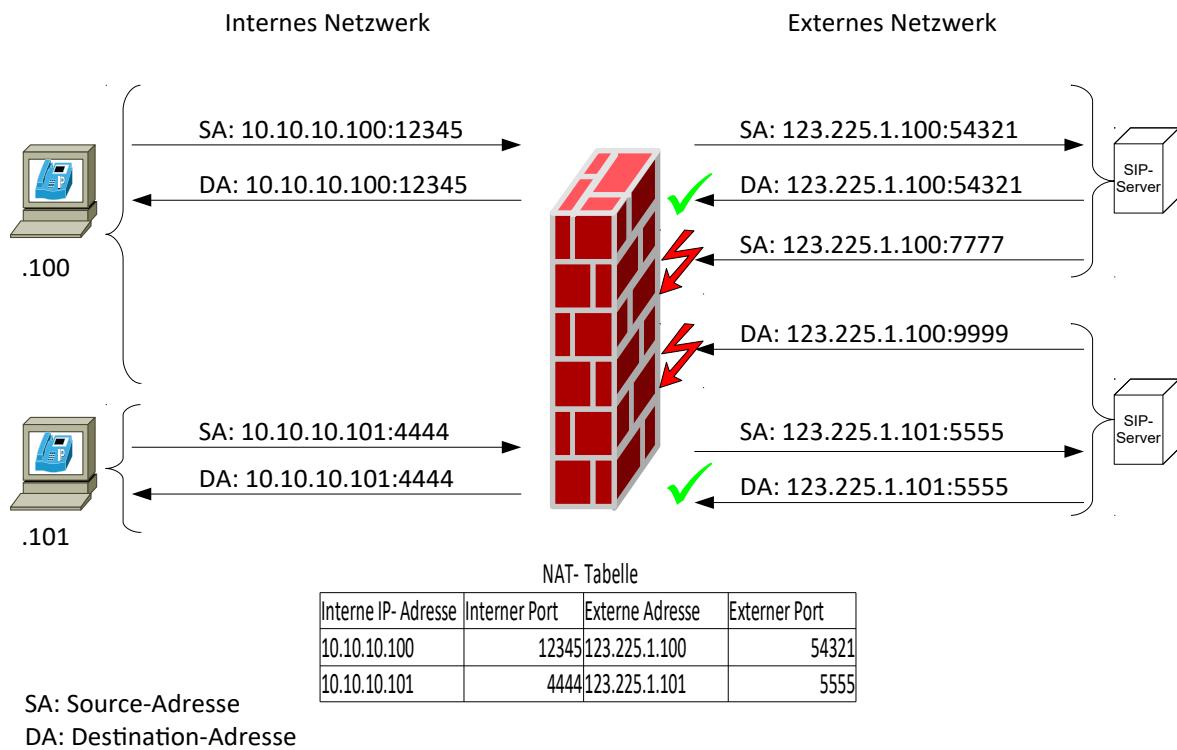


Abbildung 370 : NAT Port Restricted Cone

Der obere Server aus dem externen Netzwerk kann nur auf dem Port (54321) antworten, auf dem bereits eine Verbindung aufgebaut war. Über den anderen Port(7777) kann nicht kommuniziert werden. Der untere Server aus dem externen Netzwerk kann von sich aus keine Verbindung zum oberen Client initiiieren. Auch zum unteren Client kann der untere Server erst dann Daten senden wenn eine Verbindung aufgebaut war.

24.13.3.4 - Symmetric Cone

Wie beim Port Restricted Cone werden die IP-Adress-Port Pärchen dynamisch erzeugt. Allerdings ist nicht mehr sicher gestellt, dass immer die selben IP-Adressen Verwendung finden. Dies bedeutet für eine Applikation ein unlösbares Problem. Eine Anwendung kann von sich aus dieses Problem nicht lösen.

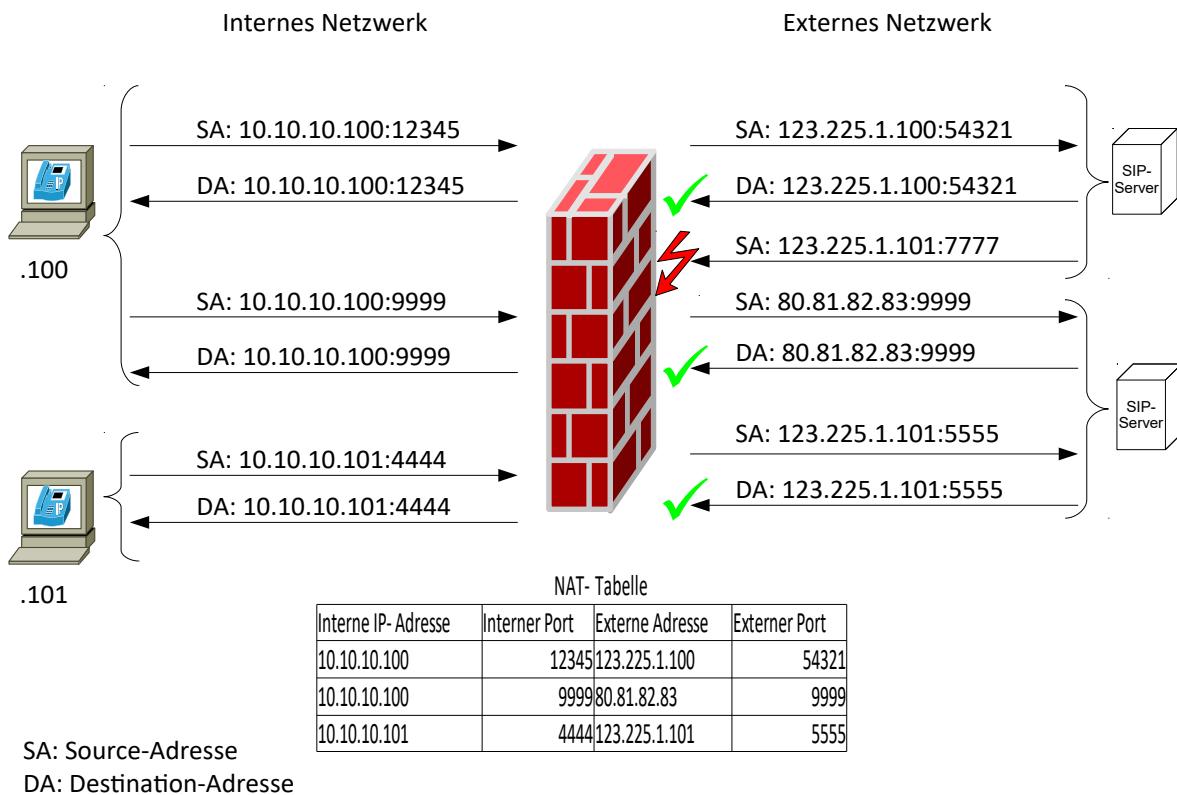


Abbildung 371 : NAT Symmetric Cone

24.13.4 - Lösung der Probleme mit NAT

Je nachdem welche Version von NAT bei einer Kommunikationsstrecke zum Tragen kommt, muss mit weiteren technischen Kunstgriffen nach gebessert werden um eine Kommunikation von außen nach innen zu initiieren.

24.13.4.1 - VPNs

Ein Virtual Private Network verbindet zwei private Netzwerke über ein unsicheres Netzwerk wie z. B. das Internet. Das NAT-Problem kann dadurch umgangen werden, dass entweder der Tunnel auf dem Gerät, welches auch NAT durchführt, implementiert wird oder der Tunnel parallel zum Router der NAT praktiziert parallel durchführt. Damit ist das NAT-Problem erst einmal sauber umgangen. Allerdings ist bei der Übertragung von Daten über ein VPN mit erhöhten Latenzzeiten zu rechnen. Bei Applikationen, die wie VoIP Delay-kritisch sind, kann dies zu Problemen führen. Zudem können Geräte, die am Tunnel-Aufbau nicht teilnehmen können, ebenso an der Kommunikation nicht teilnehmen.

24.13.4.2 - Einstellen der Ports

Es ist eine gängige Methode auf einer Firewall Ports von außen nach innen einer bestimmten IP-Adresse zuzuweisen. Es ist ebenso auch möglich ein ganzes Portband zu öffnen. Allerdings wird dann eine Firewall schnell ad absurdum geführt.

Damit gibt es für den internen Client die folgenden Möglichkeiten.

24.13.4.3 - Manueller Porteintrag

Die externe IP-Adresse wird auf dem internen Client manuell eingetragen. Diese Lösung ist bei vielen Peer-to-Peer Anwendungen möglich jedoch auch umständlich. Problematisch und gänzlich unpraktikabel ist das bei einem DSL-Anschluss des Routers, da er bei jedem Aufbau der Verbindung zum Internet eine neue IP-Adresse bekommt.

24.13.4.4 - STUN

Automatisch Ermittlung des Clients der externen IP-Adresse beim Router. Das Verfahren ist im RFC 3489 beschrieben. STUN steht für Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs).

Nach dem Start sendet die Applikation an den STUN Server ein Testpaket. Die IP-Adresse des Servers ist entweder über DNS gelernt worden oder manuell von Administrator eingetragen worden. Der STUN Server sendet dem Client die externe IP-Adresse zurück. Mit dieser Adresse kann sich die Applikation z. B. am SIP Server anmelden. Dieses Verfahren ermöglicht es dem Client sogar herauszufinden welche NAT-Variante verwendet wird. Bis auf einen symmetrischen Cone ist jede NAT-Variante bearbeitbar.

24.13.4.5 - Dynamisches DNS

Anstelle der IP-Adresse gibt der Client seinen DNS-Namen bekannt. Sobald der Router eine Neue IP-Adresse bekommt wird diese bei der DNS-Verwaltung korrigiert.

24.13.4.6 - Application Layer Gateway

Eine Firewall, die als Application Layer Gateway (ALG) implementiert ist, kann nicht nur die Header bearbeiten, sondern auch die Daten, die weiter hinten im Datenteil stehen. Damit kann für diverse Protokolle an den entsprechenden Stellen nachgeschaut werden und die notwendigen NAT-Einträge durchgeführt werden. Da dies jedoch nicht für alle Protokolle implementiert ist kann es vorkommen dass es Applikationen gibt, die an dieser Stelle scheitern. Ein Beispiel aus dieser Kategorie sind derzeit Multimedia-Protokolle.

24.13.4.7 - Universal Plug'n'Play (UPnP)

Dabei müssen sowohl die Applikationen sowie der Router das Verfahren unterstützen. Die Applikation erfragt beim Router die externe IP-Adresse ab. Diese IP-Adresse wird bei den SIP-Servern und den Gesprächspartner beim Gesprächspartner hinterlegt. Danach gibt sie dem Router Bescheid welche Ports zu öffnen sind. Der Router wird die eintreffenden Pakete über die geöffneten Ports an die Applikation weiter leiten. Sobald die Applikation sich beendet gibt sie dem Router den Auftrag die Ports wieder zu schließen.

Vorteilhaft ist hier, dass sich der Anwender um nichts kümmern muss. Der Nachteil liegt daran, dass hierbei eine Applikation einen Router mit Firewall-Funktionalität ferngesteuert wird. Außerdem können NAT-Kaskaden nicht bearbeitet werden da immer nur der erste NAT-Router gesteuert werden kann.

24.13.4.8 - MIDCOM

Es handelt sich hierbei um eine Lösung, welche von IETF entwickelt wurde. MIDCOM bedeutet Middlebox Communication. Hierbei handelt es sich um eine ähnliche Lösung wie bei UpnP. Allerdings wird die Steuerung des Routers nicht durch eine Applikation auf einem Client sondern von einem speziellen Server durchgeführt. Diese Lösung ist für Unternehmen konzipiert. Leider gibt es hierzu nur RFCs (3303, 3304, 3989, 4097) und keine Lösungen.

24.13.4.9 - TURN

Es handelt sich hierbei um ein mehrstufiges Verfahren. In der ersten Stufe wird der TURN Server gesucht. Dies geschieht entweder durch Konfiguration oder einen speziellen SRV-Eintrag im DNS-Server. Sobald der Client den TURN Server kennt meldet er sich dort an.

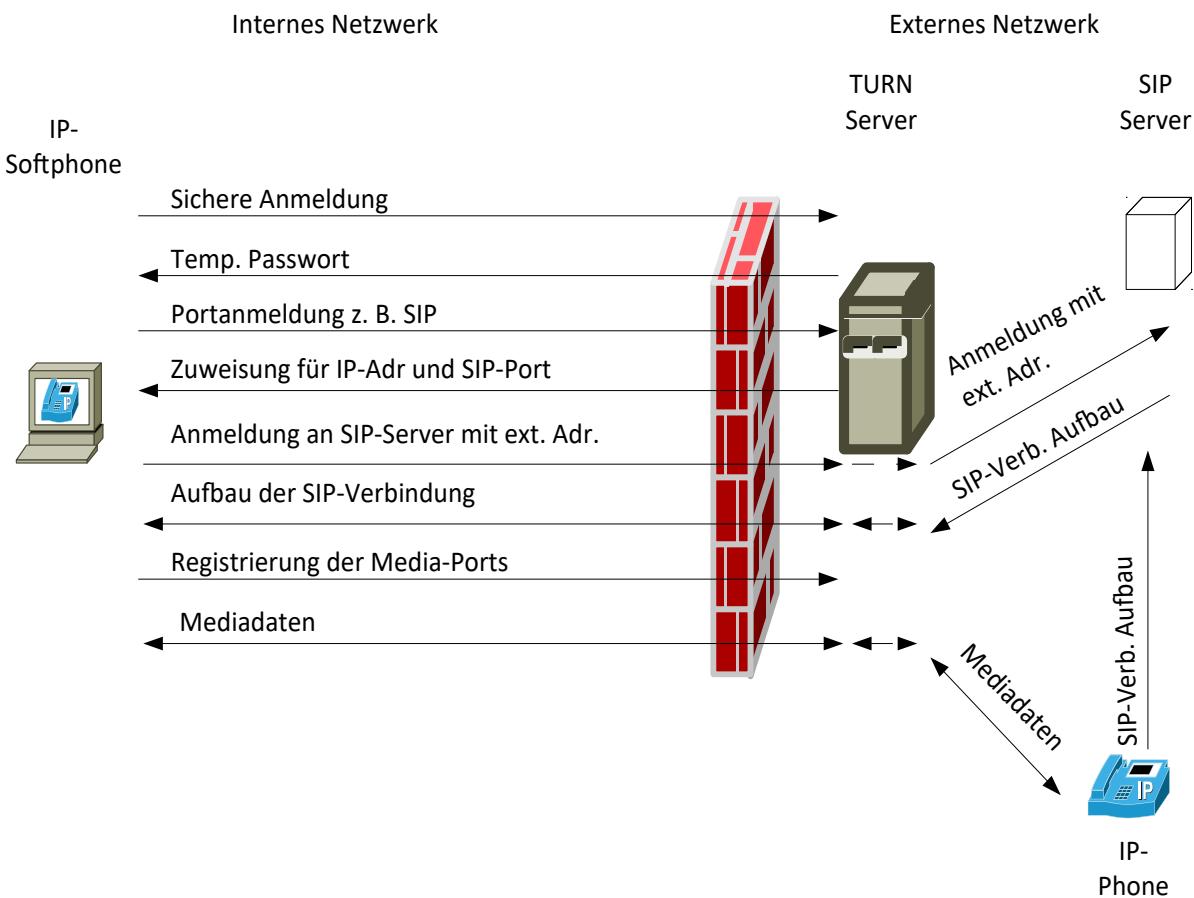


Abbildung 372 : NAT TURN

Nach einer erfolgreichen Anmeldung erhält der Client ein temporäres Passwort bis zur Abmeldung für alle Pakete des Clients an den TURN-Server verwendet wird. Danach meldet der Client alle Ports beim TURN-Server an, über die er von außen erreichbar sein will. Daraufhin bekommt der Client vom TURN-Server die öffentliche IP-Adresse genannt mit der er von außen erreichbar ist.

Mit diesen Informationen kann sich der Client dann am externen SIP-Server anmelden.

Mit einem TURN-Server kann sogar Symmetric Cone NAT überwunden werden. Ein TURN-Server ist kein ALG da er die Daten nicht weiter untersucht und bearbeitet sondern sich nur um IP-Adressen und Ports kümmert.

Ein gravierender Nachteil der TURN-Lösung ist die derzeitige Nichtexistenz. Es gibt bis heute noch keine käuflich erwerbbaren TURN-Server.

24.14 - ARP-Request (Address Resolution Protocol)

24.14.1 - Problemstellung

Normalerweise kennt die Applikation auf der Sendeseite nur den Namen oder die IP-Adresse des Ziels. Die Daten zwischen zwei Netzteilnehmern werden mit einem Unicast ausgetauscht. Dazu muss der Sender die MAC-Adresse des Zielrechners kennen.

Um nun die MAC-Adresse seines Ziels zu ermitteln, sendet die Sende-Station einen ARP-Request mit der IP-Adresse des Empfängers in das Netz und fordert den Netzteilnehmer mit der Ziel-IP-Adresse auf, seine MAC-Adresse zurück zu melden. Da dies ein Broadcast ist, geht die Anfrage an alle Geräte, die im Moment aktiv sind.

Ist eine Station im Netz, welche die IP-Adresse des Ziels besitzt, dann teilt sie der sendenden Station ihre MAC-Adresse mit einem ARP-Response mit. Dies ist ein Unicast. Nun kann der Sender Daten mit einem Unicast an einen Empfänger senden.

ARP ist ein Protokoll der Ebene 3. Beschrieben wird ARP im RFC 826

Aufbau eines ARP-Frames

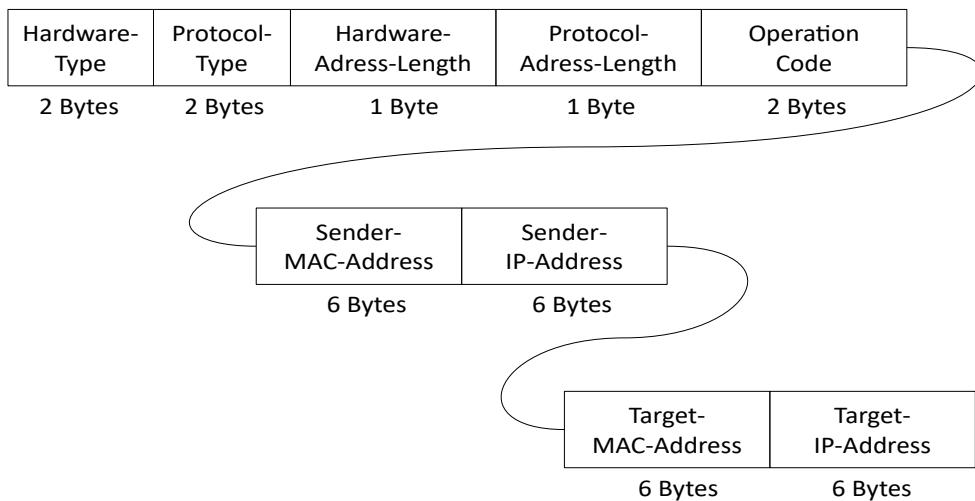


Abbildung 373 : ARP-Datenaufbau

24.14.2 - Ablauf

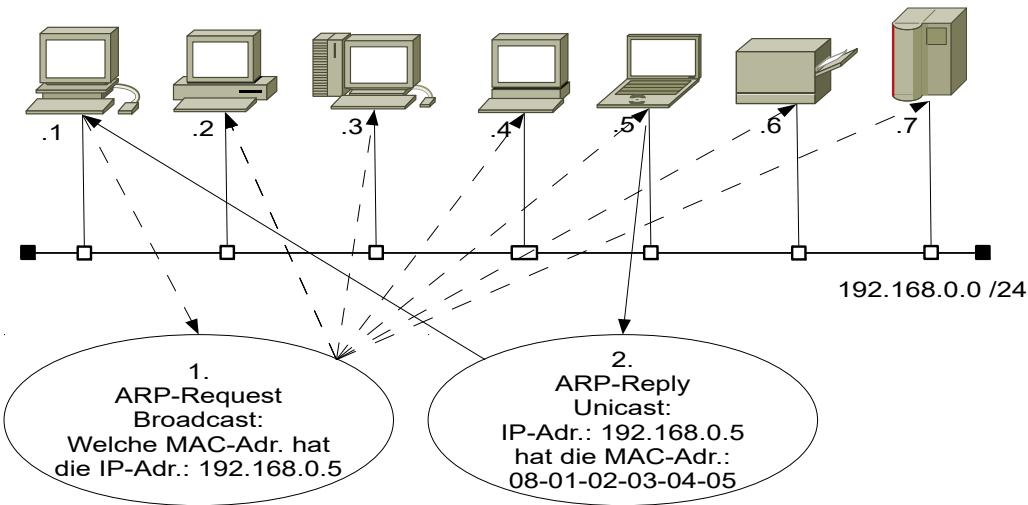


Abbildung 374 : ARP-Ablauf

Damit dieser Ablauf nicht bei jedem Senden eines Pakets ausgeführt werden muss, merkt sich ein Rechner die Zuordnung von MAC-Adresse zu IP-Adresse in einem so genannten ARP-Cache.

Der ARP-Cache kann mittels des ARP-Befehls bearbeitet werden. Er ist auf alle gängigen Betriebssystemen verfügbar.

arp -a	Ausgabe des ARP-Cache-Inhalts
arp -s <ip-adr> <mac-adresse>	ARP-Eintrag manuell vornehmen
arp -d <ip-adresse>	ARP-Eintrag löschen

ARP-Cache-Einträge, die über einen ARP-Request ermittelt werden unterliegen einem Aging-Algorithmus. Dies bedeutet, dass die Einträge wenn sie nicht genutzt werden nach einer bestimmten Zeit (normalerweise 5 Minuten) gelöscht werden. Dies ist notwendig, damit eine neue Netzwerk-Karte (mit einer neuen MAC-Adresse) bei einem Rechner oder ein Rechner-Umzug an einen anderen Switchport keine Probleme bereitet.

24.15 - RARP-Request (Reverse Address Resolution Protocol)

24.15.1 - Problemstellung

Kennt nun ein Netzwerkteilnehmer nicht einmal seine eigene IP-Adresse, kann er sie sich von einem RARP-Server geben lassen.

Dazu sendet der Netzwerkteilnehmer (ohne IP-Adresse) einen RARP-Request in das Netzwerk. Dies ist ein Broadcast.

Der RARP-Server sendet daraufhin die IP-Adresse und die MAC-Adresse von sich und der anfragenden Station an die anfragende Station zurück.

RARP ist ein Protokoll der Ebene 3.

24.15.2 - Ablauf

Station A möchte seine eigene IP-Adresse erfahren.

Deshalb sendet Station A einen RARP-Request mit einem Broadcast an alle (Wer kennt mich?) (1.)

Der RARP-Server kennt die IP-Adresse und sendet sie an die Station A. (2.)

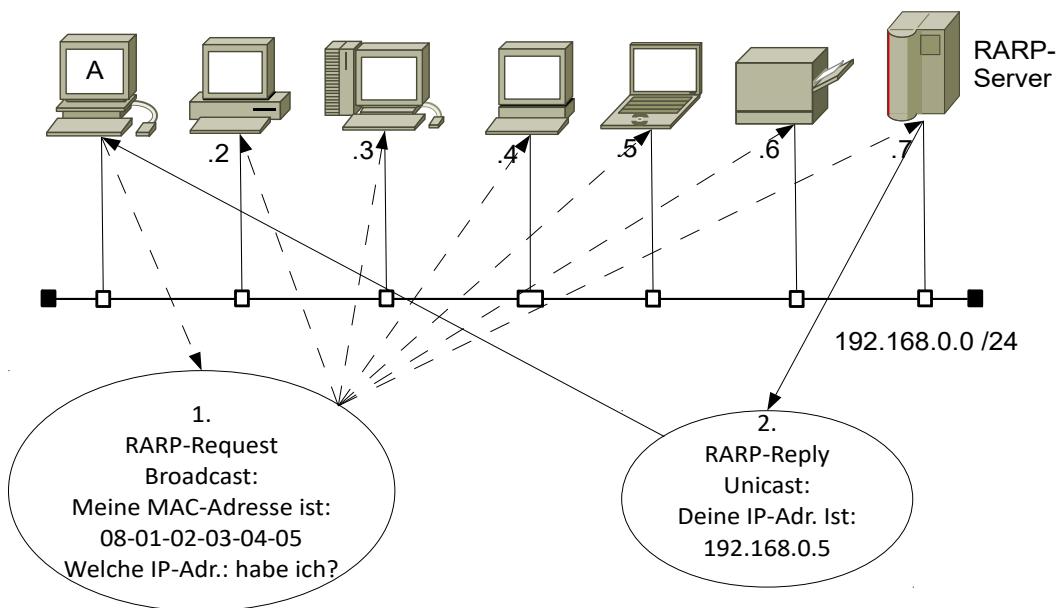


Abbildung 375 : RARP-Ablauf

24.16 - Proxy ARP

24.16.1 - Einleitung

Es kann vorkommen, dass Teile eines LAN über serielle Leitungen via Modem angebunden sind. Siehe folgende Abbildung. Da der ARP-Request ein Broadcast ist, kann er nicht über die Modem-Strecke übertragen werden. Somit kann der Rechner A den Rechner B nicht mit einem ARP-Request erreichen.

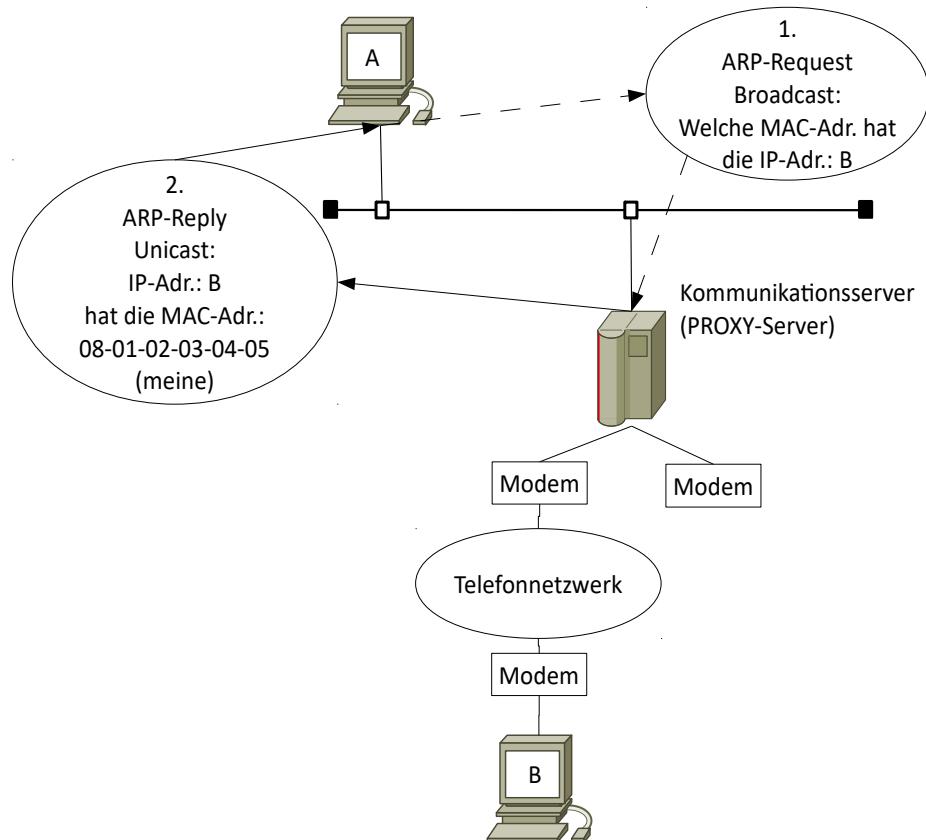


Abbildung 376 : PROXY-ARP

24.16.2 - Abhilfe

Da der Rechner B auf den ARP-Request nicht reagieren kann, tut dies der Kommunikations-Server. Er sendet anstelle des Rechners B seine MAC-Adresse mit einem ARP-Reply an den Rechner A. Daraufhin wird der Rechner A seine Daten an den Kommunikations-Server senden. Der Kommunikations-Server leitet die Daten dann weiter an den Rechner B. Somit fungiert der Kommunikations-Server mit seiner MAC-Adresse als Stellvertreter (Proxy) für den Rechner B. Der Kommunikations-Server muss nur als PROXY-Server parametriert werden.

24.17 - UNARP

24.17.1 - Allgemeines

Im RFC1868 wird die ARP-Erweiterung UNARP vorgestellt. Darin wird die Möglichkeit angesprochen, dass ein Rechner, der heruntergefahren wird, sich noch vorher bei allen anderen Netzwerkteilnehmern verabschieden kann. Damit kann der ARP-Cache eines jeden Rechners bereinigt werden.

24.17.2 - Problembeschreibung

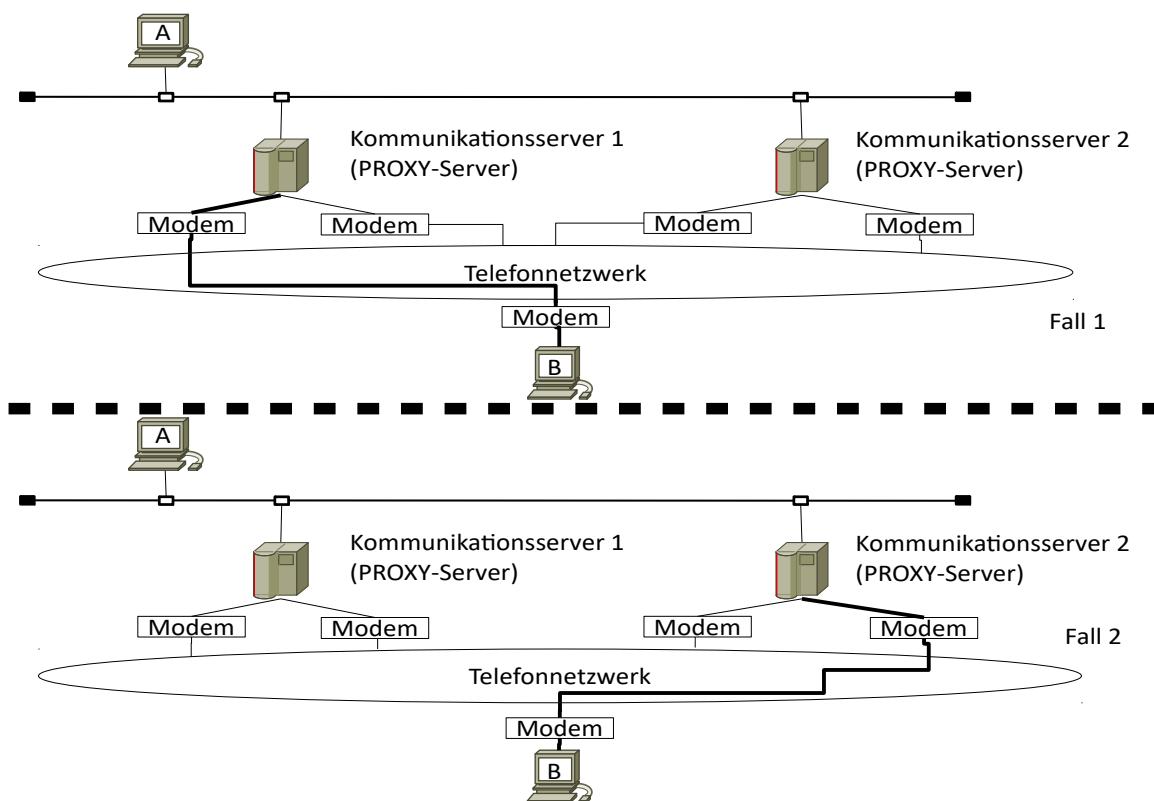


Abbildung 377 : UNARP

In der obigen Abbildung ist die Problematik in Verbindung mit der PROXY-ARP-Konstellation dargestellt. Im oberen Teil hat der Rechner B eine Verbindung aufgebaut. Durch den Kommunikations-Server I hat der Rechner B im LAN eine IP-Adresse und eine MAC-Adresse (die MAC-Adresse des Kommunikations-Servers I) bekommen. Die Kommunikation läuft in beiden Richtungen problemlos.

Sobald jedoch der Rechner B die Verbindung beendet und kurz darauf nochmals aufbaut, kann es zu Problemen kommen (untere Hälfte). Dies liegt daran, dass die neue Verbindung evtl. über den Kommunikations-Server II aufgebaut wird. Der hat eine andere MAC-Adresse als der Kommunikations-Server I. Will der Rechner A Daten an den Rechner B senden, glaubt er die richtige MAC-Adresse im ARP-Cache zu haben. Hat er aber nicht! Somit kann die Kommunikation nicht zustande kommen.

Abhilfe

Würde der Kommunikations-Server I, der die erste Verbindung abbaut, ein UNARP-Datagramm senden, dann könnte der Rechner A seinen ARP-Cache bereinigen. Damit wäre bei einem erneuten Senden von Daten ein ARP-Request fällig, den diesmal der Kommunikations-Server II beantworten würde. Damit könnte eine funktionierende Verbindung über den Kommunikations-Server II aufgebaut werden.

24.17.3 - Ablauf

Der Kommunikations-Server I müsste ein UNARP-Datagramm mit folgenden Inhalt senden:

...	Protokoll IP (0x800)	Hardware-Adress-Länge (0)	Protokoll-Adress-Länge (4)	Opcode (2 = Reply)	Source-Hardware-Adresse (Nicht relevant)	Source-Protokoll-Adresse (IP-Adresse des Rechners mit der abgebauten Verbindung)	Ziel-Hardware-Adresse (Nicht relevant)	Ziel-Protokoll-Adresse 255.255.255.255
-----	----------------------	---------------------------	----------------------------	--------------------	--	--	--	--

24.18 - BOOTP

24.18.1 - Ablauf

Dieses Protokoll hat RARP abgelöst. Hierbei kann ein Gerät seine gesamte Konfiguration, ja selbst sein Betriebssystem und seine Programme von einem BOOTP-Server im Anlauf abholen. Dabei wird TFTP (Trivial File Transfer Protocol) nach dem Client Server-Prinzip verwendet. BOOTP wurde im RFC 951 und 1497 definiert. Mittlerweile wurde BOOTP weitgehend von DHCP abgelöst.

24.18.2 - Paket-Aufbau

Siehe DHCP

24.19 - DHCP

Diese Abkürzung bedeutet: „Dynamic Host Configuration Protocol“; deutsch: dynamisches Geräte Konfigurationsprotokoll.

24.19.1 - Allgemeines

DHCP ist in den RFCs 1533, 1534, 1541 und 1542 beschrieben. DHCP verwendet die UDP-Ports 67 und 68.

Damit kann einem Gerät unter anderem eine IP-Adresse und die zugehörige Subnetmask von einem DHCP-Server vergeben werden. Das ist vor allem bei Notebook-Benutzern beliebt, die in unterschiedlichen Netzwerken tätig sind. Die umständliche Zuordnung einer IP-Adresse und der u. U. erforderliche Neustart des Rechners kann automatisiert werden. Allerdings sollte das nicht auf alle Geräte eines Netzwerks angewendet werden. Systemadministratoren wären nicht erfreut, wenn sich die IP-Adresse eines Servers bei jedem Anlauf ändert. Allerdings entfällt mit DHCP das Problem mit doppelt vergebenen Netzwerkadressen, da der DHCP-Server die Zuordnung der IP-Adressen automatisiert.

Einstellung von DHCP auf einem Windows-Rechner

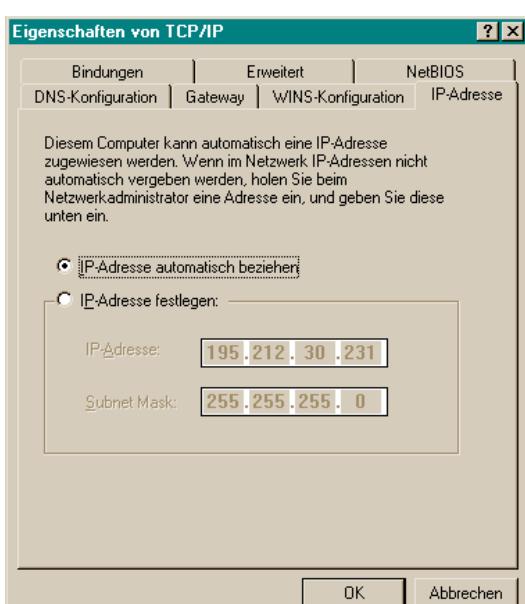


Abbildung 378 : DHCP unter WINDOWS

Einem Gerät kann bei der IP-Stack-Parametrierung angegeben werden, dass die IP-Adresse von einem DHCP-Server zu beziehen ist. Der Systemverwalter definiert auf dem DHCP-Server einen IP-Adress-Bereich. Aus diesem Bereich vergibt der Server bei einer DHCP-Anfrage eines Gerätes eine IP-Adresse.

Der Systemadministrator hat sogar die Möglichkeit, die IP-Adresse einer MAC-Adresse zuzuordnen. Damit bekommt ein Notebook, das seine IP-Adresse über DHCP bezieht, immer die gleiche IP-Adresse zugewiesen.

Zusätzlich kann die Dauer der Zuordnung festgelegt werden. Die so genannte Leasedauer.

Durch DHCP-Relay-Agents können DHCP-Meldungen in Netzwerk-Segmente übertragen werden, die nicht über einen DHCP-Server verfügen. Damit ist nicht für jedes Netzwerk-Segment ein eigener DHCP-Server nötig. Bei Cisco-Routern ist für diese Vorgehensweise die IP-Helper-Adresse einzustellen.

24.19.2 - Ablauf eines DHCP-Lease

Die Zuweisung einer IP-Adresse für eine bestimmte Zeit wird Lease (deutsch: Pacht, Miete..) genannt.

Der Ablauf erfolgt in 4 Phasen:

24.19.2.1 - IP-Adresse anfordern

Mit einer rudimentären IP-Funktionalität fordert der Client mit einem Broadcast den DHCP-Server auf, eine IP-Adresse zu übermitteln. Da der Client noch keine IP-Adresse hat, trägt er in sein Paket die Sende-IP-Adresse 0.0.0.0 ein. Die Ziel-Adresse ist die Broadcast-Adresse 255.255.255.255, da der Client noch keine Ahnung von Subnetzen hat. Der DHCP-Zustand wechselt hier von INIT nach DISCOVER.

24.19.2.2 - Angebot einer IP-Adresse von den vorhandenen DHCP-Servern

Alle im Netzwerk erreichten DHCP-Server antworten und bieten dem Client eine IP-Adresse an. Dies ist möglich, da aus Redundanzgründen mehrere DHCP-Server installiert sein können. Ein DHCP-Client wartet eine Sekunde auf eine Antwort von einem DHCP-Server. Kommt in diesem Zeitraum keine Antwort, dann ist entweder kein DHCP-Server vorhanden, oder der verfügbare Adress-Bereich ist ausgeschöpft. Es gibt also keine IP-Adressen mehr. Der DHCP-Client versucht es im Abstand von 9, 13 und 16 Sekunden nochmals mit einem Broadcast. Kommt es in dieser Zeit immer noch nicht zu einer IP-Adress-Zuweisung, wird alle 5 Minuten ein weiterer Versuch unternommen. Der DHCP-Zustand ist hier OFFER

24.19.2.3 - Auswahl der IP-Adresse

Das erste Angebot wird vom Client angenommen. Er sendet allen Servern mit einem Broadcast eine Antwort, dass er diesen ersten angebotenen Lease anfordert. Evtl. weitere eintreffende Angebote werden nicht bearbeitet, da durch den Broadcast alle weiteren Server aufgefordert wurden, ihre Angebote zu verwerfen. Der DHCP-Zustand ist hier REQUEST

24.19.2.4 - Bestätigung der IP-Adresse

Die nun angeforderte Lease wird im angesprochenen Server vermerkt und an den Client bestätigt. Alle anderen DHCP-Server nehmen daraufhin ihr Angebot zurück. Der DCHP-Zustand ist hier BOUND

24.19.2.5 - Lease-Erneuerung

Damit ist der DHCP-Client in der Lage TCP/IP-Pakete auszutauschen. Mit der Bestätigung des Lease wurde dem Client noch die Leasedauer mitgeteilt. Aus der Leasedauer erzeugt der Client zwei Timer.

$t1 = 0,5 * \text{Leasedauer}$

Nach dieser Zeit muss der Client die Lease erneuern und sendet einen DHCP-Request aus. Damit ist der Client im Zustand RENEWING Empfängt der Client innerhalb einer zeit $\leq t2$ einen DHCP-ACK, dann ist er wieder im Zustand BOUND.

$t2 = 0,875 * \text{Leasedauer}$

Empfängt der Client innerhalb der Zeit $t2$ keine Nachricht vom Server fällt er in den Zustand REBINDING. Dann versucht er über einen DHCP-Request als Broadcast an alle verfügbaren DHCP-Server.

Bekommt der Client eine Antwort fällt er in den Zustand BOUND. Kommt allerdings keine Antwort oder er erhält ein DHCP-NAK, fällt er in den Zustand INIT.

24.19.3 - DHCP-Zustände

Die DHCP-Zustände in der folgenden Abbildung zeigen den Ablauf eines DHCP-Lease.

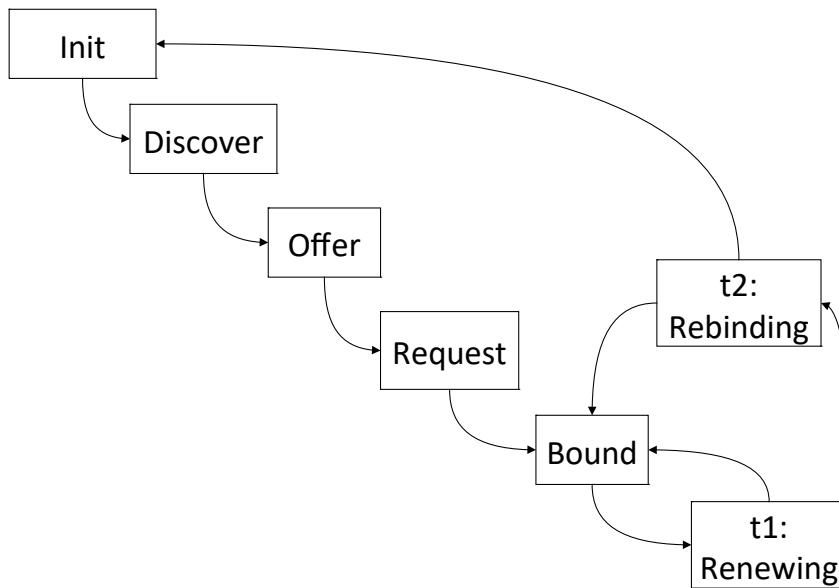


Abbildung 379 : DHCP-Zustände

24.19.4 - DHCP-Nachrichten**24.19.4.1 - DHCP-Discover**

Damit versucht der anfordernde Client den DHCP-Server zu finden und ihn aufzufordern, ein Adress-Angebot zu senden.

24.19.4.2 - DHCP-Offer

Antwort des DHCP-Server auf eine DHCP-Discover-Nachricht.

24.19.4.3 - DHCP-Request

Damit wird die angebotene IP-Adresse akzeptiert und alle anderen Angebote abgelehnt.

24.19.4.4 - DHCP-ACK

Nachricht des DHCP-Servers mit dem gültigen Lease.

24.19.4.5 - DHCP-NAK

Nachricht des DHCP-Servers mit der Ablehnung des angeforderten Lease.

24.19.4.6 - DHCP-Release

Nachricht des DHCP-Client an den DHCP-Server, dass die bisher genutzte IP-Adresse nicht mehr benötigt wird. Damit kann der DHCP-Server die Adresse wieder zur Verfügung stellen.

24.19.5 - Kommandos auf DOS-Ebene

`ipconfig /all` Ausgabe der DHCP-Informationen (IP-Adresse, Leasedauer usw.)

`ipconfig /renew` Anfordern eines DHCP-Lease.

`ipconfig /release` Manuelle Freigabe eines DHCP-Lease

24.19.6 - Paket-Aufbau

op (1)	htype (1)	hlen (1)	hops (1)		
xid (4)					
secs (2)		flags (2)			
ciaddr (4)					
yiaddr (4)					
siaddr (4)					
giaddr (4)					
chaddr (16)					
sname (64)					
file (128)					
options (312)					

Feld	Anzahl der Bytes	Bedeutung
op	1	Message op code / message type. 1 = BOOTREQUEST, 2 = BOOTREPLY
htype	1	Hardware address type, see ARP section in "Assigned Numbers"RFC; e.g., '1' = 10mb ethernet.
hlen	1	Hardware address length (e.g. '6' for 10mb ethernet).
hops	1	Client sets to zero, optionally used by relay-agents when booting via a relay-agent.
xid	4	transaction ID, a random number chosen by the client, used by the client and server to associate messages and responses between a client and a server.
secs	2	Filled in by client, seconds elapsed since client started trying to boot.
flags	2	Flags
ciaddr	4	Client IP address; filled in by client in DHCPREQUEST if verifying previously allocated configuration parameters
yiaddr	4	'your' (client) IP address
siaddr	4	IP address of next server to use in bootstrap; returned in DHCPOFFER, DHCPACK and DHCPNAK by server
giaddr	4	Relay agent IP address, used in booting via a relay-agent
chaddr	16	Client hardware address
sname	64	Optional server host name, null terminated string
file	128	Boot file name, null terminated string; "generic" name or null in DHCPDISCOVER, fully qualified directory-path name in DHCPOFFER
options	312	Optional parameters field. See the options documents for a list of defined options

24.19.7 - APIPA

Ein Rechner der über DHCP keine IP-Adresse empfangen hat, hat trotzdem noch die Möglichkeit über IP zu kommunizieren. Dazu dient das APIPA-Protokoll (Automatic Private IP Addressing)

Ab Windows 98 gibt sich ein Rechner der über DHCP keine Adresse zugewiesen bekommen hat, selbst eine Adresse. Es wird eine Adresse aus dem B-Klasse-Netzwerk 169.254.0.0 mit einer Subnetzmaske 255.255.0.0 verwendet. Microsoft hat sich diese Netzwerk-Adresse eigens für diesen Zweck reservieren lassen. Einzige Voraussetzung dafür ist dass der Rechner auf DHCP eingestellt ist.

Der Rechner gibt sich selbst eine IP-Adresse aus dem Netzwerk 169.254.0.0. Z. B. die Adresse 169.254.0.1. Da er nicht wissen kann ob die Adresse bereits verwendet wird, muss er dies überprüfen. Dies macht er indem er einen ARP-Request in das angeschlossenen Netzwerk sendet. Bekommt er keine Antwort, kann er davon ausgehen, dass die Adresse noch nicht in Verwendung ist. Damit ist die Adresse für ihn verwendbar. Dieser Mechanismus reicht aus um mehrere Rechner miteinander zu vernetzen ohne dass ein DHCP-Server laufen muss. Allerdings kann nicht in andere Netzwerke kommuniziert werden da das Default-Gateway fehlt.

Der Rechner hat zwar eine Adresse jedoch möchte er trotzdem seine Adresse lieber von einem DHCP-Server verwaltet wissen. Deshalb sendet er in Abständen von 5 Minuten einen DHCP-Request in das Netzwerk. Antwortet dann irgendwann ein DHCP-Server, tauscht er die Adresse des DHCP-Servers gegen seine selbst zusammengestanzte aus.

Um herauszubekommen ob der Rechner einen DHCP-Adresse oder eine APIPA-Adresse hat kann der Befehl ipconfig /all in einer DOS-Box verwendet werden.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Dokumente und Einstellungen\Eberhard Schweyer>ipconfig /all

Windows-IP-Konfiguration

    Hostname . . . . . : eberhard-1100
    Primäres DNS-Suffix . . . . . :
    Knotentyp . . . . . : Unbekannt
    IP-Routing aktiviert . . . . . : Nein
    WINS-Proxy aktiviert . . . . . : Nein
    DNS-Suffixsuchliste . . . . . : Domain

Ethernetadapter LAN-Verbindung:
    Verbindungsspezifisches DNS-Suffix: Domain
    Beschreibung . . . . . : 3Com EtherLink XL 10/100 PCI-TX-NIC
<3C905B-TX>
    Physikalische Adresse . . . . . : 00-50-04-35-EF-4E
    DHCP aktiviert . . . . . : Ja
    Autokonfiguration aktiviert . . . . . : Ja
    IP-Adresse . . . . . : 192.168.1.5
    Subnetzmaske . . . . . : 255.255.255.0
    Standardgateway . . . . . : 192.168.1.254
    DHCP-Server . . . . . : 192.168.1.254
    DNS-Server . . . . . : 192.168.1.254
                                217.237.151.161
                                217.237.151.33
    Lease erhalten . . . . . : Samstag, 23. April 2005 15:00:16
    Lease läuft ab . . . . . : Sonntag, 24. April 2005 03:00:16

C:\Dokumente und Einstellungen\Eberhard Schweyer>_
```

24.20 - ICMP (Internet Control Message Protocol)

Das Internet Protocol (IP) wird benutzt, um Datagramme über eine Host-zu-Host-Verbindung zu übertragen. Diese Verbindung kann auch über mehrere Netzwerke hinweg geschehen. Geräte, welche die Netzwerke verbinden, sind Gateways oder Router. Diese Netzwerks-Verbindungs-Geräte kommunizieren untereinander mit dem Gateway to Gateway Protocol(GGP) zu Steuerungszwecken.

Gelegentlich kann es passieren, dass ein Gateway oder ein Router dem Quell-Host Fehlermeldungen zukommen lassen will. Für diese Zwecke wird das Internet Control Message Protocol (ICMP) benutzt. ICMP ist im RFC792 beschrieben.

ICMP benützt IP, so als sei es selbst in einer höheren Schicht. Jedoch ist es ein integraler Bestandteil von IP und muss in jeder IP-Implementierung enthalten sein! Man kann auch sagen, dass, obwohl ICMP auf der Ebene 3 aufsetzt, es nicht zur Ebene 4 gehört, da es den höher liegenden Schichten keinen Dienst (SAP) zur Verfügung stellt.



IP ist nicht absolut zuverlässig! Es gibt keine Sicherungs- oder Quittungsmechanismen. Deshalb wurde ICMP ins Leben gerufen, um einem Sender eine Rückmeldung zu geben, falls es Probleme mit dem Transport seiner Datagramme gibt. Es dient somit auch nicht dazu, IP zuverlässiger zu machen, sondern nur um auf die Unzulänglichkeiten reagieren zu können. Es gibt somit keine Garantien, dass ein IP-Datagramm oder eine ICMP-Meldung ihr Ziel erreicht! Das Sicherstellen einer zuverlässigen Verbindung zwischen zwei Rechnern ist und bleibt somit den höheren Schichten überlassen (z. B. Mit TCP)

Um zu vermeiden, dass durch ICMP eine unendliche Anzahl von ICMP-Meldungen erzeugt werden kann darf eine ICMP-Meldung keine weitere ICMP-Meldungen erzeugen. Dies bedeutet, dass falls ein IP-Datagramm nicht seinen Zielhost erreichen kann und ein Gateway dies bemerkt, das Gateway eine ICMP-Meldung erzeugen müsste. Passiert dies jedoch bei der Übertragung einer ICMP-Meldung ein Fehler, wird keine weitere ICMP-Meldung erzeugt!

Es werden auch nur Meldungen beim ersten fragmentierten Datagramm erzeugt (offset = 0). Alle weiteren Fragmente dürfen keine ICMP-Meldungen erzeugen.

ICMP-Meldungen benützen den IP-Header. Dort sind sie durch einen Eintrag im Protokoll-Feld = 1 gekennzeichnet. Im Quell-Adress-Feld steht die IP-Adresse des Gerätes, welches die ICMP-Meldung erzeugt hat. Im Ziel-Adress-Feld steht die IP-Adresse des Empfängers der ICMP-Meldung. Im allgemeinen ist das die IP-Adresse des Gerätes, dessen Telegramm ein Problem bereitet hat.

ICMP wird für nützliche Tools wie ping, traceroute (echo request / echo reply) verwendet.

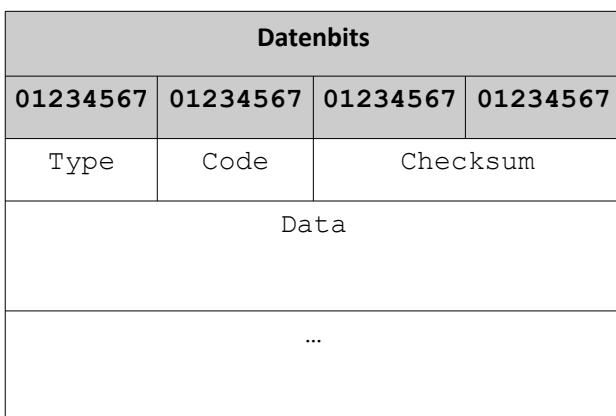
ICMP Meldungen werden in unterschiedlichen Situationen erzeugt. Diese Situationen werden durch den Eintrag im Typ-Feld unterschieden.

ICMP-Meldungen können von Netzwerkanalyse-Geräten gefiltert werden. Dies bedeutet, dass sie sich hervorragend zur Netzwerkanalyse eignen.

ICMP-Meldungen können durch Firewalls oder Router unterdrückt werden. Dies bedeutet, dass evtl. Das Kommando ping nicht über eine Firewall hinweg funktioniert.



24.20.1 - ICMP-Paket-Aufbau



Feld	Beschreibung
Type	Typenfeld, abhängig von der Art der ICMP-Nachricht
Code	Zusatzinformation zur ICMP-Nachricht
Checksum	Prüfsumme des gesamten ICMP-Paketes
Data	Abhängig von der Art des ICMP-Paketes können hier mehrere 32-Bit-Worte übertragen werden

24.20.2 - ICMP-Typen

Typ	Bedeutung
0	Echo reply
3	Destination unreachable
4	Source quench
5	Redirect (route change)
8	Echo Request
11	Time exceeded for datagram
12	Parameterproblem on datagram
13	Time stamp request
14	Time stamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask response

24.20.2.1 - ICMP-Codes (Type 0)

Dient zum Senden der Rückmeldung einer Echo-Anforderung.

Eine Echo-Anforderung dient zum Ermitteln einer Verbindung zwischen zwei IP-Netzteilnehmern. Eine Echo-Anforderung (Type=8) wird an einen Netzteilnehmer gesendet, die dieser mit seiner Rückmeldung (Type=0) beantwortet. Empfängt der Sender der Anforderung die Rückmeldung ist sichergestellt, dass die Verbindung auf IP-Ebene funktioniert.

Code	Data
Not used	Copy of data sent

24.20.2.2 - ICMP-Codes (Type 3 = Destination unreachable)

Ist der Zielhost nicht erreichbar oder die Distanz zum Netzwerk ist unendlich, kann ein Gateway eine ICMP-Meldung mit dem Typ 3 senden.

Ist auf dem Zielhost das IP-Modul nicht in der Lage das Datagramm einer höheren Schicht weiterzugeben, weil z.B. „der Port nicht aktiv“ ist, kann er eine ICMP-Meldung an den Quell-Host senden

Falls ein Datagramm bei einem Gateway oder Router fragmentiert werden muss um weiter transportiert werden zu können, kann es vorkommen, dass das DF-Flag (Don't Fragment) gesetzt ist. In diesem Fall muss das Gateway oder der Router das Datagramm verwerfen. Allerdings kann der Sender des zu langen Datagramms über den Vorfall mit einer ICMP-Meldung darüber informiert werden. So hat er die Möglichkeit entweder kürzere Datagramme zu senden oder das DF-Flag wegzulassen.

Die Codes 0,1,4 und 5 werden von einem Gateway/Router erzeugt. Die Codes 2 und 3 werden vom Zielhost erzeugt.

Code	Data
0 = Net unreachable	Not used
1 = Host unreachable	Not used
2 = Protocol unreachable	Not used
3 = Port unreachable	Not used
4 = Fragmentation needed and df (don't fragment) set	Not used
5 = source route failed	Not used

24.20.2.3 - ICMP-Codes (Type 4 = Source quench)

Tritt der Fall ein, dass ein Gateway, Router oder Switch keinen Speicherplatz mehr hat um zwischen zu speichern oder die Datagramme kommen zu schnell, müssen die Datagramme verworfen werden.

Das Netzwerkgerät, dem so ein Problem widerfährt, hat die Möglichkeit, über eine ICMP-Meldung den Sender des Datagramms zu informieren, dass seine Ressourcen erschöpft sind. Der Sender kann nun die Datenrate, mit der er sendet, so lange zurücknehmen bis keine ICMP-Meldungen mit Typ=4 mehr kommen. Danach kann er schrittweise versuchen die Datenrate wieder zu erhöhen.

Somit kann ein Netzwerkgerät die Datenrate an einem Empfangsport senken.

Es gibt die Möglichkeit, dass ein Gerät, das an seine Ressourcen-Grenze gelangt, dies bereits kurz vorher seinem Netzwerk-Partner mit ICMP-Meldungen mit Typ=4 mitteilt. Somit kann bereits, im Vorfeld, ein Engpass erkannt und vermieden werden. Damit wird versucht die Daten nicht weg zu werfen.

Der Code = 0 wird von einem Gateway oder von einem Host gesendet .

Code	Data
0 (not used)	Header + die ersten 64 Bits

24.20.2.4 - ICMP-Codes (Type 5 = redirect)

Ein Gateway g1 empfängt ein Datagramm von einem Host aus einem Netzwerk, zu dem es gehört. Das Gateway überprüft seine Routing-Tabelle und ermittelt die nächste Gateway-Adresse g2 für das Datagramm. Falls die Adresse von g2 und die Adresse des Quell-Hosts im gleichen Netzwerk liegen, wird an den sendenden Host eine ICMP-Meldung (mit Code=5) gesandt. Denn g2 wäre auch vom Quellhost zu erreichen gewesen und somit hätte g1 nicht mit dem Datagramm belästigt werden müssen. Das Datagramm wird nicht verworfen, sondern an g2 weitergeleitet. Allerdings ist der Weg direkt über g2 kürzer und somit schneller. Bereits Windows NT ist in der Lage, nach einem ICMP-Redirect in Zukunft das richtige Default-Gateway anzuwenden.

Für Datagramme mit der Source-Route-Option und der Gateway-Adresse im Destination-Adress-Feld wird keine ICMP-Meldung erzeugt; auch falls es eine bessere Route gäbe.

Der Code = 0, 1, 2 und 3 wird von einem Gateway gesendet .

Code	Data
0 = network redirect	Not used
1 = host redirect	Not used
2 = type of service network redirect	Not used
3 = type of service host redirect	Not used

24.20.2.5 - ICMP-Codes (Type 8 = Echo request)

Dient zum Senden einer Echo-Anforderung.

Eine Echo-Anforderung dient zum Ermitteln einer Verbindung zwischen zwei IP-Netzteilnehmern. Eine Echo-Anforderung (Type=8) wird an einen Netzteilnehmer gesendet, die dieser mit seiner Rückmeldung (Type=0) beantwortet. Empfängt der Sender der Anforderung die Rückmeldung ist sichergestellt, dass die Verbindung auf IP-Ebene funktioniert.

Da dieses Datagramm von einem Anwender nicht direkt erzeugt werden kann dient das Programm ping als Benutzerschnittstelle.

Code	Data
0 (Not used)	Data to be returned

24.20.2.6 - ICMP-Codes (Type 11 = Time to live exceeded)

Falls ein Gateway/Router erkennt, dass der Wert im TTL-Feld (Time-To-Live) auf 0 reduziert wurde, muss das Datagramm vernichtet werden. Damit der Sender darüber informiert werden kann, sendet das Gateway oder der Router eine ICMP-Meldung an den Quell-Host. Wird z. B. bei traceroute/tracert verwendet.

Falls beim Reassemblieren eines fragmentierten Datagramms etwa Teil-Datagramme innerhalb des Zeitlimits fehlen, wird das Datagramm vernichtet und eine ICMP-Meldung an den Quell-Host gesendet.

Der Code = 0 wird von einem Gateway gesendet . Der Code = 1 wird von einem Host gesendet.

Code	Data
0 = ttl exceeded	
1 = Fragmentation reassembly timeout	

24.20.2.7 - ICMP-Codes (Type 12 = Parameter Problem)

Falls ein Gateway oder ein Host Probleme bei der Bearbeitung des Datagramm-Headers hat, muss er das Datagramm verwerfen. Damit der Sender darüber informiert werden kann, sendet das Gateway, der Router oder der Host eine ICMP-Meldung an den Quell-Host.

Der Code = 0 wird von einem Gateway oder von einem Host gesendet .

Code	Data
0 (not used)	Pointer auf das fehlerhafte Feld

24.20.2.8 - ICMP-Codes (Type 13 = Timestamp-Message (Zeitstempel-Meldung))

Die Quell-IP-Adresse der Timestamp-Meldung ist der Empfänger der Zeitstempel-Antwort-Meldung. Der Zeitstempel ist ein 32-Bit-Wort mit den Millisekunden seit Mitternacht UT. Sollte die Zeit nicht in Millisekunden verfügbar sein, kann eine beliebige Zeit eingetragen werden. Das MSB des Timestamp ist auf 1 gesetzt um anzugeben, dass es sich um einen nicht standardisierten Wert handelt.

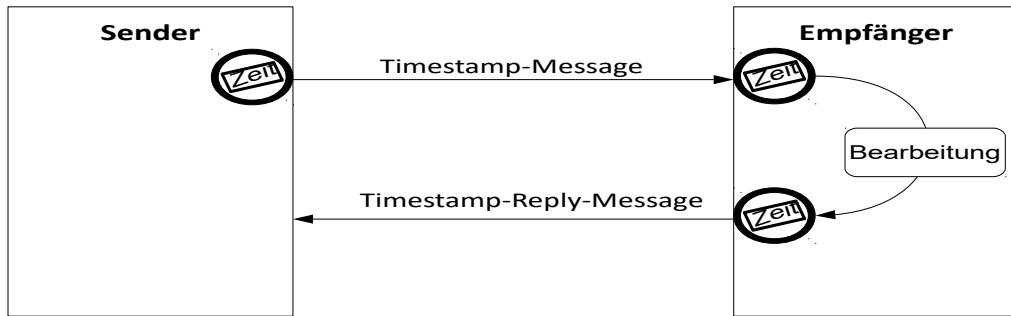


Abbildung 380 : ICMP-Timestamp

Die Zeitstempel haben folgende Bedeutung:

1. Originate Timestamp Zeit des Absendens des Senders
2. Receive Timestamp Zeit des Empfangs beim Empfängers
3. Transmit Timestamp Zeit des Sendens der Rückantwort

Um eine Zeitstempel-Antwort_Meldung zu erzeugen, werden Quell- und Ziel-IP-Adresse ausgetauscht, der Typ von 13 auf 14 korrigiert und die Checksumme neu errechnet.

Der Code ist immer 0. Identifikator und Sequenznummer sind ebenfalls immer 0.

Code	Data
0 (not used)	Originate Timestamp (32 Bit) Receive Timestamp (32 Bit) Transmit Timestamp (32 Bit)

24.20.2.9 - ICMP-Codes (Type 15 = Information-Request-Message)

(deutsch: Informationsabfrage-Meldung)

Diese Meldung wird erzeugt, wenn ein Host die Nummer seines Netzwerkes ermitteln will.

Er sendet dann die Info-Request-Message (deutsch: Informationsabfrage-Meldung). Im IP-Header ist nur die Source-IP-Adresse definiert. Die Destination-IP-Adresse ist 0 (bedeutet dieses Netzwerk). Ein IP-Modul eines anderen Rechners sendet die Antwort (Informationsantwort-Meldung) mit dem voll spezifizierten IP-Header.

24.20.2.10 - ICMP-Codes (Type 16 = Information-Reply-Message)

(deutsch: Informations-Antwort-Meldung)

Eine Informationsantwort-Meldung ist eine Reaktion auf eine Informationsabfrage. Damit wird einem Host mitgeteilt, in welchem Netzwerk er eingebunden ist.

Diese Meldung wird erzeugt, wenn ein Host die Nummer seines Netzwerkes ermitteln will.

Er sendet dann die Info-Request-Message (deutsch: Informationsabfrage-Meldung). Im IP-Header ist nur die Source-IP-Adresse definiert. Die Destination-IP-Adresse ist 0 (bedeutet dieses Netzwerk). Ein IP-Modul eines anderen Rechners sendet die Antwort Informationsantwort-Meldung mit dem voll spezifizierten IP-Header.

24.21 - Namensauflösung

24.21.1 - Einleitung

Die in IP v4 verwendeten Adressbezeichnungen mit einer Länge von 32 Bit, wie z. B. 191.192.193.194, sind nicht besonders benutzerfreundlich. Unter IP v6 verschärft sich das Problem, da 128 Bit für die IP-Adresse verwendet werden können. Anwenderfreundlicher ist es anstelle einer IP-Rechner-Adresse einen sprechenden Namen zu verwenden, bei dem eventuell noch übergeordnete Organisationsnamen wie etwa ein Firmenname oder eine Länderkennzeichnung angegeben werden können.

Anfänglich wurden für eine Namens-IP-Adresszuordnung auf den Rechnern die Datei /etc/hosts auf UNIX-Rechnern verwendet.

Unter Windows heißt diese Datei etwa c:\windows\system32\drivers\etc\hosts zu. Unter UNIX ist dies Information in der Datei /etc/hosts untergebracht.

Da diese Dateien umständlich auf allen Rechnern eines Netzwerks zu pflegen waren wurden zentral verwaltete Lösungen geschaffen.

24.21.2 - Internet Name Service

Die erste Lösung mit einer solchen Eigenschaft heißt Internet Name Service und ist unter der Internet Engineering Note 116 (IEN 116) veröffentlicht. Sie stammt aus dem Jahr 1979. Damit können logische Namen in IP-Adressen umgesetzt werden. Es setzt direkt auf dem UDP-Protokoll auf. Es handelt sich hierbei um eine relativ einfache Applikation. Auf dem lokalen, abfragenden Rechner ist der Name-Server in einem Name-Server-Konfigurations-File zu parametrieren.

Im Name Server File können bis zu drei Name-Server hinterlegt werden. Es gibt einen so genannten Primary Name Server der immer als erster angesprochen wird. Ist der Primary Name Server nicht erreichbar wird die Anfrage an den Secondary Name Server gesendet.

Primary Name Server 192.1.2.1

Secondary Name Server 192.1.2.5

Der Abfragende Rechner sendet einen Name-Request und erhält vom Name-Server einen Name-Reply zurück. Zur Sicherstellung, dass die Antwort auch zur Anfrage passt wird im Reply-Paket der angefragte Name nochmals zusammen mit der ermittelten IP-Adresse übertragen.

24.21.3 - DNS

Die zentrale Hosts-Datei, die früher vom Network Information Center des Defense Data Networks als hosts.txt verteilt wurde, war irgendwann nicht mehr vernünftig wartbar. Als Ersatz wurde eine verteilte Datenbankanwendung entwickelt.

DNS steht für Domain Name Service und wurde 1983 erstmals von Paul Mockapetris in den RFCs 881, 882 und 883 beschrieben. Sie wurden mittlerweile durch die RFCs 1034 und 1035 abgelöst.

Ergänzend können noch die folgenden RFCs dem Thema zugeordnet werden:

- ➊ RFC 920 Domain Requirements
- ➋ RFC 921 Domain Name Implementation Schedule-Revised
- ➌ RFC 973 Domain System Changes and Observations
- ➍ RFC 974 Mail Routing and the Domain System

Es handelt sich um eine dezentrale Verwaltung mit einer Baumstruktur für den Namensraum. Weiterhin kann sichergestellt werden, dass Namen eindeutig sind und die Funktion erweitert werden kann.

Bei der Baumstruktur haben die Blätter (Knoten) werden als Labels bezeichnet. Ein Label darf nur alphanumerische Zeichen und den Bindestrich (-) enthalten. Der Bindestrich darf nicht am Ende stehen. Ein kompletter Domainname besteht aus einer Verkettung aller Labels eines Pfades. Ein Label ist eine Zeichenkette mit mindestens einem Byte und maximal 64 Bytes (RFC 2181). Die Labels werden mit Punkten innerhalb eines Domänenamens miteinander verbunden/getrennt.

Das DNS nutzt UDP als Transportschicht und verwendet dort den Port 53. TCP ist ebenfalls möglich und wird auf jeden Fall für die Zonentransfers (Verteilung der Informationsdateien zwischen den DNS-Servern) genutzt.

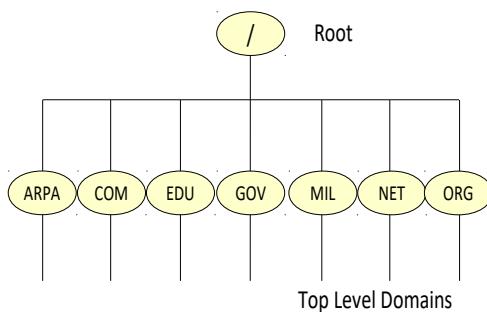
Der Service lässt sich in beiden Richtungen betreiben:

- ➊ Für einen Rechnernamen die zugehörige IP Adresse ermitteln (lookup)
- ➋ Für eine IP-Adresse den zugehörigen Namen ermitteln (reverse lookup)

Das DNS besteht aus den drei Hauptkomponenten:

- ➊ Domain-Namensraum
- ➋ Nameserver
- ➌ Resolver

24.21.3.1 - Domain Namensraum



Der Domain-Namensraum hat eine baumförmige hierarchischen Aufbau.

Von der Root ausgehend entwickelt sich der Baum.

Bei der Baumstruktur werden die Blätter (Knoten) als Labels bezeichnet.

Ein Label darf nur alphanumerische Zeichen und den Bindestrich (-) enthalten. Der Bindestrich darf nicht am Ende stehen.

Ein kompletter Domainname besteht aus einer Verkettung aller Labels eines Pfades.

Abbildung 381 : Generische Top-Level-Domains (gTLDs)

Ein Label ist eine Zeichenkette mit mindestens einem Byte und maximal 64 Bytes (RFC 2181). Die Labels werden mit Punkten innerhalb eines Domännamens miteinander verbunden/getrennt.

Jede Verzweigung entspricht einer Zone.

Die erste / oberste Ebene wird als Top-Level-Domains (TLD) bezeichnet. TLDs wurden vom Network Information Center (NIC) definiert.

Ein kompletter Domännamen (FQDN = Fully Qualified Domain Name) wird mit einem Punkt abgeschlossen und darf inklusive aller Punkte 255 Byte lang sein. Je weiter ein Label im Domännamen rechts steht, desto höher steht es im Baum.

Für die USA bestehen derzeit die oben beschriebenen Domains. In der Reihe fehlen nur noch die Country-Codes, (ccTLD).

Beispiele für Country-Codes:

- ➊ .de Deutschland
- ➋ .au Österreich
- ➌ .li Lichtenstein
- ➍ .lu Luxemburg

Ein Domain-Name wird immer von links nach rechts delegiert und aufgelöst. Dies bedeutet, dass das Label welches am weitesten rechts steht, im Baum am höchsten steht.

Ein vollständiger Domain-Name wird auch Fully Qualified Domain Name (FQDN) genannt. Beispiel: www.siemens.com.

Der letzte Punkt gehört zum DNS-Namen, kann jedoch weg gelassen werden.

Die DNS-Objekte werden als Satz von Resource-Records in einer sogenannten Zonendatei (auch Zone genannt) gehalten und auf den autoritativen DNS-Servern über Zonentransfers abgeglichen.

24.21.3.2 - Nameserver

Ein Nameserver ist ein Programm und für die Auflösung der Namensanfragen innerhalb einer Zone zuständig. Allerdings wird der Rechner, auf dem das Nameserver-Programm läuft, auch Nameserver genannt. Er kennt immer nur den Server der Zone über und unter ihm. Der Beginn einer Domain-Zone befindet sich immer in einem Knotenpunkt im Domain-Baum und umfasst die daran anschließenden Zweige.

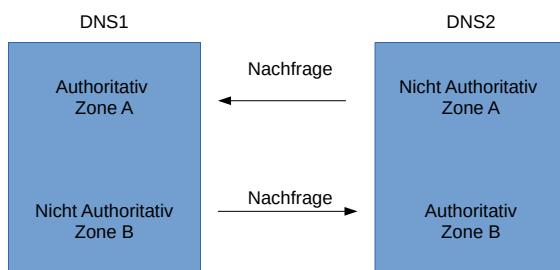
Die DNS-Objekte einer Domäne, z. B. Die Rechnernamen, werden als Satz von Resource Records meist einer Zonendatei auf dem Name-Server gehalten.

Es gibt autoritative und nicht autoritative Server.

Autoritative Server sind für eine Zone zuständig. Ihre Informationen über die Zone werden als gesichert angesehen. Für jede Zone gibt es mindestens einen, den Primary Nameserver. Er wird im SOA-Resource-Record (Start of Authority) einer Zonendatei aufgeführt. Aus Last- und Redundanzgründen wird ein Nameserver meistens als Cluster realisiert. Die Zonendatei ist identisch mit denen auf weiteren Rechnern (Secondary Nameserver). Die Synchronisation zwischen Primary Nameserver und den Secondary Nameservern erfolgt per Zonentransfer.

Der SOA-Resource-Record (spezifiziert im RFC 1035) ist der wichtigste Bestandteil einer Zonendatei, er enthält Angaben zur Verwaltung der Zonendatei und zum Zonentransfer.

Nicht autoritative Server sind Server, die Ihre Informationen von einem weiteren Server beziehen. Die Informationen werden damit als nicht gesichert angesehen. Die Daten werden in einem Cache gehalten werden. Um nicht Daten von mittlerweile ungültigen Namen-IP-Adress-Beziehungen zu propagieren haben die Einträge einen Time To Live (TTL)-Wert. Dieses Verfallsdatum wird vom autoritativen Server vergeben. Es ist abhängig von der Häufigkeit mit der die Zuordnungen geändert werden. Dies kann bedeuten, dass Cache-Einträge für längere Zeit falsche Informationen beinhalten können!



Nameserver können also autoritativ und nicht autoritativ sein. Zwei Nameserver können diese Eigenschaft auch über Kreuz abhandeln.

Die Aufrufe der Nameserver können über zwei unterschiedliche Auflösungsarten vorgenommen werden.

Bei der iterativen Vorgehensweise gibt ein DNS-Server die IP-Adresse des nächsten Servers an den Resolver zurück falls er keine Auflösung vornehmen kann. Dann muss der Resolver selbst den nächsten Server abfragen.

Bei der rekursiven Vorgehensweise fragt der DNS-Server, der keine Auflösung vornehmen kann, selbst beim nächsten DNS-Server nach.

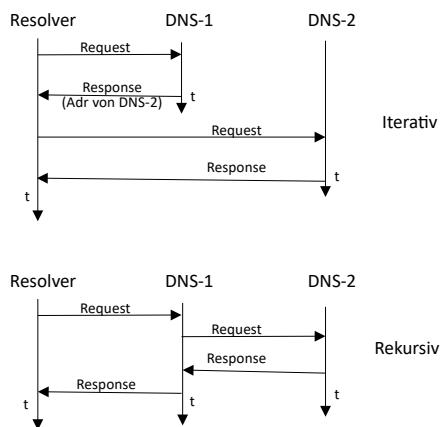


Abbildung 382: DNS-Auflösung: Iterativ vs.
Rekursiv

Protokolle

Ein Spezialfall ist ein Caching Only Nameserver. Er ist für keine Zone verantwortlich und muss alle eintreffenden Anfragen über weitere Forwarder (Nameserver) abhandeln. Dazu gibt es zwei Strategien:

1. Delegierung

Teile des Domain-Namensraumes können an Subdomains mit eigenem Nameserver ausgelagert werden. In der Zonendatei sind die Subdomain-Nameserver hinterlegt. Ein Nameserver wird die eintreffende Anfrage für die Subdomain an die entsprechenden Nameserver weiter leiten.

2. Weiterleitung

Falls der angefragte Namensraum außerhalb der eigenen Domäne liegt wird an einen fest konfigurierten Nameserver weiter geleitet.

Auflösung über Root-Nameserver

Falls ein Nameserver der über Weiterleitung angesprochen wurde nicht existiert / nicht antwortet wird der Root-Nameserver angefragt.

Root-Nameserver beantworten aus Performancegründen nur iterative Anfragen.

Root-Nameserver sind in einer statischen Datei mit Namen (A bis M) und ihrer IP-Adresse hinterlegt.

24.21.3.3 - Resolver

Programm auf einem Client der die Anfrage von der Applikation entgegen nimmt und falls im Cache kein Eintrag vorliegt eine Anfrage an den Domain-Name-Server sendet. Dies kann rekursiv oder iterativ stattfinden.

Ablauf einer rekursiven Namensaüflösung

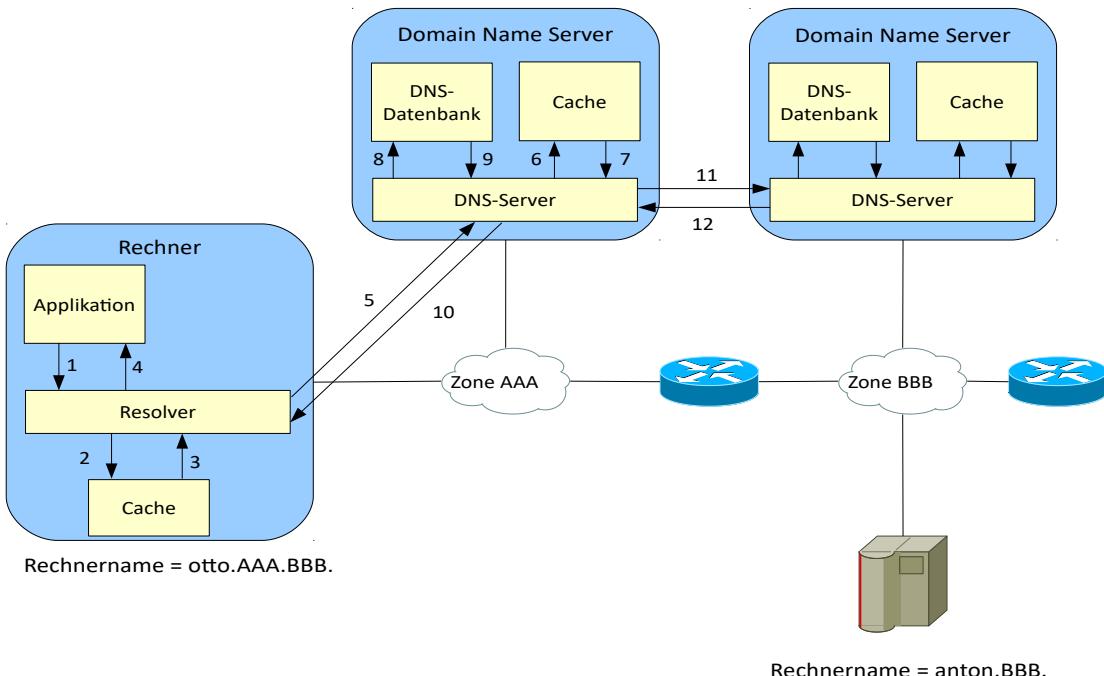


Abbildung 383 : DNS-Namensaüflösung

Will eine Applikation mit einem Server Kommunizieren und kennt nur dessen DNS-Namen, muss dieser zuerst die IP-Adresse des Servers ermittelt werden.

1. Zuerst stellt die Applikation die Anfrage an den rechnerinternen Resolver.
2. Der sucht in seinem Cache ob der Name bereits bei einem früheren Datenaustausch ermittelt wurde.
3. Ist dies der Fall kann der Name direkt aufgelöst werden.
4. Der Resolver kann den Namen direkt auflösen.
5. Findet der Resolver jedoch in seinem Cache keine Eintrag wendet er sich an den DNS-Name Server.
6. +7. Der DNS Name Server sucht zuerst in seinem Cache. Wird er fündig sendet er die Antwort an den Resolver zurück 10.
8. Ist im DNS Server-Cache kein Eintrag wird in der DNS Datenbank gesucht.
9. Wird der Server fündig wird die Antwort an den Resolver zurückgegeben.
11. +12. Wird der Server nicht fündig fragt der Server bei einem weiteren DNS-Server nach.

Beispiel:

Der Rechner otto.aaa.bbb. benötigt die IP-Adresse des Rechner anton.bbb.

Falls noch nie eine Kommunikation der beiden untereinander stattfand ergibt sich der folgende Ablauf:

1. -> 2. -> 5. -> 6. -> 8. -> 11. -> 12. -> 10. -> 4.

falls der Rechner anton.bbb. bei seinem DNS-Name-Server bekannt war.

24.21.3.4 - Resource Records

Die von den DNS-Servern verwalteten Informationen sind in den so genannten Resource Records (RR) hinterlegt. Die RR werden als ASCII-Datei in den Zonendateien oder in den DNS-Transport-Paketen in komprimierter Form verarbeitet.

24.21.3.4.1 - Resource Records Format

Im ASCII-Format haben die RRs den folgenden Aufbau

ASCII-Format: <name> [<ttl>] [<class>] <type> <rdata>

- <**name**> Der Domänenname des Objekts, zu dem der Resource Record gehört (optional)
- <**ttl**> *time to live* (in Sekunden). Gültigkeit des Resource Records (optional)
- <**class**> Protokollgruppe, zu der der Resource Record gehört (optional)
- <**type**> beschreibt den Typ des Resource Records
- <**rdata**> (resource data) Daten, die den Resource Record näher beschreiben (zum Beispiel eine IP-Adresse für einen A-RR, oder einen Hostnamen für einen NS-RR)
- <**length**> Länge der folgenden Daten

Als Class wird heutzutage nur noch IN, für Internet verwendet. Alle anderen Einträge sind historisch.

24.21.3.4.2 - Resource Records Typen

Die wichtigsten RR-Typen sind folgende

Typ	Bedeutung
A	IPv4-Adresse eines Hosts
AAAA	IPv6-Adresse eines Hosts
AFSDB	Resource Record für Cell Database Server des Andrew File Systems
A6	Resource Record des Verfahrens A6 zur teilweisen Adressauflösung unter IPv6, inzwischen veraltet
CERT	Resource Record für das Speichern von Zertifikaten (siehe RFC 4398)
CNAME	Kanonischer Name für einen Host (die Domain mit diesem RR ist ein Alias)
DNAME	ähnlich CNAME, aber für komplette Domains, siehe RFC 2672
DNSKEY	enthält einen dem Namen zugeordneten Public-Key – löste bei DNSSEC ab 2004 den Typ KEY ab.
DS	dient der Verkettung DNSSEC-signierter Zonen
GPOS	Geographische Position, veraltet
HINFO	Host-Information (Prozessortyp und Betriebssystem)
ISDN	ISDN-Nummer, wird nur selten verwendet
LOC	Lokation
KEY	enthält einen dem Namen zugeordneten Public-Key – wird von DNSSEC seit 2004 nicht mehr verwendet
MB	Mailbox domain name (<i>Experimentell</i>)
MD	Mail destination (nicht mehr in Gebrauch – heutzutage wird MX verwendet)
MF	Mail forwarder (nicht mehr in Gebrauch – heutzutage wird MX verwendet)
MG	Mail group member (<i>Experimentell</i>)
MINFO	Mailbox oder <i>mail list information</i>
MR	Mail rename domain name (<i>Experimentell</i>)
MX	Mail Exchange – der für diese Domain zuständige Mailserver
NAPTR	Naming Authority Pointer – Erweiterung des A Resource Record
NSAP	Network Service Access Point
NSEC	(next secure) verkettet DNS-Einträge in DNSSEC signierten Zonen – löste 2004 den Typ NXT ab
NSEC3	(next secure hashed) Alternative zum NSEC RR ohne Zone Enumeration Problem (seit 2008)
NULL	Null Resource Record (<i>Experimentell</i>)
NS	Hostname eines autoritativen Nameservers. Verknüpfungen (Delegationen) der Server untereinander
NXT	veraltet – wurde durch den praktisch identischen NSEC-Resource-Record abgelöst

OPT	Pseudo-RR, markiert ein EDNS-Paket
PTR	Domain Name Pointer (für das Reverse Mapping, um IP-Adressen Namen zuzuweisen)
RP	Verantwortliche (responsible) Person
RRSIG	enthält eine digitale Unterschrift (wird seit 2004 von DNSSEC (=DNS Security) verwendet und ersetzt SIG)
SIG	enthält eine digitale Unterschrift (veraltet, wurde bis 2004 von DNSSEC (=DNS Security) verwendet)
SOA	Start of Authority
SPF	Sender Policy Framework
SRV	angebotener Dienst (Service)
SSHFP	SSH Fingerprint, zum Veröffentlichen der Fingerprints von SSH-Schlüsseln, siehe RFC 4255
TXT	freidefinierbarer Text, wird u. a. auch für Sender Policy Framework (SPF) verwendet. Wird auch oft genutzt für Google-Site Verification
WKS	Well known service description
X25	X.25-Adresse, wird nur selten verwendet
	Quelle: Wikipedia

Protokolle

Der SOA-Resource-Record ist ein wichtiger Bestandteil einer Zonendatei. Er enthält Angaben zur Verwaltung der Zone und zum Zonentransfer. Er ist spezifiziert im RFC1035.

Typ	Bedeutung
Name	Zonen-Name
IN	Zonenklasse Internet
Primary	Zonenmaster. Bestimmt an wen dynamische Updates gesendet werden.
Mail-Address	Mailadresse des Administrators. Datei wird das @-Zeichen durch „.“ ersetztPunkte vor dem @-Zeichen werden durch „\.“ ersetzt. Damit wird aus otto.huber@abc.com otto\huber.abc.com
Seriennummer	Wird bei jeder Änderung inkrementiert. Hat vorzugsweise das Format JJJJMMTTVV und ist ein Hinweis auf die letzte Änderungen
Refresh	Sekundenabstand in dem sekundäre Nameserver beim primären Nameserver die Seriennummer abfragen um Änderungen zu erkennen. RIPE-NCC-Empfehlung 86400 = 24 Stunden
Retry	Nach ausbleibender Antwort soll nach x Sekunden beim Primary Nameserver nachgefragt werden. Muss < als Refresh sein. RIPE-NCC-Empfehlung 7200 = 2 Stunden
Expire	Nach dieser Zeit in Sekunden soll bei ausbleibender Antwort vom Primary Nameserver nicht mehr auf Zonenabfragen geantwortet werden. Muss größer sein als Σ von Refresh + Retry
TTL	Time to Live für negatives Caching. RIPE-NCC-Empfehlung 172800 = 2 Tage

DNS arbeitet mit einem Informationsblock der in 5 Bereiche eingeteilt ist:

1. Kopf
2. Anfrageteil
3. Antwort
4. Name-Server-Information
5. Sonstige Information

Felder des DNS-Protokollkopfes

0		15
ID		
QR	OPCODE	AA TC RD RA Z RCODE
QDCOUNT		
ANCOUNT		
NSCOUNT		
ARCOUNT		

Feld	Länge	Bedeutung
ID	2 Byte	Dient zur Identifizierung des Infoblocks. Wird vom anfragenden Programm erzeugt und vom Nameserver in die Antwort kopiert
QR	1 Bit	0 = Anfrage / 1 = Antwort
OPCODE	4 Bit	Spezifizierung des Anfragetyps
AA	1 Bit	Authoritative Answer. 1 = Nameserver ist Primary Server der Zone
TC	1 Bit	Truncation Gibt an dass das Protokollelement nicht vollständig übertragen wurde
RD	1 Bit	Recursion desired 1 = Nameserver soll rekursiv arbeiten
RA	1 Bit	Recursion available 1 = Nameserver kann rekursiv arbeiten
Z	3 Bit	Feld für zukünftige Verwendung
RCODE	4 Bit	Response-Code (Fehlerinformation)
QDCOUNT	2 Byte	Gibt die Anzahl der Einträge in der Infoblock Anfrage an
ANCOUNT	2 Byte	Anzahl der Resource Records im Infoblock Antwort
NSCOUNT	2 Byte	Anzahl der Resource Records im Infoblock Name-Server-Information
ARCOUNT	2 Byte	Anzahl der Resource Records im Infoblock Sonstige

24.21.4 - Dynamisches DNS (DDNS)

Bei DDNS gibt es die Möglichkeit die Einträge des Name Servers dynamisch zu ändern oder zu ergänzen. Bei einer Serveranbindung über xDSL ergibt sich durch die dynamischen IP-Adresszuweisungen das Problem, dass alte DNS-Einträge auf dem Name Server ins Leere zeigen und bei der Namensauflösung die falschen Adressen zurück liefern.

Abhilfe kann hier dynamisches DNS bieten.

Im Internet stehen hierzu verschiedene Provider zur Verfügung die für private Anwendungen kostenlos und für kommerzielle Anwendungen günstige Angebote bieten. Hier bieten DynDNS oder ähnliche Provider ihre Dienste an.

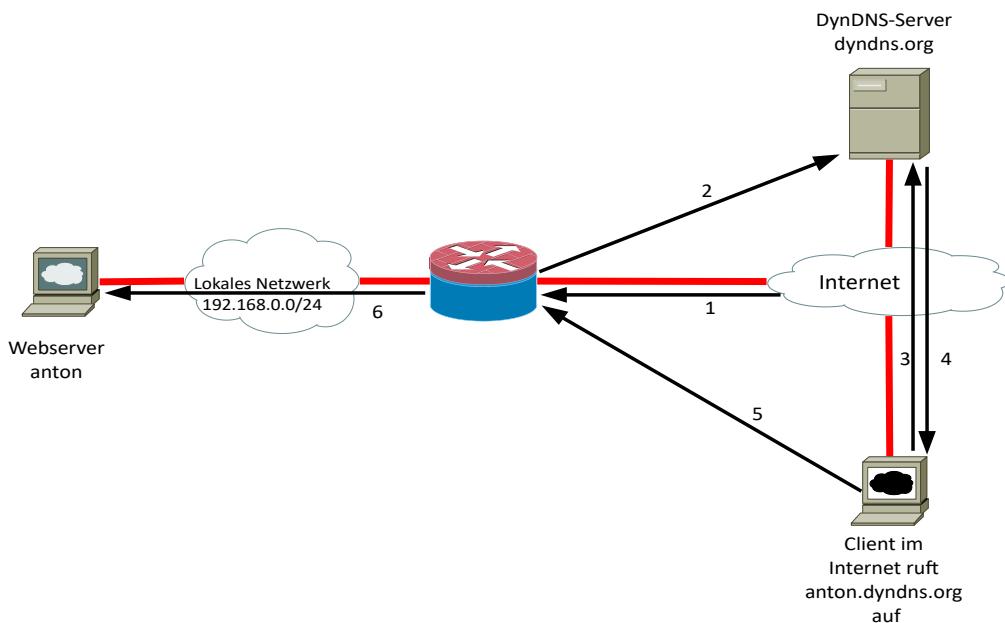


Abbildung 384 : DDNS

1. Der Provider teilt dem Router seine im Internet gültige IP-Adresse mit.
 2. Der Router teilt seine neue IP-Adresse dem DynDNS-Server mit.
 3. Ein Client will auf anton.dyndns.org zugreifen. Für die Namensauflösung wendet er sich an den DynDNS.
 4. Der DynDNS-Server teilt die aktuelle IP-Adresse dem Client mit.
 5. Nun kann der Client auf den Server über den Router mit Firewall zugreifen. (6.)
- Wird dem Router eine neue IP-Adresse mitgeteilt, meldet er diese wiederum an den DynDNS-Server.

DDNS wird im RFC 2136 und 2137 beschrieben. DDNS gibt es in einer ungesicherten und in einer durch Authentifikation gesicherten Version.

24.22 - IP-Version 6 (IPv6)

24.22.1 - Historisches

Bisher war die weitestgehend genutzte IP-Version, die Version 4, die 1981 veröffentlicht wurde. Hier besteht eine IP-Adresse aus 4 Bytes (= 32 Bits). Damit stehen $2^{32} = 4.294.967.296$ IPv4-Adressen zur Verfügung.

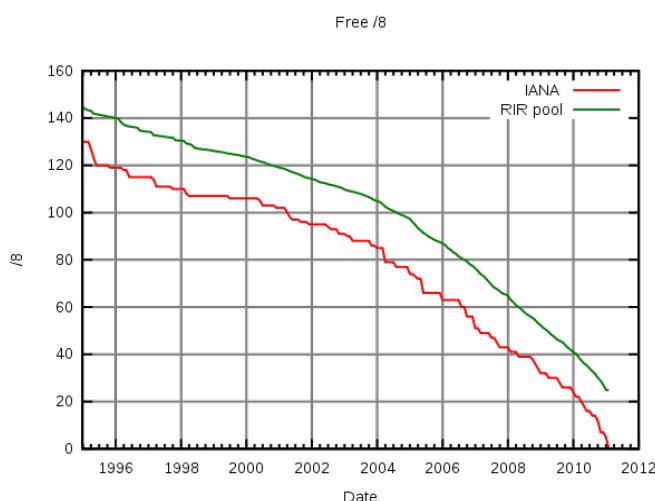


Abbildung 385 : Letzte IPv4-Adressen

Die rasante Entwicklung des Internets ließ bereits Anfang der 1990er Jahre, die Verantwortlichen, auf die schnell schwindende Anzahl freier IP-Adressen, aufmerksam machen.

Bereits 1994 wurde von der IETF (Internet Engineering Task Force) mit der Arbeit an IPv6 begonnen. Die Version 5 war bereits für das flow-orientierte Internet Stream Protocol Version 2 (ST2, RFC 1819) verwendet worden. Mittlerweile ist die Standardisierung von IPnG (IP next Generation), wie IPv6 manchmal auch genannt wird, abgeschlossen. Japan, China Australien und die USA führen derzeit IPnG großflächig ein. Google und eBay bieten bereits Dienste an, die nur auf IPv6 laufen. Der Druck, der von der Erschöpfung der IPv4-Adressen ausgeht, wurde durch CIDR (Classless Inter Domain Routing) und NAT (Network Address Translation) gemildert.

Allerdings hat der Boom mobiler Endgeräte und das Internet der Dinge mit festen IP-Adressen das bisherige IPv4 umrüstungsreif gemacht. Durch Stromzähler, die im Zuge von Smart Grids mit einer IP-Adresse ausgestattet werden, gehen die IPv4-Adressen aus. Wie aus der Presse entnehmbar war, ist das letzte IPv4-Adressband am 3. Februar 2011 von der IANA an die RIR's (Regional Internet Registries), also den regionalen Verteilerorganisationen, wie z. B. RIPE verteilt worden.

Damit endet die Nutzbarkeit des Internets nicht schlagartig, sondern es können einfach keine neuen Nutzer mehr mit festen IP-Adressen ausgestattet werden.

Die Adressen-Knappheit war einer der ersten Anstöße für die Entwicklung einer IP-Version, die einen Adressraum von $2^{128} = 340.282.366.920.948.463.374.607.431.768.211.456$ IPv6-Adressen also rund 340 Sextillionen Adressen zur Verfügung stellt, mit dem sich annähernd jedes Sandkorn auf der Erde adressieren lässt. Bei einem angenommenen Erdradius von 6373km können pro Quadratmillimeter Erdoberfläche ca. 667 Billiarden IPv6-Adressen bereitgestellt werden. Bei IPv4 waren es gerade mal 8,4 Adressen pro Quadratkilometer.

IPv6 wurde unter dem RFC 1550 und 2460 entwickelt und 1995 als RFC 1752 veröffentlicht. 1997 wurden die RFCs 1883, 1884, 1885, 1886 und 1933 mit Details veröffentlicht. 1998 wurden die RFCs nochmals überarbeitet. Dabei wurde der Header geändert. Als Grundlage dient heute der RFC 2460.

Seit 2009 gibt es beim RIPE NCC unter dem Link <http://www.ripe.net/ripe/docs/ripe-373.html> die Möglichkeit Provider-unabhängige IPv6-Adressblöcke (IPv6 End User Site Assignment Request Form) zu beantragen.

Seit Ende Februar 2022 beträgt der Anteil der genutzten IPv6-Adressen in Deutschland mehr als 52%. Damit hat IPv6 IPv4 als das meistgenutzte IP-Protokoll abgelöst.

Außer der Lösung der Adressenverknappung gibt es weitere Vorteile, die durch den Einsatz von IPv6 zum Tragen kommen:

- Wegfall von NAT und allen in diesem Zusammenhang stehende Probleme
- Effizientere Ausnutzung von Netzwerkressourcen durch kürzere Paketbearbeitungszeiten und verbesserte Fragmentierungsregeln.
- Durch den bereits implementierten Einsatz von IPsec wird die Sicherheit verbessert.
- Erweiterung der Always-On-Funktionalität erhöht für mobile Enduser die Erreichbarkeit
- Durch die Einführung von Flow-Labels wird QoS (Quality of Service) ermöglicht, was den Einsatz von Multimedia-Anwendungen wie z.B. interaktives internetbasiertes Fernsehen.
- Autokonfiguration von Endgeräten
- Flexible Sensornetzwerke für z. B. Krisensituationen oder Gebäudemanagement
- Internet der Dinge (Z. B. Vehicle-to-X)

24.22.2 - Neue Terminologie

Das **Internet4** ist der über IPv4 erreichbare Teil des Internets und das **Internet6** ist der über IPv6 erreichbare Teil.

Ein **Node** ist ein Gerät, das über ein oder mehrere Interfaces, an einem oder mehreren Netzwerken angeschlossen ist.

Ein **Router** ist ein spezieller Node. Er besitzt Routing-Eigenschaften und kann damit den Netzwerk-Verkehr über Netzwerk-Grenzen hinweg ermöglichen.

Ein **Host** ist ein Node ohne Routing-Eigenschaften.

Ein **Interface**, oder auch **Link**, ist die Verbindung zum Netzwerk. Alle weiteren an diesen Link angeschlossenen Nodes sind **on-link** und damit **Nachbarn (Neighbours)**. Nodes, die nicht direkt erreicht werden können (etwa nur über eine Router), sind **off-link**.

24.22.3 - Header-Aufbau

24.22.3.1 - Allgemeines

Ein IP-Paket besteht aus einem Header-Teil und einem Nutzlast-Teil, der so genannten Payload. Der IPv6-Header hat einen anderen Aufbau als sein Version-4-Vorgänger. Bei der neuen Version wurden die Fehler der Vorgängerversionen vermieden. So gibt es z. B. keine Prüfsumme mehr, da diese in der unterlagerten Schicht bereits angewendet wird und dies somit eine redundante Bearbeitung verursacht. Es gibt auch keine optionale Header-Erweiterung mehr. Die Header-Größe beträgt 40 Bytes und kann nur durch so genannte Extensions erweitert werden. Dies ermöglicht eine schnellere Bearbeitung in Routern. Neue Optionen wurden in den Header-Aufbau übernommen, um eine flexiblere Bearbeitung zu erreichen. (z. B. Flow-Labeling und Priorität)

Version (4Bit)	Traffic Class (8Bit)	Flow-Label (20Bit)		
Payload (16Bit)		Next Header (8Bit)	Hop Limit (8Bit)	
Source Address (128Bit)				
Destination Address (128Bit)				
Data				

Name	Länge in Bit	Bedeutung
Version	4	Versionskennung. Hat immer den Wert 6
Traffic Class	8	Die Traffic Class entspricht dem TOS (Type of Service unter IP-V4). Werte von 0 bis 7 werden für den lastgesteuerten Datenverkehr verwendet. Werte von 8 bis 15 sollen für Echtzeit Datenverkehr verwendet werden
Flow Label	20	Dient zur Kennzeichnung eines „Flows“
Payload Length	16	Gibt die Datenmenge in Bytes an, die den Header folgen. Hier ist eine Datenmenge bis 64 kByte möglich. Die Jumbo Payload-Option erlaubt Datagramme bis 4 GByte
Next Header	8	Hier wird die nächsthöhere Protokollsicht angegeben.
Hop Limit	8	Der Inhalt dieses Feldes wird bei jeder Übertragung durch Router um 1 decrementiert. Wird der Wert 0 erreicht, dann wird das Paket verworfen.
Source-Adresse	128	Quell-Adresse. Der Adress-Aufbau folgt.
Destination-Adresse	128	Ziel-Adresse. Der Adress-Aufbau folgt.
Data		Zu übertragene Daten die dem Header folgen

24.22.3.2 - Unterschiede zum IPv4-Header

Im Vergleich zu IPv4 fehlen einige Felder:

Fragmentation/Reassembly

Eine Fragmentierung gibt es bei IPv6 nicht. Zu große Pakete werden von den Routern verworfen und müssen deshalb bereits beim Sender richtig dimensioniert werden. Dazu sendet der Router ein ICMPv6-Paket an den Absender und teilt ihm mit, dass die Paketgröße kleiner zu wählen ist. Die minimale MTU-Size wird von 576 Bytes bei IPv4 auf 1280 bei IPv6 angehoben.

Die Ermittlung der maximal möglichen MTU-Size, also der MTU-Size entlang des gesamten Weges vom Sender zum Ziel, dem so genannten MTU-Path, gewinnt hiermit an Bedeutung.

Checksumme

In der unterlagerten Schicht wurde bereits eine Checksumme bearbeitet. Dies wäre eine redundante Bearbeitung. Die Checksummen-Bearbeitung müsste jedes mal, wenn der Next-Hop-Wert decrementeert wird, ebenfalls durchlaufen werden. Dies reduziert die Latenzen (Durchlaufzeit vom Empfang bis zum weiter senden) in den Routern.

Optionen

Optionen werden durch einen Extension-Header möglich der im Next Header Feld eingetragen wird.

Name	Typ	Größe	Beschreibung	RFCs
Hop-By-Hop Option	0	variabel	Enthält Optionen, die von allen IPv6-Geräten, die das Paket durchläuft beachtet werden müssen. Wird für Jumbograms verwendet.	2460 2675
Routing	43	variabel	Durch diesen Header kann der Weg des Paketes durch das Netz beeinflusst werden. Anwendungsfall Mobile IPv6.	2460 3775 5095
Fragment	44	64 Bit	Parameter für eine Fragmentierung	2460
Authentication Header (AH)	51	variabel	Enthält Daten zur Sicherstellung der Vertraulichkeit des Paketes	4302
Encapsulation Security Payload (ESP)	50	variabel	Dient zur Verschlüsselung des Paketes	4302
Destination Options	60	variabel	Enthält Optionen die vom Zielrechner des Paketes beachtet werden müssen.	2460
No Next Header	59	leer	Platzhalter für den letzten Extension-Header	2460

24.22.4 - IPv6-Adressen

24.22.4.1 - Scope

Im Unterschied zu IPv4 haben IPv6-Nodes mehrere IP-Adressen. Das sind sowohl Unicast als auch Multicast-Adressen.

Jede dieser Adressen hat einen Scope, um zu beschreiben, in welchen Teilnetzen oder Netzbereichen die Adresse ihren Gültigkeitsbereich und damit auch ihre Reichweite hat. Der Scope kann die folgenden Bereiche festlegen:

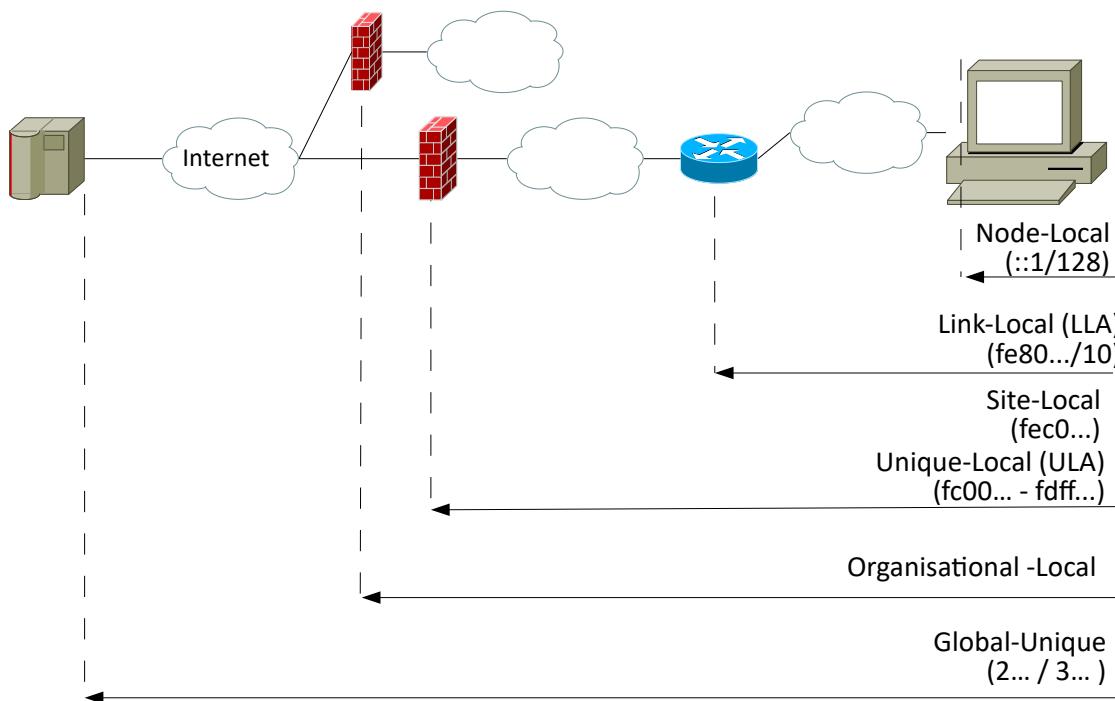


Abbildung 386 : Scope

Node Local Scope

Diese Adressen gelten nur innerhalb des Nodes. (::1/128) Sie entspricht der Localhost-Adresse bei IPv4 (127.0.0.1)

Link Local Scope

Diese Link Local Adressen (LLAs) sind nicht routebar und haben nur am Netzwerk-Link eine Bedeutung. Sie haben nur innerhalb des Subnetzwerks Gültigkeit, denn sie werden vom Gerät selbst ohne einen weiteren Instanz vergeben. Sie entsprechen somit den APIPA (Zeroconf) Adressen (169.254.x.x) unter IPv4 und haben den Präfix: fe80::/10. Um die Adresse im Gültigkeitsbereich eindeutig zu machen reicht es aus, wenn als weiteren Bestandteil der Adresse, die MAC-Adresse verwendet wird. Unter IPv4 wurden sie nur genutzt wenn keine DHCP-Adresse verfügbar war. Unter IPv6 wird die Adresse z. B. genutzt, um sich beim Router eine global gültige IPv6-Adresse zu beschaffen. Siehe hierzu auch Neighbour Discovery Protocol (NDP) und die Stateless Address Auto Configuration (SLAAC).

➊ Site Local Scope

Diese Adressen sind routebar, allerdings nur bis zum Border-Router der Site. Damit entsprechen sie den RFC1918-Adressen von IPv4. Ursprünglich war für diese Adressen der Präfix: fec0::/10 vorgesehen. Die Site bezeichnet ein großes Netzwerk, das über den Link-Local-Scope hinausgeht. An einem Standort (Site) kann es ja schließlich mehrere Netzwerke geben. Allerdings ist der Site-Local-Scope nicht genau definiert. Deshalb sollten sie nicht mehr zum Einsatz kommen (siehe RFC3879). Ihren Platz nehmen die Unique Local Adressen (ULAs) ein.

➋ Unique Local Scope (ULA, RFC 4193)

Diese Adressen sind zwar routebar, werden im Internet nicht geroutet und haben den Präfix: fc00... /7 bis fdff... /7.

Sie entsprechen wie die Site-Local-Adressen den RFC-Adressen bei IPv4. Damit hat man die gleichen Probleme wie unter IPv4, denn es muss um die Adressen weltweit nutzen zu können, ein Network Address Translation (NAT) (in diesem Fall sogar ein NAT66) gemacht werden.

Es gibt die Empfehlung ULA-Netzwerke gar nicht erst zu verwenden, denn jeder Administrator kann sie nach eigenen Vorstellungen verwenden. Deshalb müssen, um Kollisionen zwischen den ULA-Netzen zu vermeiden, die ULAs unterschieden werden können. In den ULAs ist eine 40 Bit lange Global ID enthalten. Diese sollte per Algorithmus gesetzt sein.

Bei der Anwendung von Management-Netzwerken ist die Verwendung von ULAs sinnvoll den die bleiben auf eine Organisation beschränkt.

ULAs werden in 2 Gruppen unterschieden mit unterschiedlicher Bedeutung:

- ◆ fc00 - Adressen. Sie sind unique local und werden zentral verwaltet und vom Provider vergeben.
- ◆ fd80 - Adressen. Sie sind unique local und werden lokal vom Administrator verwaltet.

➌ Unique Globally Scope

Diese Adressen werden im Internet geroutet und können dort auch verwendet werden.

24.22.4.2 - Aufbau

IPv6-Adressen sind 128 Bit groß. Damit sind rund 340 Sextillionen (2^{128}) Geräte adressierbar. Sie sind typischerweise in 2 Teile strukturiert. In einen 64Bit (Sub)Netzwerk-Teil und einen 64 Bit Hostteil. Damit lassen sich identische Host-Adressen mit jeweils separaten Präfixen in unterschiedlichen Netzen einsetzen.

Der wichtigste und gebräuchlichste Adress-Aufbau ist der in RFC 3587 beschriebene globale Unicast-Adresse, der eine Adresse in einer allgemeinen Form beschreibt.

64 - n Bits	n Bits	64 Bits
Global Routing Präfix	Subnetz-ID	Interface ID

Der Global Routing Präfix entspricht dem Netzwerk-Teil einer IPv4-Adresse und legt ein international eindeutig gültiges, an ein weltweites Internet anschließbares Netzwerk fest.

Die Subnetz-ID bestimmt die Unterteilung in interne Sub-Netze, die für das öffentliche Internet ohne Belang sind.

In der Praxis hat sich die Real-World-Struktur durchgesetzt. Dabei ist der Global Routing Präfix auf 48 Bit festgelegt und die Subnetz-ID auf 16 Bit. Die Interface-ID hat 64 Bits.

48 Bits	16 Bits	64 Bits
Global Routing Präfix	Subnetz-ID	Interface ID

Damit stehen einem Administrator $2^{16} = 65.536$ Bits zur Festlegung von Subnetzen zur Verfügung. In jedem der vom Administrator vergebenen Subnetz sind $2^{64} = 18.446.744.073.709.600.000$ Interface-IDs möglich.



Derzeit steht ein Achtel der möglichen Adressen zur Verteilung zur Verfügung. Der Rest ist einer künftigen Verteilung vorbehalten.

Ein Internet Service Provider (ISP) bekommt normalerweise ein /32-Bereich zugeteilt. In begründeten Fällen ist auch ein /29-Bereich möglich.

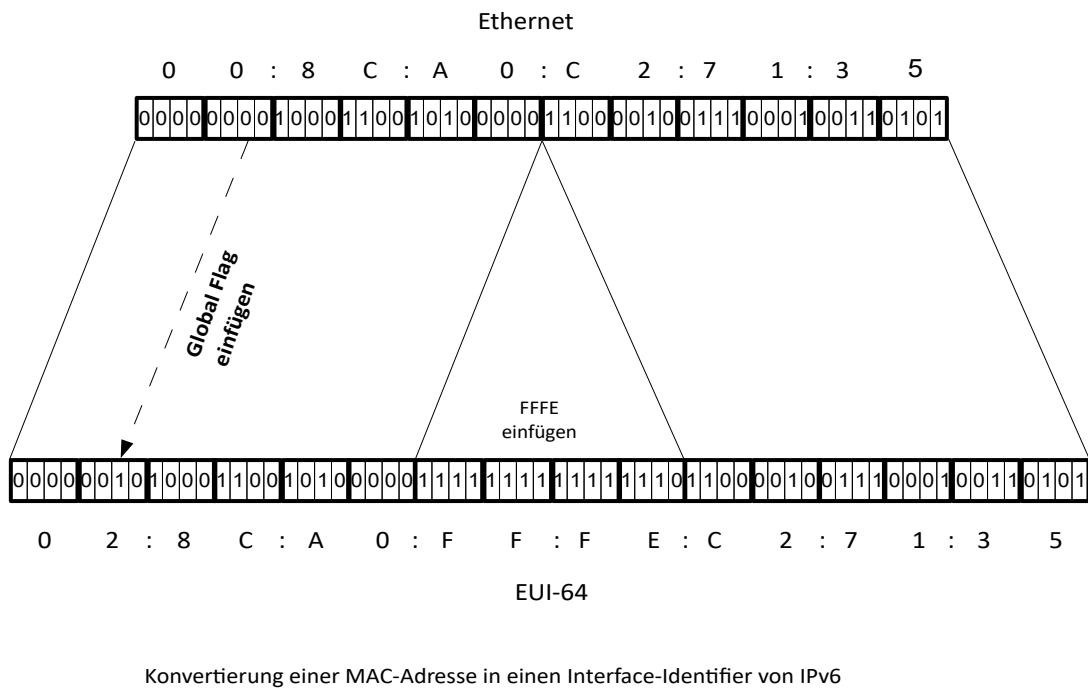
Vergibt der Provider seinem Kunden ein /48-Bereich kann er (falls er einen /29-Bereich bekommen hat) 2^{19} Kunden mit Netzwerken ausstatten.

Vergibt ein Provider einer Privatperson einen /56-Bereich könnte er 2^{27} Privatpersonen mit Netzwerken ausstatten.

Letztendlich stehen in jedem Subnetz 2^{64} Interface-IDs zur Verfügung, die direkt miteinander kommunizieren können.

24.22.4.3 - EUI-64 Adresse

Die Interface-ID wird im RFC 3513 spezifiziert und wird aus einer modifizierten EUI-64 ID gewonnen. Dabei kann entweder bereits eine EUI-64-Adresse oder eine MAC-Adresse verwendet werden.



Konvertierung einer MAC-Adresse in einen Interface-Identifier von IPv6

Abbildung 387 : MAC- EUI-64 Konvertierung

Es wird zwischen globalen und lokalen Adressen im Bit 7 unterschieden. 0 bedeutet lokale Adresse 1 bedeutet globale Adresse. Folgende Regel findet Anwendung:

Hat das Interface eine EUI-64-Adresse wird das 7 Bit invertiert.

Hat das Interface eine MAC-Adresse werden die 48 Bit in zwei 24-Bit-Teile zerlegt und in der Mitte mit FFFE aufgefüllt. Zusätzlich wird das 7 Bit (Global Flag) der MAC-Adresse invertiert.

Hier wird sichtbar, dass viel über die veränderte Internet-Adressierung nachgedacht wurde. Der Aufbau macht es möglich, jedem Gerät eine eigene IP-Adresse fest zu vergeben. Damit kann man dann innerhalb des lokalen Netzwerks auch ohne Global Routing Präfix und Subnetz-ID erst einmal kommunizieren. Ein Gerät hat damit von sich aus die Möglichkeit, einen Router zu suchen. Dieser Router gibt dann dem Rechner den noch fehlenden Adress-Teil der IPv6-Adresse und weitere Informationen wie z. B. die MTU-Size.

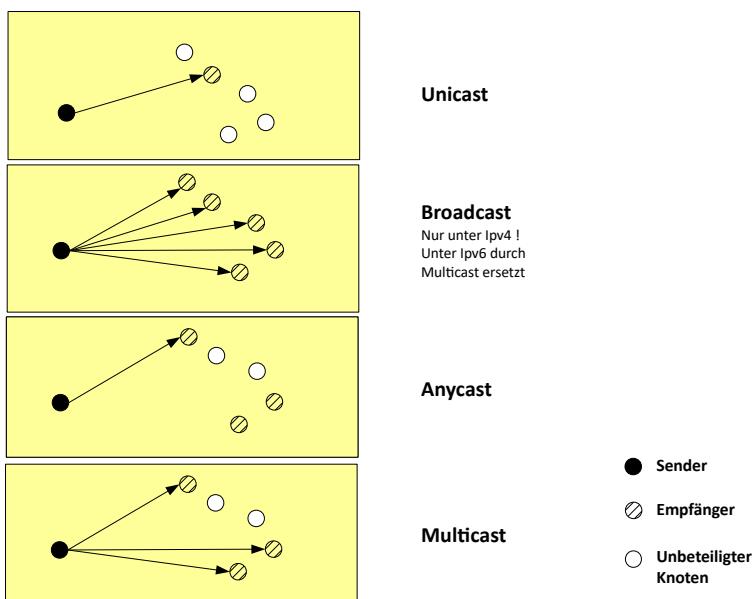
Danach kann der Rechner mit Rechnern in anderen Netzwerken, eine Verbindung herstellen. An dieser Stelle kann man schon ahnen, dass die Inbetriebnahme von IPv6 einem Administrator für Clients (Desktops, Notebooks, Drucker,...) weniger Arbeit macht als die von IPv4.

Die feste IP-Adresse hat aber auch einen Sicherheits-Nachteil. Eine gültige feste EUI-64-Adresse kann in allen Netzen getrackt werden. Zusammen mit der Providerinformation ist die Bestimmbarkeit einer Person möglich. Damit fällt eine IP-Adresse, übrigens wie bereits bei IPv4, unter die personenbezogenen Daten im Sinne des BDSG. Dieses Problem wird mit dem RFC 3041 gelöst. Hier wird vorgeschlagen mehrere Interface-IDs zu verwenden. Die mit DNS registrierte Adresse wird für eingehende Verbindungen verwendet. Die zufällig ausgewählten anderen Adressen werden für ausgehende Verbindungen verwendet.

Es sind also bei einem IPv6 Knoten erst mal keine administrativen Tätigkeiten notwendig . Dagegen ist die Intelligenz und somit auch der Parametrieraufwand in den Routern untergebracht. Wichtig bei diesen Zusammenhängen, ist auch die unterschiedliche Bedeutung der IP-Adress-Typen, im Vergleich zu IPv4.

24.22.4.4 - Adress-Typen

Bei IPv6 gibt es 3 Typen von Adressen.



24.22.4.4.1 - IPv6-Unicasts

Unicasts dienen der Kommunikation zwischen zwei Interfaces. Sie sind auch eine Kennzeichnung für eine einzelne Schnittstelle. Ein Paket, das an eine Unicast-Adresse gesendet wird, wird an die durch diese Adresse gekennzeichnete Schnittstelle übertragen. Diese Adresse sollte nur einmal vorhanden sein! Global - Unicast-Adressen besitzen derzeit den Präfix 2000::/3. Unique-Local-Adressen haben den Präfix fc00::/7.

Abbildung 388 : Kommunikationstypen

24.22.4.4.2 - IPv6-Anycast

Anycasts sind vorgesehen für Router oder Server, die den selben Dienst (wie HTTP oder DNS) zur Verfügung stellen und Redundanz oder Load-Sharing gewünscht ist. Anycasts wurden bereits 1993 für IPv4 im RFC1546 beschrieben. Zum Einsatz kamen Anycasts bei den DNS-Root-Serveren nachdem 2001 die World-Trade-Center eingestürzten und DNS-Root-Server unter sich begruben. Die im RFC1546 vorgeschlagenen speziellen Anycast-Adressen wurden jedoch nicht eingesetzt. Zum Zug kamen so genannte „Shared Unicast Adressen“. Dabei wird eine normale Unicast Adresse mehreren Interfaces zugewiesen und als Host-Route-Eintrag in den Routing-Tabellen hinterlegt. Bei einem Aufruf der Adresse kommt der Eintrag mit der besten Metrik zum Zug. Allerdings hat ein Sender keine Kontrolle darüber welches Empfänger-Interface angesprochen wird, da die Auswahl auf Routing-Ebene entschieden wird.

Beispielsweise nutzen DNS und Mobile IPv6 Anycasts.

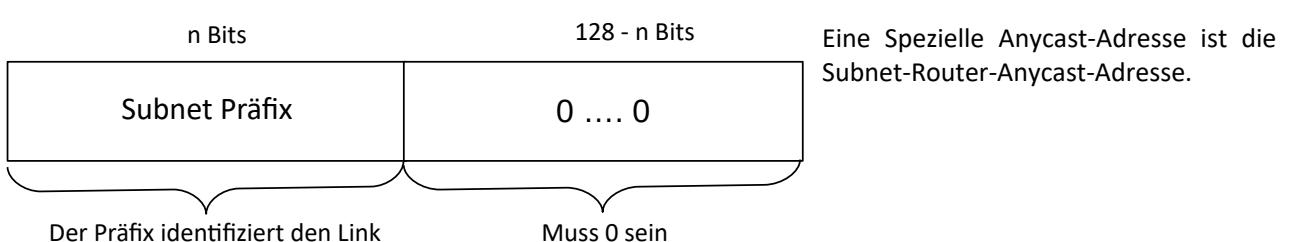
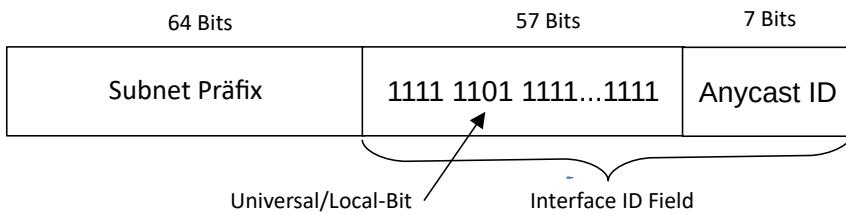


Abbildung 389: Format der Subnet-Router-Anycast-Adresse

Im RFC 2526 sind weitere Informationen zum Format von Anycast-Adressen hinterlegt. Bei Adressen im EUI-64-Format ist das Universal/Local-Bit auf 0 zu setzen um zu signalisieren, dass diese Adresse nicht Global eindeutig ist.

Anycast Adresse mit 64 Bit Interface im EUI-64-Format



Anycast Adresse für alle anderen IPv6 Adresstypen (nicht im EUI-64-Format)

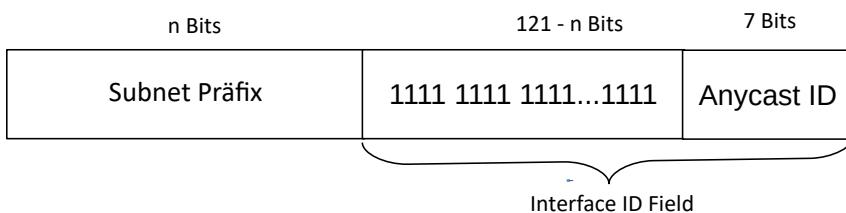


Abbildung 390: Format von Anycast-Adressen

Als Anycast-ID ist derzeit nur Mobile IPv4 mit einem Wert von 0x7e (126) festgelegt. Alle anderen Werte sind derzeit noch reserviert.

Dezimalwert	Hexadezimalwert	Beschreibung
0 - 125	00 - 7D	reserviert
126	7E	Mobile IPv6 Home-Agents-Anycast
127	7F	reserviert

Tabelle 37: Anycast-IDs

24.22.4.4.3 - IPv6-Multicast

Kennzeichnet eine Menge von mehreren Schnittstellen, die typischerweise zu unterschiedlichen Knoten gehören. Ein Paket das an eine Multicast-Adresse gesendet wird, wird an alle durch diese Adresse gekennzeichneten Knoten gesendet. Diese Adresse kann mehrmals vorhanden sein. Näheres ist in einem der folgenden Kapitel beschrieben.

24.22.4.4.4 - Weitere Unterschiede zu IPv4-Adressen

- Es gibt keine Broadcast-Adressen mehr! Die Funktionalität der IPv6-Broadcast-Adressen wurden von der IPv6-Multicast-Adresse Link-Local-All-Nodes-Multicast-Address ff02::1 übernommen.
- In IPv6 sind „All-0“ = „All Zeros“ und „All-1“ = „All Ones“ zunächst zulässige Werte für Adressen. Die vollständige „All-0“ und „All-1“ über alle Felder sind nach wie vor ungültig!
- Speziell Präfixe (also die vorderen Teile einer Adresse) können Felder mit Nullen enthalten. Wichtig für den Beginn der Datenkommunikation ist die Interface ID innerhalb der IPv6-Adresse. Sie wird aus der MAC-Adresse gebildet. Alle anderen vorangestellten Teile lassen sich später ermitteln.
- IPv6-Adressen werden den Schnittstellen (Interfaces) zugewiesen. Nicht den Knoten (Nodes)! Da jede Schnittstelle zu einem Knoten gehört, kann jede Schnittstellen-Unicast-Adresse dazu verwendet werden den Knoten zu bezeichnen.
- Alle Schnittstellen müssen mindestens eine „Link-Local-Unicast-Adresse“ haben. Damit kann eine Schnittstelle mehrere Adressen von jedem Typ (Uni-, Any- oder Multicast) oder Scope haben.
- Unicast Adressen mit mehr als der Link-Scope-Adresse werden als Ziel- oder Quell-Adresse nicht benötigt. Damit kann innerhalb eines Netzwerks kommuniziert werden. Dies ist vor allem für Punkt-zu-Punkt-Verbindungen angenehm.
- Ausnahme:
Eine Unicast-Adresse oder reine Menge von Unicast-Adressen können zu mehreren Schnittstellen zugewiesen werden, wenn die Implementierung für alle darüber liegenden Schichten die Schnittstellen als eine einzige Schnittstelle behandelt. Dies ist nützlich für Loadsharing (deutsch: Last-Teilung) über mehrere physikalische Schnittstellen.

24.22.4.5 - Aussehen einer IPv6-Adresse

Die IPv6-Adressarchitektur ist im RFC 4291 beschrieben. Die Vergabe erfolgt durch die IANA. Am Anfang wurden die IPv4-Adressen sehr großzügig vergeben. Das hatte zur Folge, dass Universitäten und manche Firmen ganze A-Klasse-Netze zugesprochen bekamen. Vergebene IPv4-Adressen können von der IANA nicht mehr zurückfordert werden. Hier hat man dazu gelernt. Die IPv6-Adressen werden nur noch geliehen und können bei Bedarf zurückfordert werden!

24.22.4.5.1 - Die bevorzugte Form

Bei der Schreibweise hat man sich auf Hexadezimalziffern geeinigt, da die Umwandlung von Hexadezimalzahlen in Binärzahlen für einen Rechner einfacher, und somit schneller geht, als die Umwandlung von Dezimalzahlen in Binärzahlen. (Bei den IPv4-Adressen war die Dezimalschreibweise noch sinnvoll, da man sie sich so besser merken konnte. Durch die erheblich größere Länge einer IPv6-Adresse entfällt dieser Vorteil)

Grundsätzlich hat eine IPv6-Adresse das folgende Format.

x:x:x:x:x:x

wobei x eine 16-Bit-Hexadezimalzahl ist. Die Buchstaben (a,b,c,d,e,f) werden immer klein geschrieben. So sieht eine IPv6-Adresse beispielsweise so aus:

2001:00a3:0000:0000:0308:0000:fec3:528a

Führende Nullen können entfallen. Damit verkürzt sich die obige IPv6-Adresse auf die folgende Form:

2001:a3:0:0:308:0:fec3:528a

Bei langen Null-Folgen ist es möglich, eine beliebig lange Folge mit :: abzukürzen. Diese Möglichkeit besteht pro Adresse jedoch nur einmal! Sollte es mehrere gleich lange Null-Folgen geben, wird die erste Null-Folge zu :: verkürzt. Das liegt daran, dass ein Rechner, der eine IPv6-Adresse nutzt, immer die gesamten 128 Bit verwendet. Dazu muss er den mit :: beschriebenen Bereich mit Nullen auffüllen. Das wäre bei mehreren Bereichen eventuell nicht möglich.

Die obige IPv4-Adresse kann damit zur folgenden Zeichenkette verkürzt werden:

2001:a3::308:0:fec3:528a

Damit sind folgende Adress-Beispiele mit unterschiedlichen Schreibweisen möglich.

Ausgeschriebene Form	Komprimierte Form	Bedeutung
2080:0000:0000:0000:0008:0800:200C:417a	2080::8:800:200C:417a	Unicast-Adresse
ff01:0000:0000:0000:0000:0000:0000:0101	ff01::101	Multicast-Adresse
0000:0000:0000:0000:0000:0000:0000:0001	::1	Loopback-Adresse
0000:0000:0000:0000:0000:0000:0000:0000	::	Unspezifizierte-Adresse

Tabelle 38: IPv6-Adressbeispiele

Soll eine IP-v6-Adresse in einer URL zusammen mit einer Port-Beschreibung eingegeben werden, kommt es mit den Doppelpunkten zu einem Konflikt.

Die IPv6-Adresse 2001::0dac:1 müsste vom Port 8080 mit einem Doppelpunkt abgetrennt werden was zu Interpretationsproblemen im Browser führt. Deshalb ist die IPv6-Adresse mit einer eckigen Klammer (Square Brackets) zu kennzeichnen. Damit würde die Kombination aus IPv6-Adresse und Portnummer folgendes Aussehen haben:

[2001::0dac:1]:8080

24.22.4.5.2 - Mischformen von IPv4 und IPv6

Bei einer aus IPv4 und IPv6 gemischten Umgebung ist es möglich die Punkt-Schreibweise der IPv4-Adressen mit der Doppelpunkt-Schreibweise bei IPv6 zu mischen. Dies erleichtert vor allem den Umstieg von IPv4 auf IPv6. Hierbei sind die folgenden möglichen Formen denkbar:

24.22.4.5.2.1 - Unter IPv6 genutzte IPv4 -Adressen

x:x:x:x:d.d.d.d

x entspricht einem 16-Bit-Hexadezimalwert (0 – FFFF) auf der höherwertigen Seite der Adresse.

d entspricht einem 8-Bit-Dezimalwert (0 – 255) auf der niederwertigen Seite der Adresse.

Diese Schreibweise dient nur der internen Darstellung und wird nie als Quell- oder Zieladresse versendet!

0:0:0:0:0:d.d.d.d

Beispiel:

::abba:815 = 0:0:0:0:0:171.186.8.21 = ::171.186.8.21

24.22.4.5.2.2 - IPv4-mapped IPv6-Adresse

Hierbei sind die ersten 80 Bits auf 0 gesetzt. Danach werden die nächsten 16 Bits auf 1 gesetzt.

Beispiel:

Ausgeschriebene Form	Komprimierte Form
----------------------	-------------------

0:0:0:0:ffff.129.144.52.38	::ffff.129.144.52.38
----------------------------	----------------------

24.22.4.6 - Adress-Präfix

24.22.4.6.1 - Bedeutung

Mit einem Präfix oder Format-Präfix werden Adressen näher spezifiziert. So können Klassen oder Typen näher beschrieben werden.

24.22.4.6.2 - Adress-Präfix-Schreibweise

Die Schreibweise entspricht der aus IPv4 bekannten CIDR-Schreibweise mit dem Schrägstrich. Dargestellt wird die Adresse sowie eine Längenangabe getrennt mit dem Schrägstrich:

<IPv6-Adresse> / <Präfixlänge in Bits>

Die IPv6 Adresse entspricht einer Adresse in einer der oben beschriebenen Formen.

Die Präfixlänge entspricht einer Dezimalzahl mit der Anzahl der Bits von links gezählt.

Mögliche gültige Darstellungen des 60-Bit-Präfix 12ab00000000cd3 sind:

12ab:0000:0000:cd30:0000:0000:0000:60

12ab::cd30:0:0:0/60

12ab:0:0:cd30::/60

Ungültige Darstellungen dieser Adresse sind: (Fehler sind unterstrichen)

12ab:0:0:cd3 daraus würde 12ab:0:0:0cd3:0:0:0

12ab::cd30/60 daraus würde 12ab:0:0:0:0:0:cd30

12ab::cd3/60 daraus würde 12ab:0:0:0:0:0cd3

24.22.4.7 - Adress-Typ-Darstellung

Adress-Typen können an den MSB (Most Significant Bits; deutsch: höchstwertigste Bits) erkannt werden. Somit stehen sie bei einer IPv6-Adresse an der linken Seite. Sie werden auch Format-Präfix genannt.

Die derzeit interessanten Adress-Typen sind **fett** gedruckt. *Kursiv* gedruckte Adress-Typen stehen für reservierte Bereiche, Testnetze, Übergangsverfahren und experimentelle Protokolle.

Bedeutung	Präfix in Binärschreibweise	Präfix in Hexadezimal
Unspezifizierte Adresse (RFC4291)	0000 0000	::/128
Loopback-Adresse (Host Scope) (Entspricht 127.0.0.1 in IPv4) (RFC4291)	0000 0001	::1/128
Reserviert oder spezifisch	0000 0000	0000::/8
Reserviert für NASP Belegung	0000 0010	0200::/8
Nicht zugewiesen (ehemals für IPX reserviert)	0000 0100	0400::/8
Aggregierbare globale Unicast-Adresse	0010	2000::/3
Teredo (RFC 4380)	0010 0000 0000 0001 0000 0000 0000 0000	2001::/32
Benchmarking	0010 0000 0000 0001 0000 0000 0000 0010 0000 0000 0000 0000	2001:2::/48
ORCHID (RFC4843)	0010 0000 0000 0001 0000 0000 0001 0000	2001:10::/28
Documentation (RFC 3849)	0010 0000 0000 0001 1101 1011 0001 0000	2001:db8/32
6to4-Adresse	0010 0000 0000 0010	2002::/16
Unique Local (Entspricht den RFC 1918-Adressen in IPv4) (RFC 4193)	1111 110	fc00::/7
Link-Local Unicast-Adresse entspricht 169.254.0.0 unter IPv4 (APIPA) (RFC4291)	1111 1110 1000	fe80::/10
Site-Local Unicast-Adresse	1111 1110 1100	fec0::/10
Multicast-Adresse entspricht 224.0.0.0/4 bei IPv4 (RFC4291)	1111 1111	ff00::/8
IPv4-Mapped-Adresse (RFC4038)	0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 1111 1111 1111 1111 0000 0000	::ffff:0:0/96
IPv4 compatible Adresse (RFC 4291)	0000 0000	:/96

24.22.4.8 - Übersicht der vorgeschriebenen Adressen

Laut RFC 4291 muss jeder Node, an jedem Interface, die folgen den Adressen erkennen können:

- ➊ Loopback-Adresse
- ➋ Eine Link-Local-Adresse
- ➌ Die Link-Local-All-Nodes-Multicast-Adresse
- ➍ Alle Unicast- oder Anycast-Adressen, die dem Interface zugewiesen wurden
- ➎ Für jede Unicast- oder Anycast-Adresse die zugehörige Link-Local-Solicited-Node-Multicast-Adresse
- ➏ Die Multicast-Adressen denen das Interface angehört

Für Router gilt zusätzlich:

- ➐ Die Subnet-Router-Anycast-Adresse für jedes Interface mit Routing-Funktionalität
- ➑ Alle Anycast-Adressen für die der Router konfiguriert wurde
- ➒ Die Link-Local- und die Site-Local-All-Routers-Multicast-Adresse (ff02::2 und ff05::2)

24.22.4.9 - Aufbau von Multicast-Adressen

Laut RFC4291 bauen sich Multicast-Adressen unter IPv6 folgendermaßen auf:

ff0s:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

Dabei steht s für den Scope:

Wert	Scope	Bedeutung
1	Node Local	Multicast Loopback
2	Link Local	Nicht routebar. Nur am betreffenden Link gültig
4	Administration Local	Administrativ zusammenhängende Netzwerke innerhalb einer Site
5	Site Local	Alle Netzwerke eine Site
8	Organisational Local	Alle Netzwerke einer Organisation
e	Global	Global Routing fähig

Protokolle

Für XXXX:XXXX:XXXX:XXXX:XXXX:XXXX gelten die folgenden Zuordnungen (siehe auch RFC 2375)

Wert	Bedeutung	Gültig in Scope			
		1 (Node Local)	2 (Link Local)	5 (Site Local)	X (All Scopes)
::1	All Nodes	X	X		
::2	All Routers	X	X	X	
::4	DVMRP-Routers		X		
::5	OSPFIGP		X		
::6	OSPFIGP Designated Routers		X		
::7	ST Routers		X		
::8	ST Hosts		X		
::9	RIP Routers		X		
::A	EIGRP Routers		X		
::B	Mobile Agents		X		
::1:2	All DHCP Agents		X		
::1:3	All DHCP-Servers			X	
::1:4	All DHCP-Relays			X	
::1:1000 – ::1:13ff	Service Location			X	
::100	VMTCP Managers Group				X
::101	Network Time Protocol (NTP)				X
::102	SGI-Dogfight				X
::103	Rwhod				X
::104	VNP				X
::105	Artificial Horizons - Aviator				X
::106	Name Service Server (NSS)				X
::107	AUDIONEWS – Audio News Multicast				X
::108	SUN NIS+ Information Service				X
::109	MTP Multicast Transport Protocol				X
::10a	IETF-1 Low-Video				X

Wert	Bedeutung	Gültig in Scope			
		1 (Node Local)	2 (Link Local)	5 (Site Local)	X (All Scopes)
::10b	IETF-1 Audio				X
:					X
::110	MUSIC-Service				X
::118	microsoft-ds				X
::127	cisco-rp-announce				X
::128	cisco-rp-discovery				X
::2:FFF	SAP Dynamic Assignments				X

24.22.4.10 - Weitere Protokolle im Umfeld von IPv6

Für IPv6 sind natürlich noch weitere Hilfsprotokolle wichtig.

Protokoll	Beschreibung
ICMPv6	Internet Control Message Protocol RFC2463. Diesem Protokoll kommt eine zentrale Bedeutung zu. Es darf von Firewalls nicht mehr geblockt werden wie bei IPv4.
DNSv6	Domain Name Service RFC3596
NDP	Neighbour Discovery Protocol. Damit wird das ARP-Protokoll abgelöst.
DHCPv6	Dynamic Host Configuration Protocol RFC3315
RIPng for IPv6	Routing Information Protocol RFC2080
OSPF for IPv6	Open Shortest Path First RFC2740

24.22.4.11 - RFCs im Zusammenhang mit IPv6

Im Zusammenhang mit IPv6 gibt es über 200 RFCs. Hier eine Auswahl.

RFC	Inhalt	Bemerkung
	entication Header	
1881	IPv6 Address Allocation Management (IB, IESG)	
1887	An Architecture for IPv6 Unicast Address Allocation	
1918	Address Allocation for Private Internets	
1981	Path MTU Discovery for IP version 6	
2185	Routing Aspects of IPv6 Transition	
2375	IPv6 Multicast Address Assignments	
2460	Internet Protocol, Version 6 (IPv6)	
2463	Internet Control Message Protocol (ICMPv6) for the Unernet Protocol Version 6 (IPv6)	
2464	Transmission of IPv6 Packets over Ethernet Networks	
2471	IPv6 Testing Address Allocation	
2473	Generic Packet Tunneling in IPv6 Specification	
3053	IPv6 Tunnel Broker	
3056	Connection of IPv6 Domains via IPv4 Clouds	
3142	An IPv6-to-IPv4 Transport Relay Translator	
3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	
3493	Basic Socket Interface Extensions for IPv6	
3513	IP Version 6 Addressing Architecture	Löst RFC 1884, 2373 ab
3587	IPv6 global Unicast Address Format	
3595	Textual Conventions for IPv6 Flow Label	
3596	DNS Extensions to Support IP Version 6	Löst RFC 1886, 3152 ab
4193	Unique Local IPv6 Unicast Addresses	
4213	Basic Transition Mechanisms for IPv6 Hosts als Routers	Löst RFC 1933, 2893 ab
4303	IP Encapsulating Security Payload (ESP)	Löst RFC 1827, 2406 ab
4380	Teredo: Tunneling IPv6 over UDP through Network Address Translations NATs	
4391	Transmission over IP over InfiniBand (IPoIB)	

RFC	Inhalt	Bemerkung
4835	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payloads (ESP) and Authentication Header (AH)	Löst RFC 2402, 1826, 2406, 4305 ab
4861	Neighbour Discovery for IP Version 6 (IPv6)	Löst RFC 1970, 2461 ab
4862	IPv6 Stateless Address Autoconfiguration	Löst RFC 1971, 2462 ab
4891	Using IPsec to Secure IPv6-in-IPv4 Tunnels	
4941	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	Löst RFC 3041 ab
4966	Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status	Löst RFC 2766 ab
5095	Deprecation of Type 0 Routing Headers in IPv6	
5214	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	Löst RFC 4214 ab
5308	Routing IPv6 with IS-IS	
5340	OSPF for IPv6	Löst RFC 2740 ab
5454	Dual-Stack Mobile IPv4	
5555	Mobile IPv6 Support for Dual Stack Hosts and Routers	
5568	Mobile IPv6 Fast Handovers	Löst RFC 5268 ab

24.22.5 - Der Übergang von IPv4 zu IPv6

Ein Austausch der IP-Ebene betrifft nicht nur die überlagerten Ebenen (TCP und UDP), sondern auch die unterlagerte physikalische Ebene.

Applikations-Ebene	HTTP, FTP, SMTP, ...	NFS, DNS, SNMP, TFTP, ...
Transport-Ebene	TCP	UDP
Netzwerk-Ebene	IP	
Physikalische-Ebene	ISDN, ATM, SDH, LAN, FR, WDM, ...	

Mittlerweile gibt es eine ganze Reihe von möglichen Migrationsstrategien. Dazu gehören:

- ➊ Dual-Stack-Technik
- ➋ Tunneltechniken
 - ➊ Tunnel-Broker
 - ➋ 6in4
 - ➌ 6over4
 - ➍ ISATAP
- ➌ Translation-Technik
 - ➊ 6to4
 - ➋ Teredo
 - ➌ Stateless IP/ICMP Translator (SIIT)
 - ➍ Transport Relay Translator

24.22.5.1 - Dual-Stack-Technik

Die Dual-Stack-Technik ist im RFC 4213 beschrieben. Hierbei ist es wichtig zu wissen, dass es auf der Ebene-2 möglich ist, mehrere Ebene-3-Protokolle parallel zu betreiben.

Bei der Dual-Stack-Technik können die Endgeräte entweder beide IP-Varianten oder IPv4 oder IPv6 implementiert haben. Router, die beide Varianten bedienen sollen, müssen natürlich beide Stacks implementiert haben.

Der Parallelbetrieb von 2 Stacks kann evtl. ein Sicherheitsrisiko bedeuten, wenn nur einer der beiden Stacks mit Schutzmechanismen ausgestattet ist. Ein zusätzlicher Minuspunkt ist die erhöhte Belastung der Netzwerk-Geräte durch die doppelte Ausprägung des Stacks. Dies bedeutet eine erhöhte Anforderung an die CPU-Leistung und den Hauptspeicher (z. B. zum Realisieren von zwei Routingtabellen eines Routers). Außerdem ist ein IPv6 DNS Server erforderlich.

Protokolle

Die Dual Stack Technik kennt zwei Ausprägungen der Realisierung:

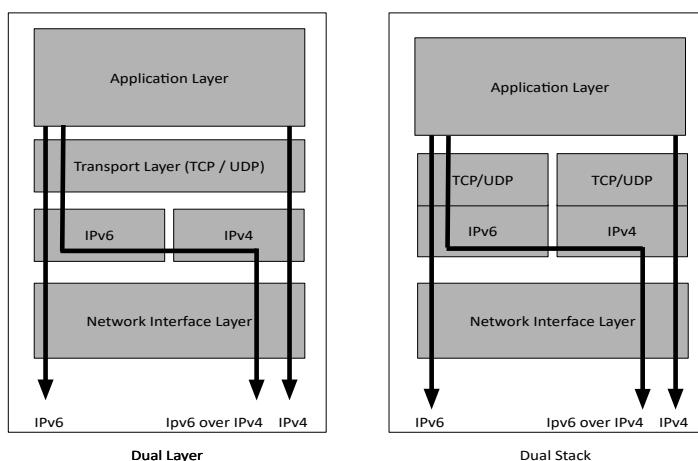


Abbildung 391 : Dual Layer - Dual Stack

- Zum einen ist sowohl die Ebene 3 und die Ebene 4 doppelt realisiert. Dann spricht man von der Dual-Stack-Technik. Windows Server 2003 und Windows XP verwenden diese ältere Realisierung.
- Zum Anderen ist die Ebene 4 nur einmal vorhanden und kann die beiden Ebene-3 Implementierungen parallel nutzen. In diesem Fall wird der Begriff Dual-Layer-Technik verwendet. Windows Server 2008 und Vista nutzen diese Technik.

Da sich die beiden Realisierungen nach außen hin gleich verhalten wird allgemein nur der Begriff der Dual Stack Technik verwendet.

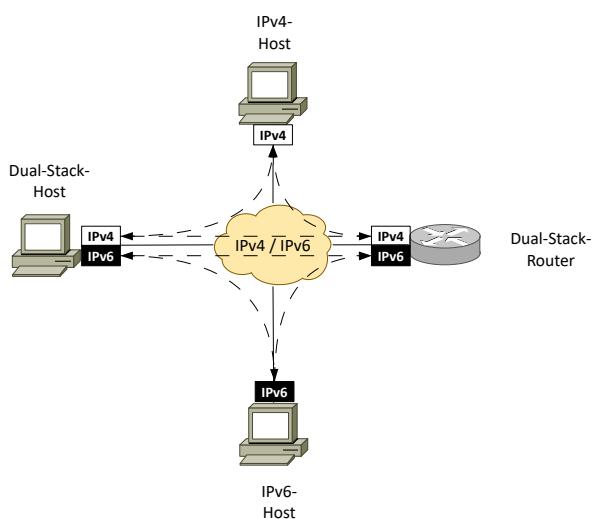


Abbildung 392 : Verbindungs möglichkeiten bei Dual-Stack-Technik

Die Endgeräte kommunizieren dabei durchgängig mit dem gleichen Protokoll. (IPv4 ↔ IPv4 oder IPv6 ↔ IPv6). Ein Übergang von einem Protokoll zum anderen findet nicht statt. Damit können die alten IPv4-Endgeräte weiter betrieben werden wie bisher. Ein Aufbau einer IPv6-Landschaft kann parallel erfolgen.

Ein direkter Zugriff von einem IPv4-Client auf eine neuen IPv6-Server ist nicht möglich. Soll eine Verbindung von einem IPv4-Endgerät auf ein IPv6-Endgerät erfolgen, muss die Verbindung über einen Dual-Stack-Router geschleift werden.

Laufen die Server und Router mit einer Dual-Stack-Implementierung, können die Endgeräte mit einem Single-Stack betrieben werden. Bei Peer-to-Peer Anwendungen wie Telefonie over IP müssen die Endgeräte bei einem Implementierungsmix auch einen Dual-Stack aufweisen. Ansonsten können sie immer nur, wie bereits ausgeführt, mit Kommunikationspartner, welche die gleich IP-Version implementiert haben, kommunizieren. Die Stacks können sowohl voneinander getrennt, oder in einer Hybrid-Implementierung, betrieben werden. Aktuelle Geräte weisen die Hybridvariante auf. Dabei arbeiten die Sockets so, dass sie beide Varianten bearbeiten können. Wird IPv4 verwendet, nutzen hybride Stacks intern eine IPv6 Semantik und stellen die IPv4-Adressen im „IPv4-gemappten Adressformat“ dar.

24.22.5.2 - Tunnel-Techniken

Eine Übertragung von IPv6-Daten über IPv4-Bereiche hinweg oder umgekehrt kann mit einem Tunneling-Verfahren vorgenommen werden. Dabei wird ein Protokoll in ein anderes eingepackt. Dies geschieht dadurch dass z. B. einem IPv4 Header ein IPv6-Header vorangestellt wird.

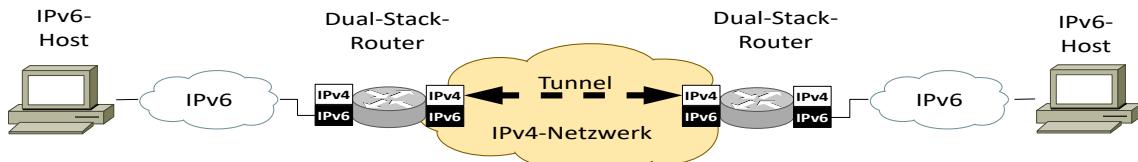


Abbildung 393 : Tunnelverfahren

24.22.5.2.1 - 6in4

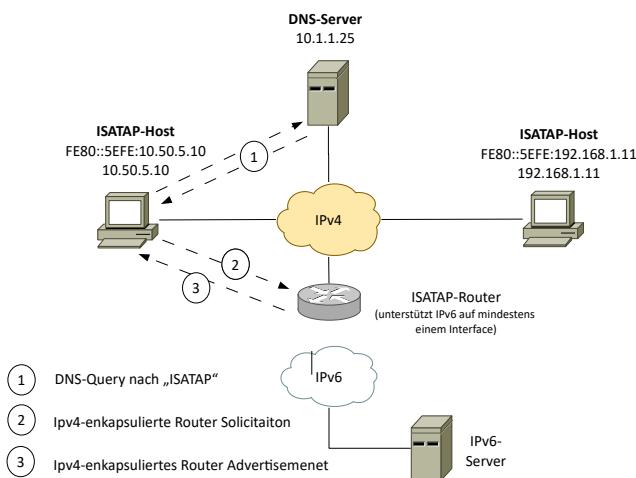
Die Vorgehensweise ist im RFC 4213 beschrieben. Es werden well known Anycast Adressen, die im Internet mehrfach vergeben sind genutzt. Dabei wird der Protokolltyp 41 verwendet. Die IPv6-Pakete werden in IPv4-Pakete enkapsuliert. Da die maximale Paketgröße (MTU-Size) bei IPv4 1500 Bytes beträgt, ist die die Paketgröße für die IPv6-Pakete auf 1480 Bytes begrenzt. Die Tunnel werden manuell statisch parametriert. Daher hat diese Technik auch den Namen „proto-41 static“. Mittlerweile gibt es auch eine dynamische Variante, die mit dem Tool AICCU (Automatic IPv6 Connectivity Client Utility) verwaltet werden kann. Dazu wird ein Tunnel Broker mit einem Tunnel Information and Control Protocol (TIC) Server eingebunden. Diese Technik sollte nicht mit der 6over4- oder 6to4-Technik verwechselt werden!

24.22.5.2.2 - 6over4

Dazu muss jeder Host, der diese Technik verwenden will, sich eine virtuelle IPv6-Adresse ermitteln. Die hierzu gehörige link local Adresse setzt sich aus 2 Bestandteilen zusammen. Die ersten Bits können folgendes aussehen haben: FE80:0000:0000:0000:0000. Die letzten / niedrigerwertigsten 32 Bits werden aus der IPv4-Adresse erzeugt. So hat z.B. die IPv4-Adresse 192.168.2.12 in hexadezimaler Notation das folgende Aussehen: C0A8:020C. Damit hat die IPv6-Adresse in Kurzschreibweise die Notation FE80::C0A8:020C.

Diese Tunneltechnik transportiert IPv6 über ein IPv4-Multicast Netzwerk. Um die notwendige Erkennung von Routern und anderer Knoten im Netzwerk (neighbour discovery) durchzuführen, werden Pakete an die IPv4-Multicast Ziel-Adresse 239.192.x.y gesendet. Dabei ist x das vorletzte und y das letzte Byte der IPv6-Adresse. Nur da wo Multicast auf IPv4-Basis verfügbar ist kann diese Technik auch eingesetzt werden. Deshalb ist 6over4 nicht auf allen Betriebssystemen verfügbar.

24.22.5.2.3 - ISATAP



Das Intra Site Automatic Tunnel Addressing Protocol ist im RFC 5214 beschrieben. Es ermöglicht IPv6-Clients über eine reine IPv4-Infrastruktur zu kommunizieren. Hierbei wird IPv4 als Sicherungsschicht (Ebene-2 im OSI-Referenzmodell) betrachtet.

Die IPv6-Clients haben dabei sowohl eine IPv4-Adresse als auch eine IPv6-Adresse, bei der die IPv4-Adresse ein gemappter Bestandteil ist.

Dabei gilt, dass lokal administrierte Clients die Kennung ::0:5EFE:a.b.c.d haben. a.b.c.d ist dabei die IPv4-Address-Anteil. Im linken Beispiel ist die Windows Default Einstellung mit dem Präfix FE80:: vorangestellt anstelle der ::0.

Für öffentliche IPv4-Adressen gilt die Kennung ::200:5EFE:a.b.c.d.

Abbildung 394 : ISATAP-Tunnelaufbau

Der Tunnel in die IPv6-Welt wird erst bei Bedarf eingerichtet, wobei ein IPv6-fähiger Router erforderlich wird. Zuerst wird beim DNS-Server nach ISATAP nachgefragt. Die Antwort des DNS-Servers ist die IPv4-Adresse des ISATAP-Routers. An den sendet der Client eine in IPv4-inkapsulierte Anfrage (Solicitaion). Als Antwort bekommt der Client das Router Advertisement mit den für IPv6 notwendigen Parametern. Darin enthalten sind z. B. die Präfixe, die der Client für die Autokonfiguration verwenden muss.

24.22.5.3 - Translation-Technik

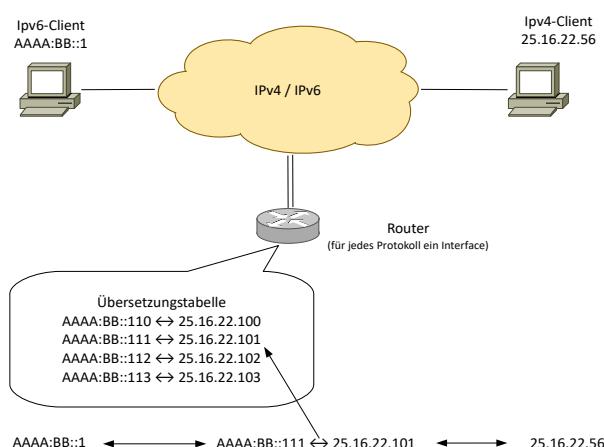


Abbildung 395 : Translation-Technik

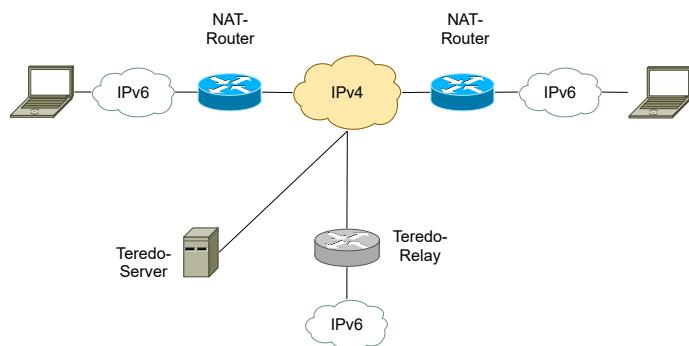
Sobald Geräte eingesetzt werden, die nur IPv4 oder IPv6 unterstützen muss eine Übersetzung zwischen den beiden Kommunikationspartnern erfolgen.

Die Translation-Technik, die auch mit NAT-PT (Protocol Translation) bezeichnet wird, baut einen IPv6-Header in einen IPv4-Header um und agiert dabei wie bei einer NAT-Übersetzung mit einer internen Verwaltungstabelle.

Realisiert wird diese Funktion normalerweise auf einem Router oder Layer-3-Switch. Für die Paketkonvertierung wird SIIT (Stateless IP/ICMP Translator) eingesetzt.

Besonderes Augenmerk ist auf die Maximale Datenpaketgröße (MTU-Size) zu legen. IPv6 nutzt die dynamische Erkennung mittels Path MTU Discovery, während IPv4 eine individuelle Wahlmöglichkeit vorsieht. Zusätzlich sollten die ICMP-Nachrichten, die teilweise unter IPv6 nicht mehr zur Verfügung stehen, betrachtet werden.

24.22.5.3.1 - Teredo / Miredo



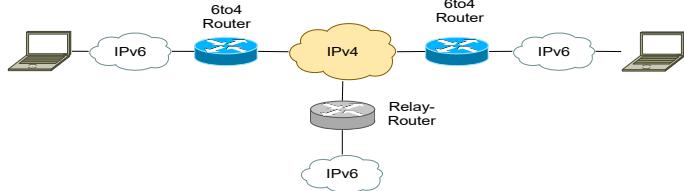
Teredo (Microsoft) oder Miredo (UNIX-Systeme) ist auch als IPv4 NAT Traversal (NAT-T) bekannt und im RFC 4380 spezifiziert. Dabei kann bei der Verwendung von NAT Teredo zum Einsatz kommen. NAT sollte allerdings im IPv6-Umfeld die Ausnahme sein. Mit dieser Tunneltechnik können IPv6-Clients eine Verbindung über ein öffentliches IPv4-Netzwerk, auch über mehrere NAT-Komponenten aufbauen. Dabei werden die IPv6 Pakete in IPv4-UDP-Datagramme (Port: 3544) verpackt.

Zwischen den Routern werden so genannte Teredo-Tunnel aufgebaut die mit dem Teredo-Server verwaltet werden.

Teredo gilt als „last resort“ für NAT Traversal und wird derzeit von 6to4 abgelöst.

Abbildung 396 : Teredo

24.22.5.3.2 - 6to4



Hierbei werden IPv6-Headern IPv4-Header vorangestellt und als Punkt-zu-Punkt-Verbindung über einem bestehenden IPv4-Backbone transportiert.. Die Protokolltypenbezeichnung hierfür ist 41 (wie bei der 6in4-Technik). Die 6to4-Router benötigen mindestens eine offizielle IPv4-Adresse. Die Vorteile des IPv6-Protokolls, beispielsweise das schnellere Routen, kann hier nicht genutzt werden. Um eine Verbindung zu einer IPv6-Welt kann über einen Relay-Router hergestellt werden. Im Vergleich zur 6in4-Technik wird hier die IPv4-Adresse aus der eingekapselten IPv6-Adresse gewonnen.

Abbildung 397 : 6 to 4

24.22.6 - Maßnahmen zur Migration von IPv4 zu IPv6

Bei der Migration zu IPv6 sind verschiedene Schritte erforderlich. Nach Möglichkeit sollte die folgenden Reihenfolge eingehalten werden:

1. Adress-Planung
2. Router-Migration
3. Server-Migration
4. Endgeräte-Migration
5. Firewall-Migration

Es gibt natürlich auch Fälle bei denen diese Reihenfolge nicht eingehalten werden kann.

24.22.6.1 - Adress-Planung

Zuerst sollte die Adress-Planung erfolgen. Wurden bereits flächendeckend offizielle IPv4-Adressen verwendet können die Adressen mittels Addressmapping erzeugt werden. Bei RIPE können global routable Adressen beantragt werden. Wurden unter IPv4 Multicast Adressen verwendet muss die Migration auf IPv6 Multicast zusätzlich geplant werden.

24.22.6.2 - Router-Migration

Zuerst sollten die Router, die den Internetzugriff ermöglichen auf IPv6 migriert werden. Die Provider sind nach den EU-Empfehlungen gehalten die Migration bis 2011 durchzuführen. Die Router können hierbei sowohl als Dual-Stack oder Gateway konfiguriert werden. Im Anschluss sollten die Layer-3 Switches folgen die auch mit einer Dual-Stack-Implementierung ausgestattet werden können.

24.22.6.3 - Server-Migration

Sie Server werden im Allgemeinen mit einer Dual-Stack-Implementierung ausgestattet. Damit ist sichergestellt, dass die alte IPv4-Welt noch bis zur Ablösung betrieben werden kann.

Zusätzlich zur Servermigration sollte ein IPv6-fähiger DNS Service eingerichtet werden.

24.22.6.4 - Endgeräte-Migration

Nachdem die Server zur Verfügung stehen können die Endgeräte umgestellt werden. Wurden alle Server auf IPv6 umgestellt kann eine IPv6-only Implementierung der Endgeräte erfolgen. Falls dies nicht möglich war, ist wiederum eine Dual-Stack-Implementierung erforderlich, um alle Server zu erreichen.

24.22.6.5 - Firewall-Migration

Bei allen Filterregeln sind so gut wie alle Regeln betroffen da meistens auch IP-Adressen enthalten sind. Besonders die Regeln für ICMP sind die Regeln neu zu erstellen da sich die Funktionen, die Protokollnummer, der Typ- und die Code-Zuordnungen geändert haben. NAT als Sicherheitsmechanismus ist unter IPv6 nicht mehr vorgesehen, da mit dem eingebauten IPsec unterstellt wird, dass IPv6 „immanent sicher“ ist. Im RFC 4864 ist beschrieben, wie sich NAT auf IPv6 abbilden lässt.

24.22.6.6 - Funktionen

Die Lizenzen der verwendeten Geräte müssen IPv6 unterstützen. Dies bedeutet, dass auch evtl. die Betriebssysteme und Applikationssoftware untersucht werden muss.

Die Geräte sollten die stateless Autokonfiguration beherrschen. DHCPv6 sollte zur Verfügung stehen (stateful Adress configuration), da die stateless Autokonfiguration evtl. Probleme mit den DNS-Servern hat.

Namensmapping auf IPv6 ist mittels DNSv6 zur Verfügung zustellen.

Die Nachbarerkennung mit dem NDP (Neighbour Discovery Protocol) ist erforderlich.

Die Layer-4 Komponenten müssen mit OSPFv3 (RFC5340) VRRPv3 (RFC5798) und evtl. mit RIPv6 zurecht kommen, wobei OSPFv3 gegenüber RIPv6 vorzuziehen ist.

Sowohl Diagnose- als auch Management-Tools sind auf die neue Landschaft anzupassen. Hierzu gehören IKEv2, IPv6 Multicast Anwendungen MLDv1, MLDv2, IPv6 Multicast Routing (MLDv1, v2, PIM-SM (Protocol Independent Multicast - Sparse Mode), PIM-DM (Protocol Independent Multicast - Dense Mode))

Bei der Verwendung von WAN-Verbindungen ist auf BGP-MP, PPP oder MPLS überprüft werden.

24.23 - GLBP (Gateway Load Balancing Protocol) HSRP / VRRP

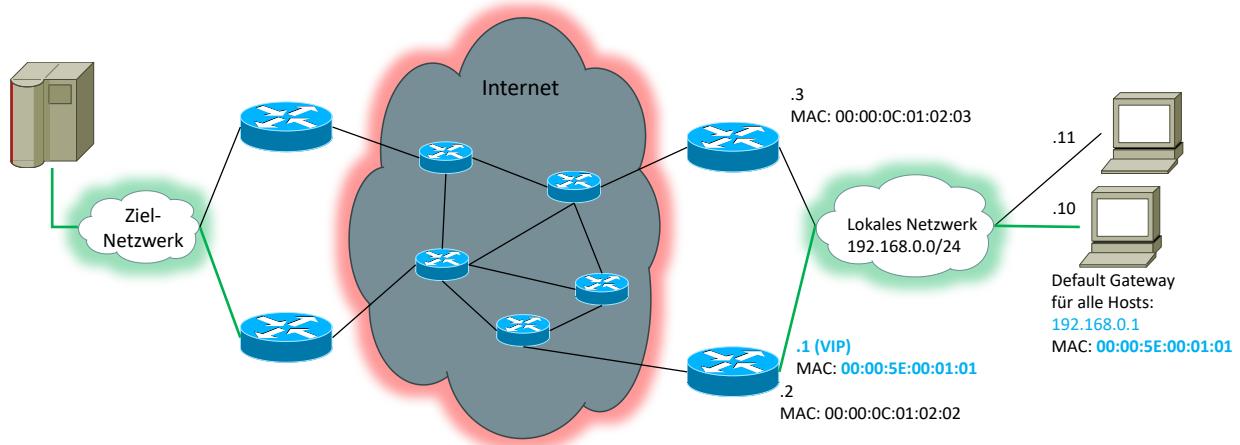


Abbildung 398: VRRP: Wirkungsbereich

24.23.1 - Einführung

Das Hot Standby Router Protocol (HSRP) und das Virtual Router Redundancy Protocol (VRRP) können zur Erhöhung der Verfügbarkeit bei Router-Ausfall eingesetzt werden und gehören zur Gruppe der GLBP (Gateway Load Balancing Protocol).

Wie im obigen Bild dargestellt, kann das Protokoll nur im lokalen Netzwerk und im Ziel-Netzwerk angewendet werden. Für die Wegefindung im Internet ist es nicht geeignet. Dort wird mit OSPF und EGP agiert.

HSRP ist Cisco-geschützt und kann somit von anderen Herstellern nicht angeboten werden. VRRP wird von den meisten Router-Herstellern unterstützt (auch Cisco). Da beide Standards ähnlich funktionieren, wird hier VRRP behandelt.

Mindestens 2 Router bilden einen virtuellen Router, der von den Hosts als Default Gateway genutzt werden kann. Einer der beiden realen Router wird zum Master und übernimmt die Default Gateway Funktion des virtuellen Routers. Der andere Router wird zum Backup-Router.

24.23.2 - VRRP

24.23.2.1 - Grundlagen

VRRP ist in der Version 3 im [RFC-5798] beschrieben. Erklärende Literatur ist unter [BOR-NT-2002] zu finden. VRRP basiert auf IPv4/IPv6 und hat in beiden Versionen die Protocol Nummer 112. Die Kommunikation erfolgt über die Multicast-IP-Adresse 224.0.0.18 / FF02::12. Die entsprechende MAC-Adresse lautet nach IGMP Abbildungsformel 01:00:5E:00:00:12. Der TTL-Wert ist auf 255 zu setzen.

24.23.2.2 - Definitionen

Zur Beschreibung des Protokolls sind einige Definitionen erforderlich.

24.23.2.2.1 - VRRP-Router

Router, die VRRP nutzen werden VRRP-Router genannt.

Die Verwendung von VRRP erfordert mindestens 2 VRRP-Router.

24.23.2.2.2 - Virtueller Router

Mehrere VRRP-Router können zusammen einen virtuellen Router (**VR**) bilden. Zum virtuellen Router gehört ein Satz von IP-Adressen sowie eine **Virtuelle Router ID (VRID)**.

Einen VR können alle Teilnehmer eines LANs als Default Router nützen. In einem Netzwerk ist es möglich mehrere VR zu definieren. Um die VR voneinander zu unterscheiden, gibt es eine 1 Byte große virtuelle Router ID (VRID).

24.23.2.2.3 - Master Router

Der Master Router ist der Router, der für den Datentransport als Default Gateway aktuell zuständig ist. Er verwaltet eine **virtuelle IP- Adresse (VIP)**. Diese IP-Adresse ist bei den Hosts als Default Gateway-IP Adresse hinterlegt.

Anfragen an diese Adresse beantwortet er somit in seiner Eigenschaft als als Default Gateway (ARP- / ICMP- Requests usw.)

Die VIP-Adresse kann entweder eine reale IP-Adresse sein, oder eine zusätzliche IP-Adresse, die weder von den Routern, noch von den Hosts verwendet wird.

Als Best Practise hat sich erwiesen, die erste oder letzte möglich IP-Adresse des Adressbandes als zusätzliche VIP zu nehmen. Die realen IP-Adressen der Router schließen daran an.

Der Master Router kann auf unterschiedliche Weise festgelegt werden.

- ➊ IP Adress-Owner
- ➋ Priorität
- ➌ Höchste IP-Adresse, bei mehreren Routern mit gleicher höchster Priorität

24.23.2.2.4 - IP Adress-Owner

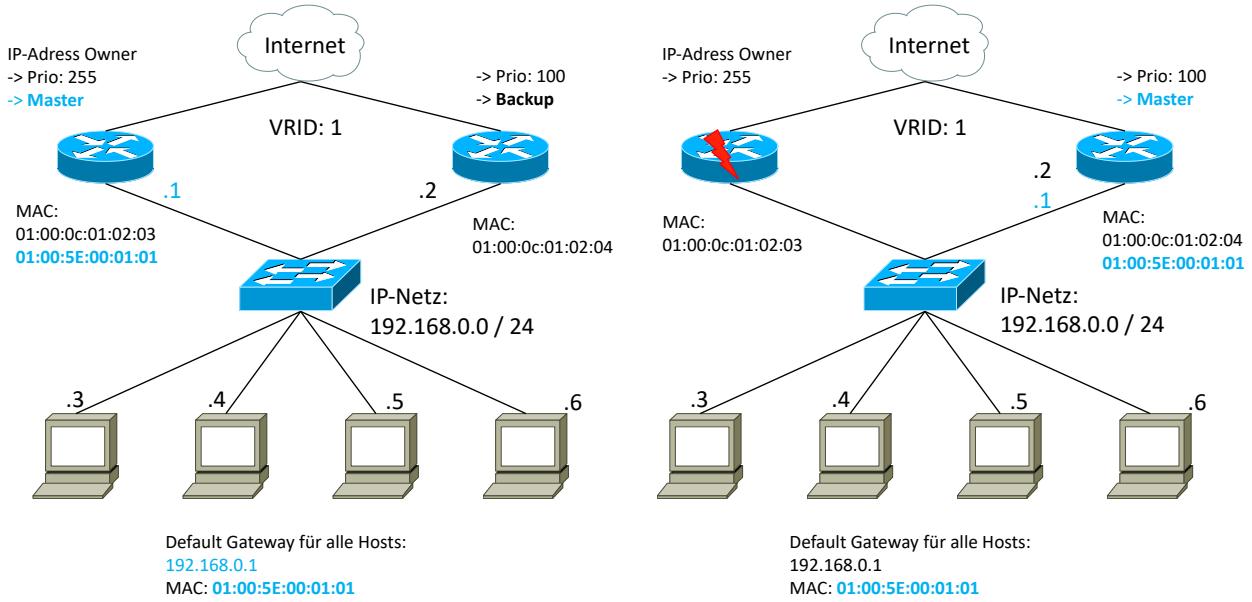


Abbildung 399: IP-Adress Owner

Es ist möglich, dass ein Router die virtuelle IP- Adresse des VR auf eines seiner realen Interfaces bindet. Die reale IP Adresse wird damit zur virtuellen IP-Adresse. Dadurch wird der Router der so genannte IP Adress-Owner. Durch diese Zuordnung bekommt er automatisch die höchste mögliche Priorität (255), was ihn automatisch zum Master Router macht solange er aktiv ist. Bei der Konfiguration eines Adress-Owners ist die Prioritätsreihenfolge mit Priorität und IP-Adresse außer Kraft gesetzt, da eine explizite IP-Adresse für den Master festgelegt wurde. Diese Vorgehensweise benötigt nur die beiden IP-Adressen für die Router.

Im Fehlerfall macht sich der Backup-Router zum Master Router in dem er die virtuelle IP-Adresse sowie die virtuelle MAC-Adresse übernimmt und die Advertisements sendet.

Die Priorität bleibt erhalten, da sie aktuell die größte ist. Der neue Master sendet unsolicited ARP-Requests um bei den Switches die ARP-Tabelle zu aktualisieren.

Bei den Hosts ändert sich nichts.

24.23.2.2.5 - Prioritätszuordnung

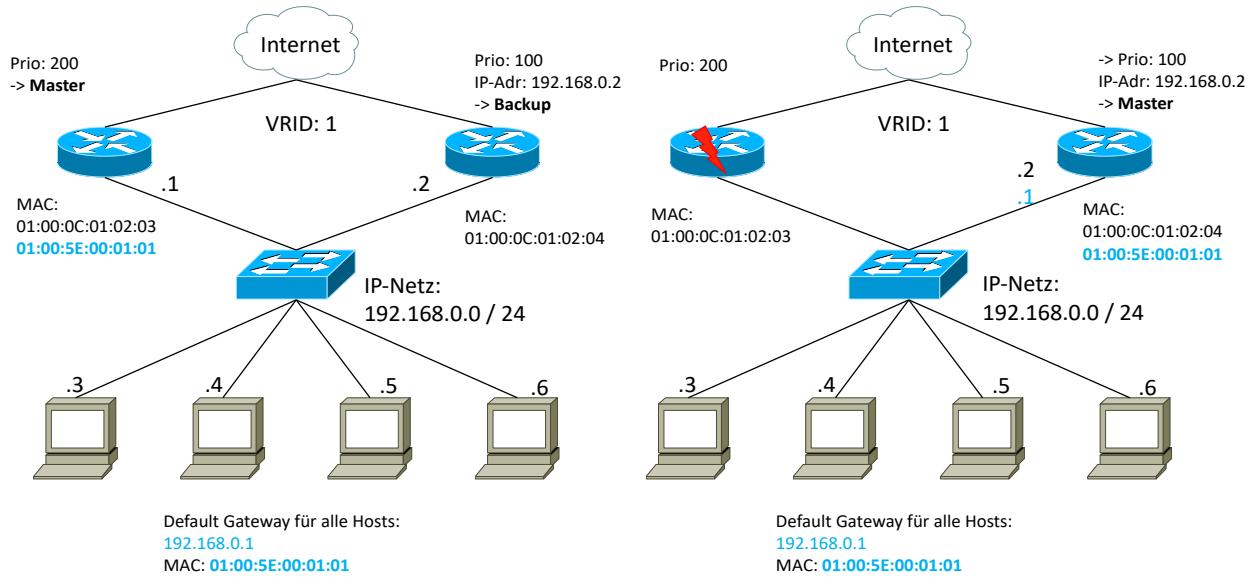


Abbildung 400: VRRP: Anwendung der Priorität

Es ist möglich mit einer Zuordnung von Prioritäten den Master und die Backup-Systeme zu bestimmen. Damit kann bei den Backup-Routern eine Reihenfolge festgelegt werden, in der sie beim Master-Ausfall versuchen selbst Master zu werden.

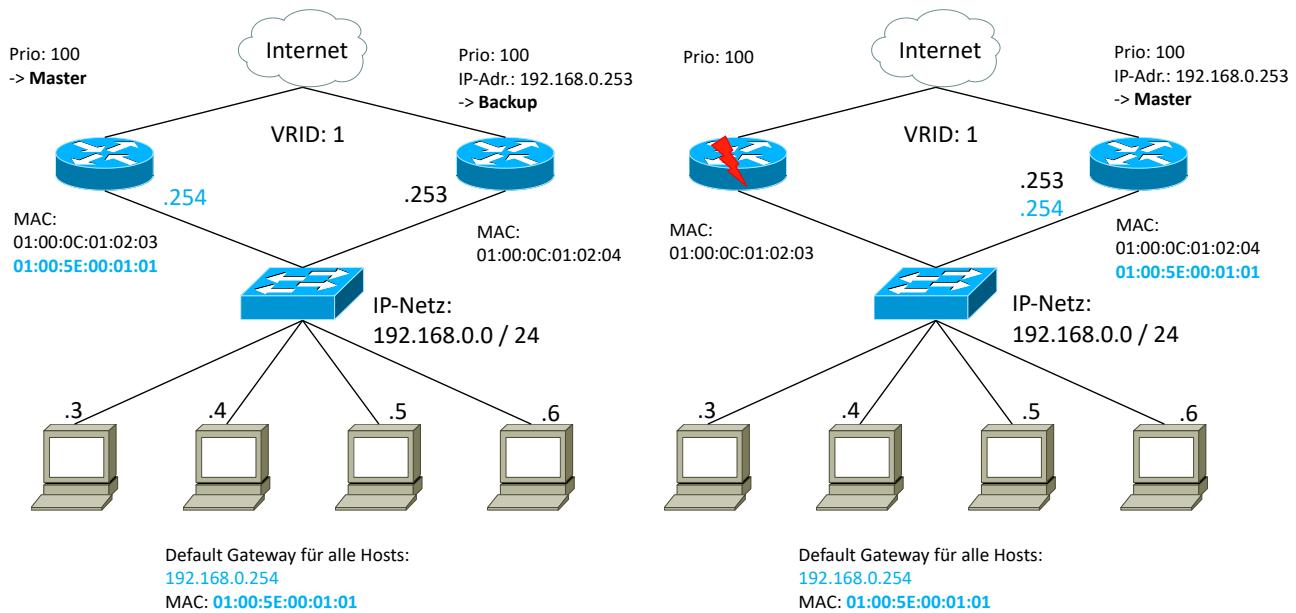
Die Priorität ist ein Byte groß und hat den Defaultwert 100. Größere Werte bedeuten eine größere Priorität. Wie beim Spanning Tree ist es auch hier ratsam den Master festzulegen.

Im Fehlerfall macht sich der Backup-Router zum Master Router in dem er die virtuelle IP-Adresse sowie die virtuelle MAC-Adresse übernimmt und die Advertisements sendet.

Die Priorität bleibt erhalten, da sie aktuell die größte ist. Der neue Master sendet unsolicited ARP-Requests um bei den Switches die ARP-Tabelle zu aktualisieren.

Bei den Hosts ändert sich nichts.

24.23.2.2.6 - Höchste IP-Adresse



Wurde kein Adress-Owner festgelegt und sind die Prioritäten der Router gleich, wird derjenige VRRP-Router zum Master, der die höchste reale Interface IP Adresse hat.

Im Fehlerfall macht sich der Backup-Router zum Master Router in dem er die virtuelle IP-Adresse sowie die virtuelle MAC-Adresse übernimmt und die Advertisements sendet.

Die Priorität bleibt erhalten, da sie aktuell die größte ist. Der neue Master sendet unsolicited ARP-Requests um bei den Switches die ARP-Tabelle zu aktualisieren.

Bei den Hosts ändert sich nichts.

24.23.2.2.7 - Nutzung einer speziellen VIP-Adresse

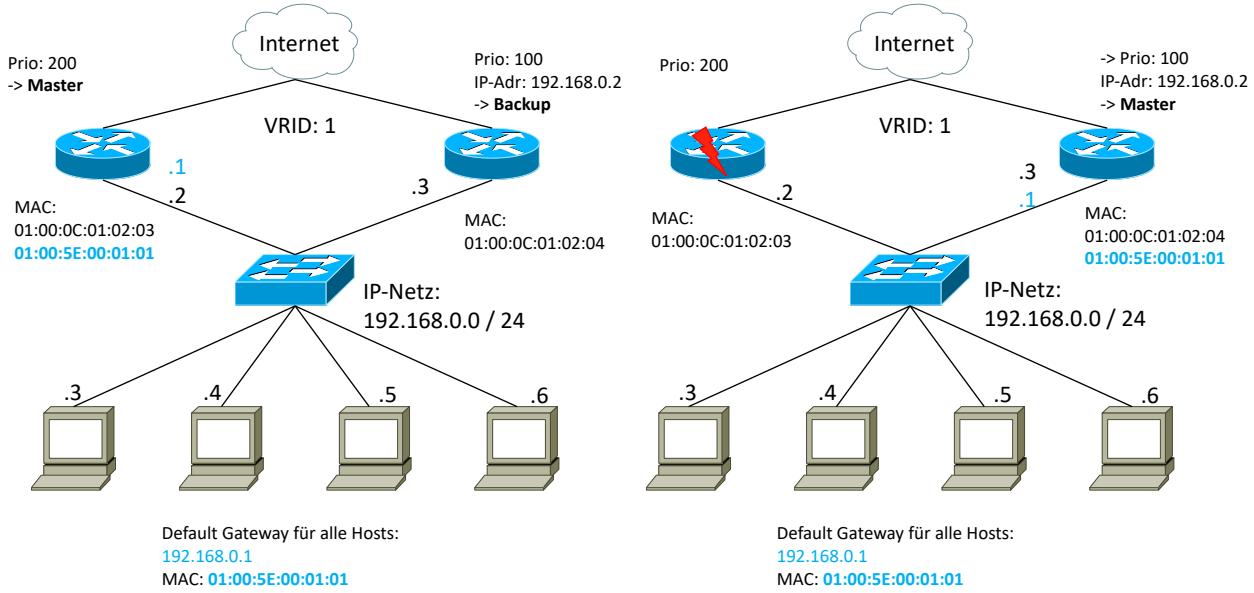


Abbildung 401: VRRP: Verwendung einer zusätzlichen VIP

Bei den bisherigen Lösungen wurden die realen IP-Adressen der vorhandenen Routern genutzt. Um eine klare Unterscheidung zwischen virtuellen IP-Adressen und realen IP-Adressen zu ermöglichen, kann eine zusätzliche virtuelle IP-Adresse verwendet werden. Dadurch bleibt für die Hosts eine IP-Adresse weniger nutzbar.

Im Fehlerfall macht sich der Backup-Router zum Master Router in dem er die virtuelle IP-Adresse sowie die virtuelle MAC-Adresse übernimmt und die Advertisements sendet.

Die Priorität bleibt erhalten, da sie aktuell die größte ist. Der neue Master sendet unsolicited ARP-Requests um bei den Switches die ARP-Tabelle zu aktualisieren.

Bei den Hosts ändert sich nichts.

24.23.3 - Betrieb

Der Master Router bearbeitet Pakete, die an die VIP gesendet wurden. Andere Router sind zwar aktiv, agieren jedoch nur als Backup-Router, ohne dass sie Daten transportieren. VRRP-Router können Backup-Router für mehrere VR sein.

Nur der Master Router sendet seinen Status an die anderen VRRP-Router in Form von Advertisements, die im Default einmal pro Sekunde gesendet werden. Damit teilt er auch seine Priorität mit.

Backup-Router senden keine Advertisements. Bleiben die Meldungen des Masters 3 Sekunden lang aus (Default) werden die Backup-Router aktiv. Die eigentliche Umschaltung vom alten auf den neuen realen Router findet dadurch statt, dass der neue Router die VIP und die virtuelle MAC-Adresse (VMAC) übernimmt. Damit das eventuell verbaute Switches in den ARP-Tabellen korrigieren sendet der neue Master-Router einen Unsolicited ARP-Reply.

Der Master-Ausfall wird von einem Backup-Router nach der folgenden Formel berechnet:

$$\text{Master Down Interval} = (3 * \text{Advertisement Interval} + \text{Skew Time}) \quad (95)$$

$$\text{Skew Time} = (256 - \text{Router Priority}) / 256 \quad (96)$$

$$\text{Router Priority} = \text{VRRP Priorität eines Backup-Routers} (\text{Default } 100) \quad (97)$$

Bei mehreren Backup-Routern bedeutet dies, dass der Backup-Router mit der größten Priorität sich selbst am schnellsten zum Master macht indem er Advertisement-Meldungen an die anderen Router des VR sendet. Sind 3 oder mehr Router in einem VR-Verbund, können, während des Umschaltzeitpunkts, Pakete dupliziert werden. Bei Nutzung der Defaultwerte ist dieser Zeitraum < 1 Sekunde.

Wird der alte Master wieder aktiv, dann stellt er fest, dass er eine höhere Priorität als der aktuelle Master hat und übernimmt die Masterfunktion wieder. Dieser Vorgang heißt Preemption und kann ein- und ausgeschaltet werden. (Preemption_Mode = true (default))

Zusätzlich zu seiner IP-Adresse (Owner oder VIP) hat ein Master auch noch eine virtuelle MAC-Adresse (VMAC), die er einem Client auf einen ARP-Request hin zurücksendet.

Die MAC-Adresse baut sich bei IP-v4 folgendermaßen auf:

01-00-5E-00-01-<VRID>

01-00-5E ist der IANA-OUI

00-01 ist bei **IPv4** der für VRRP zugewiesene Adressblock

<VRID> ist die 1 Byte große Kennung für die VR

Die MAC-Adresse baut sich bei IP-v6 folgendermaßen auf:

01-00-5E-00-02-<VRID>

01-00-5E ist der IANA-OUI

00-02 ist bei **IPv6** der für VRRP zugewiesene Adressblock

<VRID> ist die 1 Byte große Kennung für die VR

Damit eventuell vorhandene Layer-2-Switches zwischen einem VR und einem Endgerät die Virtuelle MAC-Adresse schnell lernen, sendet der Master regelmäßig ARP-Requests, mit der virtuellen MAC-Adresse als Quell-Adresse an die VIP.

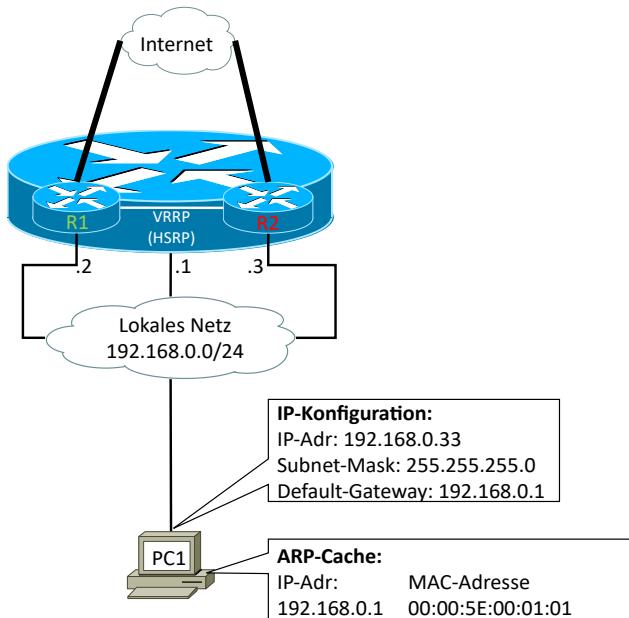


Abbildung 402: HSRP / VRRP

Ablauf

1. PC1 will eine Abfrage in das Internet senden. Dafür baut er einen Frame auf. Um den Frame aufzubauen benötigt er die MAC-Adresse seines Default-Gateways.
Dazu sendet PC1 einen ARP-Request als Broadcast aus, in dem er sein Default-Gateway mit der IP-Adresse 192.168.0.1 bittet, seine MAC-Adresse mitzuteilen.
2. Der Master-Router (R1) sendet die virtuelle MAC-Adresse (01-00-5E-00-01-01) mit einem ARP-Reply an den PC1 zurück und dieser vermerkt die MAC-Adresse in seinem ARP-Cache.
3. Danach kann der PC1 seinen Frame in das Internet über den aktiven Router (R1) senden.

Der Vorteil dieses Aufbaus ist, dass nur eine Konfiguration auf den Routern erforderlich ist. Durch die Verwendung von virtuellen MAC-Adressen muss bei einem Router-Wechsel der ARP-Cache bei den Netzwerkteilnehmern (ausgenommen Switches. Siehe oben) nicht aktualisiert werden.

Alternativen

Da VRRP Patente von Cisco verwendet, haben die Entwickler von Open BSD das Common Address Redundancy Protocol (CARP) als Alternative entwickelt.

Beispiel:

Virtuelle Router ID = 1

R1 (192.168.0.2) ist Master-Router. (Prio 200)

R2 (192.168.0.3) ist Backup-Router. (Prio 100)

Die zusätzliche virtuelle IP-Adresse (VIP) des Masters ist 192.168.0.1.

Der Master-Router übernimmt zusätzlich zu seiner eigenen IP-Adresse noch die virtuelle IP-Adresse und auch die zugehörige virtuelle MAC-Adresse.
(01-00-5E-00-01-01)

Der Master (R1) sendet mit einem Intervall von einer Sekunde Advertisements.

Fällt der Master-Router aus, übernimmt der Backup-Router die virtuelle IP-Adresse und die virtuelle MAC-Adresse innerhalb von 3 Sekunden.

24.23.4 - VRRP-Packet-Format

Relevante Teile des IP-Headers (v4/v6)								
TTL = 255 / Hop Limit = 255	Protocol = 112 (Next Header = 112)							
IP-Quelladresse								
IPv4-Zieladresse (224.0.0.18) / IPv6-Zieladresse (FF02:0:0:0:0:0:0:12)								
Version = 3 (4 Bit)	Type (4 Bit)	Virtual Router ID (8 Bit)	Priority (8 Bit)	Count IPvX Address (8 Bit)				
(reserviert) (4 Bit)	Max Advertisement Interval (12 Bit)		Checksum (16 Bit)					
IPvX Adressen (32 Bit / 128 Bit)								

IP-Quell-Adresse

Das ist die primäre IP-Adresse des sendenden Interfaces

IP-Zieldresse

Das ist die Multicastadresse (IPv4: 224.0.0.18 / IPv6: FF02:0:0:0:0:0:0:12). Router dürfen Pakete mit dieser Zieladresse nicht weiter leiten.

Time to Live = TTL (IPv4)/ Hop Limit (IPv6)

Dieser Wert muss immer auf 255 gesetzt sein. Bei anderen Werten wird das Paket verworfen. Damit ist sichergestellt, dass VRRP-Pakete aus anderen Netzwerken nicht verarbeitet werden.

Protocol (IPv4) / Next Header (IPv6)

Dieser Wert ist in allen IP-Versionen 112

Version

die aktuelle VRRP-Version ist 3

Type

Derzeit gibt es nur den Type 1 = ADVERTISEMENT

Virtual Router ID

In diesem Feld wird die virtuelle Router ID (VRID), die für dieses Paket gilt, definiert.

Priority

Hier spezifiziert der sendende Router seine Priorität für den virtuellen Router. Ein höherer Wert bedeutet eine höhere Priorität.

Die Priorität des VRRP-Routers, der Owner der IP-Adresse des virtuellen Router (VR) ist, muss den Wert 255 haben.

Backup-Router müssen eine Prioritätswert von 1 bis 254 haben. Der Default-Wert für die Priorität ist 100.

Mit dem Prioritäts-Wert 0 signalisiert der Master-Router, dass er seine VRRP-Teilnahme eingestellt hat. Damit müssen die Backup-Router nicht auf den Timeout warten und werden beschleunigt aktiv.

Count IPvX Address

Hier wird die Anzahl von IP-Adressen für dieses Advertisement festgelegt.

Reserviert

In diesem Feld muss 0 beim Senden stehen. Beim Empfang ist das Feld zu ignorieren.

Max Advertisement Interval

Zeitintervall für die Advertisements in Centi-Sekunden. Der Default wert ist 100 = 1 Sekunde.

Anwendungsbeispiele:

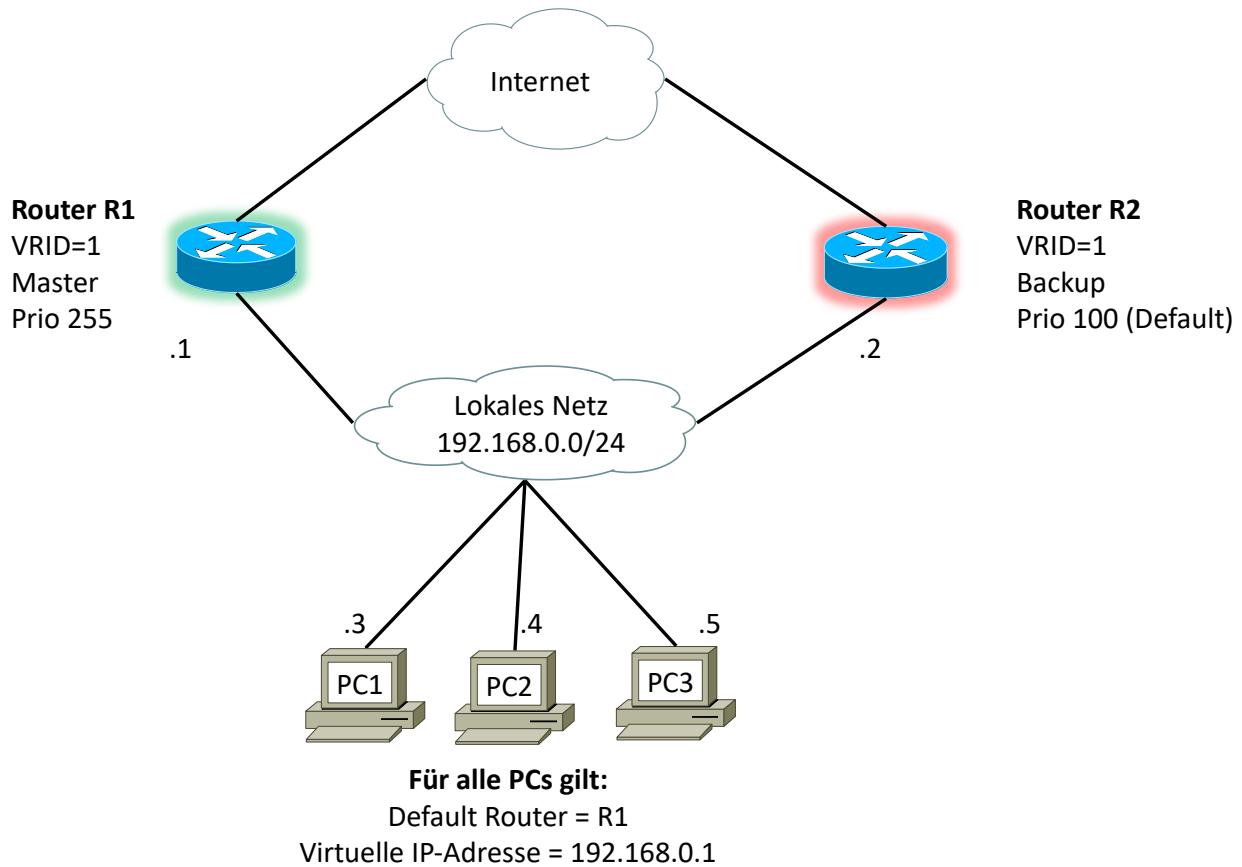


Abbildung 403: VRRP: Anwendungsbeispiel-1

An ein lokales Netzwerk (192.168.0.0/24) sind mehrere PCs angeschlossen. Alle haben als Default-Gateway-IP-Adresse die 192.168.0.1 eingetragen. Es gibt nur eine VRID und einer der beiden Router wird zum Master. Der andere Router wird zum Backup. Leider wird der Backup-Router nicht genutzt und so muss die gesamte Netzlast vom Master-Router abgearbeitet werden. Der Backup-Router hat Langeweile.

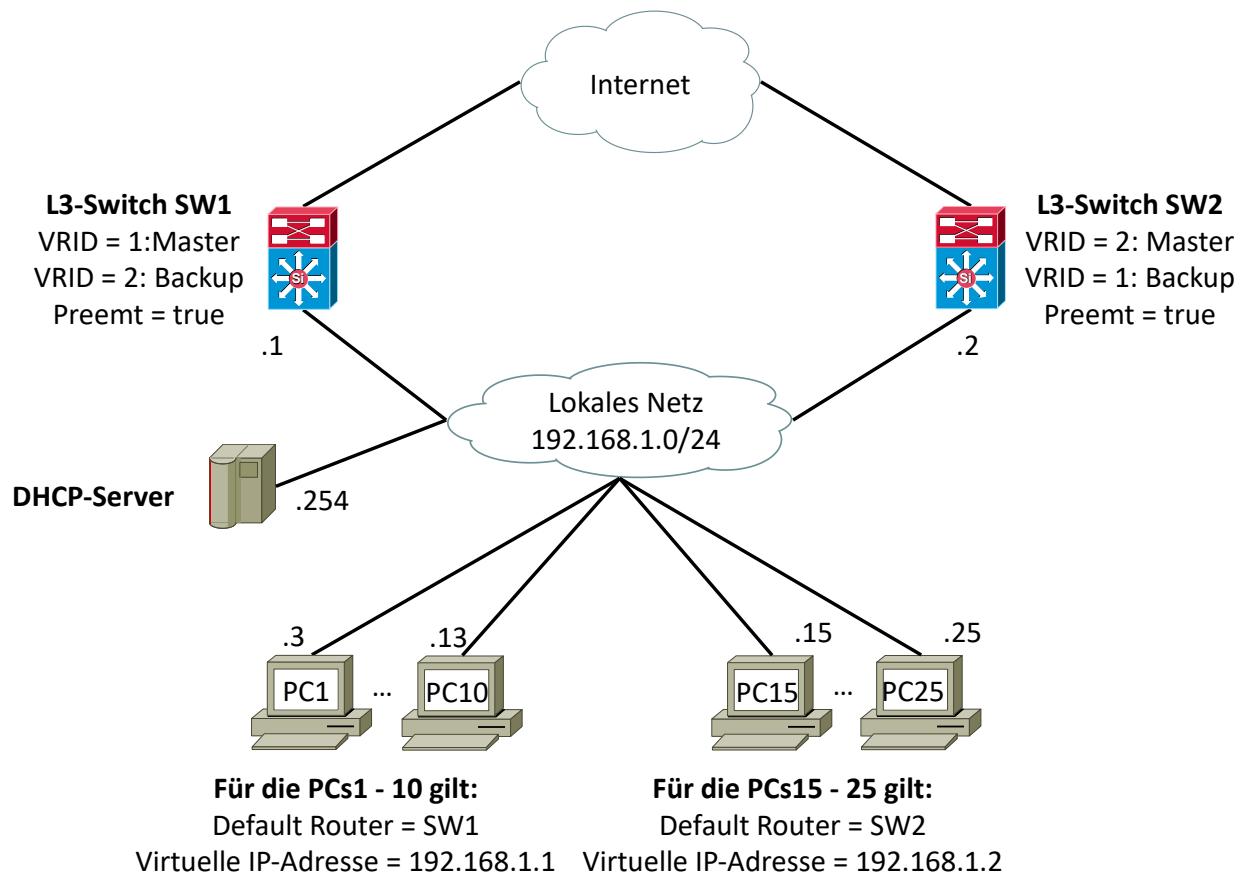


Abbildung 404: VRRP: Anwendungsbeispiel-2

Gibt es einen DHCP-Server im Netzwerk, kann ein Teil der angeschlossenen PCs dem L3-Switch SW1 und der andere Teil dem L3-Switch SW2 als Default-Gateway zugeordnet bekommen. Damit wird die Netzlast auf das auf beide L2-Switches verteilt und damit die vorhandenen Hardware besser ausgenutzt.

Dazu sind zwei VRIDs notwendig, die sich über Kreuz überwachen können. Damit kann der Ausfall einer der beiden L3-Switches abgefangen werden.

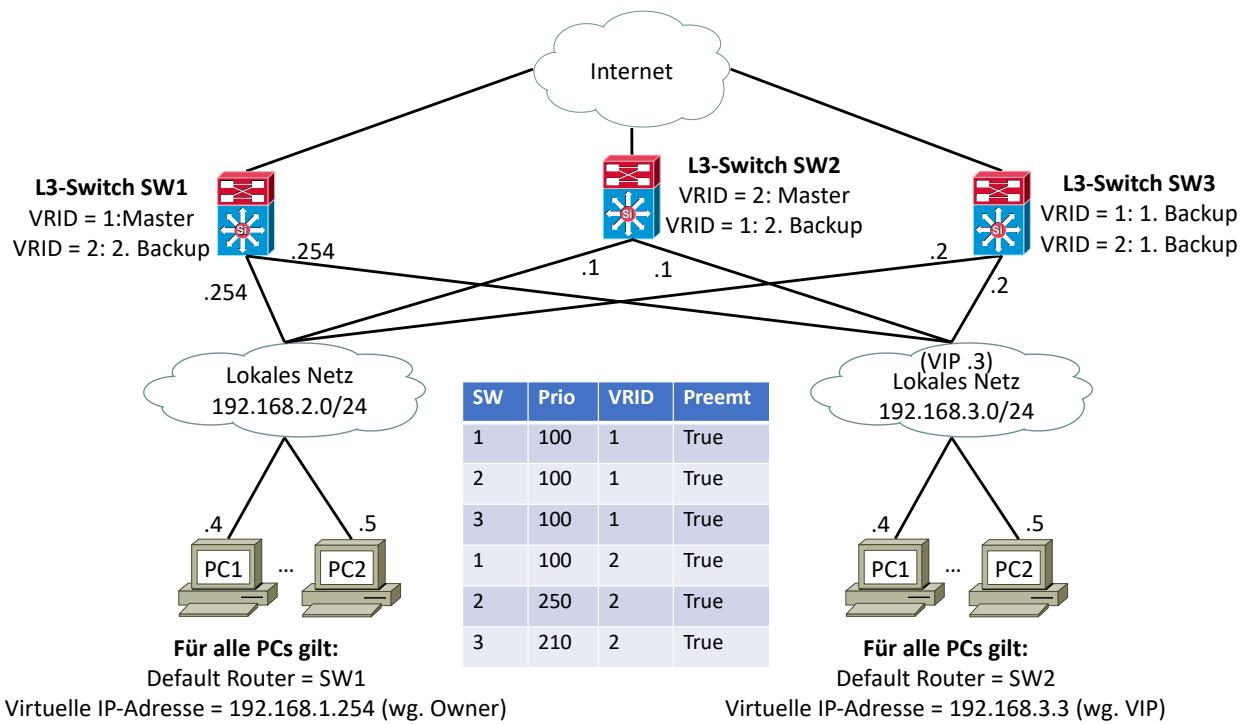


Abbildung 405: VRRP: Anwendungsbeispiel-3

Soll selbst bei einem Ausfall eines Routers immer noch eine Verteilung der Netzlast stattfinden, kann das mit einem dritten L3-Switch, wie im obigen Beispiel, umgesetzt werden.

Alle drei L3-Switches haben die gleiche Priorität für die VRID=1. Bei gleicher Priorität wird der L3-Switch mit der höchsten IP-Adresse zum Master. Deswegen wird SW1 zum Default Gateway für das Netzwerk 192.168.2.0/24.

Die VRID=2 wird mittels der Priorität gesteuert. Da der SW2 in der VRID=2 die Priorität 250 hat wird er zum Master. Er hat im Normalbetrieb zusätzlich die Virtuelle-IP-Adresse (192.168.3.3) auf sein Interface (mit der IP-Adresse 192.168.3.1) gebunden.

Damit wird gezeigt, dass es möglich ist, unterschiedliche Konfigurationsgrundlagen zu nutzen. Allerdings sollte für einen sicheren Betrieb eine konsistente (überall gleiche) Konfigurationsgrundlage genutzt werden. Hierbei ist die Zuordnung mit der höchsten IP-Adresse am unsichersten, denn durch weitere Router mit weiteren IP-Adressen, kann das gewünschte Ergebnis verloren gehen.

24.24 - ICMPv6

24.24.1 - Allgemeines

ICMPv6 wurde als Ergänzung für IPv6 entwickelt. Ihm kommt mehr Bedeutung und Funktionalität als bei der IPv4-Version zu. So wurden die Protokolle ARP und RARP in ICMPv6 integriert. Deshalb dürfen ICMPv6-Pakete nicht mehr grundsätzlich von Firewalls geblockt werden.

Folgende Funktionen werden behandelt:

- ➊ Fehlermeldungen
- ➋ Informationsmeldungen

24.24.2 - ICMPv6-Fehlermeldungen

Typ-Feld-Wert	Fehlermeldung	Code-Feld-Wert	Beschreibung
1	Destination unreachable	0 = No Route to Destination 1 = Communication administratively prohibited 2 = Not Assigned 3 = Address unreachable 4 = Port unreachable	Diese Meldung wird erzeugt falls das Paket nicht an das Ziel übergeben werden kann. Details stehen im RFC 2463
2	Packet too big	0	Bei zu großer MTU-Size wird das Paket verworfen und dem Sender wird damit mitgeteilt, dass er eine kleinere MTU-Size verwenden muss
3	Time Exceeded	0 = Hop-Limit exceeds 1 = Fragment-Reassembly-Time exceeded	Wenn ein Router ein Paket mit dem Hop-Limit-Wert = 0 empfängt, oder er selbst den Wert auf 0 dekrementiert, verwirft er das Paket und sendet diese Meldung an den Sender. Details stehen im RFC 2463
4	Parameter-Problem	0 = Fehlerhaftes-Header-Feld 1 = Unbekannter Next-Header 2 = Unbekannte IPv6-Option	Ein Parameter-Problem wurde erkannt. Details stehen im RFC 2463

24.24.3 - ICMPv6-Informationen

Typ-Feld-Wert	Information	Code-Feld-Wert	Beschreibung
128	Echo Request	0	Wird beim IPv6-Ping als Anfrage verwendet
129	Echo Reply	0	Wird beim IPv6-Ping als Antwort verwendet
130	Multicast Listener Query		
131	Version 1 Multicast Listener Report		
132	Multicast Listener done		
133	Router Solicitation Message	0	Ein Host fordert damit einen Router auf die Router-Advertisements zu senden. Siehe RFC 4861
134	Router Advertisement Message	0	Ein Router sendet seine Informationen in regelmäßigen Abständen oder auf Anforderung. Siehe RFC 4861
135	Neighbour Solicitation Message	0	Damit wird von einem Node eine Aufforderung zu Mitteilung seiner Link-Layer-Adresse gesendet, sowie die eigene Link-Layer-Adresse mitgeteilt. Siehe RFC 4861
136	Neighbour Advertisement Message	0	Damit wird von einem Node die eigene Link-Layer-Adresse mitgeteilt. Siehe RFC 4861
137	Redirect Message	0	Damit wird einem Host mitgeteilt, dass es eine bessere Route als die gerade verwendete gibt. Siehe RFC 4861
138	Router Renumbering		
139	ICMP Node Information Query		Siehe RFC 4620
140	ICMP Node Information Response		Siehe RFC 4620
141	Inverse Neighbour Discovery Solicitation Message		Siehe RFC 3122
142	Inverse Neighbour Discovery Advertisement Message		Siehe RFC 3122
143	Version 2 Multicast Listener Report		Siehe RFC 3810
144	Home Agent Address Discovery Request Message		Siehe RFC 3775

Typ-Feld-Wert	Information	Code-Feld-Wert	Beschreibung
145	Home Agent Address Discovery Reply Message		Siehe RFC 3775
146	Mobile Prefix Solitication		Siehe RFC 3775
147	Mobile Prefix Advertisement		Siehe RFC 3775
148	Certification Path Solicitation Message		Siehe RFC 3971
149	Certification Path Advertisement Message		Siehe RFC 3971
150	ICMP Message for experimental mobility protocols		Siehe RFC4065
151	Multicast Router Advertisement		Siehe RFC 4286
152	Multicast Router Solicitation		Siehe RFC 4286
153	Multicast Router Termination		Siehe RFC 4286
200	Private experimentation		
201	Private experimentation		
255	Reserved for Expansion of ICMPv6		

24.24.4 - Typ-Längen-Werte (TLVs) / Optionen für Neighbour Discovery ICMP Meldungen

Type	Option	Beschreibung
1	Source-Link-Layer-Address	Enthält die Link-Layer-Adresse des Senders. Wird bei Neighbour-Solicitation- und bei Router-Advertisement-Paketen verwendet
2	Target-Link-Layer-Address	Enthält die Link-Layer-Adresse des Ziels. Wird bei Neighbour-Solicitation- und bei Router-Advertisement-Paketen verwendet
3	Prefix-Information	Dient zur Versorgung von Hosts mit on-link-Prefixes und für die Address-Autoconfiguration
4	Redirect-Header	Bei Redirect-Vorgängen wird ein Teil oder das gesamte Paket dem Sender mitgeteilt
5	MTU	Wird bei Router-Advertisements verwendet um sicher zu stellen, dass alle Nodes die gleiche MTU-Size verwenden

24.25 - DHCPv6

24.25.1 - Allgemeines

Das Dynamic Host Control Protocol musste im Rahmen des Umstiegs von IPv4 auf IPv6 eine Renovierung über sich ergehen lassen und bekam, passend zur Nummerierung von IP, auch die Version 6.

Ziel der Konzeption von IPv6 war eine automatische Vergabe von IP-Adressen, um eine rudimentäre Kommunikation zu ermöglichen. Dies wird in einem Autokonfigurationsvorgang durchgeführt.

Im Gegensatz zur Vorgängerversion von IP, ist für die Vergabe von IP-Adressen um im lokalen Netzwerk zu kommunizieren, ist kein DHCP-Service erforderlich. Dafür übernehmen die Router für die grundlegende Kommunikation eine aktive Rolle.

24.25.2 - Autokonfiguration

Wird ein Client eingeschaltet, so durchläuft er die folgenden Schritte, um sich mit IP-Adressen zu versorgen.

1. Senden einer Router-Solicitation-Nachricht an die Link-Local-All-Routers-Multicast-Adresse (ff02::2).
2. Ist ein Router im Netzwerk vorhanden, wird er mit einer Router-Advertisement-Nachricht antworten. Darin ist der globale IPv6-Präfix enthalten. Aus diesem Präfix kann der Client zusammen mit seiner MAC-Adresse und dem EUI-Verfahren (Extended Unique Identifier) seine global gültige IP-Adresse aufbauen.
3. Verwendet der Client die Privacy Extensions, wird zusätzlich zur globalen IP-Adresse (mit EUI-64-MAC-Adresse) eine temporäre IP-Adresse erzeugt. Dabei kommt anstelle der MAC-Adresse, ein vom Betriebssystem zufällig ermittelter Wert, für den Interface-Teil der IPv6-Adresse zum Einsatz. Um sicher zu stellen, dass eine zufällig erzeugte IP-Adresse nicht bereits im Netzwerk existiert, wird mittels einer Duplicate Address Detection (DAD) die neu erzeugte IP-Adresse überprüft, bevor sie verwendet werden kann.

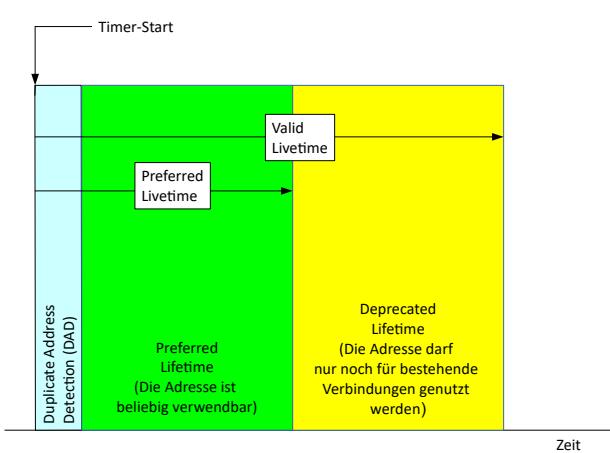


Abbildung 406 : IP-Adress-Lifetime

Über RAs erzeugte IP-Adressen haben einen Valid-Lifetime. Das entspricht der Lease-Time von mit DHCP erzeugten IP-Adressen. Die Valid-Lifetime ist die gesamte Gültigkeitsdauer von der Erzeugung bis zum Löschen. Innerhalb dieses Zeitraums ist eine Adresse zuerst preferred danach deprecated. Während der Preferred-Lifetime verwendet der Rechner diese IP-Adresse. Danach (während der Deprecated-Lifetime) wird die IP-Adresse nur noch für bestehende Verbindungen genutzt. Nach Ablauf der Valid-Lifetime wird die IP-Adresse gelöscht.

Mit der Absender-Adresse des Routers wird gleichzeitig auch das Default Gateway festgelegt.

Unterstützen Router und Client die RDNSS-Option (Recursive DNS Server) wie im RFC 6106 beschrieben, kann die Adresse des DNS-Servers auch über die RAs mitgeteilt werden.

Damit ist die Autokonfiguration mittels der Router-Advertisements (RA) abgeschlossen. Da die IP-Adressen der Clients nirgendwo gespeichert / verwaltet werden, heißt dieses Verfahren Stateless Address Autoconfiguration (SLAAC).

Die Router senden in regelmäßigen Zeitabständen die RAs an die Link-Local-All-Nodes-Multicast-Adresse (ff02::1), damit die Clients die Konfiguration auf dem neuesten Stand halten können.

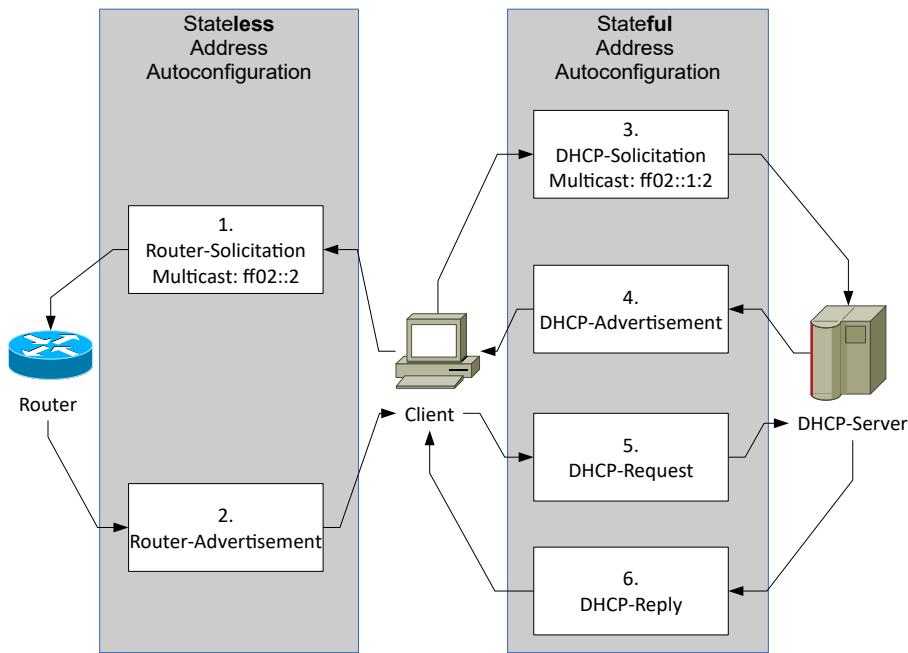


Abbildung 407 : DHCPv6-Ablauf

24.25.3 - Bearbeitung der DHCP-Informationen

Für weitere Informationen, wie etwa die IP-Adresse des NTP-Servers, ist dann allerdings ein DHCP-Server erforderlich.

Dafür verwendet DHCPv6 die folgenden udp6-Ports:

546 (Client)

547 (Server)

Der Ablauf hierzu sieht - ähnlich wie bei IPv4 - folgendermaßen aus:

1. Der Client sendet eine Solicitation-Nachricht an die Link-Local-All-DHCPServers-Multicast-Adresse ff02::1:2.
2. Darauf hin antworten die vorhandenen Server mit einer Advertisement-Nachricht. Sie enthält die IP-Adresse des Clients sowie die IP-Adressen von DNS- / NTP-Server und sonstige Informationen.
3. Der Client wählt sich seine Parameter aus und fordert sie beim entsprechenden DHCP-Server mit einer DHCP-Request-Nachricht an.
4. Der DHCP-Server speichert die Information mit der Client ID und Antwortet dem Client mit einer DHCP-Reply-Nachricht. Da die Information im DHCP-Server verwaltet wird, nennt man diese Vorgehensweise Stateful Address Autoconfiguration. Alle anderen evtl. vorhandenen DHCP-Server.

Damit kann der Client nun im Netz kommunizieren.

Der größte Unterschied im Vergleich zu IPv4 liegt darin, dass die Default-Route vom Router mittels der RAs und nicht vom DHCP-Server vergeben wird.

Zur vollständigen Autokonfiguration sind also RAs und der DHCP-Service erforderlich.

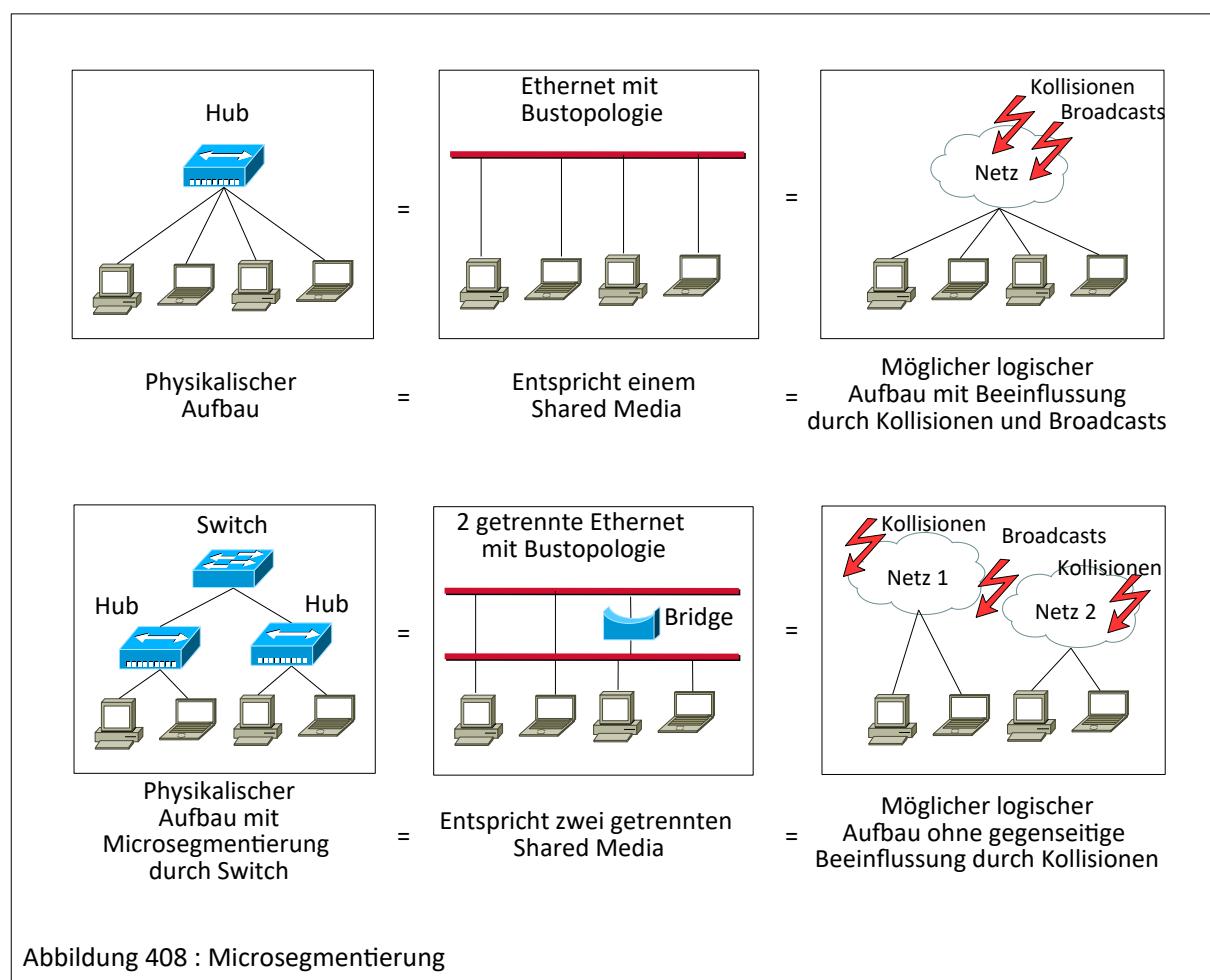
Derzeit wird ein Vorschlag diskutiert der die Verteilung der Default-Gateways auch über den DHCP-Service (also ohne RAs) vorsieht. Allerdings ist noch offen, ob dieser Vorschlag zum Tragen kommt.

24.26 - Virtuelles LAN (VLAN)

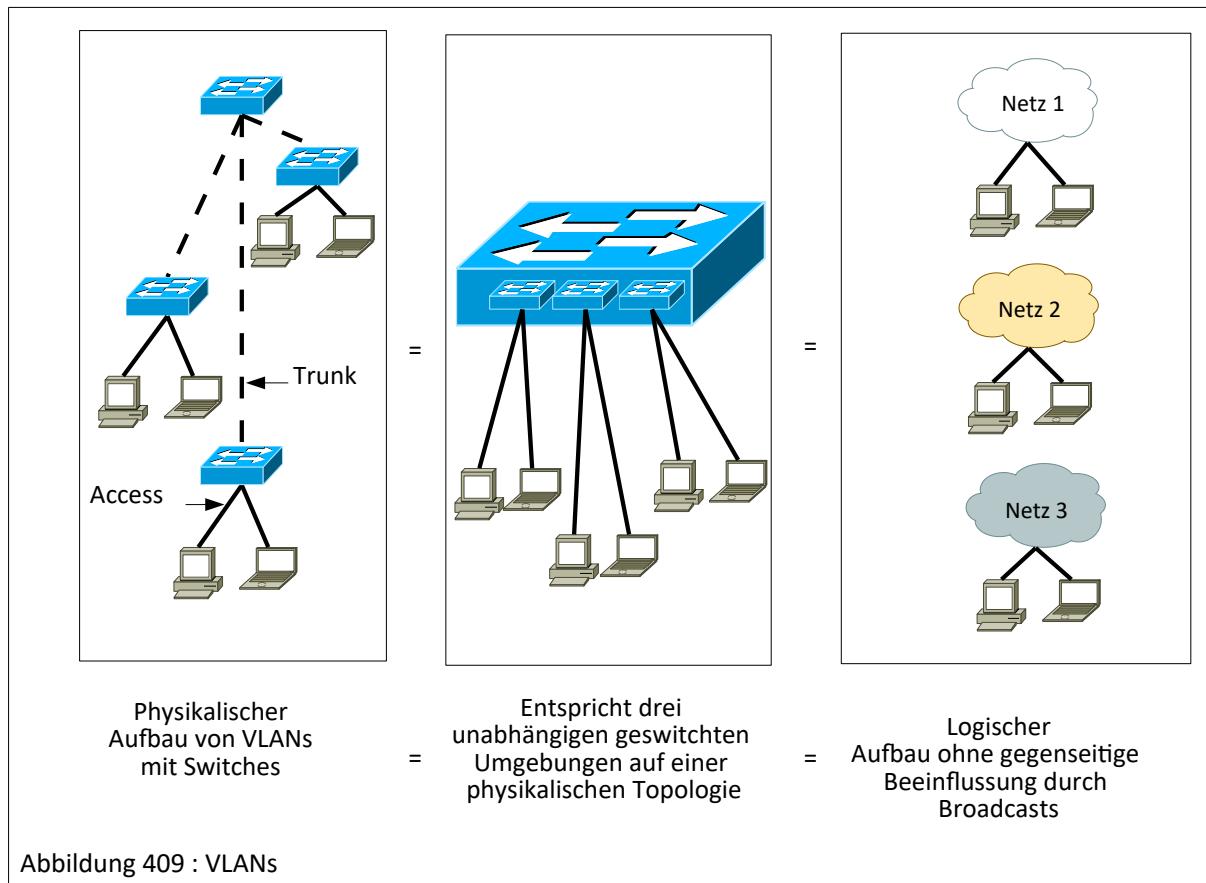
25 - Einführung

Ein LAN ist abhängig von der physikalischen Struktur und damit von den verwendeten Komponenten mit denen es realisiert wurde. So können z. B. die angeschlossenen Knoten mit Hubs zusammengefasst werden oder an einen Bus mit Transceivern angeschlossen werden. Es sind auf einem Ethernet mehrere logische Netzwerke realisierbar. Obwohl sie gegenseitig nicht angesprochen werden können (solange es keinen Router zwischen den Netzwerken gibt), beeinflussen sich die Netzwerke durch evtl. auftretende Kollisionen oder Broadcasts. Damit sind alle Knoten in einer Collisiondomain / Broadcastdomain zusammengefasst.

Dies bedeutet sowohl eine gegenseitige Beeinflussung als auch eine Aufteilung der verfügbaren Bandbreite über alle angeschlossenen Knoten.



Durch Microsegmentierung mit Switches oder Brücken können die Collisiondomains verkleinert werden. In den Microsegmenten gibt es immer noch Kollisionen! Außerdem sind alle angeschlossenen Knoten immer noch innerhalb einer Broadcastdomain.



Um VLANs in seiner vollen Funktionalität anzuwenden, ist die Verwendung managebaren Switches erforderlich. Moderne nicht manageable Switches können mit getaggten Paketen umgehen, jedoch keine Tags einfügen und auch nicht entfernen.

Ein VLAN wird mit Switches realisiert. Dies bedeutet, dass es keine Kollisionen mehr gibt. Jeder geswitchte Port kann einem VLAN zugeordnet werden. Für die Teilnehmer einer Gruppe sieht es so aus als ob es nur diese Gruppe gäbe. Die Anzahl der VLANs ist auf maximal 4096 begrenzt.

Ein VLAN ist eine Broadcast-Domain was bedeutet, dass alle Ports, die einem VLAN zugeordnet sind, die Broadcasts dieses VLANs erhalten. Ports eines Switches die nicht zu diesem VLAN gehören, erhalten die Broadcasts nicht.

Somit sind Kollisionen eliminiert und Broadcasts reduziert.

Weiterhin gibt es für jedes VLAN einen Spanning-Tree.

26 - VLANs portbasiert oder getagged

26.1.1.1 - Portbasiert

Die Hersteller ordnen bei der Auslieferung alle Switchports einem Default VLAN, dem VLAN-1, zu. VLANs können jedoch bei manageablen Switches vom Administrator einem Switchport zugewiesen werden. Diese Ports sind „portbasiert“ einem VLAN zugewiesen. Damit kann an diesem Port nur das konfigurierte VLAN transportiert werden.

Wie in der folgenden Abbildung auf der rechten Seite zu sehen ist, sind die einzelnen VLANs logisch voneinander isoliert und haben untereinander keine Verbindung.

Auf jedem Switch sind die VLANs voneinander getrennt! Um die grünen Ports auf dem linken Switch mit den grünen Ports auf dem rechten Switch zu verbinden, müsste bei portbasierten VLANs, eine eigene Verbindung hergestellt werden. Dies gilt für jedes VLAN! Damit müssten mehrere Verbindungen hergestellt werden die unter Umständen schlecht ausgelastet wären.

26.1.1.2 - Getaggt

Um zwischen Switchen unterschiedliche VLANs über nur eine Verbindung zu transportieren, müssen die Switches die Pakete unterschiedlicher VLANs voneinander unterscheiden können, um sie bei der Auslieferung an den richtigen Ports ausgeben zu können.

Dazu erhalten die Pakete bei einer Verbindung, die unterschiedliche VLANs transportieren kann Zusatzinformationen, die so genannten Tags. Die Pakete werden vor der Ausgabe an einem getaggten Port mit der 4 Byte großen Tag-Information ergänzt. Darin sind die VLAN-Eigenschaften eines jeden Paketes hinterlegt. Ports, die Pakete mit einem Tag transportieren können, werden Trunk- oder Tagged-Ports genannt. Moderne Switches, die nicht manageable sind, können zwar VLANs transportieren, jedoch keine Tags bearbeiten.

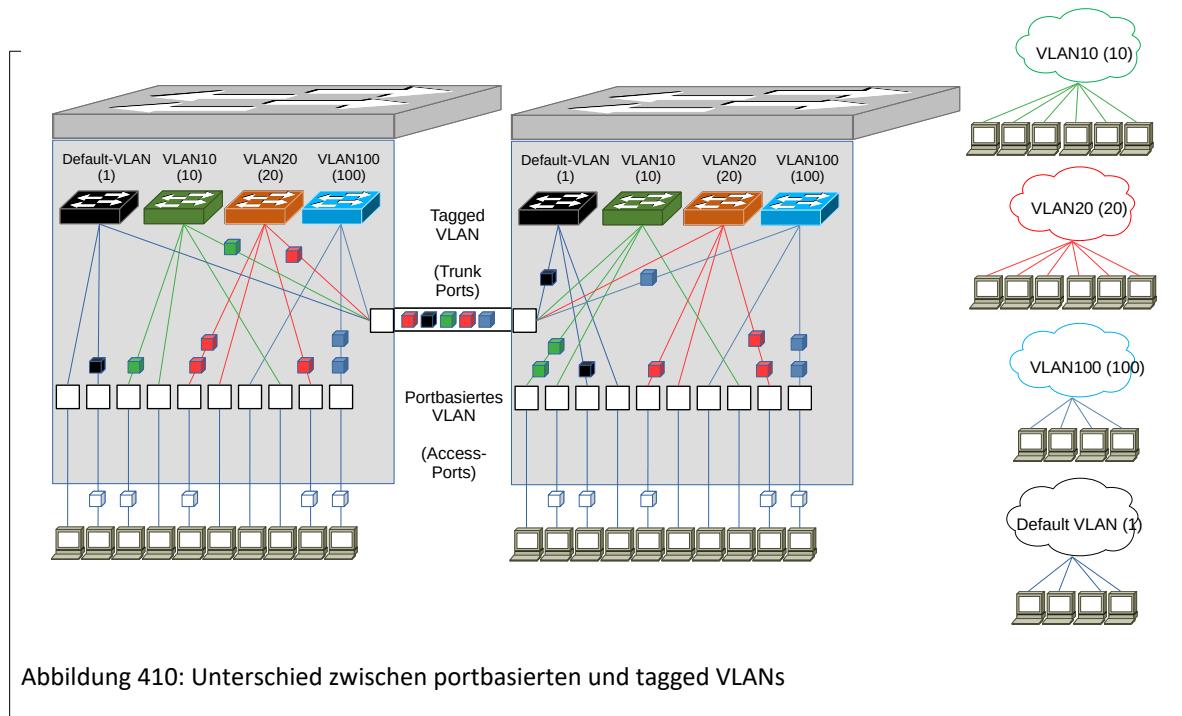


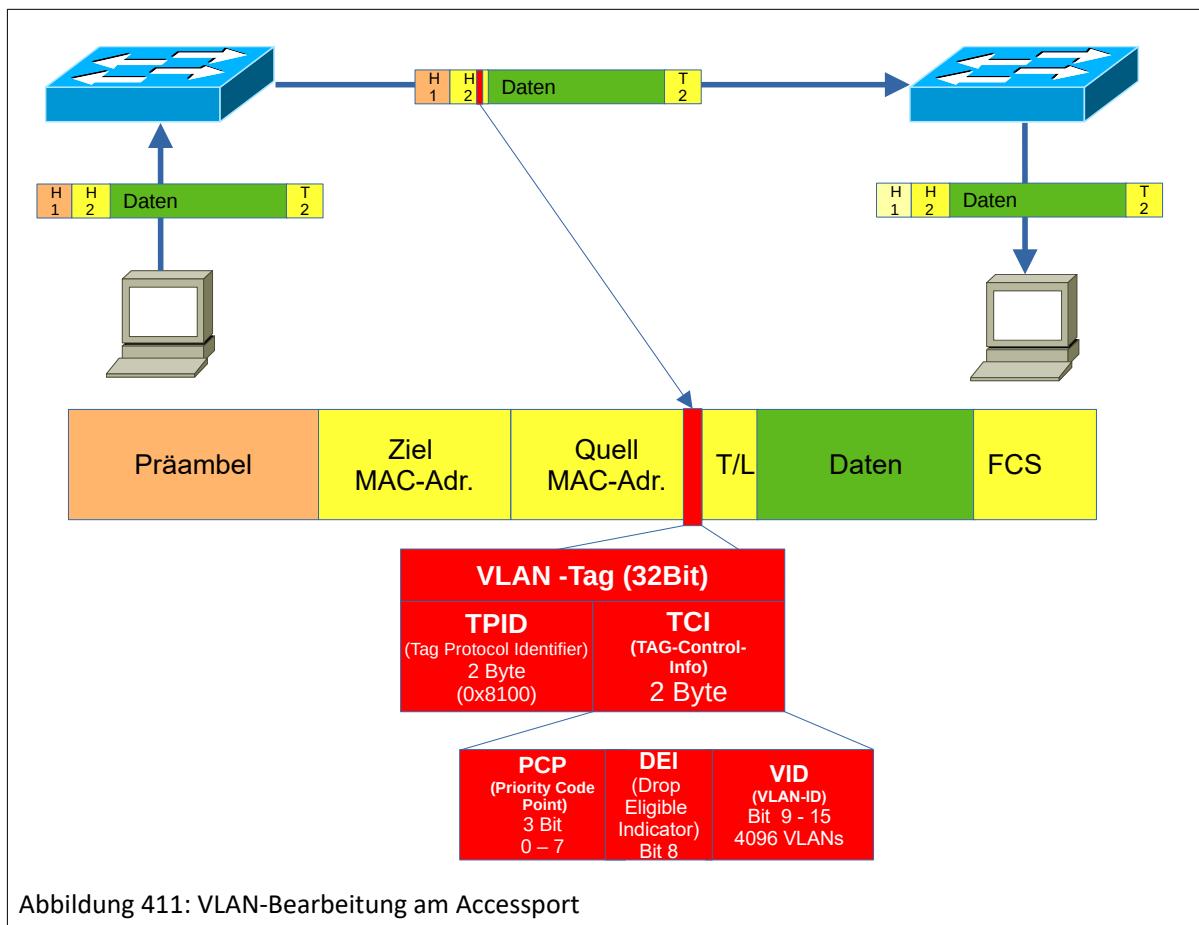
Abbildung 410: Unterschied zwischen portbasierten und tagged VLANs

In der obigen Abbildung sind die Ports der Switches an der unteren Seite alle portbasiert den VLANs zugeordnet. An den Ports können nur die Pakete der zugewiesenen VLANs bearbeitet werden.

Die Verbindung zwischen den Switches ist getaggt. Hier können alle VLANs transportiert werden.

27 - VLAN-Tagging

Protokolle



Sobald ein Switchport einem VLAN zugeordnet ist kann die Verbindung vom Endgeräten zum Switch im Access-Modus betrieben werden. Dabei wird keine VLAN-Information zwischen Switch und Endgerät ausgetauscht. Ein Endgerät an einem Accessport bekommt von einem VLAN nichts mit. Deshalb muss der Accessport an einem Switch, ein von einem Endgerät kommendes Paket, um die VLAN-Information ergänzen. Beim einem Paket, das an ein Endgerät ausgeliefert werden soll, ist die VLAN-Information zuerst vor der Auslieferung zu entfernen.

Der Tag wird zwischen der Ziel-MAC-Adresse und dem Typ- / Längen-Feld eingefügt.

Mit den 12 Bits für die VLAN-ID können bis zu 4096 unterschiedliche VLANs adressiert werden.

Mit den 3 Bits für die Priorisierung können 8 unterschiedliche Prioritäten festgelegt werden. So lassen sich z. B. Sprachdaten vor HTTP-Daten bevorzugen.

Die Verbindungen zwischen den Switches werden in Trunk-Modus betrieben. Im Trunk-Modus können mehrere unterschiedliche VLANs über eine Verbindung transportiert werden. Dazu werden die Verbindungen entweder über proprietäre Protokolle wie das ISL (Inter Switch Link von CISCO) oder nach IEEE-802.1q (VLAN Tagging) betrieben.

Um unterschiedliche VLANs zu verwalten gibt es noch weitere proprietäre Protokolle wie z. B. das VTP (Virtual Trunk Protocol) von Cisco.

Der eingefügte Tag kann zu Problemen führen falls der Frame bereits die maximale Framegröße von 1518 Bytes hatte. Dadurch würde sich der Frame um weitere 4Bytes auf eine unzulässige Größe aufblähen.

28 - VLANs in unterschiedlichen Ebenen

VLANs können auf verschiedenen Ebenen aufgebaut werden:

- Layer 1

Switch-Port basierend

Jedem Switchport wird durch den Administrator ein VLAN zugewiesen. Dies kann von einer zentralen Managementstation aus oder direkt am Switch über eine Consol-Verbindung durchgeführt werden. Unterlässt der Administrator dies, werden alle Ports in das Default-VLAN (VLAN 1) übernommen. Damit können Switches auch ohne eine VLAN-Parametrierung in Betrieb genommen werden. Allerdings hat man dann alle Endgeräte in der gleichen Broadcastdomain untergebracht. Die einzelnen VLANs sind autonom. D. h. es gibt vorerst keine Verbindung zwischen den VLANs dazu muss eine Routinginstanz die Verbindungen herstellen.

- Layer 2

MAC-Adressen basierend

Alle Rechner werden an zentraler Stelle mit ihrer MAC-Adresse einem VLAN zugeordnet. Dazu ist auf einem Server die Zuordnungstabelle allen Switches zur Verfügung zu stellen die sich im Bedarfsfall die Tabelle vom Server beziehen. Sobald nun ein Rechner mit einem Switch verbunden wird, kann aufgrund der MAC-Adresse der Switchport in das zugeordnete VLAN übernommen werden. Hier ist z. B. Das Cisco-Protokoll VMPS (VLAN Membership Policy Server) angesiedelt.

- Layer 3

Protokoll basierend

Hier werden IP-Adressen einem VLAN zugeordnet. Die Zuordnung der Ports zu VLANs erfolgt über ein dynamisches VLAN-Protokoll.

- Layer 4

TCP/IP-Port basierend

Hier werden TCP- oder UDP-Ports einem VLAN zugeordnet. Die Zuordnung der Ports zu VLANs erfolgt über ein dynamisches VLAN-Protokoll.

29 - Sicherheit von VLANs.

Als relativ sicher kann nur ein statisches VLAN, also auf Layer 1, angesehen werden. MAC oder IP-Adressen sind einfach zu fälschen. Doch selbst ein statisches VLAN kann nicht als 100%iger Schutz angesehen werden. Es gibt hierzu diverse Angriffsszenarien die die Trennung der portbasierten VLANs aufheben können. So haben z. B. die Switches diverser Hersteller die Eigenschaft, sobald die Last in eine Sättigungsbereich läuft, alle VLANs, an allen Ports weiterzuleiten. Eine weitere unschöne Erscheinung sind Programme wie macof oder dsniff. Sie sind in der Lage Rahmen mit unterschiedlichen Sende-MAC-Adressen zu generieren. Dadurch werden die MAC-Adresstabellen der Switches geflutet. Sobald sie die Grenzen erreichen schalten Switches in die nächst schlechtere Betriebsart und mutieren somit zum Repeater. Damit werden alle Rahmen auf allen Ports ausgegeben und ein Angreifer kann somit den gesamten Traffic aller Ports mitbekommen.

VLANs können statisch oder dynamisch verwaltet werden.

- Durch einen Administrator können Ports statisch zugeordnet werden.
- Bei der dynamischen VLAN-Verwaltung wird einem Port dann ein VLAN zugewiesen wenn das entsprechende Endgerät angeschlossen wird. Hierbei wird z. B. mittels der MAC-Adresse die VLAN-Zugehörigkeit ermittelt und dem Switchport, an dem das neue Gerät angeschlossen ist, zugewiesen. Beispiel VMPS (VLAN Membership Policy Server) von Cisco.

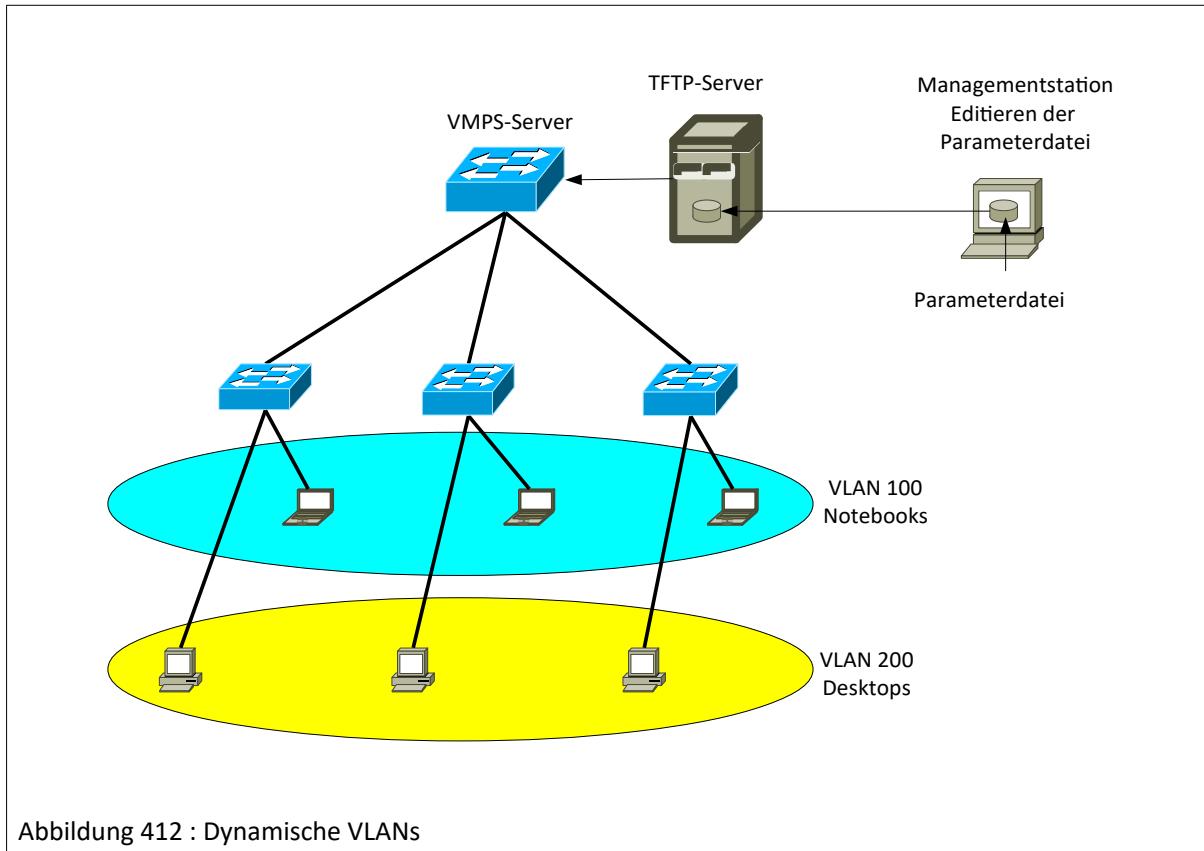


Abbildung 412 : Dynamische VLANs

Im obigen Beispiel werden die VLANs den Geräten an den Switchports zugewiesen. Es sind 2 VLANs definiert. Ein VLAN dient zum Verbinden aller Desktop Geräte und das andere VLAN dient zum Verbinden der Notebooks. Sobald nun ein Gerät an einen beliebigen Switch angeschlossen wird, stellt der Switchport die MAC-Adresse des Geräts fest. Aufgrund der MAC-Adresse wird der Switchport einem VLAN zugeordnet und freigeschaltet. Um die Port-Zuordnung durchführen zu können ist eine Parameterdatei zu erstellen und auf einem TFTP-Server zur Verfügung zu stellen. Ein VMPS-Master-Server (Switch) holt die Parameterdatei von TFTP-Server und verteilt sie auf alle Switches, die diese Informationen verarbeiten sollen.

Damit kann ein Mitarbeiter an einem beliebigen Arbeitsplatz, an dem ein Switchport verfügbar ist mit seinem Gerät arbeiten ohne, dass ein zusätzlicher administrativer Eingriff notwendig ist.

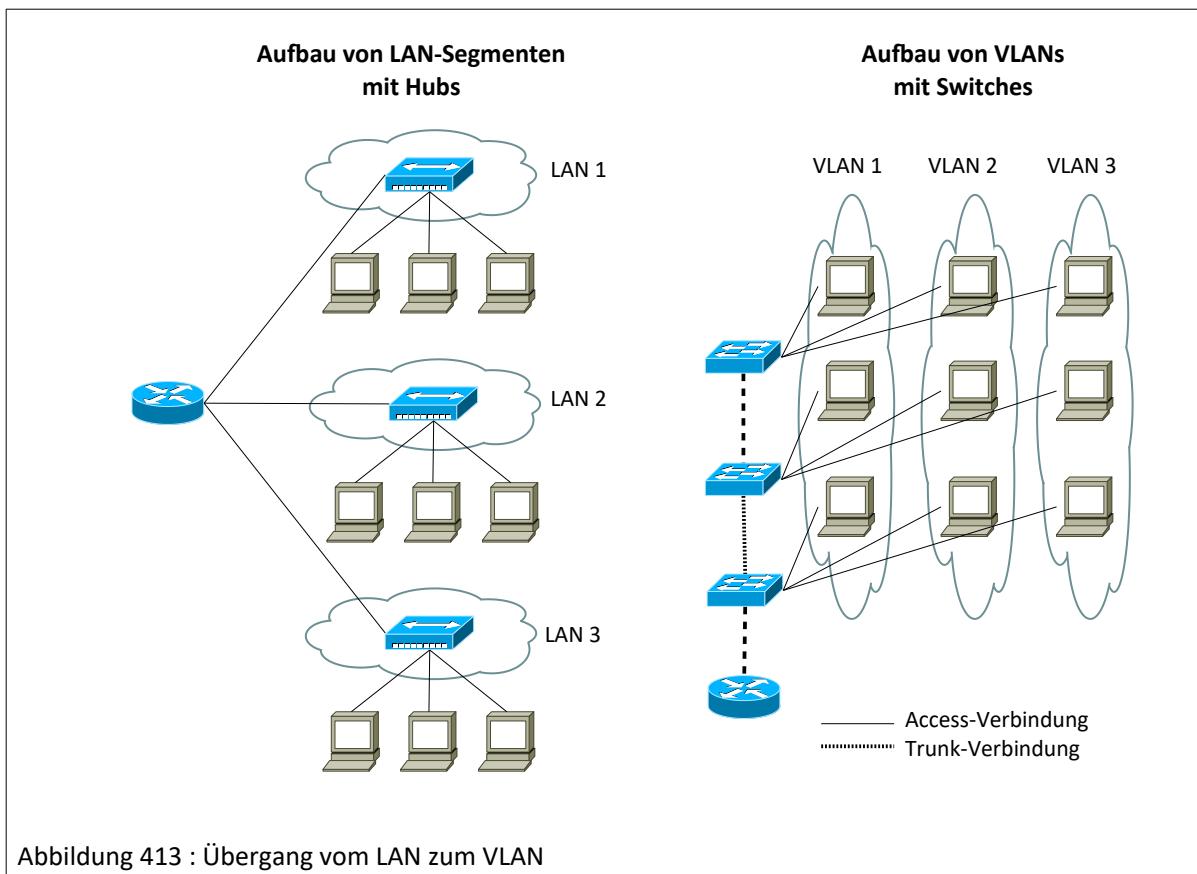


Abbildung 413 : Übergang vom LAN zum VLAN

30 - Beispiel 1:

Einzelne LANs können mit Hubs oder Switches aufgebaut werden. Ein Router kann die einzelnen LANs miteinander verbinden und ermöglicht somit eine Kommunikation über Netzwerkgrenzen hinweg.

Will nun ein Netzteilnehmer aus einem LAN in den Bereich eines anderer LANs umziehen, dann muss entweder eine neue Verkabelung für ihn aus dem alten in den neuen Bereich installiert werden, oder es werden VLANs eingesetzt.

Werden die Hubs durch VLAN-fähige Switches ersetzt, dann kann an jedem Switchport ein beliebiges VLAN parametriert werden. Die Verbindungen zwischen den Switches werden zu Trunks zusammengefasst. Trunks sind in der Lage verschiedene VLANs zu übertragen. Dazu sind spezielle Protokolle notwendig. Z. B. ISL (CISCO-proprietäre Variante von IEEE-802.10), VLT (Virtual LAN Trunk) von 3COM oder IEEE-802.1q.

31 - Beispiel 2:

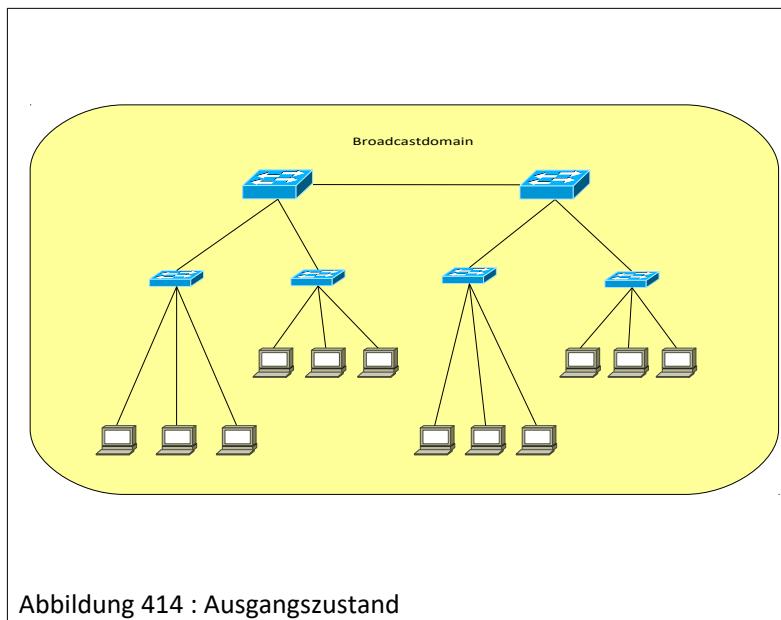


Abbildung 414 : Ausgangszustand

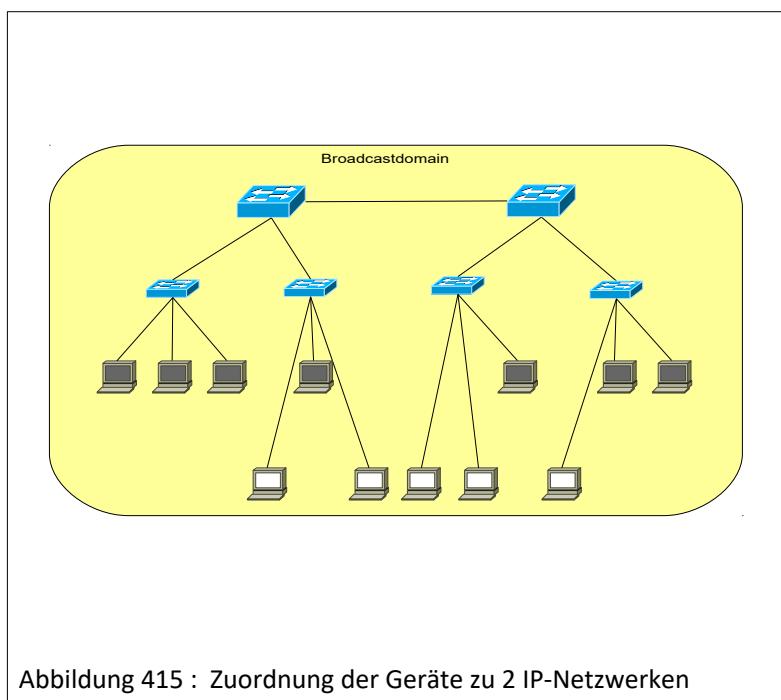
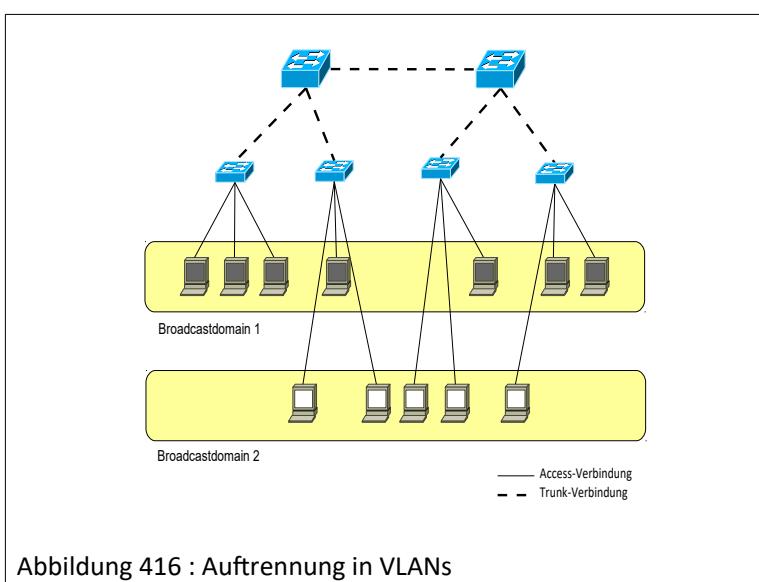


Abbildung 415 : Zuordnung der Geräte zu 2 IP-Netzwerken

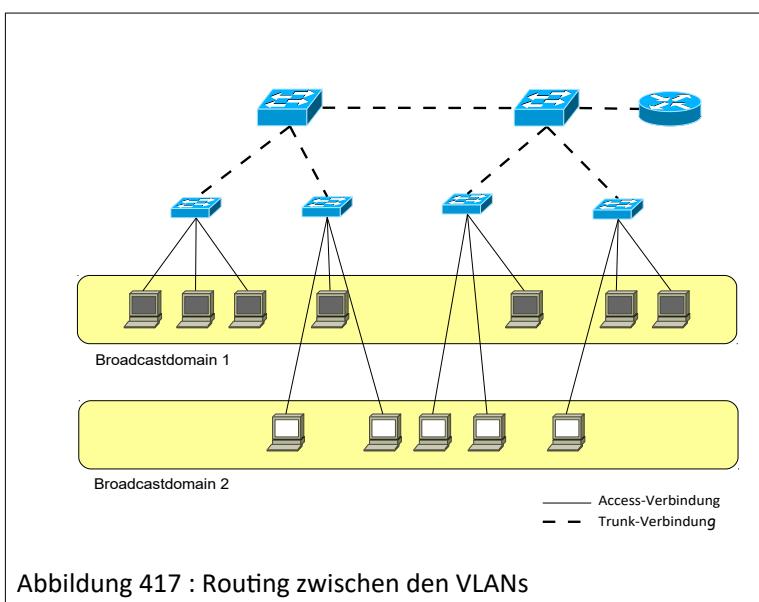


Im nächsten Schritt werden die beiden IP-Netzwerke zu zwei unterschiedlichen VLANs zugeordnet.

Nun beeinflussen sich die beiden Netzwerke (VLANs) nicht mehr gegenseitig.

Die Switchports werden in Access-Ports oder Trunk-Ports unterteilt.

Allerdings haben die Netzwerke immer noch keine Verbindung miteinander. Dies bedeutet, dass nur innerhalb eines Netzwerks kommuniziert werden kann. Über Netzwerk-Grenzen hinweg gibt es noch keine Kommunikations-Möglichkeit.



Die Trunks sind in der Lage alle Rahmen, die den verschiedenen VLANs angehören, zu übertragen. Dazu werden die Rahmen mit Markierungen (Tags) versehen, um sie den einzelnen VLANs zuzuordnen.

Damit auch zwischen den Netzwerken kommuniziert werden kann ist ein Router notwendig.

Hierzu stehen entweder externe Router oder Routing-Module für die Switches zur Verfügung. Ein Switch mit Routing-Funktionalität, wird auch Layer3-Switch genannt.

32 - Eigenschaften von VLANs

Vereinfacht IMAC/D (Insert, Move, Add, Change und Disposal) von Netzwerkeinheiten.

Erhöhen Workgroup und Netzwerksicherheit.

Nur auf die definierten VLANs kann an den einzelnen Ports zugegriffen werden.

Begrenzung von Broadcasts

Netzlast durch Broadcasts gibt es in jedem Netzwerk. In einem schlecht geplanten Netzwerk kann das Netzwerk durch Broadcasts stark beeinträchtigt werden.

Zentralisieren von Administration möglich

VLANs können einfach von einer zentralen Managementstation aus verwaltet werden.

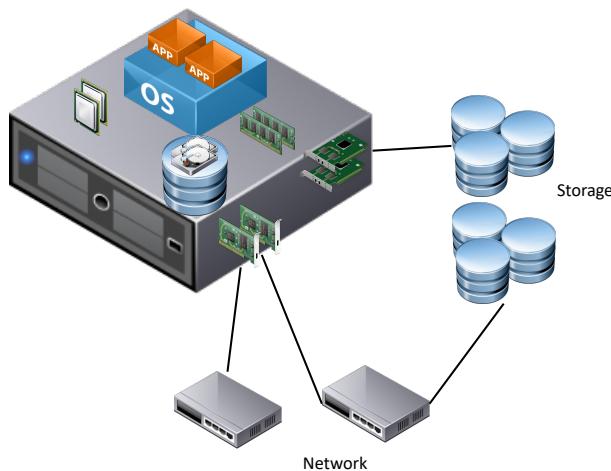
Priorisierung von Protokollen und somit von Applikationen ist möglich.

Für die Verwaltung von Netzwerk-Komponenten (Router oder Switches) empfiehlt sich die Einrichtung eines eigenen Management-VLANs.

Dies hat den Vorteil, dass die IP-Adressen für die Parametrierung der Netzwerk-Komponenten für einen normalen Benutzer nicht sichtbar sind da er sich in einem anderen Netzwerk befindet.

32.1 - Software Defined Networks (SDN)

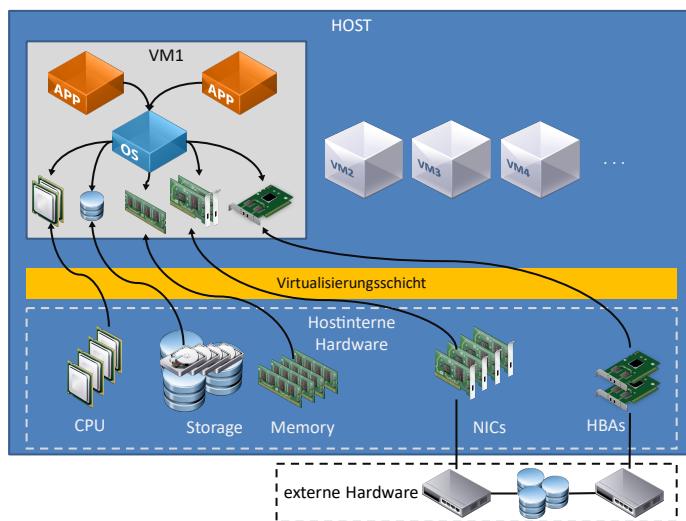
32.1.1 - Einführung



In klassischen Servern sind die Hardware-Komponenten Motherboard, CPU, Speicher, SSDs und Festplatten sind in einem Gehäuse verbaut.

Extern sind Netzwerke und Storage-Systeme über die entsprechenden Controller (NICs und HBAs) anschließbar

Die Applikationen sind über das Betriebssystem mit den Hardwarekomponenten und den externen Systemen verbunden



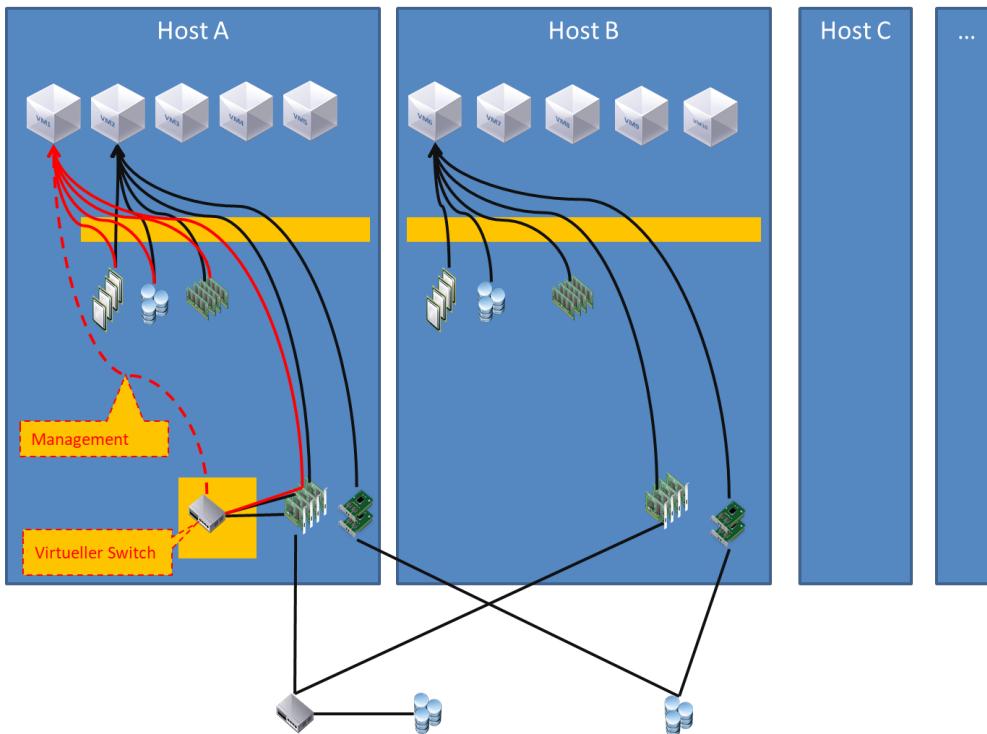
Durch Virtualisierung können auf einem Host-System unterschiedliche Mengen der vorhandenen Host internen Hardware-Komponenten einer virtuellen Maschine (VM) zugewiesen werden.

Die Applikationen können über das Betriebssystem (OS) auf die Komponenten der VM zugreifen.

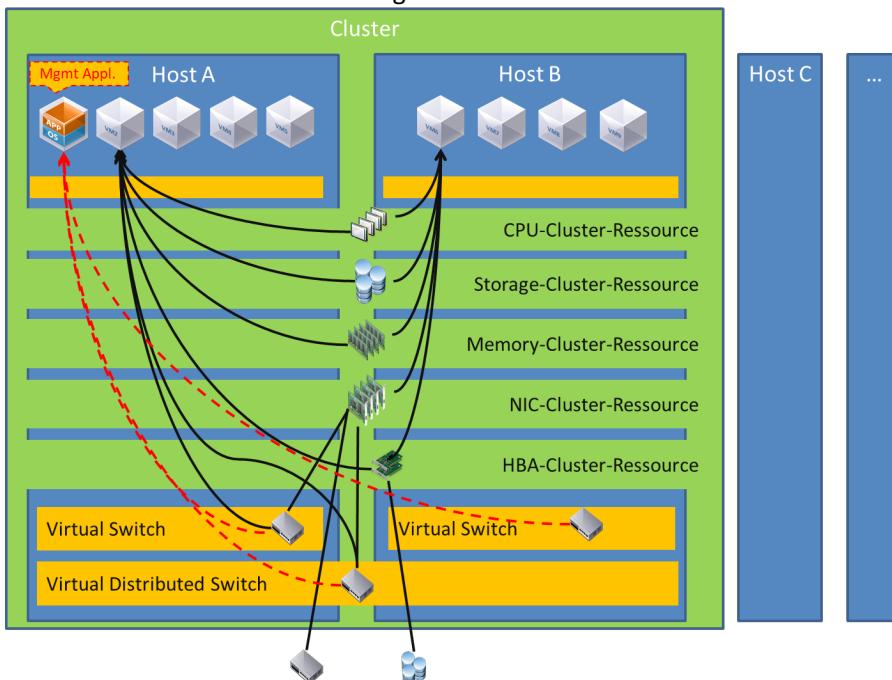
Aus Sicht der Applikationen verhält sich das OS auf der virtuellen Maschine wie auf einer physikalischen Maschine.

Die Verbindung zur Außenwelt wird mittels der NICs und HBAs (die zugewiesen wurden) hergestellt.

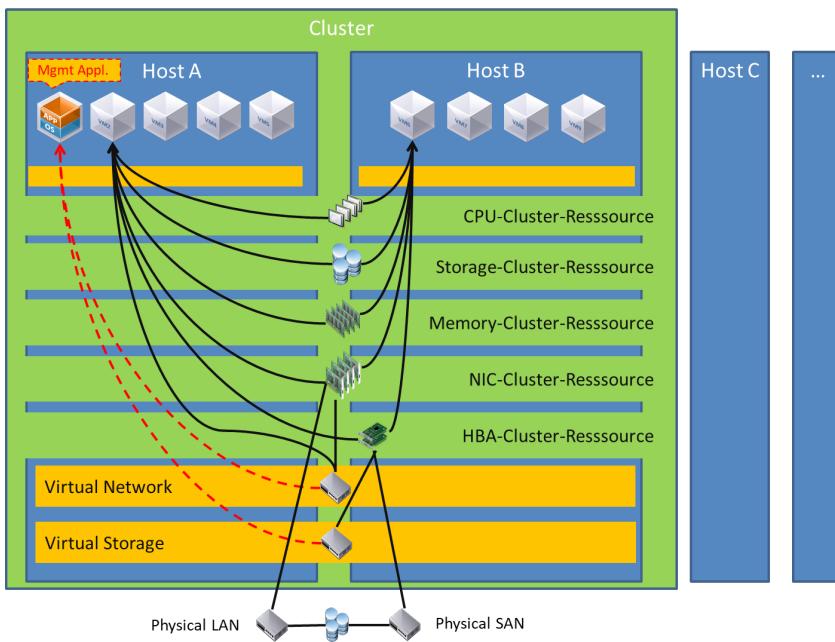
Protokolle



Die Virtualisierung kann Funktionen von externen Komponenten wie z. B. Switches auch in virtueller Form auf einem Host zur Verfügung stellen. Damit ist es möglich auf einem Host virtuelle Switches zu definieren die den unterschiedlichen VMs unterschiedliche VLANs zur Verfügung stellen können. Die Verbindungen nach Außen werden über NICs und HBAs ermöglicht.



Mehrere Hosts können zu einem Cluster zusammengeschaltet werden. Dadurch erhöht sich sowohl die Anzahl der Ressourcen als auch die Verfügbarkeit (z. B. im Falle eines Netzteil- oder Motherboard-Ausfalls). Die Switches können auf einen Host begrenzt sein (Virtual Standard Switch (VSS)), oder über mehrere Hosts hinweg (Virtual Distributed Switch (VDS)) die VLANs den VMs zur Verfügung stellen.

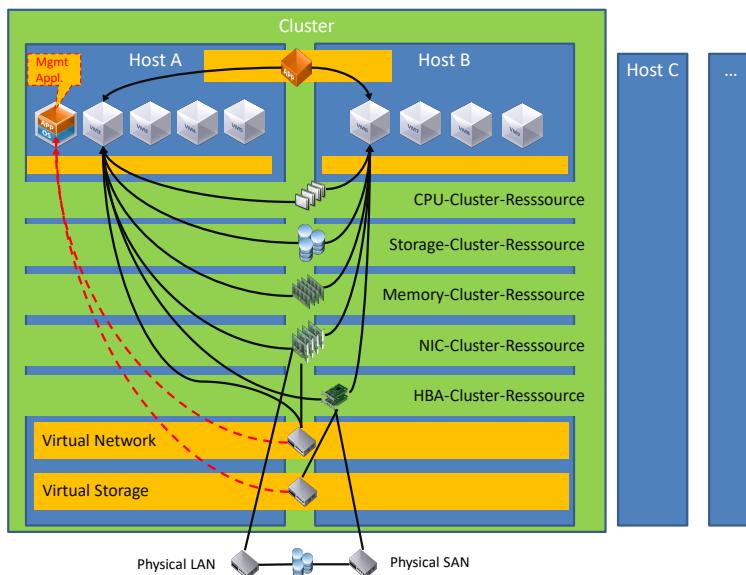


Die Verwaltung der virtuellen Switches kann mittels einer Applikation auf einer VM bewerkstelligt werden. Voraussetzung ist, dass die Hosts über die NICs miteinander verbunden sind.

Nach der Virtualisierung des Netzwerks ist noch nicht Schluss.

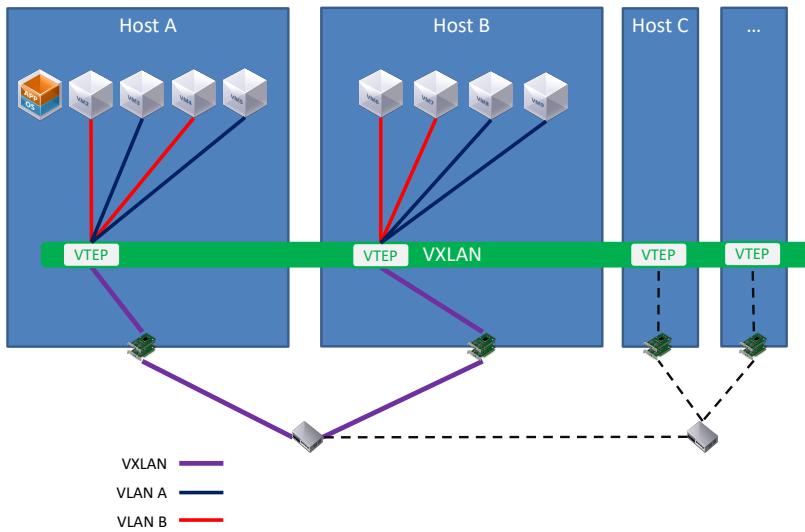
So ist auch eine Virtualisierung des Storage möglich. Dabei ist es unerheblich, ob das Storage über NICs oder HBAs verbunden wird.

Damit werden die Host internen Ressourcen um die Externen Ressourcen erweitert.



Der Aufwand wird betrieben um die vorhandenen Ressourcen besser zu nutzen und die Verfügbarkeit zu erhöhen, denn mit einer so geschaffenen Infrastruktur ist es einfacher Applikationen schnell zwischen VMs, Hosts und somit auch Standorten wechseln zu lassen.

Protokolle



So kann nach und nach eine Cloud aufgebaut werden.

Da nur 4096 unterschiedliche VLANs (in IEEE802.1q) möglich sind, würden z. B. Cloud-Provider schnell Grenzen stoßen.

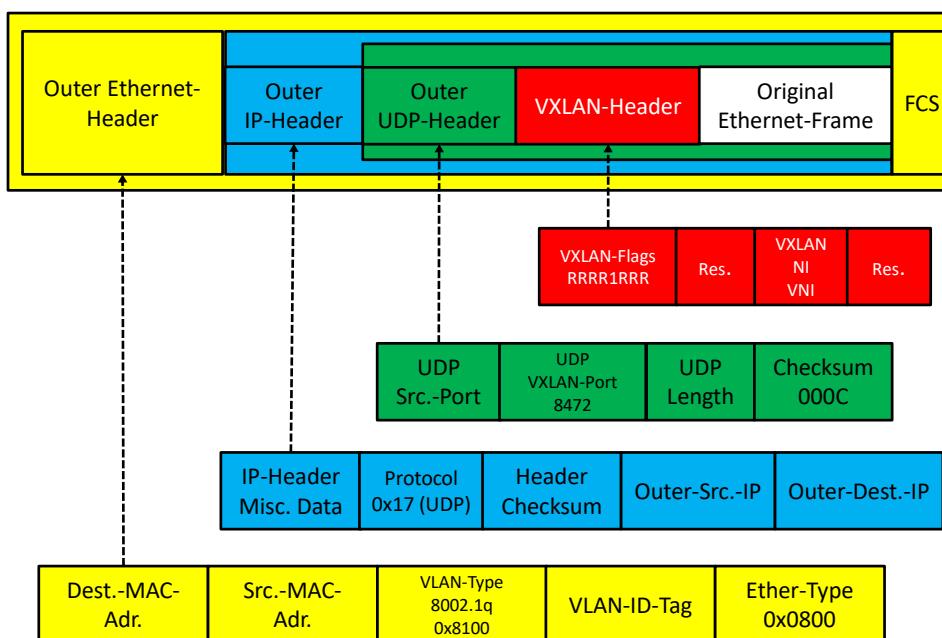
Um diese Grenze zu überwinden kommt VXLAN (Virtual Extensible VLAN) zum Einsatz.

Dabei wird ein VLAN-Rahmen in einen VXLAN-Rahmen eingepackt.

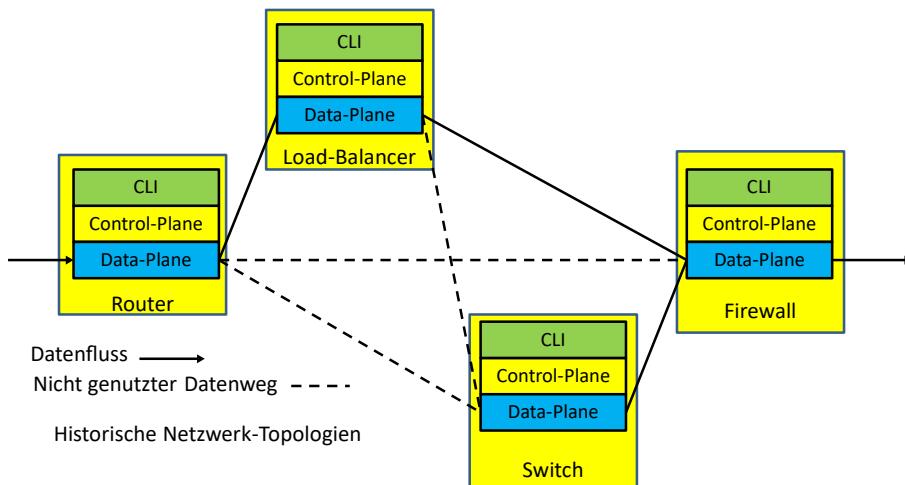
Da die VXLAN-ID mit 24 Bits mehr als 16 Millionen VXLANs ermöglicht, ist es möglich über Server- / RZ- / Standortgrenzen hinweg L2-Netzwerke aufzuspannen.

Die Endpunkte der VXLANs bilden die VTEP (Virtual Tunnel End Point)

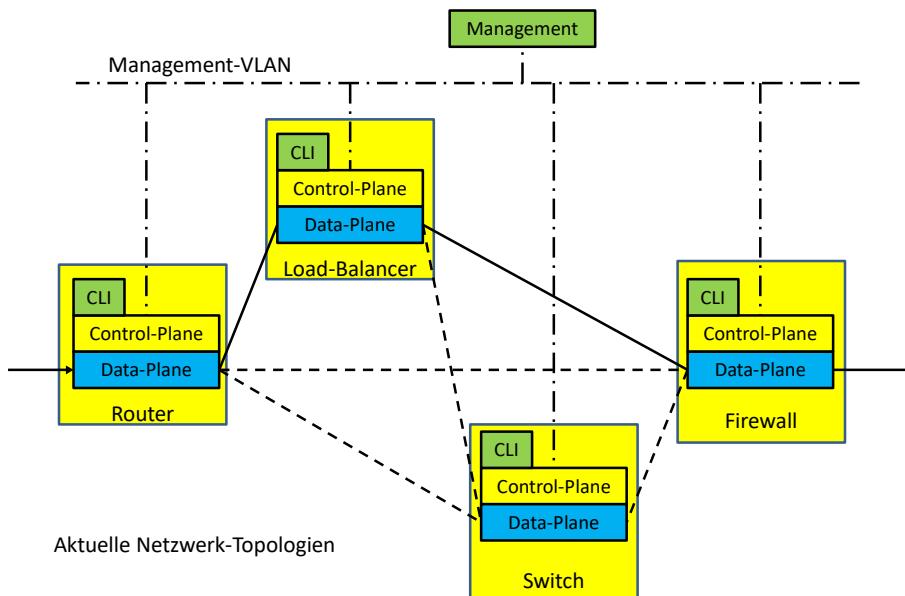
Hinter den VTEPs können dann die VLANs wie gewohnt genutzt werden.



32.1.2 - Veränderung der Netzwerk-Komponenten unter SDN



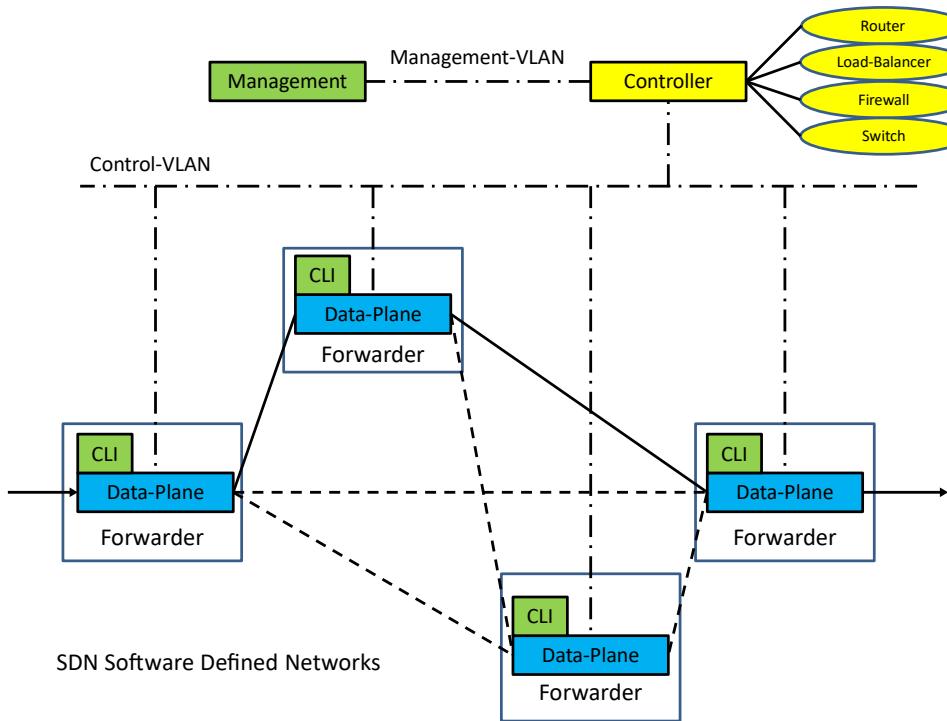
Klassisch gesehen hatte die Netzwerk-Komponenten wie Switches Router usw. ein Command Line Interface (CLI) mit dem der Administrator die Konfiguration des Gerätes vornehmen konnte



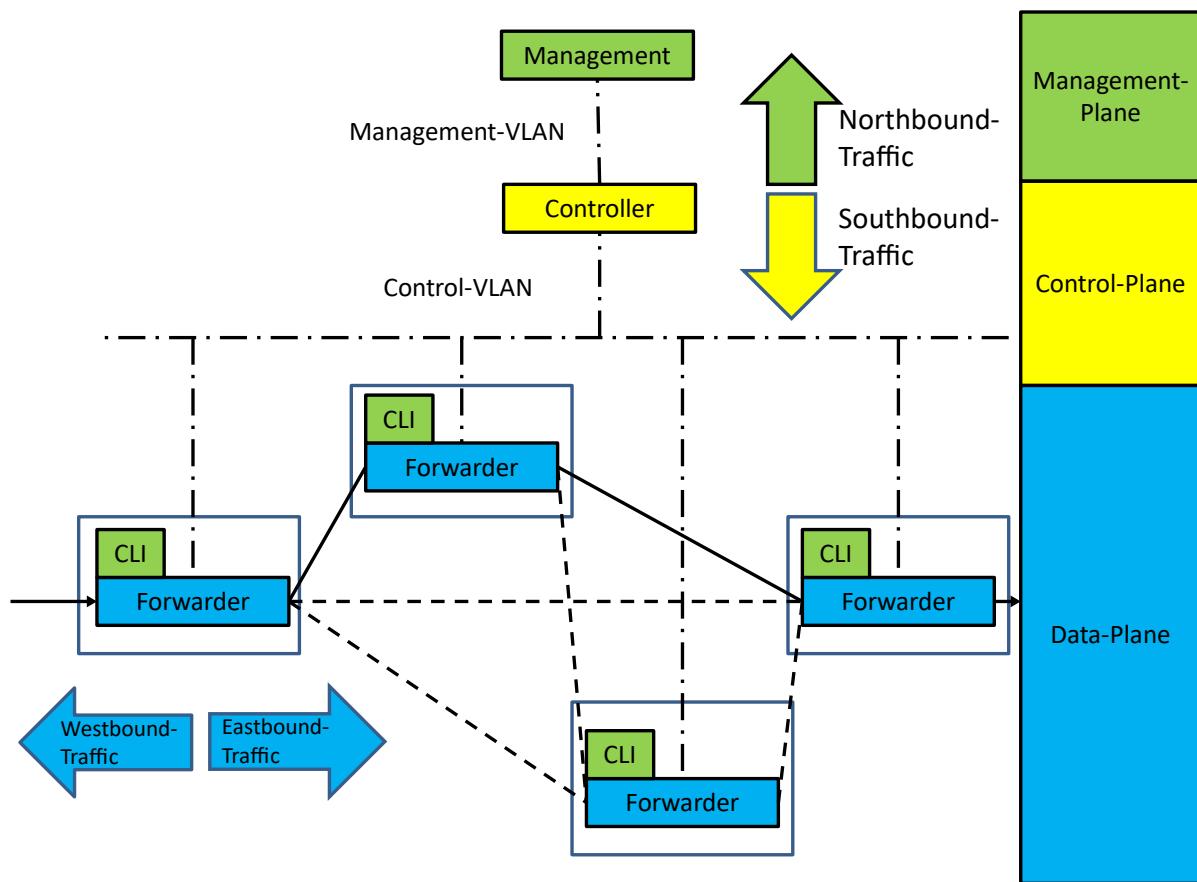
Durch die Einführung von Management-Systemen konnte von einer zentralen Managementstation die Konfiguration der Netzwerk-Komponenten vorgenommen werden. Dadurch konnten Konfigurations-Stände und Betriebssystemversionen zentral verwaltet werden.

Zusätzlich konnte durch Realisierung des Management-Netzwerks als eigenständiges und damit geschütztes VLAN die Sicherheit des Managements gewährleistet werden.

Das CLI dient bei Ausfall des Managements als Fallback-Lösung.



Durch die Einführung einer Control-Plane konnte die Funktion eines Netzwerk-Gerätes abstrahiert , und im Controller zentralisiert werden.



Damit findet eine Dreiteilung statt.

Über die Northbound-API kann ein Management-System die Konfiguration des Netzwerks bewerkstelligen.

Die eigentlichen Funktionen finden in den Controllern statt.

Die Geräte werden zu dummen Forwardern reduziert. Jedes eintreffende Paket wird auf einen Eintrag in einer Forwarding-Liste hin überprüft. In der Liste ist der Port, an dem das Paket weiter zu leiten ist, hinterlegt.

Fehlt der Eintrag, da ein Paket für diese Verbindung noch nicht am Gerät vorbei gekommen ist, muss beim Controller über die Southbound-Schnittstelle nachgefragt werden. Der aktualisiert die Forwarding-Liste des Gerätes.

Damit sind in der Data-Plane nur noch einfache Forwarder erforderlich. Der eigentliche Datenverkehr wird auch als Westbound/Eastbound-Traffic bezeichnet.

Funktionen wie Routing, Firewalling oder Load-Balancing werden im Controller abgebildet und verwaltet.

Um die Forwarder aufzusetzen wird ein CLI noch mitgeliefert.

32.2 - UDP-Protokoll

32.2.1 - Allgemeines

UDP bedeutet User Datagramm Protokoll.

UDP ist im Internet entstanden und dort neben TCP für die Bearbeitung der Ebene-4 zuständig.

UDP wird im RFC 768 beschrieben und arbeitet im Gegensatz zu TCP verbindungslos. Dies bedeutet, dass bei einem Datenaustausch die Daten auf das Netz gegeben werden ohne zu wissen, ob jemand auf die Daten wartet.

Deshalb muss auch kein Verbindungsaufbau und Verbindungsabbau stattfinden. Dies vereinfacht und beschleunigt die Datenübertragung erheblich. Deshalb verwenden Datenbanken zur Datenübertragung UDP. Allerdings gibt UDP keine Gewähr, ob die Daten auch beim Empfänger ankommen. Darum müssen sich bei Verwendung von UDP die höheren Schichten kümmern. UDP stellt eine ungesicherte Verbindung dar. Übertragene Telegramme werden nicht quittiert.

32.2.2 - UDP im ISO-RM

Von der Ebene3 her hat UDP nur eine Verbindung zu IP. Zu den Ebenen > 4 gibt es wie bei TCP vielerlei verschiedene Dienste, die auf UDP aufsetzen.

Dienst	Ebene
SNMP,DHCP, BOOTP, NTP, TFTP, Rservices, DNS, RPC, usw.	> 4
UDP	4
IP	3

32.2.3 - Header-Aufbau

2 Bytes	2 Bytes	2 Bytes	2 Bytes
Source-Port	Destination-Port	Message-Length	Checksum

Die über UDP transportierten Daten werden Datagramme genannt.

32.3 - TCP-Protokoll

32.3.1 - Allgemeines

TCP bedeutet Transmission Control Protocol. 1981 wurde TCP im RFC793 der Öffentlichkeit vorgestellt. TCP ist neben UDP für die Bearbeitung der Ebene-4 zuständig. Heute wird die gesamte Internet-Kommunikation mit TCP abgewickelt.

TCP ist im Gegensatz zu UDP verbindungsorientiert. Dies bedeutet, dass vor einem Datenaustausch, zuerst ein Verbindungsaufbau stattfinden muss. Zusätzlich muss nach einem Datenaustausch ein Verbindungsabbau durchgeführt werden.



TCP stellt eine gesicherte Verbindung dar. Übertragene Daten werden quittiert.

32.3.2 - TCP im ISO-RM

Von der Ebene 3 her hat TCP nur eine Verbindung zu IP. Zu den Ebenen > 4 gibt es vielerlei verschiedene Dienste die auf TCP aufsetzen.

Dienst	Ebene
HTTP, TELNET, FTP SMTP, Rservices, RFC1006, RPC, usw.	> 4
TCP	4
IP	<4

32.3.3 - Header-Aufbau

Source-Port (16Bit)								Destination-Port (16Bit)															
Sequence-Number (32 Bit)																							
Acknowledgement-Number (32 Bit)																							
Header-Length (4Bit)	Reserved (6Bit)	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size (16 Bit)															
Check-Sum (16 Bit)								Urgent-Pointer (16 Bit)															
Options (falls vorhanden)																							
Daten																							

Source-Port

Portnummer der Quelle

Destination-Port

Portnummer des Ziels

Sequence –Number

Sequenznummer des Datenpakets (entspricht der Anzahl der bisher gesendeten Daten + Initialisierungs-Sequenznummer)

Acknowledgement-Number (ACK)

Quittung für die zuvor gesendete Sequenznummer. Die ACK-Sequenz-Nummer gibt dem Partner an, ab welcher Position im Datenstrom die nächste Sequenz erwartet wird.

Header-Length (4 Bit)

FLAGS

Normalerweise ist nur ein (maximal 2)Flag(s) gesetzt. Pakete, bei denen alle Flags gesetzt sind, werden Kamikaze-Paket, nastygram, Christmas tree packet oder Lamptest genannt. Wird zum Test von TCP-Stacks verwendet. Siehe hierzu RFC1025 (TCP and IP Bake Off)

Im tcpdump-Output werden die Flags durch einen Buchstaben gekennzeichnet:

U=URG

S=SYN

F=FIN

R=RST

PSH

.=Kein Flag gesetzt

Protokolle

URG

Flag. (1 Bit) URG bedeutet urgent; deutsch dringend. Damit wird das Paket vom Sender als dringlich eingestuft. Der Urgent-Pointer ist damit gültig.

ACK

Flag. (1 Bit) Acknowledgement; deutsch Bestätigung. Damit werden Datentelegramme bestätigt.

PSH

Flag. (1 Bit) PSH bedeutet push; deutsch Anstoß oder Initiative. Damit wird die empfangende TCP-Seite angewiesen, die Daten auf dem schnellsten Weg der Empfänger-Applikation zu übergeben. Das PSH-Flag wird von TCP gesetzt, wenn der Sendepuffer beim Senden geleert wurde, was meistens bei den Datenübertragungen der Fall ist. Es gibt auch TCP-Implementierungen, die grundsätzlich das PSH-Flag beim Senden von Daten setzen. In modernen APIs ist es dem Programmierer nicht möglich das PSH-Flag zu setzen

RST

Flag. (1 Bit) RST bedeutet reset; deutsch zurücksetzen. Damit wird eine Kommunikations-Beziehung abgebrochen. Alle Puffer werden geleert bzw. freigegeben.

SYN

Flag. (1 Bit) SYN bedeutet synchronize; deutsch synchronisieren. Dies ist eine Verbindungsaufbau-Anforderung.

FIN

Flag. (1 Bit) FIN bedeutet finalize; deutsch beenden . Damit wird einseitig eine Kommunikations-Beziehung abgebaut.

Window-Size (16 Bit)

Deutsch: Fenster-Größe. Damit teilt ein Kommunikationspartner seinem Gegenüber mit, wie viel Platz in seinem Empfangs-Puffer noch frei ist. Diese Datenmenge kann in den nächsten Segmenten maximal übertragen werden, ohne dass eine Quittung erforderlich ist.

Checksum (16 Bit)

Prüfsumme

Urgent-Pointer (16 Bit)

Zeiger auf das Ende des dringlich zu behandelnden Datenteils.

Options

Im ursprünglichen TCP-RFC 793 werden nur 3 Optionen definiert:

- End of option list
- No option
- MSS

Diese wurden im RFC 1323 um 2 Optionen erweitert:

- Window Scale Factor
- Timestamp

Jedes Optionen Feld beginnt mit einem Kind-Byte (deutsch: Art-Byte) Die Optionen mit Kind = 0 und 1 belegen nur ein Byte. Damit ist die Länge bereits definiert. Optionen mit Kind > 1 haben als nachfolgendes Byte eine Längendefinition, die die Länge der definierten Option beschreibt. Es können mehrere Optionen im Optionen-Feld hintereinander erscheinen. Es muss nur sichergestellt sein, dass alle Option-Bytes zusammen ein Vielfaches von 4 Byte ergeben.. Für ein evtl. benötigtes Auffüllen wird die No-Option verwendet. Sie füllt aufgrund ihren 1 Byte-Länge ein Byte auf.

32.3.4 - Verbindungsstati

Für die Verwaltung der Verbindungen sieht TCP verschiedene Stati vor. Die Stati sowie die Übergänge dazwischen und deren Auslöser sind in der folgenden Abbildung beschrieben.

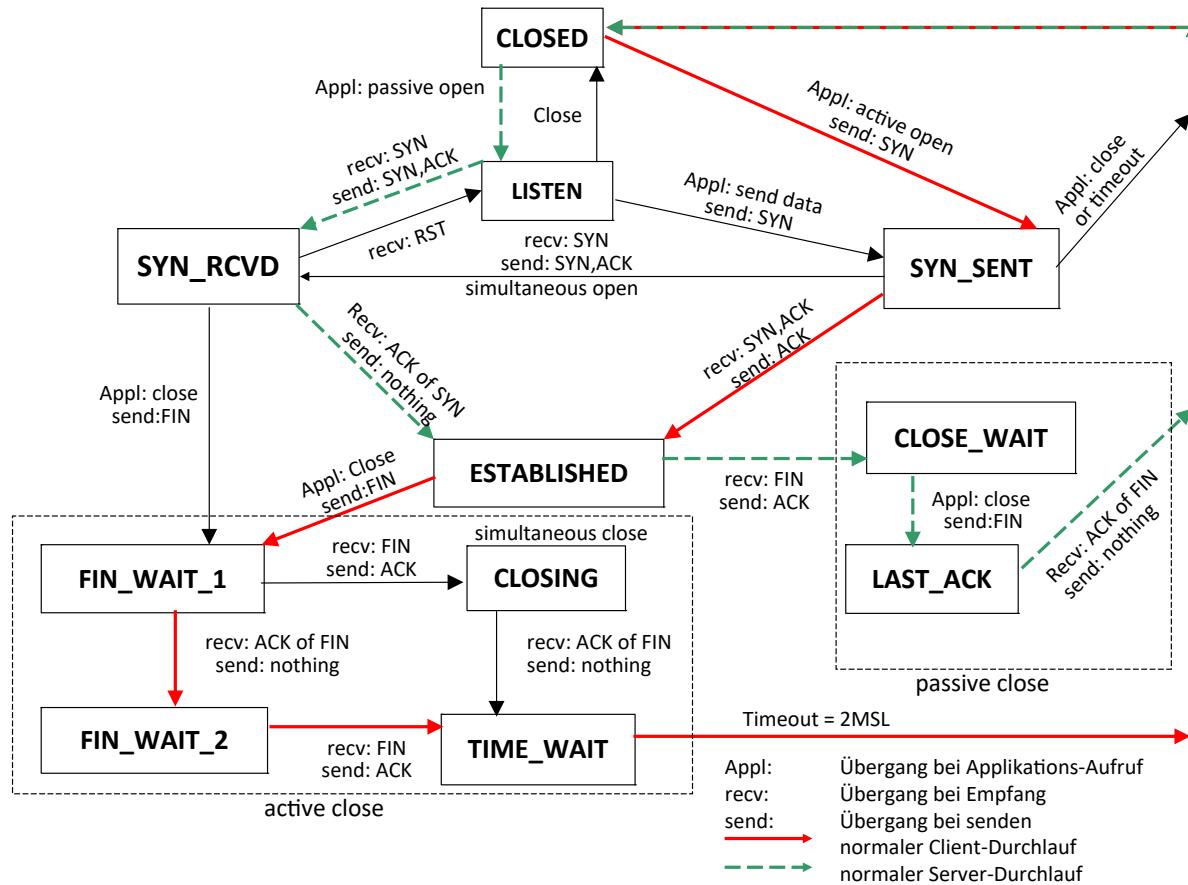


Abbildung 418 : TCP-Verbindungsstati

Die Übersicht in der obigen Abbildung ist folgendermaßen zu interpretieren:

Die Stati selbst sind umrahmt. Sie können z. B. auf einem Rechner mit dem Kommando netstat –a ausgegeben werden.

Die Verbindungslinien dazwischen sind zweizeilig ausgeführt. Bei Appl: wird der Applikations-Aufruf beschrieben, der zum Übergang führt. recv: bedeutet den Empfang eines Segments, was zum Übergang in einen anderen Status führt. Die untere Zeile (send:) beschreibt das Senden eines Segment, was in den nächsten Status führt.

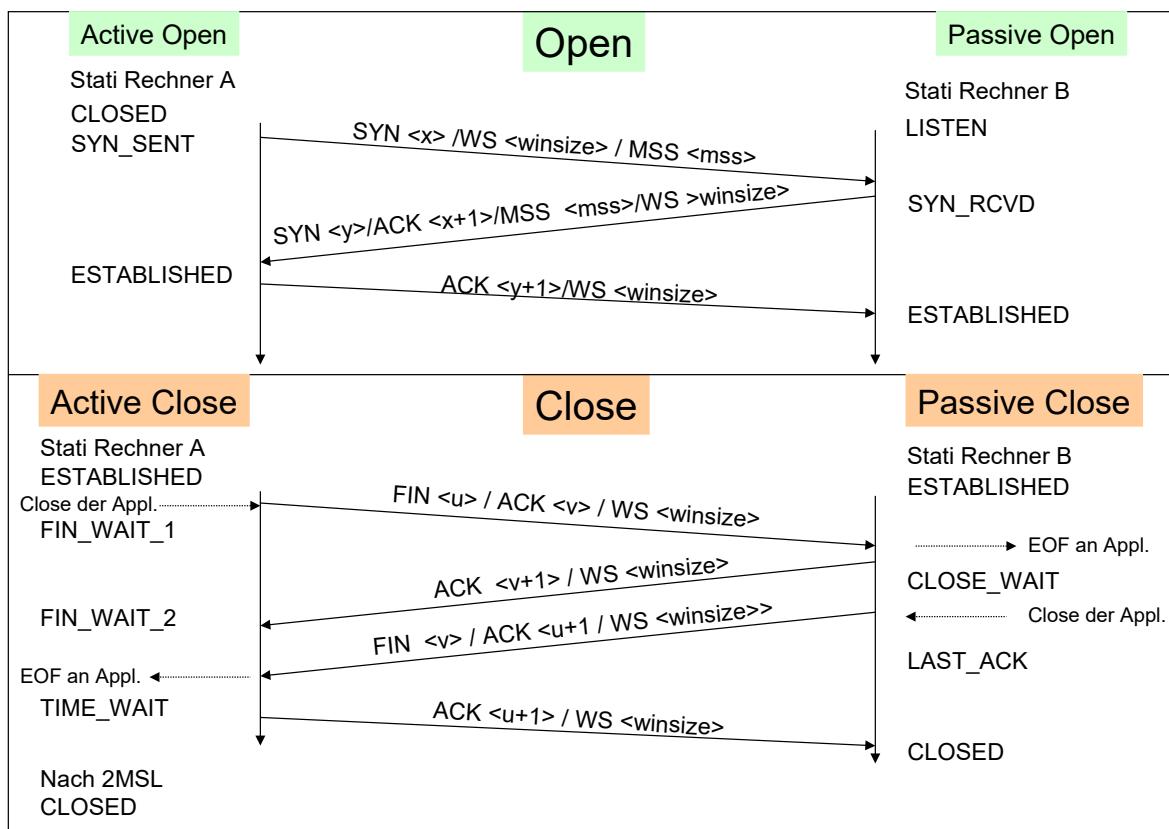
Es sind nicht alle möglichen Kombinationen aufgeführt. So fehlt z. B. die Reaktion auf ein RST-Flag bei den Stati. Allerdings sind hier die normalen Abläufe für eine TCP-Session aus Client und aus Serversicht abgebildet.

32.3.5 - Ablauf des Verbindungsaufbaus

Er wird oft als 3-Wege-Handshake bezeichnet.

Es wird davon ausgegangen, dass ein Rechner die Initiative für den Verbindungsaufbau übernimmt (active Open). Bevor er dies tut, ist der Verbindungsstatus auf seiner Seite auf CLOSED (deutsch: geschlossen)

Auf der Gegenseite muss jedoch schon jemand auf den Verbindungsaufbauwunsch warten (passive Open). Dies ist bei einer Client-Server-Beziehung der Server. Der Server wartet darauf, dass jemand etwas von ihm will und er bedienen (engl.: serve) kann. Der Status auf dieser Verbindungsseite ist LISTEN (deutsch: hören)



TCP_OPEN_CLOSE

E.Schweyer

Stand: 3.7.2010

Abbildung 419 : TCP-Open/Close

In der vorigen Abbildung wird der Ablauf eines aktiven Verbindungsaufbaus dargestellt (active open). Die zuerst anfordernde Seite (normalerweise der Client) sendet ein SYN-Segment mit folgendem Inhalt:

Portnummer des Servers, mit dem er sich verbinden möchte.
Eigene Portnummer (Wird bei der TCP-Initialisierung ab 1024 hochgezählt)
Initialisierungs-Sequenznummer ISN (Im RFC793 wird die ISN als 32-Bit-Zähler definiert, der alle 4 Mikrosekunden inkrementiert wird). Es gibt jedoch auch Implementierungen, die alle halbe Sekunde den Zähler um 64000 erhöhen. Dies entspricht einem Zähler, der alle 8 Mikrosekunden inkrementiert wird. Zusätzlich wird bei jedem Verbindungsaufbau der Zähler um 64000 erhöht.
Die ISN soll dazu dienen, die neue Verbindung nicht mit alten Verbindungen zu verwechseln.
Maximale Segment-Größe (MSS), die er zu erhalten wünscht
Window-Size. Dies entspricht der Puffergröße, die TCP für diese Verbindung zur Verfügung stellt.

Der Server antwortet mit einem eigenen SYN-Segment. Dabei quittiert er die ISN des Clients mit einem ACK für die Sequenznummer ISN + 1. Im Segment enthalten sind:

Portnummer des Clients, mit dem er sich verbinden möchte.
Eigene Portnummer
Eigene ISN. Diese ISN unterscheidet sich von der ersten ISN!
Quittung auf die vorhergehende ISN (ACK)
Maximale Segment-Größe (MSS), die er zu erhalten wünscht
Window-Size. Dies entspricht der Puffergröße, die TCP für diese Verbindung zur Verfügung stellt.

Nun wird der Verbindungsaufbauwunsch des Servers vom Client mit einem ACK beantwortet. In der Antwort sind enthalten:

Portnummer des Servers
Eigene Portnummer
Quittung auf die vorhergehende ISN (ACK)
Window-Size. Dies entspricht der Puffergröße, die TCP für diese Verbindung zur Verfügung stellt.

Damit ist die Verbindung auf beiden Seiten hergestellt (engl: established). Mit netstat -a können die Stati der Verbindung ausgegeben werden.

Dies war die normale Vorgehensweise mit einem active open und einem passive open. Es gibt jedoch noch die Möglichkeit eines beidseitigen active open.

Verhalten bei fehlendem Kommunikationspartner

Nach dem Senden des ersten SYN wird nach 5-6 Sekunden der Verbindungsaufbau-Versuch wiederholt. Es wird ein identisches SYN nochmals gesendet.

Kommt nun immer noch keine Rückmeldung, wird das SYN-Segment nach weiteren 28 Sekunden nochmals gesendet.

Nach weiteren 45 Sekunden wird die Applikation darüber informiert, dass die Verbindung nicht zustande gekommen ist.

Damit ist die gesamte Ablaufzeit für einen fehlgeschlagenen Verbindungsaufbau 75 Sekunden. Diese Zeiten sind von der Implementierung abhängig. Die Zeit lässt sich für den eigenen Rechner ermitteln, indem z. B. Eine TELNET-Session auf eine nicht vorhandene IP-Adresse geöffnet wird.

32.3.6 - Ablauf des Verbindungsabbaus

Ein Verbindungsabbau wird mit einem 3-Wege-Handshake abgehandelt. Der Verbindungsabbau benötigt jedoch 4 Segmente. Dies liegt am TCP-Half-Close. Da eine TCP-Verbindung eine Full-Duplex-Verbindung ist(jede Richtung ist eigenständig), muss jede Richtung für sich beendet werden. Es muss also zweimal (half; deutsch: halb) geschlossen werden, bis die Session ganz beendet ist.

Jede der beiden Seiten kann mit dem Verbindungsabbau beginnen. Im close-Aufruf der Applikation wird dies durch das Senden eines FIN-Segments durchgeführt. (active close)

Auf der anderen Empfängerseite des FIN muss die Applikation über den Abbauwunsch informiert werden. Deshalb wird ein EOF (End Of File ; deutsch Dateiende) an die Applikation übergeben.

Dies entspricht dem passive close. Der Empfang des FIN wird mit einem ACK quittiert.

Damit ist eine Richtung der Verbindung beendet. Der Empfang eines FIN bedeutet, dass aus dieser Richtung keine Daten mehr kommen. In der anderen Richtung können jedoch noch Daten gesendet werden. Obwohl dieser Vorteil von TCP möglich ist, wird er nur von wenigen Applikationen verwendet.

Wie beim open gibt es beim close die Möglichkeit, dass beide Seiten einen active close durchführen können.

Hier folgt der Ablauf. Rechner A initiiert den Verbindungsabbau mit einem FIN-Segment. Darin enthalten sind:

FIN-Flag
Portnummer des Empfängers
Portnummer des Senders
Sequenznummer
Quittung der letzten empfangenen Sequenz
Windowsize

Der Empfänger des FIN quittiert den Empfang der Segments mit dem Senden eines ACK-Segments. Darin enthalten sind:

ACK-Flag
Portnummer des Empfängers
Portnummer des Senders
Quittung der letzten empfangenen Sequenz (SNR + 1)
Windowsize

Nun übergibt der Empfänger des 1. FIN der Applikation (im allg. der Server) ein EOF.

Daraufhin sendet der Empfänger des 1. FIN sein FIN-Segment an den Sender des 1. FIN.

Dies wird natürlich mit einem ACK quittiert. Damit ist die Verbindung auf der Serverseite im Status closed. Auf der Client-Seite ist der Status auf TIME_WAIT. Hier muss noch 2*MSL (Maximum Segment Lifetime; deutsch: Maximale Segment-Lebensdauer) gewartet werden, bis der Status auch in den Zustand closed übergeht.

32.3.7 - Half-Close

Der Half-Close eröffnet die Möglichkeit, dass eine Seite die Verbindung beendet und die andere Seite noch weiter senden kann. Hier wird der close-Aufruf des ersten FIN durch einen shutdown-Aufruf ersetzt. Die andere Seite quittiert das FIN-Segment und sendet weiter Daten, bis auch hier schließlich der close-Aufruf durchlaufen wird.

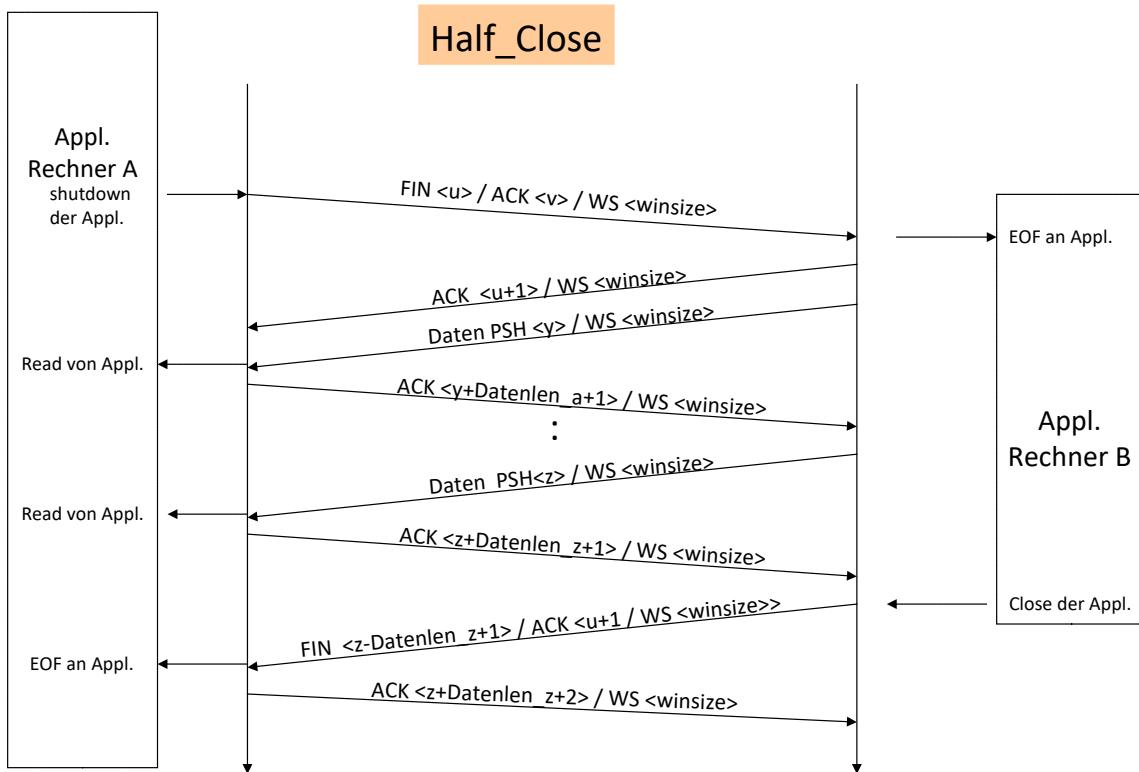


Abbildung 420 : TCP-Half-Close

32.3.8 - RST(Reset)

Wird ein SYN-Segment gesendet, ohne dass ein Port auf der anderen Seite dafür geöffnet wurde oder gleichzeitig ein SYN von der anderen Seite gesendet wird, wird der Verbindungsaufbau-Versuch zurückgewiesen. Dies wird mit einem RST-Segment das an den SYN-Sender zurückgegeben wird durchgeführt.

Ein RST-Segment wird auch gesendet, wenn ein Segment für eine nicht etablierte Verbindung eintrifft. Zu einer bestehenden Verbindung gehören jeweils zwei IP-Adressen und die zugehörigen Ports. Bei UDP wird in diesem Fall eine ICMP-Meldung zurückgesendet.

```
SYN SNR<x> WIN<y> MSS<z> ->  
<- RST SNR 0 ACK <x+1> WIN 0
```

Ein RST auf ein SYN bedeutet somit, dass bei dem Empfänger entweder die IP-Adresse nicht stimmt oder dass auf dem Port kein Partner hört.

32.3.9 - Abbrechen einer Verbindung

Normalerweise wird eine Verbindung mit FIN ... beendet. Dies wird orderly release genannt. Es ist auch möglich, eine Verbindung mit einem RST –Segment anstelle einer FIN-Sequenz zu beenden. Dies wird abortive release genannt. Dabei werden die Daten in den Puffern verworfen und ein RST-Segment wird gesendet. Dies kann mit der SO_LINGER - Socket-Option gemacht werden. Dabei wird mit einer linger-time (deutsch: Verzögerungszeit) von 0 genau dies gemacht.

32.3.10 - Erkennung von halb offenen Verbindungen

Halb offene Verbindungen entstehen, wenn ein Rechner abstürzt oder heruntergefahren wird, ohne die Session zu beenden. Solange keine Daten auszutauschen sind, wird von der Gegenseite nichts bemerkt. Wird dies mehrfach gemacht, bleiben auf einem Server viele Verbindungen halb offen und somit bleiben auch die Ressourcen belegt. Abhilfe bietet hier der Keepalive-Timer. Er führt eine Lebensüberwachung durch, wenn keine Daten zu übertragen sind.

32.3.11 - Gleichzeitiger Open (engl.: simultaneous open)

Es ist möglich, eine Verbindung aufzubauen, bei der beide Kommunikations-Partner einen active open durchführen. Hierbei arbeiten beide Seiten als Client und als Server. Dabei muss der SYN-Aufruf von beiden Seiten gleichzeitig erfolgen und es muss auf einen bekannten Port (well known port. Portnummern <1024) auf der Gegenseite zugegriffen werden. Dies wird simultaneous open genannt. Es entspricht nicht dem gegenseitigen Öffnen von TELNET-Sessions, da der Telnet-Deamon bereits einen passive open durchlaufen hat und den Port 23 in den LISTENING-Status gebracht hat. Das Ergebnis eines simultaneous open ist eine Verbindung. Bei OSI werden bei diesem Ablauf 2 Verbindungen aufgebaut. Hier werden 4 Segmente anstelle von 3 für den Verbindungsaufbau benötigt.

Simultaneous open

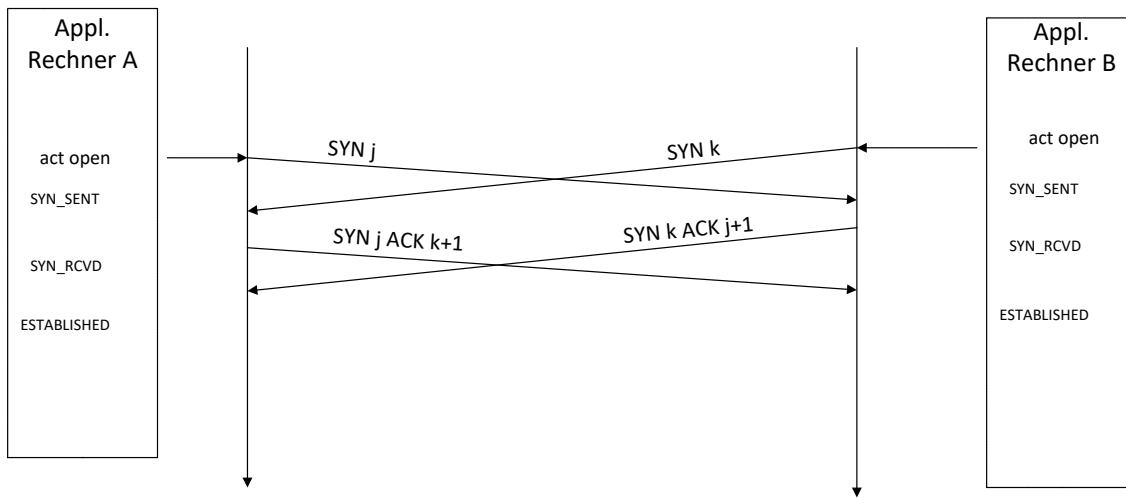


Abbildung 421 : TCP simultaneous open

32.3.12 - Gleichzeitiger Close (engl.: simultaneous close)

Es ist möglich, dass beide Partner eine Verbindung gleichzeitig schließen. Dabei wird vom ESTABLISHED-Status aus über den FIN_WAIT_1 und CLOSING in den TIME-WAIT-Status übergegangen. Hier werden 4 Segmente wie für den normalen Verbindungsabbau benötigt.

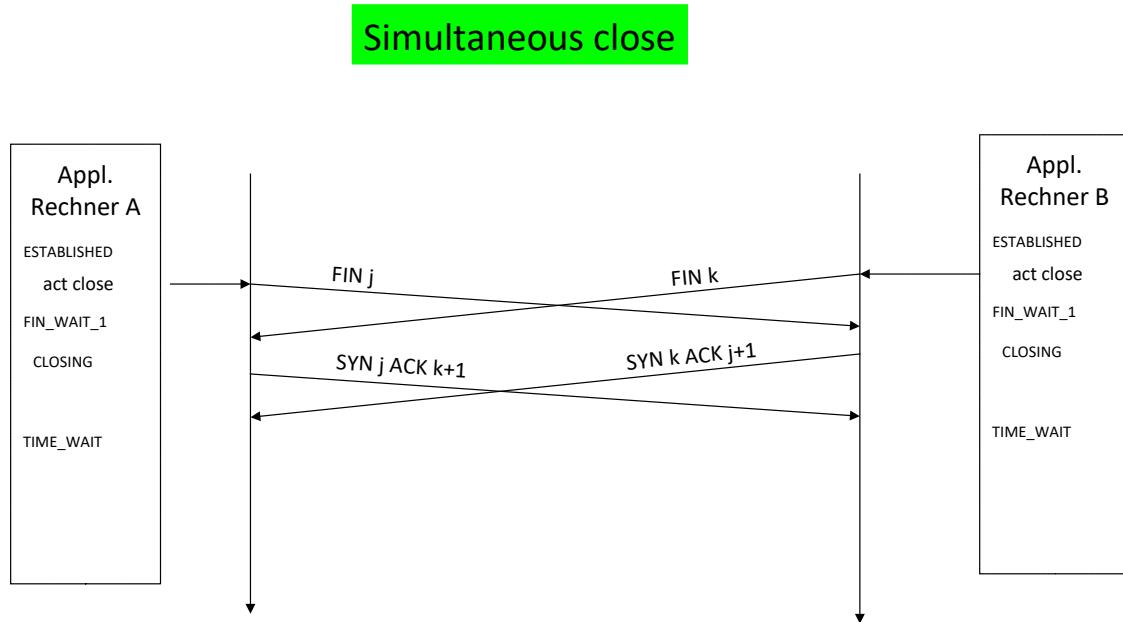


Abbildung 422 : TCP simultaneous close

32.3.13 - Datenübertragung

Grundsätzlicher Ablauf:

Daten-Sender:	Daten SNR <x> / WIN <y> →	Daten-Empfänger
	<- ACK <x+Länge> / WIN <z>	

Die Daten werden mit einer Sequenznummer(SNR) versehen. Damit sind die Daten im Datenstrom gekennzeichnet und können evtl. wiederholt werden.

Die Quittierung (engl.: Acknowledgement ACK) der Sequenznummer+Länge bedeutet, dass der Empfänger die Daten der Sequenz in ihrer gesamten Länge in ihren Puffer übertragen hat. Als nächste Sequenznummer wird die vorhergehende Sequenznummer + Länge des letzten Segments erwartet. Mit der Quittungs-Sequenznummer kann der Datensender auf die nächsten zu übertragenden Daten positionieren. Im Normalfall sind das die nächsten zu übertragenden Daten. Im Fehlerfall kann auf eine Position zurück gezeigt werden, ab der nochmals zu übertragen ist. Damit wird dem Sender mitgeteilt, ab welcher Position im Datenstrom nochmals zu übertragen ist.

Falls Daten in beiden Richtungen zu übertragen sind (z. B. bei rlogin werden die übertragenen Daten als Echo zurückgesendet), kann der Datenfluss anders aussehen. Dann kann bereits die Quittung wieder Daten enthalten.

Daten-Sender:	Daten SNR<x> / WIN <y> ->	Daten-Empfänger
	<- Daten SNR<y> ACK <x+len> / WIN <z>	
	ACK <y+len> /WIN <y>->	

Damit werden weniger Daten-Segmente und somit auch weniger Bandbreite benötigt.

Es wird also bei der Quittung berücksichtigt, ob auch Daten zu übertragen sind. TCP wartet bis zu 200 ms, ob einem ACK auch Daten mitgegeben werden können. Diese Vorgehensweise wird delayed ACK genannt. Damit ist die Quittung zwar etwas verzögert, jedoch müssen weniger Segmente übertragen werden. Das Anhängen der Quittung wird auch Piggyback (deutsch: Huckepack) genannt. Die Quittierung erfolgt somit mit einer Verzögerung zwischen 1 und 200 ms, da als Auslöser ein 200ms Timer verwendet wird, der beim Kernel-Start initialisiert wird.

Protokolle

Sind größere Datenmengen zu übertragen, werden mehrere Daten-Segmente hintereinander gesendet, ohne dass jedes Segment einzeln quittiert wird. Statt dessen können mehrere übertragene Segmente mit einem einzigen ACK quittiert werden. Die Daten-Segmente können so lange hintereinander gesendet werden, bis die Window-Size des letzten ACK gefüllt ist. Nur solange der Sender davon ausgehen kann, dass noch ein genügend großer Empfangs-Puffer auf der Empfängerseite vorhanden ist, darf er senden! Der Sender summiert die Längen seiner gesendeten Daten-Segmente. Würde das nächste Daten-Segment eine Summe entstehen lassen, welche die letzte gemeldete Window-Size übersteigt, darf nicht mehr weitergesendet werden.

Daten-Sender:	Daten SNR<a> / WIN <y> ->	Daten-Empfänger
	Daten SNR / WIN <y> ->	
	Daten SNR<c> / WIN <y> ->	
	<- ACK <c+len> / WIN <u>	
	Daten SNR<d> / WIN <y> ->	
	Daten SNR<e> / WIN <y> ->	
	Daten SNR<f> / WIN <y> ->	
	<- ACK <f+len> / WIN <u>	

Damit ist die Windowgröße eine elementare Steuergröße für die TCP-Datenübertragung. Je nachdem wie auf der Empfängerseite die Daten aus den TCP-Puffer an die Applikation übertragen werden können, ändert sich die Windowgröße bei den ACKs auf die Datenübertragungen. Die Windowgröße ist in ihrer Größe also dynamisch. Der maximale Wert ist jener, der beim Verbindungsaufbau mitgeteilt wurde.

Das Window überstreicht bei der Datenübertragung die gesendeten Daten und gibt dem Sender Auskunft, ob noch Daten gesendet werden können oder ob erst auf eine Quittung gewartet werden muss.

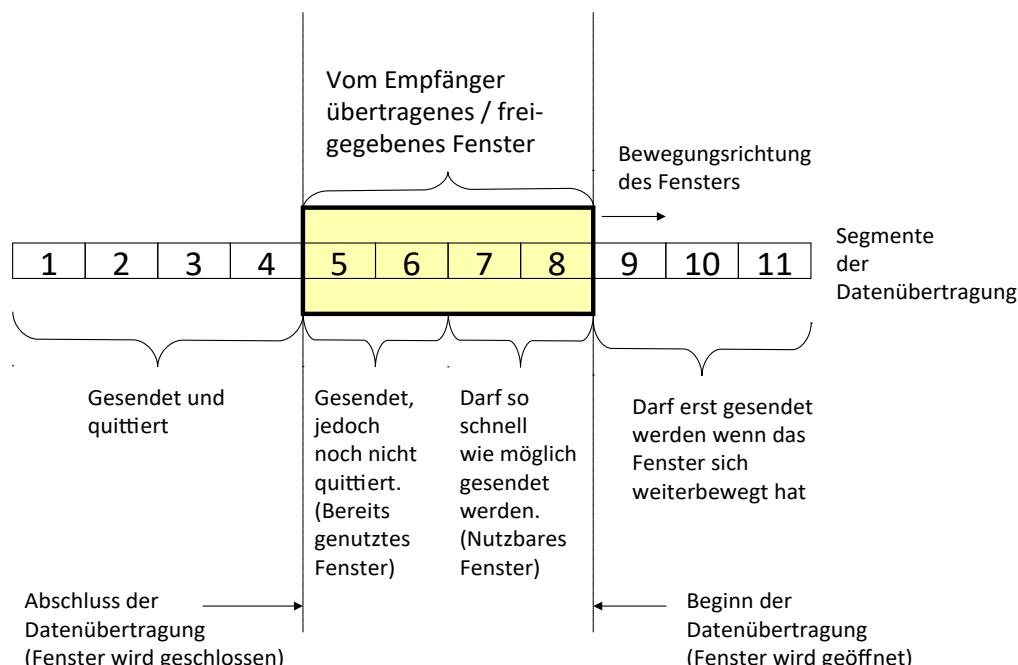


Abbildung 423 : TCP Sliding Window

Beispiel einer Datenübertragung:

Beim Verbindungsaufbau wird die MSS (Maximum Segment Size; deutsch: Maximale Segment-Größe) ausgehandelt, mit der Daten übertragen werden. Dieser Wert muss für beide Partner gleich sein. Bei ungleichen Vorschlägen wird Kleinste genommen. Zusätzlich teilt jeder Partner seinem Gegenüber mit, wie groß sein Empfangs-Puffer ist (Window-Size) ist. Dies kann bei jedem anders sein.

Damit ist die maximale Segment-Größe und die maximale Anzahl von Segmenten hintereinander, ohne dass eine Quittung erfolgen muss, festgelegt.

Im folgenden Beispiel gilt:

MSS = 1024

WIN=2048 für beide Seiten

Zu übertragende Datenmenge 4096 Byte

Der Start der Sequenznummern ist zufällig gewählt.

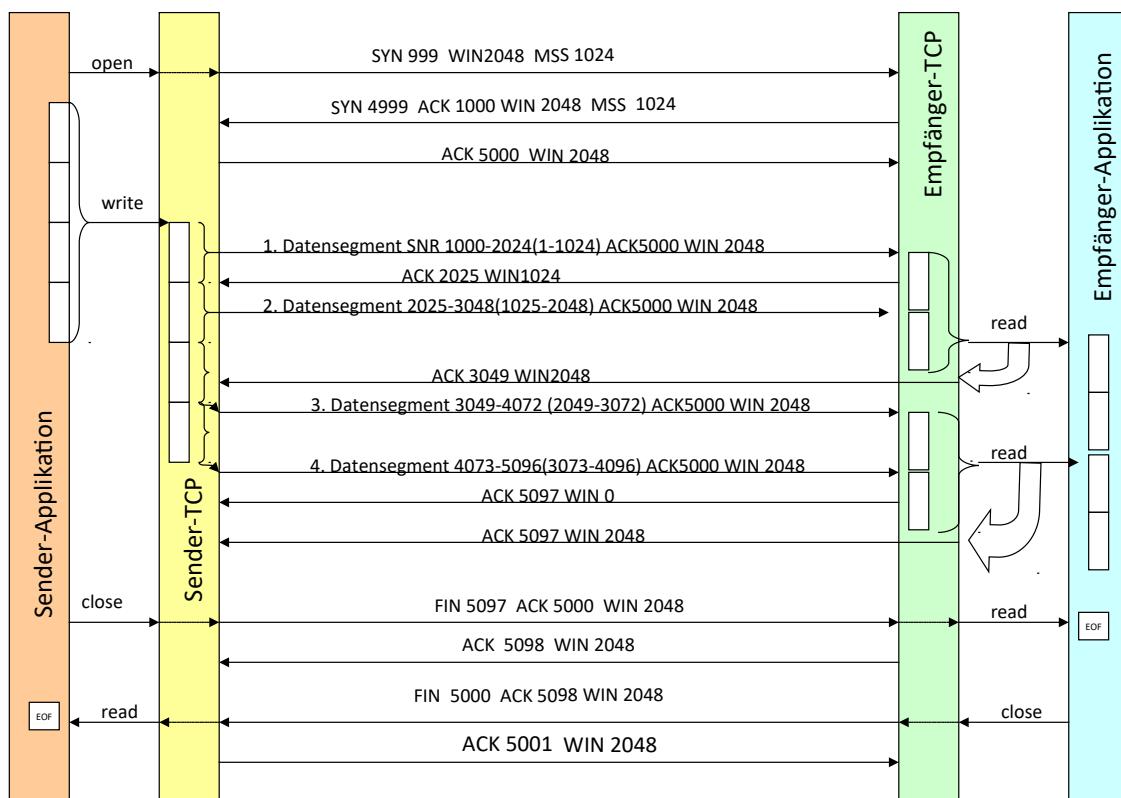


Abbildung 424 : TCP-Datenübertragungsbeispiel

Segment	Inhalt/Bedeutung
1	Das erste Datensegment wird gesendet.
2	Die Daten werden von TCP mit einem ACK quittiert. Die Windowgröße wird von 2048 auf 1024 reduziert, da TCP die Daten der Applikation noch nicht weitergegeben hat.
3	Das nächste Datensegment wird gesendet. Der Empfangspuffer des Empfängers ist jetzt voll. Der Sender weiß dies und muss warten, bis der Empfänger mit einer Windowgröße > 0 einen neuen Empfangs-Puffer zur Verfügung stellt.
4	TCP übergibt die Daten der Empfänger-Applikation. Damit kann TCP den Empfangs-Puffer räumen. Ein ACK wird dies durch die Windowgröße 2048 mitgeteilt. Der Sender kann jetzt wieder Daten senden.
5	Das 3. Datensegment wird übertragen.
6	Da noch Platz im Empfangs-Puffer sein muss, kann jetzt gleich das 4. Datensegment gesendet werden. Jetzt sind keine weiteren Daten mehr übertragbar, der Empfangs-Puffer ist voll.
7	TCP auf der Empfängerseite teilt dem TCP auf der Sender-Seite mit, dass die Daten einschließlich dem 4. Segment empfangen wurden und im Empfangs-Puffer stehen. Da dort kein Platz mehr für weitere Daten ist, wird die Windowgröße 0 in der Quittung mitgeteilt.
8	Die Daten werden der Empfänger-Applikation übergeben und somit ist der TCP-Empfangs-Puffer räumbar. Sobald der Puffer geräumt ist, wird dem Sender mitgeteilt, dass wieder ein Empfangs-Puffer > 0 zur Verfügung steht. Dies wird in einem so genannten Window-Update – Segment gemacht
9	Da die Sender-Applikation keine Daten mehr zu senden hat, durchläuft sie einen Close-Aufruf. TCP sendet daraufhin das FIN-Segment. Der Sender ist daraufhin im FIN_WAIT_1-Status
10	Das FIN-Segment wird vom Empfänger-TCP mit einem ACK bestätigt. Somit ist der Empfänger nun im CLOSE_WAIT-Status. Der Sender ist daraufhin im FIN_WAIT_2-Status. EOF wird an die Empfänger-Applikation übergeben, die daraufhin ebenfalls einen Close-Aufruf durchläuft.
11	Der Close-Aufruf auf der Empfängerseite erzeugt nun ein FIN-Segment. Der Empfänger ist im LAST_ACK-Status.
12	Der Sender-TCP quittiert den Empfang des FIN mit einem ACK und ist nun im TIME_WAIT-Status. Dieser geht nach 2MSL in den CLOSED-Status über. Nach dem Empfang des ACK ist die Empfänger-Verbindung im Status CLOSED

32.3.14 - Bandwidth-Delay-Product

Um nun die optimale Fenster-Größe, auch Verbindungs-Kapazität genannt, zu ermitteln, kann man das Bandwidth-Delay-Product (deutsch: Bandbreiten-Verzögerungszeit-Produkt) anwenden. Dies geschieht folgendermaßen:

$$\text{Verbindungs-Kapazität [Bytes]} = (\text{Bandbreite [Bits/Sec]} * \text{RTT [Sec]}) / 8 [\text{Bits/Byte}] \quad (98)$$

Beispiel:

10Mbps Datenverbindung

5ms RTT

$$\text{Verbindungs-Kapazität} = (10.000.000 * 0.005) / 8 = 6250 \text{ Bytes}$$

Dies bedeutet, je größer die Übertragungsgeschwindigkeit, desto kleiner kann die Window-Size gewählt werden. Im Umkehrschluss ist eine langsame WAN-Verbindung mit einer großen Window-Size zu versehen, um den optimalen Durchsatz zu erreichen.

Nagle-Algorithmus

Bei ausstehenden Quittungen werden weitere zu sendende Daten zurückgehalten und nicht übertragen, bis die Quittung eintrifft. Dann werden die bis dahin angesammelten Daten übertragen. Dies ist vor allem dann sinnvoll, wenn die Daten wie bei einer interaktiven Verbindung byteweise übertragen werden. Für 1 Byte wären dann 40 Byte Header notwendig. Dieses Missverhältnis ist vor allem auf langsamem WAN-Strecken schlecht. Durch den Nagle-Algorithmus greift eine elegante Regelung in den Datenfluss ein. Wenn Leitungen schnell sind, kommt die Quittung auch schnell. Ist die Verbindung langsam, wird durch das Ansammeln der Daten weniger Netzlast erzeugt. Der Nagle-Algorithmus muss u. U. ausgeschaltet werden. Z. B. Maus-Bewegungen (bei X-Windows) werden in kleinen Segmenten übertragen, allerdings sollten sie schnell übertragen werden.

Mit der API-Option TCP_NODELAY wird der Nagle-Algorithmus ausgeschaltet. Im Host-Requirement-RFC steht zwar, dass der Nagle-Algorithmus implementiert sein soll, allerdings ist er abschaltbar zu realisieren.

32.3.15 - URGENT-Mode

Beim Urgent-Mode (deutsch: Dringlichkeits-Modus) kann eine Applikation TCP anweisen, die aktuell zu übertragenen Daten möglichst schnell zu bearbeiten, damit die Applikation auf der anderen Seite möglichst schnell an wichtige (dringende) Daten kommt.

Hierbei teilt der Sender dem Empfänger zum einen mit, dass dringliche Daten vorliegen (URG-FLAG) und zum anderen, wo im Datenstrom die dringlichen Daten enden (Urgent-Pointer). Der Urgent-Pointer ist ein Offset-Pointer, der auf die Sequenznummer der letzten dringenden Bytes im Datenstrom zeigt. Diverse Berkeley-Derivate zeigen oft auf das erste nicht mehr dringende Byte (ein Byte weiter), was zu Problemen führen kann. Es gibt keine Möglichkeit dem Empfänger mitzuteilen, wo die dringenden Daten im Datenstrom beginnen! Die einzige Information, die übergeben wird, ist, dass der Urgent-Mode begonnen hat und die Sequenznummer des letzten dringenden Bytes. (Ende des Urgent-Modes)

Genutzt wird der Urgent-Mode von Telnet oder rlogin, um die Verbindung abzubrechen.

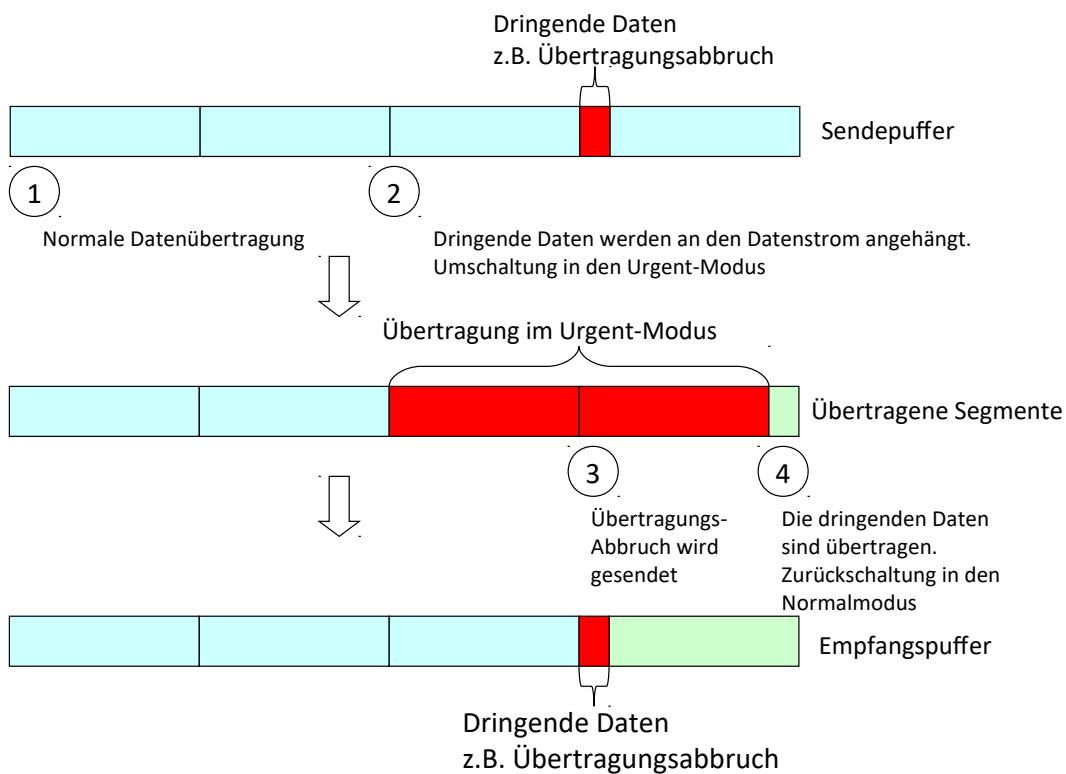


Abbildung 425 : TCP Urgent-Mode

Der Sender setzt das URG-Flag und den URG-Pointer so lange, bis die dringenden Daten übertragen sind. So lange ist der Empfänger im Urgent-Modus. Danach wird aufgrund des fehlenden URG-Flags wieder in den Normal-Modus zurückgeschaltet.

32.3.16 - Slow Start

Mit dem Slow Start (deutsch: Langsamer Anfang) ist eine Datenübertragung gemeint, die sich langsam an die optimale Daten-Übertragungs-Abwicklung annähert.

Besonders bei Verbindungen über WAN-Strecken hinweg, kann es vorkommen, dass die Segmente in den Routern zwischengespeichert werden müssen. Würden bereits zu Beginn alle möglichen Daten-Segmente (bis die Window-Size erreicht ist) vom Sender ausgesandt werden, könnte es vorkommen, dass in den Routern Datenpakete mangels Ressourcen verworfen werden müssten.

Deshalb gibt es nicht nur ein Window, welches vom Empfänger vorgegeben wird, sondern es gibt noch ein CWND (Congestion Window; deutsch Überlast-/Daten-Stau-Fenster), welches vom Sender gepflegt wird.

Dabei wird zu Beginn einer Datenübertragung das CWND auf die Größe eines Segments gesetzt. Dies ist im Normalfall die MSS, welche beim Verbindungsaufbau ausgehandelt wird. Jedes Mal, wenn ein ACK empfangen wird, wird die CWND um einen Segment-Größe vergrößert.

Der Sender kann dann bis zum Minimum von CWND oder der Windowgröße Daten übertragen.

CWND ist eine Fluss-Kontrolle, die vom Sender aus kontrolliert wird.

WIN ist eine Fluss-Kontrolle, die vom Empfänger aus kontrolliert wird.

Damit wird beim Senden zuerst ein Daten-Segment gesendet. Sobald der zugehörige ACK eingegangen ist, werden zwei Daten-Segmente hintereinander gesendet und auf ein ACK gewartet. Sobald auch hier der zugehörige ACK eingegangen ist, werden 3 Daten-Segmente hintereinander gesendet.....

Es wird so lange gesendet, bis das Minimum von CWND oder WIN erreicht ist. Sobald der CWND-Wert die maximale Windowgröße erreicht hat, gilt nur noch die Windowgröße, da der CWND-Wert immer weiter hoch gezählt wird, jedoch das Minimum der beiden Werte relevant ist. In diesem Zustand bleibt die Datenübertragung so lange, wie es zu keinen weiteren Beeinträchtigungen kommt.

Anmerkung :

Die ICMP-Meldung Source-Quench (Überlastung bei einem Empfänger/Router) führt beim Sender dazu, dass der CWND-Wert auf 1 zurückgesetzt wird. Dies ist der Anfang eines neuen Slow-Start. Damit kann eine Überlastungsmeldung zu einer Entlastung der Datenübertragung führen.

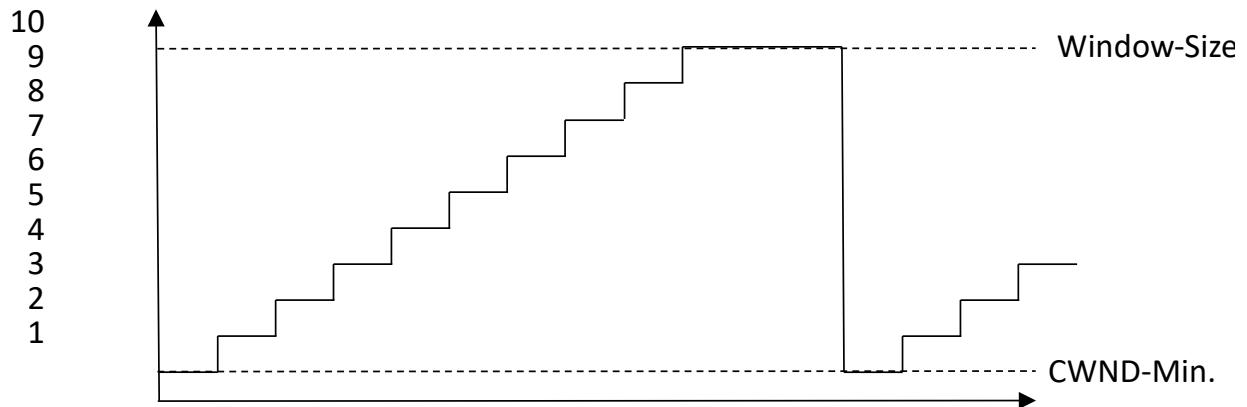


Abbildung 426: TCP-Slow-Start

32.3.17 - TCP-Timer

TCP erstellt eine gesicherte Transport-Verbindung zur Verfügung. Dies wird durch das Quittieren der übertragenen Daten erreicht. Jedoch können nicht nur Daten, sondern auch Quittungen verloren gehen. Um die Verbindung dennoch zuverlässig zu gestalten, wurden 4 Timer eingeführt, die dafür sorgen, dass verlorene Daten wiederholt werden.

Für die Implementierung einer Kommunikationsschnittstelle ist es von großer Wichtigkeit, die TCP-Timer auf die richtigen Werte zu setzen, um auf der einen Seite lange Wartezeiten und auf der anderen unnötige Datenpakete zu vermeiden.

32.3.17.1 - Retransmission Timer

Steht für die Zeitspanne, innerhalb der ein Datenpaket quittiert werden muss. Läuft der Timer ab, ohne, dass eine Quittung dafür empfangen wurde, wird das Senden der Daten wiederholt. Bei allen weiteren Versuchen wird die Wartezeit dazwischen verdoppelt. (exponentieller backoff)

Nach 12 Versuchen wird die Verbindung mit RST abgebaut.

Grundlegend für den Timeout und die wiederholten Versuche ist die RTT (round trip time; deutsch: Zeit für den Hin- und Rückweg für Datensegment und Quittung) Da sich die Wege zwischen zwei Endgeräten ändern können (Wechsel von Routen zum Ziel), kann sich die Zeit für eine Quittung für ein Datensegment ändern. Deshalb hat TCP für die Ermittlung einen Anpassungs-Mechanismus vorgesehen. Die Anpassung wird allerdings langsam, bzw. geglättet vorgenommen. Der angeglichene, neu ermittelte RTT wird auf einem Tiefpass-Filter erzeugt.

$$RTT = aRTT + (1-a)M \quad (99)$$

Der Glättungs-Faktor a wird mit 0,9 empfohlen. Damit wird der neue RTT zu 90% aus dem bisherigen RTT und zu 10% aus dem neu ermittelten (gemessenen) M zusammengesetzt.

Der RFC793 empfiehlt daraus einen RTO (Retransmission Timeout; deutsch Sendewiederholungs-Überwachungszeit) von

$$RTO = RTT + Rb * RTT \quad (100)$$

Rb ist der Verzögerungs-Faktor. Er wird mit einem Wert von 4 empfohlen.

Anmerkung :

Die ICMP-Meldung host unreachable oder network unreachable wird von TCP ignoriert. Beide Meldungen können auftreten, wenn ein Router ausfällt und die Verbindung neu aufgebaut werden muss. TCP versucht durch Wiederholungen (engl: retransmissions) bis zu 9 Minuten lang die Daten doch noch zu übertragen. Hier sind je nach Implementierung unterschiedliche Werte anzutreffen.



32.3.17.2 - Persist Timer

Eine Möglichkeit der Daten-Flusskontrolle ist bei TCP die Window-Size; deutsch: Fenster-Größe. Darin teilt ein Kommunikationspartners seinem Gegenüber mit, wie viele Bytes noch akzeptiert werden können, bevor der Empfangs-Puffer überläuft. Ist nun die Window-Größe eines Kommunikationspartners auf 0 zurückgegangen, kann vom Gegenüber nicht weitergesendet werden. Erst wenn die Fenster-Größe bei einem ACK wieder auf >0 gesetzt ist, werden wieder Daten übertragen. Falls dieses ACK-Paket jedoch verloren gehen sollte, bliebe die Kommunikation in einem Deadlock stecken, denn es werden nur Datentelegramme wiederholt. Nicht ACKs! Jeder Kommunikationspartner wartet auf den anderen. Der Eine auf Daten, der Andere auf einen ACK mit der Window-Größe > 0.

Der Persist Timer wird beim Erreichen der Windowgröße von 0 von seinem Gegenüber gesetzt. Ist der Persist Timer abgelaufen, wird ein so genanntes Window-Probe-Paket (ACK) gesendet, um beim Gegenüber nach der Window-Größe nachzufragen. Damit kann aus dieser Deadlock-Situation herausgefunden werden.

Eine Flusskontrolle, wie bei TCP verwendet, kann einem so genannten SWS (Silly Window Syndrome; deutsch: Verrücktes-Fenster Erscheinung) unterliegen. Dabei werden Datenpakete übertragen, die kleiner sind als Datenpakete mit der maximal möglichen Größe (MSS = Maximum Segment Size; deutsch: maximale Segmentgröße).

Der Grund dafür kann sowohl auf der Sende- als auch auf der Empfangsseite liegen:

Empfangsseite:

Sobald einmal die Window-Size wieder auf Werte >0 kommt, kann es passieren, dass eine Window-Größe mitgeteilt wird, die noch nicht der maximal möglichen entspricht. Da möglicherweise gleich wieder Daten gesendet werden, kann sich die Window-Size nicht mehr erhöhen.

Sendeseite:

Der Sender wartet nicht, bis die Daten für die MSS zusammengekommen sind, sondern sendet bereits vorher.

Auf beiden Seiten gibt es nun Regeln, um dem SWS zu begegnen.

Empfangsseite:

Hier braucht nicht, sobald die freie Puffergröße >0 ist, ein entsprechendes ACK gesendet werden.

Es ist sinnvoller, mindestens so lange zu warten, bis die freie Puffergröße einer halben MSS entspricht.

Sendeseite:

Erst wenn die Daten für ein Paket mit der MSS zusammengekommen sind, wird gesendet. Es kann aber auch bereits gesendet werden nachdem Daten mit der Größe einer halben MSS zusammengekommen sind.

32.3.17.3 - Keepalive Timer

Ein Keepalive Timer ist nicht Teil der TCP-Spezifikation. Eine TCP-Verbindung, die keine Daten austauscht, wechselt keine Pakete miteinander aus. Trotzdem haben viele TCP-Implementierungen einen Keepalive Timer. NFS setzt z. B. bei Verwendung von TCP immer den Keepalive Timer auf Client- und Server-Seite. Bei Rlogin und Telnet wird nur auf der Serverseite der Keepalive Timer gesetzt.

Nach 2 Stunden Inaktivität einer Kommunikations-Beziehung setzt der Server ein Probe-Segment an den Client ab. Dazu muss der Client in einem von 4 Zuständen sein:

1. Der Client ist vom Server aus erreichbar und beantwortet das Probe-Segment. Danach wird der Keepalive Timer auf 2 Stunden gesetzt. Wird innerhalb der nächsten 2 Stunden mindestens ein Datenpaket ausgetauscht, verfällt der Timer und wird am Ende des nächsten Datenaustauschs neu auf 2 Stunden gesetzt.
2. Der Client ist nicht mehr erreichbar (zusammengebrochen oder gerade am booten). Nach einem Timeout von 75 Sekunden. Im Abstand von 75 Sekunden macht der Server weitere 10 Versuche den Client zu erreichen. Scheitern alle Versuche, baut er Server die Verbindung ab.
3. Der Client war zusammengebrochen und hat wieder gebootet. Das Antwort-Paket auf das Probe-Segment ist ein RST(Restet) um die Verbindung abzubauen.
4. Der Client ist zwar am Laufen, jedoch nicht erreichbar. Die Reaktion ist wie bei 2.

32.3.17.4 - 2MSL Timer

Die 2MSL (Maximum segment lifetime; deutsch: doppelte maximale Segment-Lebensdauer) überwacht die Zeit, die eine Verbindung im TIME-WAIT-State verbringt. Im RFC793 wurde die MSL mit 2 Minuten vorgeschlagen. Da jedoch für die maximale Lebensdauer eines IP-Paketes mit dem TTL-Wert bereits eine Begrenzung vorhanden ist, hat dieser Wert nur noch eine geringe Bedeutung. Die Paket-Lebensdauer sollte nur durch die Anzahl von Hops (zu durchlaufende Router) begrenzt werden.

Allerdings soll die MSL folgenden Kriterien genügen:

Bei einem Active Close verweilt der schließende Kommunikationspartner im TIME-WAIT-State und wartet auf einen Final ACK. Nun muss genügend Zeit sein, damit ein Final ACK vom anderen Kommunikationspartner verloren gehen und wiederholt werden kann.

Unter verschiedenen Betriebssystemen ist die MSL unterschiedlich implementiert.

30Sekunden bei SunOs 4.1.3, SVR4, BSD/386 und AIX 3.2.2.

2 Minuten unter Solaris 2.2

32.4 - RIP

Das Routing Information Protocol (RIP) wurde erstmals im RFC1058 und dem Internet Standard STD56 beschrieben. Im Januar 1993 wurde RIP mit dem RFC1388 aktualisiert. Im November 1994 wurde im RFC 1723 die zweite Version RIP-v2 veröffentlicht. Es gehört zu den Routingprotokollen und dient somit den Routern, um sich über die möglichen Wege zu einem Ziel zu informieren. RIP gehört auch zu den interior Gateway Protokollen, da es im LAN-Umfeld angesiedelt ist und somit um ein internes Routing Protokoll handelt.

RIP gehört zu den Zustands unabhängigen Protokollen. Dabei wird als Metrik die Anzahl der Hops (Anzahl der Router bis ins Ziel-Netzwerk) berücksichtigt. Deshalb wird RIP als Distance Vector Routingprotokoll bezeichnet. Es handelt sich um einen Bellman-Ford-Algorithmus. Die Fähigkeiten von RIP sind beschränkt. Da nur die Hop-Anzahl zur Berechnung der besten Route verwendet wird kann die Leitungskapazität oder Kosten bei der Routing-Entscheidung nicht berücksichtigt werden.

RIP ist Timer-gesteuert. Erst nach dem Ausbleiben von RIP-Paketen wird die Routing-Tabelle neu erstellt. Dies bedeutet, dass auf zusammengebrochene Leitungen sehr träge reagiert wird.

32.4.1 - RIP Version 1

Wird als Broadcast gesendet. Dies hat zur Folge, dass alle Netzteilnehmer sich mit diesem Paket befassen müssen obwohl es nur für Router bestimmt ist. Dabei wird der UDP-Port 520 verwendet.

In dieser Version wird keine Subnetzmasken-Information übermittelt! Dies bedeutet, dass die Subnetzmaske des ersten gelernten Subnetzes die Subnetmask bestimmt. Damit ist nur eine klassenbasierte IP-Adressierung möglich.

Routing-Updates:

In regelmäßigen Zeitabständen (also timerbasiert) informieren sich die Router, wenn sich an der Topologie etwas ändert mit so genannten Routing Updates. Sobald ein Router ein Update empfängt, überprüft er die empfangene Information auf neue bzw. bessere Routen gegenüber seiner eigenen Routingtabelle. Nach einer Änderung seiner Routingtabelle sendet er sofort ein Routing-Update an andere Router.

Es werden normalerweise bis zu 25 Netzwerke in einem RIP-Paket mitgeteilt. Die maximal gültige Hop-Anzahl ist 14. Ein Netzwerk mit 15 Hops wird als nicht erreichbar übermittelt.

Extended RIP erlaubt eine Hop-Anzahl von 127 Hops. Dabei bedeutet die Hop-Anzahl von 128, dass das Netzwerk nicht mehr erreichbar ist.

Ein Router sendet beim Hochlauf einmal seine bekannten Routen. Danach alle 30 Sekunden. (Kann bei BAY-Networks z. B. für ISDN-Verbindungen auf etwa eine Std. korrigiert werden)

32.4.2 - Aufbau von RIPv1

1. Byte	2. Byte	3. Byte	4. Byte
Comand	Version		0
Family of Net 1		0	
IP-Address of Net 1			
0			
0			
Distance to Net 1 (Hops)			
Family of Net 1		0	
IP-Address of Net 2			
0			
0			
Distance to Net 2 (Hops)			
...			

Command

1 = Request (deutsch: Anfrage)

2 = Response (deutsch: Antwort auf eine Anfrage oder ein Routing-Update)

Version

1 = aktuelle Version

Family of Net 1

2 = IP-Adresse

IP-Adr. Net 1

IP-Adresse des Netzwerkes das bekannt gemacht wird

Distance Net 1

Hops bis zum Ziel-Netz 1-15 (16 = Netzwerk nicht erreichbar)

Family of Net 2

2 = IP-Adresse

:

Sobald ein Router gebootet wird, ermittelt er die direkt an ihn angeschlossenen Netzwerke und teilt diese seinen Router-Nachbarn in Form eines Broadcast mit. Von den anderen Routern erhält er die Informationen über die restlichen Netzwerke. Wie die Router sich gegenseitig mit Informationen versorgen ist am folgenden Beispiel zu sehen.

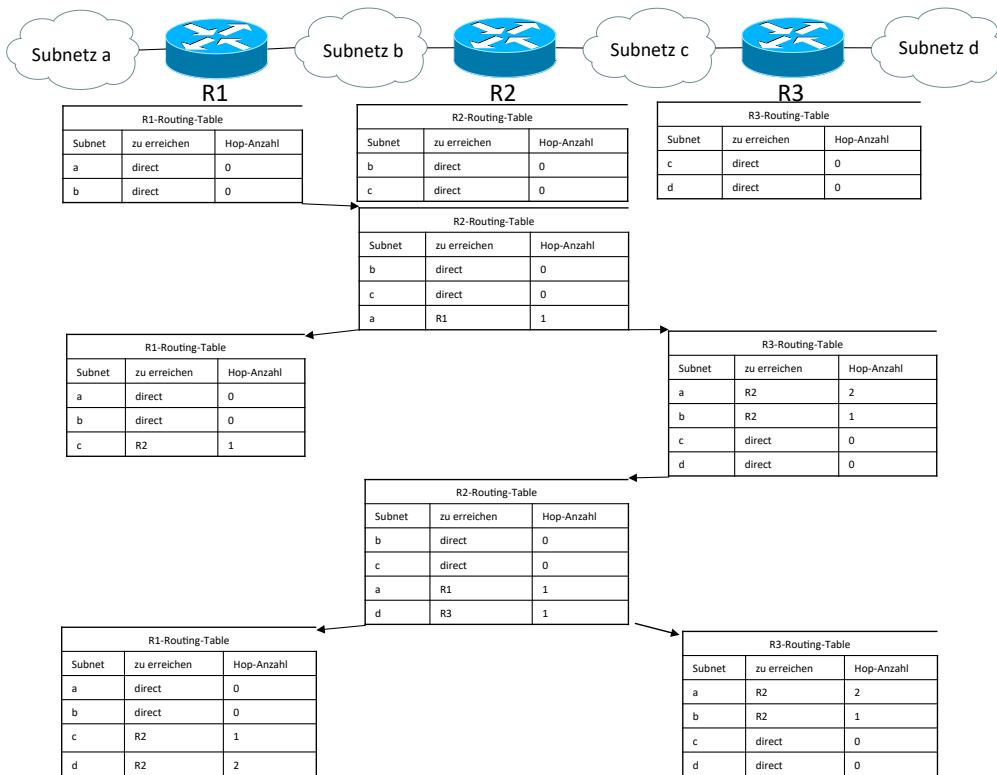


Abbildung 427 : RIP - Routing Updates

Hier wird klar, dass es lange dauert, bis alle Router die Informationen über alle Subnetze erhalten haben. Im obigen Beispiel dauert es bis zu 2 Minuten, um alle Subnetze auf allen Routern bekannt zu machen. Diese Konvergenzzeit ist der Nachteil der timerbasierten Informationsverteilung.

Protokolle

Wenn nun eine Route ausfällt (z. B. der Anschluss an das Subnetz a am Router 1) trägt der angeschlossene Router (R1) für das Subnetz a die Hop-Anzahl 15 ein. Da er auf den Timer warten muss bis er diese Information an andere Router weitergeben kann ist es möglich, dass er vom Router 2 die Information bekommt dass der Router 2 das Subnetz a mit 2 Hops erreichen kann. Deshalb trägt der Router 1 das Subnetz a als erreichbar über den Router 2 mit der Hopanzahl 3 ein. Diese Information überträgt er an den Router 2 beim nächsten Timer-Intervall. Damit zählen die Router 1 und 2 so lange die Hopcount-Zähler für das Subnetz a hoch bis der Wert 15 (also unerreichbar) erreicht wird. Auch hier wird ersichtlich, dass die Konvergenzzeit einige Minuten dauern kann.

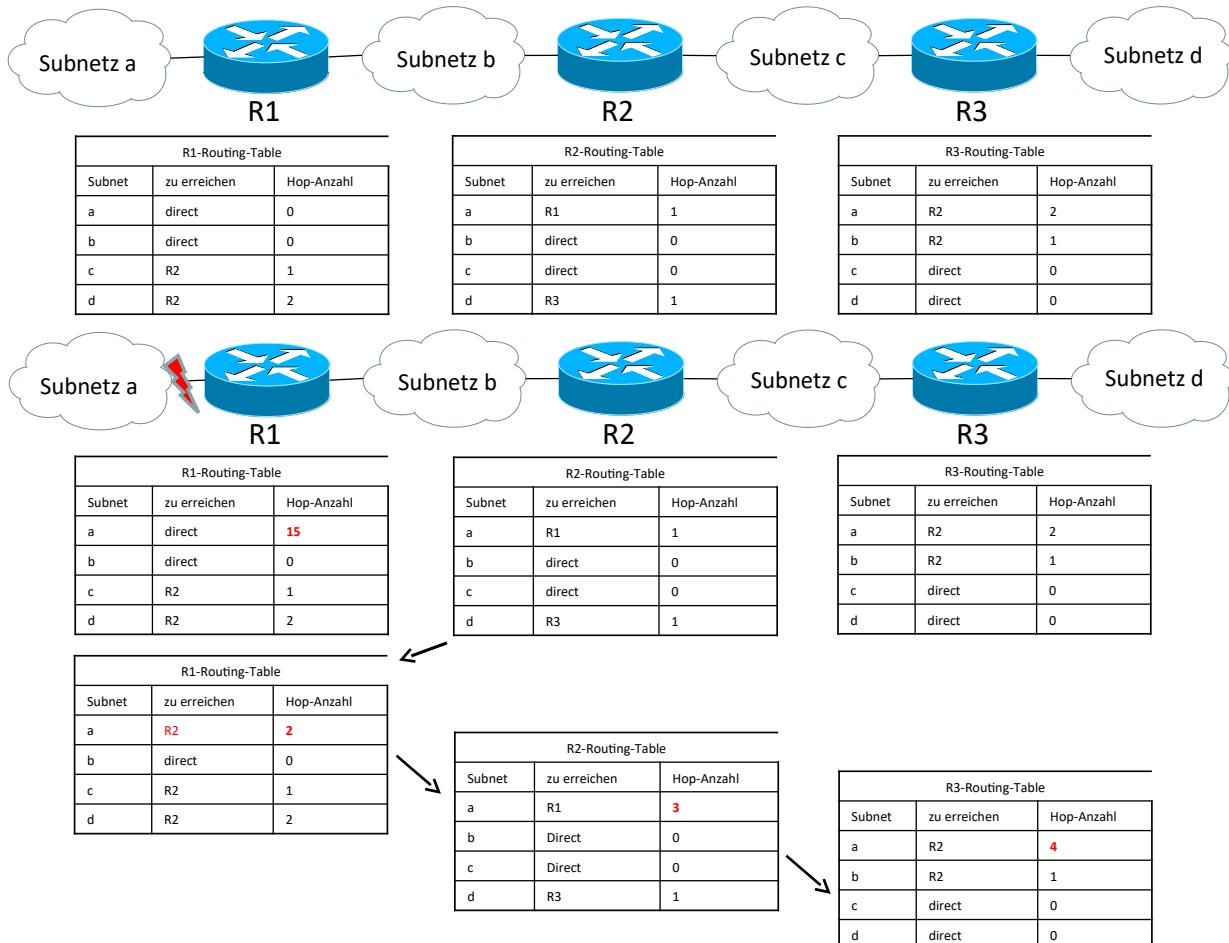


Abbildung 428 : Wegfall einer Route

Zur Beschleunigung der Konvergenzzeit wurden folgende Maßnahmen definiert.

Split Horizon (deutsch: geteilter Horizont)

Ein Router wird Informationen nur an die Subnetze weitergeben aus denen er die Informationen nicht bekommen hat. Das bedeutet, dass wenn er an einem Port ein Subnetz mitgeteilt bekommen hat, wird er dieses Subnetz an diesem Port nicht wieder verkünden.

Split Horizon und Poison Reverse (deutsch: vergifteter Rückweg)

Hierbei werden wieder alle Subnetze auf allen Ports angekündigt. Allerdings werden die Subnetze mit dem Hopcount 15 zurückgegeben aus denen sie gekommen sind.

Triggered Updates (deutsch: ausgelöste Aktualisierungen)

Hierbei wird nicht bis zum nächsten Timeralarm gewartet bis eine neuen Information verbreitet wird. Es wird sofort nachdem ein Port als „Down“ erkannt wird, die Information weitergeleitet.

Zusätzliche Maßnahmen

Routen die über RIP gelernt wurden haben nur eine Lebensdauer von 3 Minuten. Sollte in der Zwischenzeit kein Update von einem anderen Router erfolgen bekommt die Route die Metrik 16.

32.4.3 - RIP Version 2

Wird als Multicast (IP-Multicast-Adresse 224.0.0.9) gesendet. Dies hat den Vorteil, dass nur die Router von diesen Paketen betroffen sind. Alle anderen Netzteilnehmer befassen sich mit diesem Paket nicht. In dieser Version werden Subnetzmasken-Information übermittelt! Dies bedeutet, dass unterschiedliche Subnetzmasken-Längen möglich sind.

(VLMS = Variable Length of Subnet Mask; deutsch: variable Subnetzmasken-Länge). Damit ist klassenlose IP-Adressierung möglich.

Es werden normalerweise bis zu 25 Netzwerke in einem RIP-Paket mitgeteilt.

Die maximal gültige Hop-Anzahl ist 14. Ein Netzwerk mit 15 Hops wird als nicht erreichbar übermittelt.

Extended RIP erlaubt eine Hop-Anzahl von 127 Hops. Dabei bedeutet die Hop-Anzahl von 128, dass das Netzwerk nicht mehr erreichbar ist.

Ein Router sendet bei Hochlauf einmal seine bekannten Routen. Danach alle 30 Sekunden. (Kann bei BAY-Networks z. B. für ISDN-Verbindungen auf etwa eine Std. korrigiert werden)

32.4.4 - Aufbau von RIPv2

1. Byte	2. Byte	3. Byte	4. Byte
Comand	Version	Pasword	
Family of Net 1		0	
IP-Address of Net 1			
Subnet-Mask of Net 1			
0			
Distance to Net 1 (Hops)			
Family of Net 1	0		
IP-Address of Net 2			
Subnet-Mask of Net 2			
0			
Distance to Net 2 (Hops)			
...			

Command

1 = Request (deutsch: Anfrage)

2 = Response (deutsch: Antwort auf eine Anfrage)

Version

1 = aktuelle Version

Family of Net 1

2 = IP-Adresse

IP-Adr. Net 1

<IP-Adresse>

Subnet-Mask Net 1

Subnetmaske zu Netzwerk 1

Distance Net 1

Hops bis zum Ziel-Netz 1-15 (16 = Netzwerk nicht erreichbar)

Family of Net 2

2 = IP-Adresse

:

RIP 2 ist zu RIP 1 abwärts kompatibel.

32.5 - OSPF

32.5.1 - Einführung

Open Shortest Path First (OSPF) gehört zu den Routingprotokollen und dient somit den Routern um sich über die möglichen Wege zu einem Ziel zu informieren. 1988 wurde die Entwicklung bei der IETF begonnen. 1990 wurde OSPF zum Standard erklärt. Die aktuelle Version (V2) ist im RFC 1247 beschrieben. Die vollständige Geschichte ist im RFC 2328 beschrieben.

32.5.2 - Autonome Systeme

Bei OSPF sind die Router mit ihren Netzwerken zu einem Autonomen System (AS) zusammengefasst. Ein Autonomes System ist dabei eine Verwaltungseinheit, die es dem Administrator ermöglicht mit beliebigen Routing-Architekturen zu arbeiten und nach außen hin definierte Schnittstellen zu haben. OSPF ist als IGP (Interior Gateway Protocol) konzipiert und regelt somit das Routing innerhalb eines Autonomen Systems. Für das Routing zwischen autonomen Systemen sind Algorithmen nach dem EGP (Exterior Gateway Protokoll) zuständig. Im Internet wird das BGP (Border Gateway Protocol) verwendet.

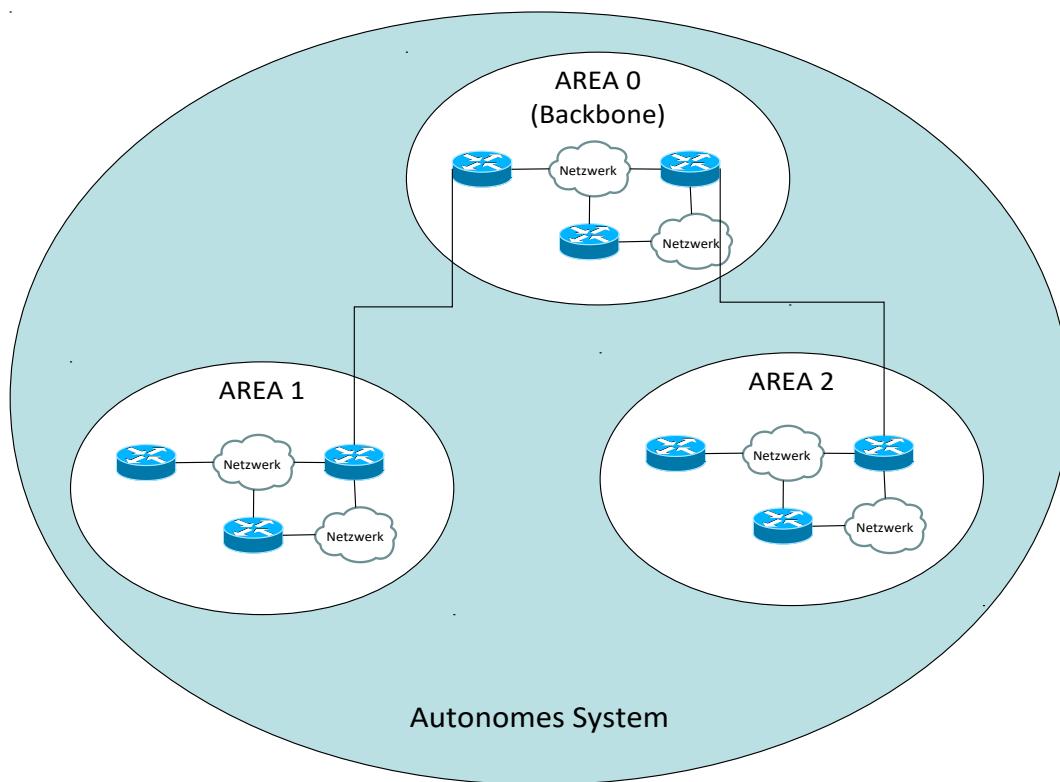


Abbildung 429 : OSPF Areas

Protokolle

Eine OSPF-Topologie ist in mehrere Hierarchie-Ebenen eingeteilt:

- Autonomes System

Gesamtheit aller über ein Backbone verbundenen Areas

- Backbone

Verbindung von Areas

- Area

Gruppierung von Netzwerken

- Netzwerk

OSPF unterstützt drei Arten von Verbindungen zwischen Netzwerken:

- Punkt-zu-Punkt-Verbindungen zwischen zwei Routern.
- Mehrfachzugriffsnetzwerke mit Broadcasting. Das sind die meisten LANs.
- Mehrfachzugriffsnetzwerke ohne Broadcasting. Das sind die meisten paketvermittelnden WANs.

Mehrfachzugriffsnetzwerke sind Netzwerke an die mehrere Router angeschlossen sind. Diese Router können direkt miteinander kommunizieren. Alle LANs und WANs haben diese Eigenschaft.

OSPF ist ein Link-State-Algorithmus. Die Routing Entscheidung wird demnach aufgrund des Link-Status ermittelt bzw. korrigiert. Dies bedeutet, im Gegensatz zu RIP, dass anstelle von Timern die Überwachung auch durch Link-Status getriggert wird. Ausnahme waren hier die Triggered Updates von RIP.

Langfristig soll OSPF RIP ablösen da einige Einschränkungen von RIP entfallen:

- Es können Netzwerke über mehr als 14 Zwischen-Systemen erreicht werden.
- OSPF konvergiert bei Netzwerk-Änderungen schneller
- Geringerer Overhead
- Unterstützung hierarchischer Netzwerk-Strukturen
- Unterstützung zur Authentifizierung

Innerhalb eines AS sind die Areas hierarchisch organisiert. Ganz oben ist die Backbone Area mit der Area-ID = 0 zu definieren. Alle anderen Areas werden an diese Area angeschlossen.

In den Areas haben die Router, je nach ihrer Position in der Area, unterschiedliche Klassen:

- Designierte Router

Ausgewählter Router der stellvertretend für alle Router einer Area mit anderen Areas Informationen austauscht. Er kann über die Multicast-Adresse 224.0.0.6 adressiert werden. Dieser Router wird über das HELLO-Protokoll aus allen Routern einer Area ausgewählt.

- Interne Router

Diese Router arbeiten innerhalb eines AS oder eines Backbones.

- Area Border Router

Dieser Router verbindet zwei Areas oder eine Area mit der Backbone-Area.

- AS Boundary Router

Diese Router verbinden autonome Systeme miteinander.

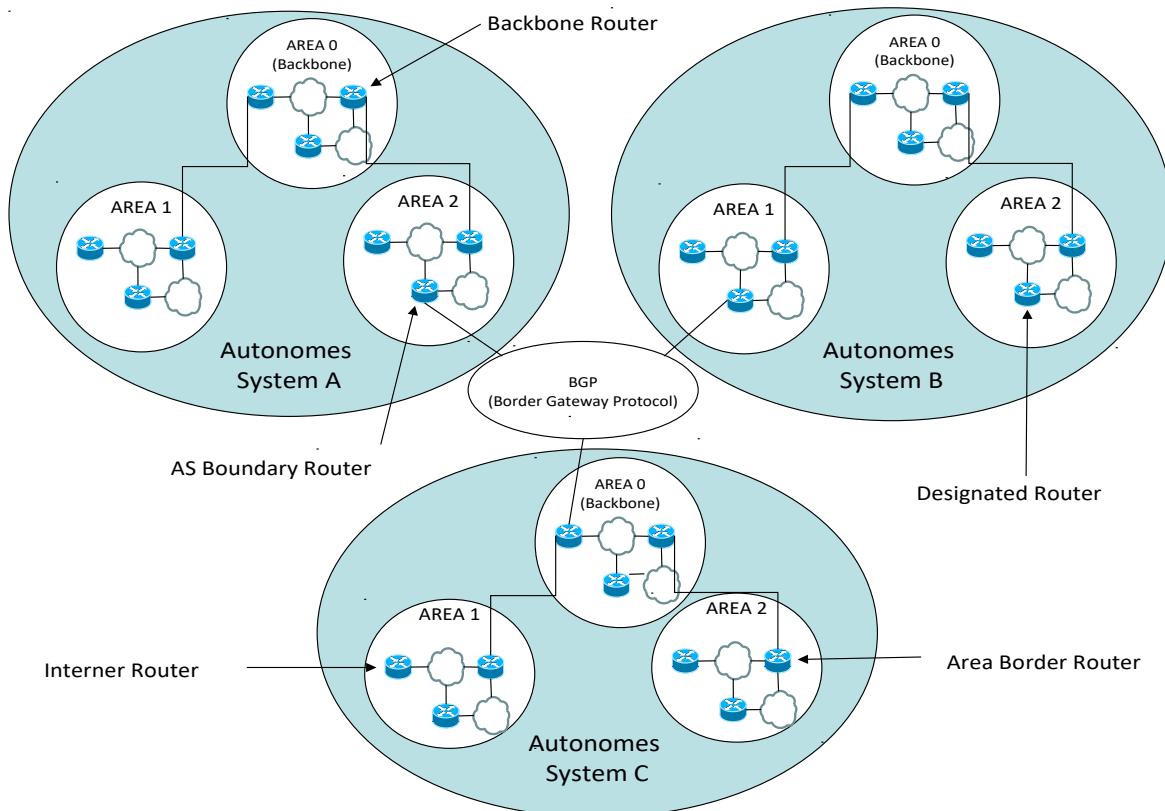


Abbildung 430 : Verbindung autonomer Systeme bei OSPF

Die Klassen können sich natürlich überlappen. So sind z. B. alle Area Border Router Teil des Backbones. Ein Router im Backbone-Bereich der nicht zu anderen Areas eine Verbindung hält ist auch ein internen Router. Dies bedeutet auch, dass Router mehrere Rollen übernehmen können.

32.5.3 - Topologie-Aufbau

Die Topologie eines autonomen Systems kann unterschiedlich dargestellt werden. Zuerst in der herkömmlichen Darstellung.

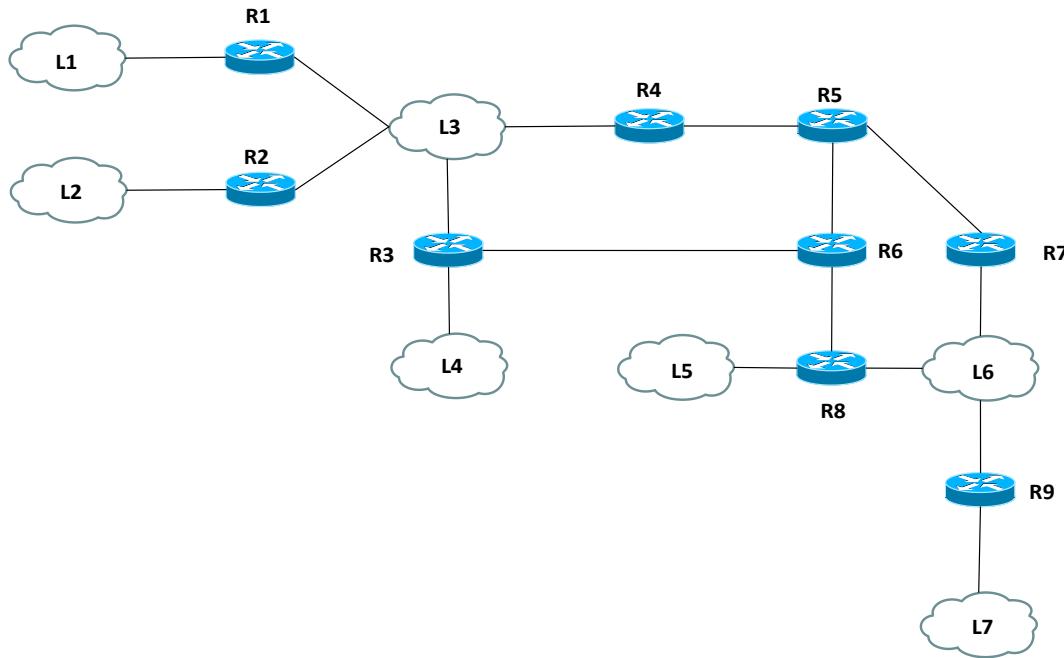


Abbildung 431 : OSPF-Topologie-1

Hier sind sowohl LANs als auch WAN-Verbindungen (Direkte Verbindungen zwischen den Routern) dargestellt. Die WAN-Verbindungen werden hier wie ein LAN mit zwei Netzwerkadressen behandelt.

In der folgenden Graphen-Darstellung werden die Kosten in die einzelnen Netzwerke dargestellt. Für die spätere Berechnung werde nur die Kosten in die Netzwerke verwendet! Deshalb ist bei Netzwerken aus denen keine Routing-Information kommen kann nur der Weg in das LAN mit Kosten bewertet. (Z.B. R1 -> L1 = 3)

Je niedriger die Kosten sind, desto attraktiver ist es für einen Router den Weg auszuwählen.

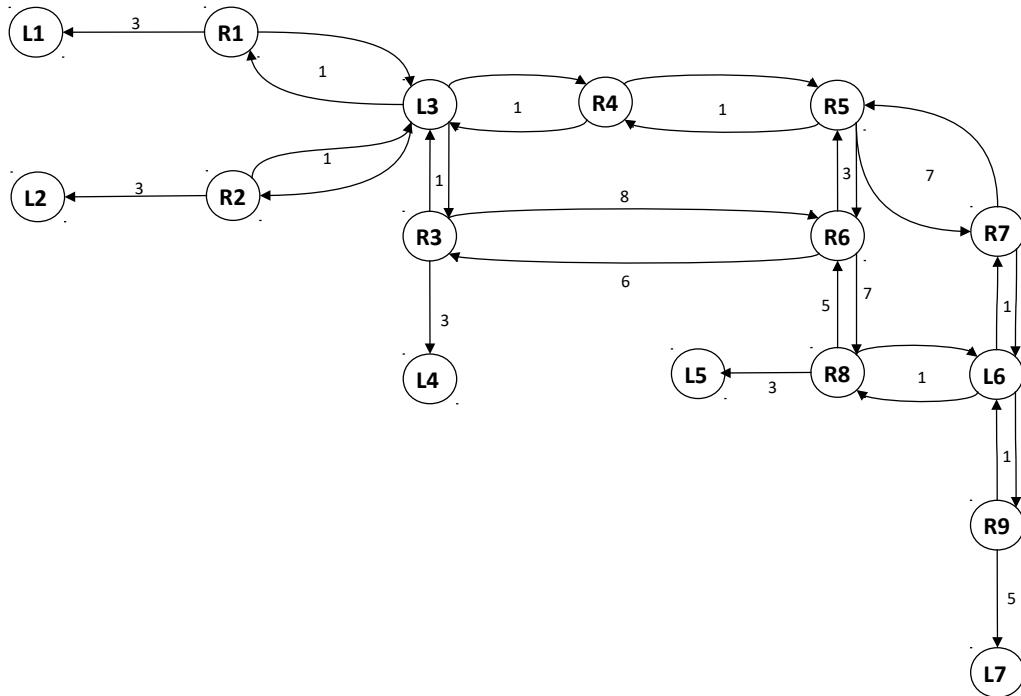


Abbildung 432 : OSPF 2

Sind mehrere Router an einem LAN angeschlossen bildet das LAN einen eigenen Knoten. Bei Punkt-zu-Punkt Verbindungen ist das dazwischen liegende Netzwerk nicht als eigener Knoten ausgebildet.

Die Wege können unterschiedlich bewertet sein. In der obigen Abbildung sind, bis auf die Ausnahme der Verbindung R3 <-> R6, die Kosten sowohl in das Netzwerk als auch aus dem Netzwerk heraus gleich.

Werden die Kosten über redundante Wege gleich gesetzt, erhält man ein einfaches Loadbalancing.

Protokolle

Für die einzelnen Router ergeben sich damit folgende angeschlossenen Netzwerke mit den zugehörigen Kosten. Damit kann für alle Router die LSDB (Link State Data Base) aufgebaut werden.

Die Datenbank ist vollständig, wenn jeder Router von jedem Router eine gültige Liste empfangen hat.

Router	Subnetze mit Kosten
R1	L1 = 3, L3 = 1
R2	L2 = 3, L3 = 1
R3	L3 = 1, L4 = 3
R4	L3 = 1
R5	-
R6	-
R7	L6 = 1
R8	L5 = 3, L6 = 1
R9	L6 = 1, L7 = 5

Damit kann jeder Router seine Sicht auf die Netzwerke zusammenbauen. Die Router R5 und R6 haben keine direkt angeschlossenen LANs und können somit nur bei der Wege-Findung behilflich sein.

Die Kostentabelle von R8 sieht damit folgendermaßen aus

Ziel-Netzwerk	Next Hop	Distance (Kosten)
L1	R7	13
L2	R7	13
L3	R7	10
L4	R7	13
L5	direct	3
L6	direct	1
L7	R9	6

Damit kann der Router R8 einen Graphenbaum aufbauen. Auffällig ist dabei, dass es in jedes LAN nur einen Weg gibt. (Siehe auch Spanning Tree) Er sieht folgendermaßen aus:

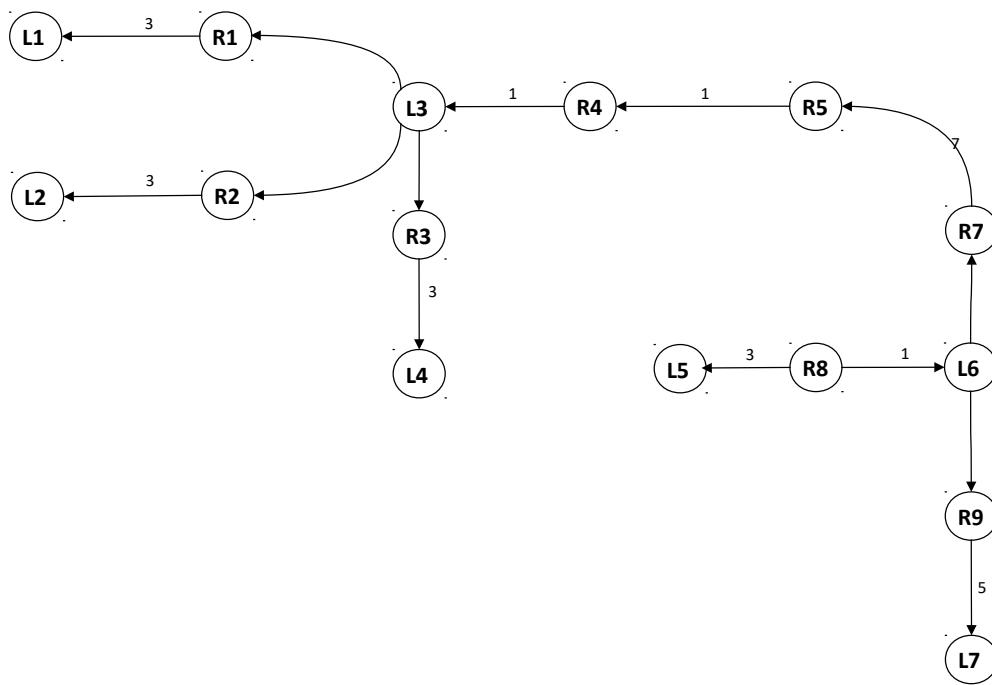


Abbildung 433 : OSPF 3

32.5.4 - Aufbau

32.5.4.1 - Grundlagen

Damit OSPF funktioniert müssen die Router vom Administrator mit einer Router-Priorität versorgt werden. Dies ist eine 8-Bit-Zahl.

Ist dies nicht der Fall, wird anstelle der Router-Priorität die Router-ID verwendet. Dies ist eine 32-Bit-Zahl. Wurde die Router-ID nicht gesetzt, wird die IP-Netzwerk-Adresse verwendet.

32.5.4.2 - Übersicht

Damit die Bearbeitung des Shortest Path First (SPF) funktioniert sind folgende Schritte sind in der angegebenen Reihenfolge durchzuführen:

1. Ermittlung der Designated Router und deren Backup-Router.
2. Ermittlung der Nachbarschaftsbeziehungen.
3. Austausch der Routing-Informationen.

32.5.4.3 - Ablauf

32.5.4.3.1 - Designated Router und Backup-Router

Damit nicht alle Router miteinander kommunizieren müssen und die Netzlast dadurch unnötig hoch ist, wird für jede Area ein Designated Router (DR) sowie sein Stellvertreter (Backup-Router) ermittelt.

Beim Starten senden alle Router HELLO-Pakete an allen Punkt-zu-Punkt Verbindungen und Multicasts in die angeschlossenen LANs an die Gruppe die von allen Routern gebildet wird (AllSPFRouters 224.0.0.5).

Der Router mit der höchsten Router-ID gewinnt die Position des Designated Routers. Da der DR einen Single-Point-of-Failure bildet, gibt es einen Backup-Router (BR). Der BR arbeitet im Hot-Standby-Verfahren. Dies bedeutet, dass er wie der DR zu allen Routern eine Nachbarschaftsbeziehung aufbaut, jedoch keine Link-State-Updates sendet. Fällt der DR aus übernimmt der BR sofort seine Funktion. Danach wird ein neuer BR ermittelt. DR und BR kommunizieren über die Multicast-Gruppe 224.0.0.6.

32.5.4.3.2 - Nachbarschaftsbeziehungen

Zur Ermittlung der Adjacency (deutsch: Nachbarschaft) werden ebenfalls die HELLO-Pakete ermittelt. Hat ein Router einen anderen erkannt, wird ermittelt wer die Master- und wer die Slave-Rolle übernimmt. Dazu dient die Router-ID.

32.5.4.3.3 - Austausch der Routing-Informationen

Ein kompletter Austausch der gesamten Routing-Informationen geschieht nur zwischen direkten Nachbarn. Dazu werden die Database-Description-Pakete ausgetauscht.

Später werden nur in Intervallen oder bei auftretenden Events die Link-State-Updates (LSU) gesendet. Die Nachrichten werden jeweils bestätigt.

Veraltete Informationen werden mittels eines Aging-Algorithmus erkannt, gelöscht und neu angefordert. Dazu dienen die Link-State-Requests.

OSPF nutzt die folgenden Paket-Typen um alle Funktionen abzudecken:

Nachrichten-Typ	Bedeutung
HELLO	Erkennung von Nachbarn und Designated Routern
Link-State-Update	Kosten mit Nachbarn austauschen
Link-State-ACK	Bestätigung eines Link-State-Update
Database Description	Neue Daten verteilen
Link-State-Request	Infos von Nachbarn anfordern

32.5.4.3.4 - Laufender Betrieb

Fällt eine Verbindung aus und ein Router merkt dies aktualisiert er seine LSDB. Danach sendet er ein LSU-Paket an seine Nachbarn.

Kommt ein Router hinzu wird folgender Ablauf abgehandelt.

1. Neuer Router lernt seine Nachbarn kennen (HELLO-Protocol).
2. Aufbau einer Nachbarschaft (Adjacency).
3. Neuer Router baut seine LSDB auf (Exchange-Protocol)
4. Synchronisieren der LSDBs mit den Nachbarn.
5. Berechnung des SPF-Baums.
6. Modifizieren der Routing-Tabellen.
7. Nach der Synchronisation werden die LSUs an die Nachbarn verteilt, die ihrerseits die LSDBs aktualisieren und die LSUs weiterreichen. (Flooding-Protocol)

32.5.5 - OSPF-Pakete

32.5.5.1 - OSPF-Header

1. Version
2. Typ 1 = Hello, 2 = Description, 3 = Request, 4 = Update, 5 = ACK
3. Paket Länge
4. Router-ID
5. AREA-ID
6. Checksumme
7. Authentication Type
8. Authentication: 64-Bit-Feld mit Authentifizierungsinformationen

32.5.5.2 - HELLO-Pakete

Network Mask (Subnetz-Maske des Router-Interface).

HELLO-Interval (z. B. 10 Sekunden).

Optionen.

Router-Priorität für die Auswahl des DR.

Router-Dead-Interval. Dies ist die Zeit bis ein Router den Ausfall seines Nachbars erkennt.

DR. Hier wird die IP-Adresse des DR eingetragen falls der DR das Paket gesendet hat sonst wird 0.0.0.0 eingetragen.

BR. Hier wird die IP-Adresse des BR eingetragen falls der BR das Paket gesendet hat sonst wird 0.0.0.0 eingetragen.

Neighbours. Hier werden die IDs der Router eingetragen von denen bereits gültige HELLO-Pakete empfangen wurden.

32.5.5.3 - Database Description (DD)

1. Interface MTU (Maximale Paketgröße bei der nicht Fragmentiert werden muss).
2. Options
3. Init-Bit. Mit dem Wert = 1 wird angezeigt, dass dies das erste Paket einer DD-Folge ist.
4. More Bit. Mit dem Wert = 1 wird angezeigt, dass weitere DD-Pakete folgen werden.
5. Master/Slave-Bit. Mit dem Wert 1 wird angezeigt, dass der Absender des Paketes Master während des LSDB-Synchronisationsprozesses ist.
6. Sequence-Number. DD-Pakete werden fortlaufend nummeriert.
7. LSA-Header. Er enthält die LSDB-Beschreibung

32.5.5.4 - Link-State-Request

LS-Type

Link-State-ID. Angabe welcher Link angefordert wird.

Advertising Router. ID des Quell-Routers des LSA. Bei DR ist hier dessen ID enthalten.

32.5.5.5 - Link-State-Update

Anzahl der LSAs die im Paket enthalten sind

LSA-Daten (LSA-Header + LSA-Daten)

32.5.5.6 - Link-State-ACK

Wiederholung des LSA-Headers

32.5.5.7 - LSA-Header

1. LSA-Age. Zeit seit der letzten LAS-Generierung

2. Link-State ID

 Typ = 1: ID des Routers der das LSA generiert hat

 Typ = 2: IP-Adresse des Interfaces des DR

 Typ = 3: IP-Adresse des Netz-Zieles

 Typ = 4: ID des Routers der die LSA gesendet hat

3. Advertising Router ID des Routers der die LSA generiert hat

4. LS Sequence Number. Fortlaufende Nummer.

5. LS Checksum. Prüfsumme

6. Length: LSA-Länge in Bytes

32.5.6 - Zusammenfassung

Es lässt sich erkennen, dass eine Topologie-Änderung schnell über alle Router hinweg konvergiert.

Es ist sichergestellt, dass es immer nur einen Weg von einem Netzwerk in ein beliebig anderes Netzwerk gibt.

Durch die Möglichkeit der Area-Bildung sowie der Priorisierung kann der Administrator sehr übersichtliche und effektive Netzwerke aufbauen.

32.6 - IGMP

In einem einzelnen Netzwerk ist Multicasting problemlos möglich. Schwierig wird es, sobald die Multicast-Pakete über Router hinweg zu transportieren sind. Sie wissen erst einmal nicht, an welchen Ports die Kommunikationspartner angeschlossen sind. Multicasts auf allen Ports weiterzuleiten, ist ebenfalls nicht sinnvoll. Daher muss ein Router ermitteln können, an welchem seiner Ports Multicast-Kommunikationspartner angeschlossen sind. Dafür ist ein eigenes Protokoll nötig. Dieses Protokoll wird IGMP (Internet Group Managing Protocol) genannt.

IGMP wird von allen Hosts und Routern unterstützt, die Multicasts bearbeiten. Wie ICMP ist IGMP ein Teil von IP. Damit werden IGMP-Meldungen in IP-Paketen transportiert. Der Wert im IP-Protokoll-Feld ist 2.

32.6.1 - Encapsulation im IP-Paket

IP-Datagramm	
IP-Header	IGMP-Meldung
20 Byte	8 Byte

32.6.2 - Aufbau einer IGMP-Meldung

0	3	4	7	8	15	16	31
4 Bit IGMP-Vers (aktuell = 1)	4 Bit IGMP-Typ (1 = Query) (2 = Response)			8 Bit Nicht benutzt		16 Bit Checksumme	
32 Bit Group-ID							

32.6.3 - Gruppen-Bearbeitung

Um mit Multicasts arbeiten zu können, muss sich ein Gerät bei der Multicast-Gruppe anmelden. Die Mitgliedschaft in einer Multicast-Gruppe ist dynamisch. Ein Prozess kann einer Multicast-Gruppe beitreten und sie wieder verlassen. Dies wird von einem entsprechenden Multicast-API unterstützt. Eine Multicast-Gruppe wird an eine Interfacekarte gebunden. Ein Prozess kann derselben Multicast-Gruppe auf mehreren Interfaces beitreten. Ein Host erkennt eine Gruppe an der Gruppen-Adresse an dem zugehörigen Interface. Die Verwaltung der Gruppen und Interfaces, führt jeder Host für sich einmal in einer Tabelle.

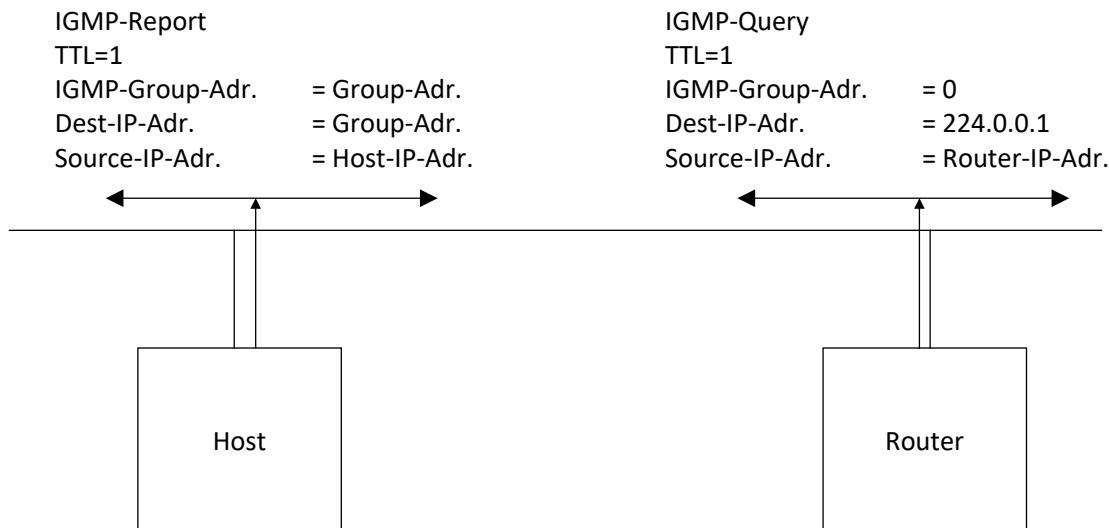


Abbildung 434 : IGMP-Datenaustausch

Wenn ein Host einer Gruppe beitritt, sendet er einen IGMP-Report. Dies geschieht nur beim ersten Beitreten zu dieser Gruppe an diesem Port. (Auch bei mehreren Prozessen) Der Report wird an dem Port ausgesendet, an dem die Gruppen-Zugehörigkeit gelten soll.

Beim Verlassen des Hosts von der Gruppe wird kein Report gesendet.

Ein Multicast Router sendet zyklisch IGMP-Query's auf allen parametrierten Interfaces um zu ermitteln, ob sich ein Multicast-Host an diesem Interface befindet. Auf diesen IGMP-Query meldet sich ein Multicast-Host mit einem IGMP-Report für jede Gruppe, die mindestens noch einen Prozess auf diese Gruppe gebunden hat. Dies geschieht mit einer zufälligen Verzögerung, damit nicht mit einer Report-Lawine auf einen Query reagiert wird und von evtl. mehreren Hosts gleichzeitig das Netzsegment blockiert wird. Außerdem kann ein Host, der einen Report senden müsste, und auf seinem Interface von einem anderen Host einen Report für seine Gruppe erkennt, auf seinen Report verzichten. Dem Router reicht es zu wissen, dass an einem Interface mindestens ein Multicast-Host angeschlossen ist. Damit baut der Multicast-Router eine Tabelle auf. Sobald ein Router einen Multicast empfängt, überprüft er anhand dieser Tabelle, auf welchem Interface er den Multicast weitergeben muss.

Bei einem einfachen Netzwerk (ohne Router) werden nur einmal IGMP-Reports gesendet wenn sich ein Prozess bei der Multicast-Gruppe anmeldet.

Der TTL-Wert ist normalerweise auf 1 gesetzt. Somit beschränkt sich die IGMP-Meldung auf ein Subnetz. Von den Routern werden keine ICMP-TTL-EXCEEDED-Meldungen erzeugt.

Für bestimmte Server gibt es den Sonderfall des Expanding Ring Search (deutsch: erweiternder Ring beim Suchen)

Dabei wird zuerst mit dem TTL-Wert = 1 nach einem Multicast-Server gesucht. Kommt keine Reaktion zurück wird es mit dem TTL-Wert = 2 versucht. Kommt auch hier keine Reaktion zurück, dann wird es mit dem TTL-Wert = 3 versucht usw.

Damit kann eine Applikation z. B. Ihren Server in mehreren Hop-Schritten finden. Es gibt einen Multicast-Group-ID-Bereich der nie weiter als einen Hop suchen kann, da der Router ihn auf keinen Fall weiterleitet:

224.0.0.0 bis 224.0.0.225

Ein Router wird das Paket auf jeden Fall, ungeachtet des TTL-Wertes, verwerfen.



32.6.4 - All-Hosts-Group

Ein Router sendet seine IGMP-Query an die Multicast-Group-ID:

224.0.0.1

Diese Adresse wird auch All-Hosts-Group-ID genannt. Jeder Host tritt automatisch dieser Gruppe auf allen Interfaces beim Initialisieren bei. Die Zugehörigkeit zu dieser Gruppe wird nie in einem Report mitgeteilt.

32.6.5 - Informationen

Informationen über die Gruppen-Zugehörigkeit liefert das netstat-Kommando. Z.B. netstat -nia

33 - Link Aggregation (LA)

Mithilfe von Link Aggregation (LA) ist es möglich, mehrere physikalische Verbindungen zu einer logischen Verbindung namens Link Aggregation Group (LAG) zu bündeln.

Damit kann:

- Durch die Parallele Nutzung von mehreren Leitungen die Gesamtdatendurchsatzrate erhöht werden.
- Solange mindestens ein Link noch funktioniert bleibt die Gesamtkonnektivität bei Ausfall einzelner Verbindungen erhalten. Eine LAG bietet ein automatisches Recovery bei Ausfällen von einzelnen physischen Links.
- Netze und Netzwerkanschlüsse lassen sich einfacher und flexibler skalieren

Je nach Hersteller werden hierfür auch die Begriffe Trunking (Brocade / Sun Microsystems), Etherchannel (Cisco), Bonding (Linux-Umfeld), Port Aggregation (HP) oder Teaming (Novell Netware / Microsoft Windows) verwendet.

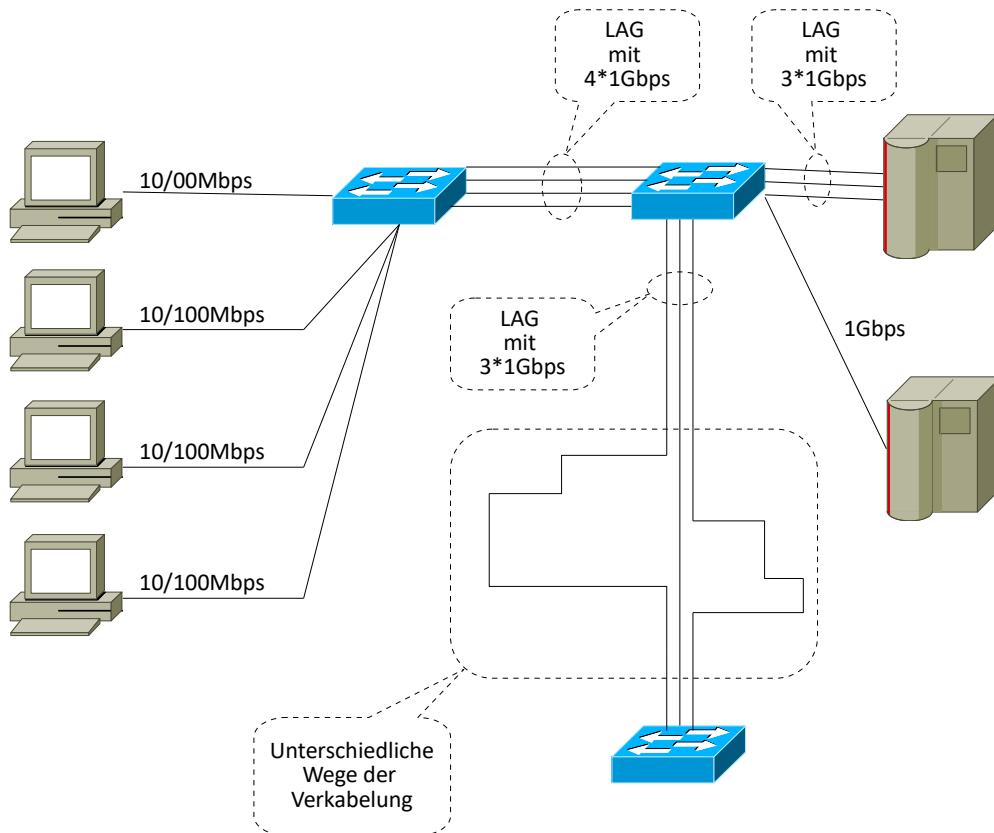


Abbildung 435: Link Aggregation

33.1 - Historisches

Nachdem einige Hersteller schon länger proprietäre Lösungen auf dem Markt hatten, arbeitete man ab Juli 1998 bei der IEEE an einem Trunking-Protokoll in einer Link-Aggregation Task Force.

Im Jahr 2000 standardisierte das IEEE die Link Aggregation im [IEEE802.3ad]. Wie am Standard 802.3 erkennbar ist, kann er nur auf Ethernet angewendet werden.

2008 erschien ein überarbeiteter Standard unter [IEEE802.1AX-2020]. Die aktuelle Version wurde 2020 veröffentlicht.

33.2 - Aufbau

Grundsätzlich gibt es 2 Varianten der Link Aggregation.

34 - Static Link Aggregation

Bei der statischen Link Aggregation werden alle Konfigurationsparameter einmalig auf beiden beteiligten Komponenten einer LAG eingerichtet. Statische LAGs reagieren nur bedingt auf Änderungen.

35 - Dynamic Link Aggregation

Mittels des Link Aggregation Control Protocols (LACP) werden die erforderlichen Parameter ausgetauscht, die Verbindungen überwacht und ggf. geändert. Die Informationen werden dabei in Form von Link Aggregation Control Protocol Data Units (LACPDU)s als Multicast mit der MAC-Adresse 01:80:c2:00:00:02 (01-80-c2-00-00-02) gesendet.

LACPDUs werden während der Detection-Phase einmal pro Sekunde gesendet.

Während des Betriebs werden die Keepalive-LACPDUs jede Sekunde (fast) / alle 30 Sekunden (slow) ausgetauscht.

Bei LACP kann jeder einzelne Port als Active LACP oder Passive LACP konfiguriert werden:

- Passive LACP: der Port bevorzugt von sich aus keine LACPDUs zu übertragen. Nur wenn die Gegenstelle Active LACP hat, überträgt der Port LACPDUs (preference not to speak unless spoken to).
- Active LACP: der Port bevorzugt LACPDUs zu übertragen und somit das Protokoll zu sprechen - unabhängig davon ob die Gegenstelle Passive LACP hat oder nicht (a preference to speak regardless).

36 - Vorteile von LACP gegenüber einer statischen Link Aggregation:

- Ein Ausfall eines physischen Links wird selbst dann erkannt, wenn die Punkt-zu-Punkt Verbindung über einen Media Konverter läuft und damit der Link-Status am Switchport auf Up bleibt. Da LACPDUs auf dieser Verbindung damit ausbleiben, wird dieser Link aus der LAG entfernt. Somit gehen darüber keine Pakete verloren.
- Die beiden Geräte können sich gegenseitig die LAG Konfiguration bestätigen. Bei statischer Link Aggregation werden Konfigurations- oder Verkabelungsfehler oft nicht so schnell erkannt.

36.1 - Funktionsweise

Bei der Link-Aggregierung werden unabhängige physikalische Verbindungen zu einer Link Aggregierungs Gruppe (LAG) zusammengefasst, die auch über unterschiedliche Wege verlegt werden können.

Teilnehmer einer Verbindung auf Ebene 2 im ISO-7-Schicht-Modell gehen davon aus, dass die Frames in der Reihenfolge ankommen, in der sie abgesendet wurden. Überholvorgänge sind nicht vorgesehen. Deshalb gibt es auf MAC-Ebene keine Mechanismen zur Überwachung und eventuell notwendigen Korrektur der Paket-Reihenfolge.

Würden die Frames über alle möglichen Verbindungen transportiert werden, wäre die Reihenfolge von Frames und somit auch Paketen eventuell nicht mehr gegeben.

Um die Reihenfolge sicher zu stellen, werden Rahmen, die zu einer Session gehören, immer über den selben Link gesendet. Die anderen Verbindungen bleiben ungenutzt. Damit wird auch ersichtlich, dass wenn immer nur eine Session zu einem Zeitpunkt Daten austauscht keine Datendurchsatz-Verbesserung möglich ist. Erst wenn mehrere Sessions gleichzeitig Daten austauschen, kann das Potential von mehreren Verbindungen genutzt werden.

Die Konsistenz der der MAC-Tabellen wird sichergestellt, indem logische Ports definiert werden, welche wiederum die physikalischen Ports beinhalten. Die logischen Ports werden darum auch Aggregierungs-Ports genannt.

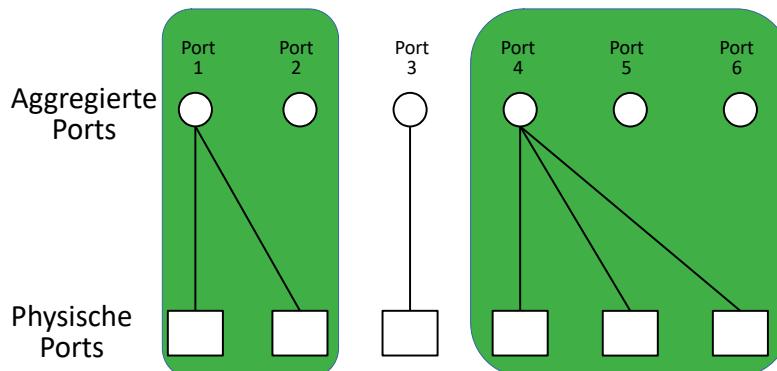


Schaubild 1: Port-Aggregierung

Um die MAC-Adresszuordnung zu vereinfachen werden alle Verbindungen auf die kleinste Portnummer (MAC-Adresse) gelegt.
Soll der Switch einer MAC-Adresse etwas zusenden verwendet er den logischen Port (hinter dem die MAC-Adressen zugeordnet sind). Selbst wenn sich bei den MAC-Adressen etwas ändert, bleibt es aus Switching-Vorgangs-Sicht, bei den logischen Ports.
[NI-2001-02]

Bei Änderungen ergeben sich Probleme, wenn ein Port mit einer niedrigeren Nummer als der aktuell niedrigsten Nummer in eine LAG eingefügt werden soll. Beim Entfernen des Ports aus der LAG ist ebenfalls ein neuer niedrigster Port zu ermitteln.

Erweiterung in der MAC-Layer

Nach oben zur LLC-Schicht hin handelt das 802.3-MAC-Client-Interface wie bisher. Damit ist die Link-Aggregation für die übergeordneten Ebenen transparent.

Die Steuerung erfolgt durch die eingefügten Schichten der Link Aggregation Control (LAC) mittels des Link Aggregation Control Protocol (LACP). Dafür gibt es ein Modell mit 3 Ebenen:

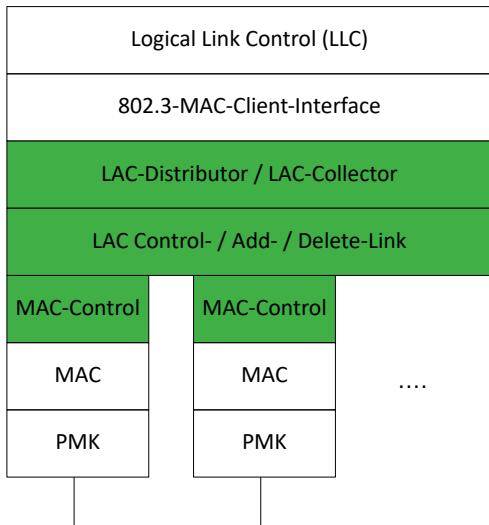


Abbildung 436: Einfügen der LAC 802.3 MAC anspricht.

- LAC Distribution/Collector – Teilschicht. Sie dient als Multiplexer / Demultiplexer. Für die Verteilung sind keine Algorithmen festgelegt. Es ist nur die Paketreihenfolge einzuhalten und es dürfen keine Frames dupliziert werden. FreeBSD verwendet dazu beispielsweise eine Hash des Protokoll Headers. Der Hash beinhaltet dabei Ethernet/MAC Quell- und Zieladressen, falls verfügbar ein VLAN-Tag, sowie IPv4/IPv6 Quell- und Zieladressen.
- LAC Control – Teilschicht, die physische Links dem logischen Aggregat hinzufügt und wegnimmt.
- MAC Control – Teilschicht, die die herkömmliche IEEE

36.2 - Voraussetzungen

Um mehrere Links zu einer LAG zu bündeln, müssen folgende Voraussetzungen erfüllt sein:

- die Datenübertragungsraten der einzelnen Verbindungen einer LAG müssen gleich sein
- Die Links müssen im Vollduplex-Modus arbeiten
- Es sind nur parallele Punkt-zu-Punkt Verbindungen möglich
- die einzelnen Links müssen auf den gleichen Geräten enden (gleicher Switch oder gleicher Server)

37 - Verkehrsaufteilung innerhalb einer LAG

Wie hoch der tatsächlich erzielbare Durchsatz für alle oder einzelne Geräte auf einer logischen Verbindung ist, hängt stark von der verwendeten Lastverteilungsmethode ab. Werden Datenframes beispielsweise aufgrund gleicher Ziel-MAC-Adressen und Absender-MAC-Adressen immer auf den gleichen physischen Port gesendet, bleibt die Datenübertragungsrate auf die Geschwindigkeit dieses physischen Links begrenzt. Einzelne Geräte profitieren in dieser Konstellation nicht von der wesentlich höheren Gesamtdatenübertragungsrate der logischen Verbindung.

38 - Firewalls

38.1 - Allgemeines

Der Begriff Firewall kommt aus dem Bereich des Brandschutzes. Mit Brandschutzmauern soll das Übergreifen eines Feuers von einem Gebäudeabschnitt auf einen anderen verhindert werden. Übertragen auf Rechnernetze soll dies bedeuten, dass Rechnernetze voneinander getrennt werden. Ein Rechnernetz das „Feuer gefangen hat“, also einem Eindringling bereits nachgegeben, hat soll gegenüber einem anderen Rechnernetzwerk abgeschottet werden.

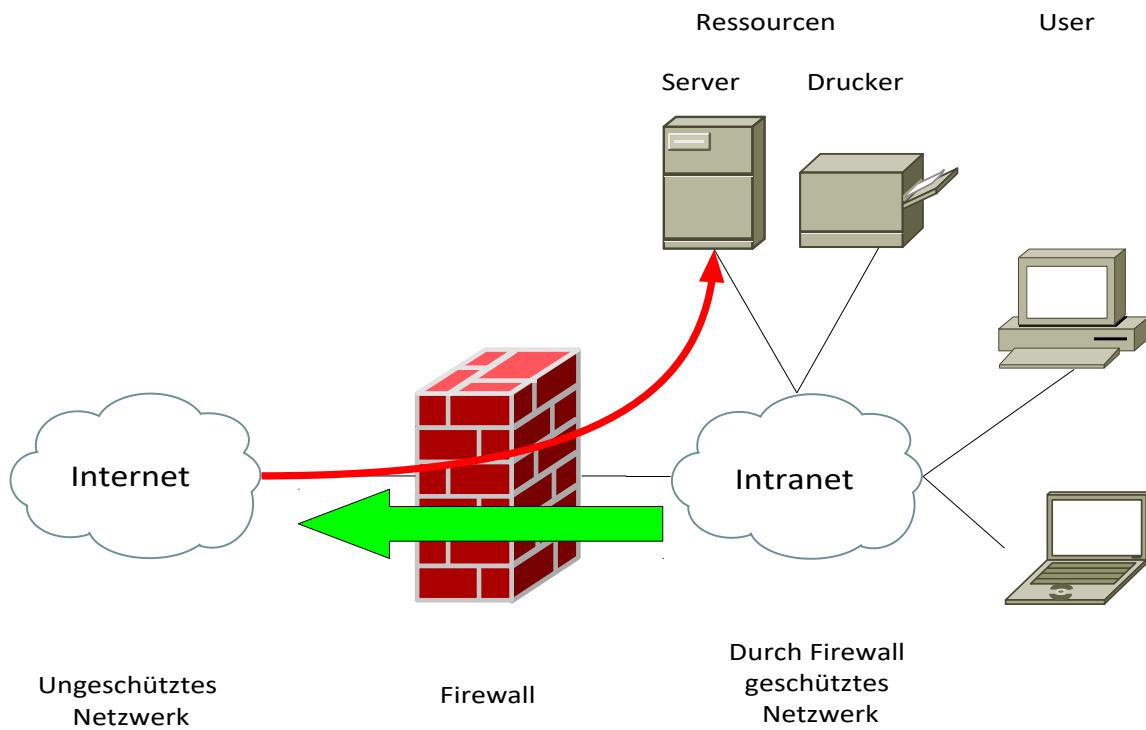


Abbildung 437 : Eine Firewall trennt Rechnernetze

Das ungeschützte Netzwerk (im obigen Beispiel das Internet) wird mit einer Firewall von einem internen Netzwerk (oben im Intranet) getrennt.

Im Normalfall kann von den Usern nur eine Verbindung von innen nach Außen aufgebaut werden. Ein Verbindungsaufbau von außen nach innen ist vorerst nicht möglich.

Es ist jedoch auch möglich den Server für Benutzer aus dem Internet zur Verfügung zu stellen. Dabei wird eine gezielte Verbindung vom Internet auf den Server zugelassen und überwacht. Im obigen Beispiel ist dies nur vereinfacht dargestellt. In der Praxis kann dies in mehreren Sicherheitsstufen, also mit mehreren Firewalls durchgeführt werden. Dabei werden die Server wiederum in speziellen Netzwerken, den DMZs (Demilitarisierte Zonen) separat untergebracht.

Grundsätzlich sollten in einer Firewall die folgenden Funktionen realisiert sein:

- Trennung von mindestens zwei Netzwerken
- Erfüllung einer Sicherheitsstrategie (engl. Policy)
- Protokollierung
- Authentifizierung

Firewalls

Firewalls werden oft als das Mittel der Wahl zum Thema Sicherheit angesehen. Zum einen versprechen die Hersteller, dass alle möglichen Angriffe damit abgewehrt werden können, zum anderen bieten Firewalls mit einer Vielzahl von zusätzlichen Eigenschaften wie z. B. die Terminierung von VPNs eine unüberschaubare Vielzahl von Funktionalitäten. Daher ist es zuerst einmal notwendig die Unterscheidungsmerkmale kennen zu lernen um später die unterschiedlichen Einsatzszenarien zu untersuchen.

38.2 - Unterscheidungsmerkmale

Firewalls können in einem ersten Schritt anhand der Anzahl der NIC (Network Interface Controller (deutsch: Netzwerk-Karten) oder auch ihrer Einbindung in die Netzwerk-Architektur unterschieden werden.

38.2.1 - Anbindung

38.2.1.1 - Dual-Homed Firewall

Eine Firewall dieser Klasse ist in zwei Netzwerken „beheimatet“. Ein Beispiel ist in der folgenden Abbildung zu sehen.

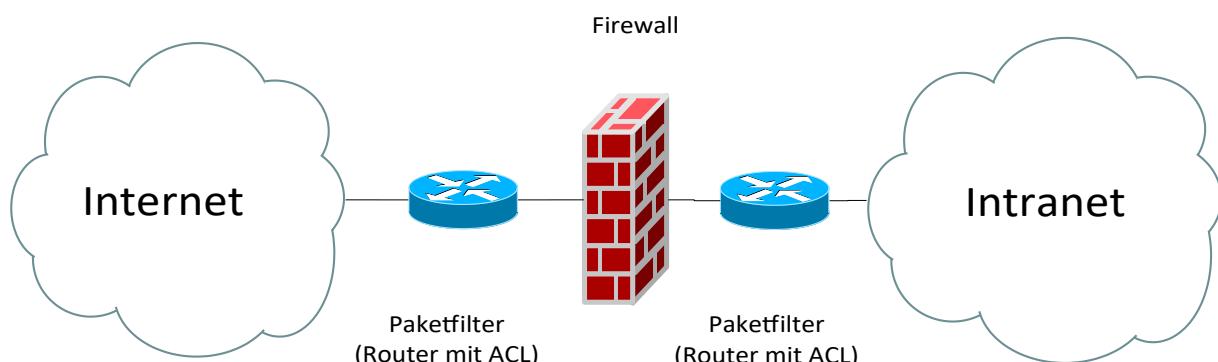


Abbildung 438 : Dual-Homed Firewall

Das Routing zwischen den beiden Netzwerk-Karten ist deaktiviert. Deshalb wird diese Architektur auch Split Screened Subnet Architecture genannt. Damit können Pakete nur auf höherer Ebene weiter geleitet werden. Dies wird durch einen Bastionsrechner mit Applikationsfilter auf Ebene 7 durchgeführt. Zusätzlich können noch Paketfilter vor und nachgeschaltet werden damit nur korrekte IP-Adressen an die Firewall zur Verarbeitung übergeben werden.

38.2.1.2 - Screened-Host Firewall

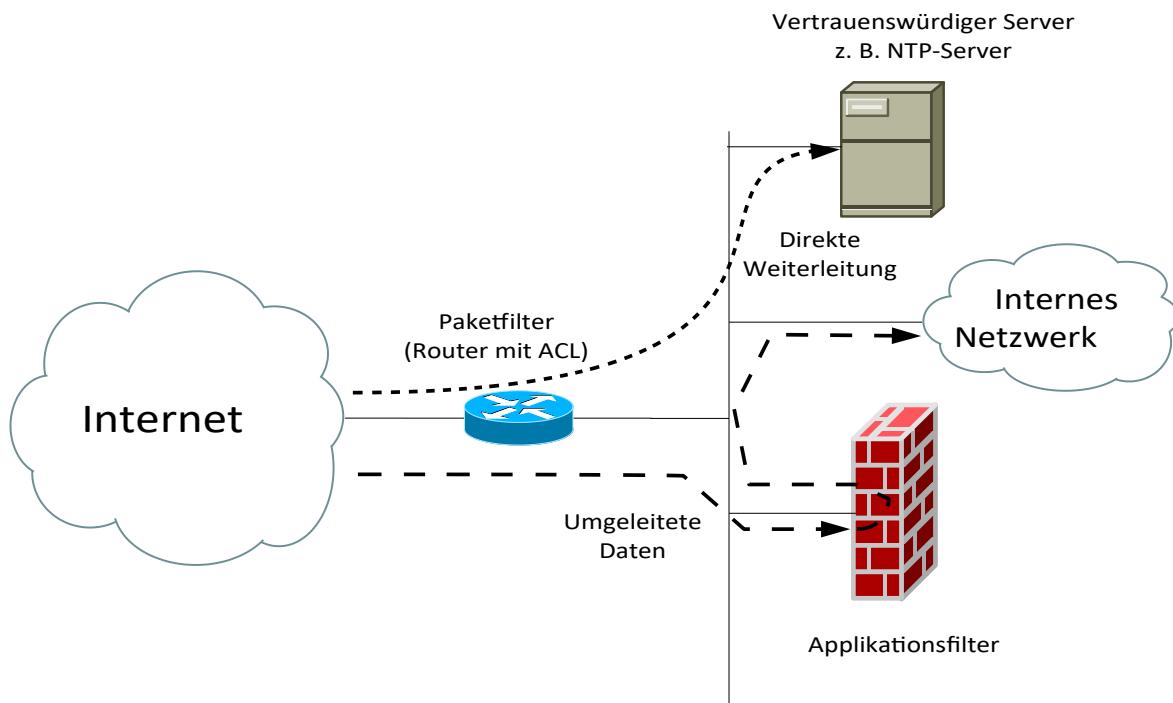


Abbildung 439 : Screened-Host Firewall

Bei dieser Architektur wird durch die Firewall das interne Netzwerk nicht mehr physikalisch abgetrennt sondern nur noch logisch.

Als zentrale Schaltstelle dient ein Paketfilter. Er leitet Pakete entweder direkt an Server die von außen zugänglich sein sollen oder an die Firewall. Die Firewall überprüft dann ob die Pakete an das interne Netzwerk weiter geleitet werden dürfen oder nicht.

Dies bietet eine erhöhte Flexibilität, die mit dem Risiko der unsachgemäßen Konfiguration verbunden ist. Deshalb sollte diese Architektur nur bei einer unumgänglichen Forderung nach dieser Flexibilität eingesetzt werden.

38.2.1.3 - Screened-Subnet Firewall

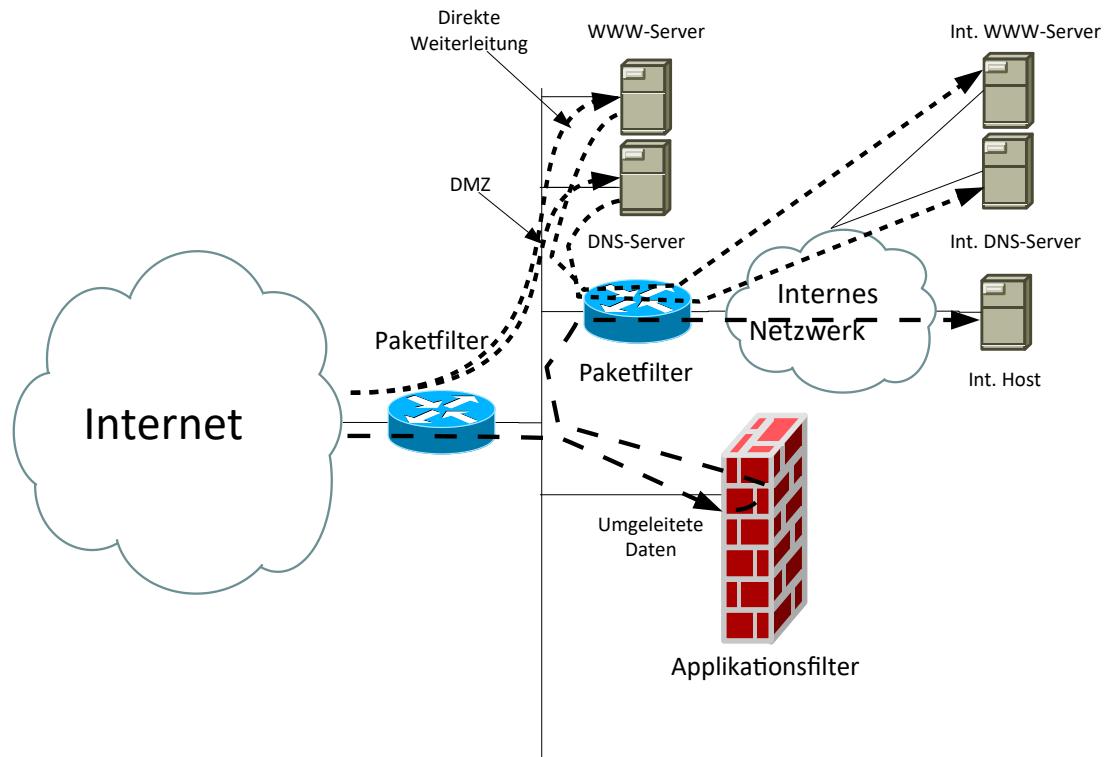


Abbildung 440 : Screened-Subnet Firewall

Durch eine Erweiterung mit einem zusätzlichen Router kann das interne Netzwerk zusätzlich isoliert werden. Damit steht die Firewall in einem eigenen Netzwerk, das auch Perimeter-Netzwerk oder DMZ (Demilitarisierte Zone) genannt wird. In diesem Subnet können noch weitere, von außen erreichbare Server platziert werden. Diese Server können im internen Netzwerk Partner haben.

38.2.2 - Typen

Je nach Ebene auf der die Filterung angesiedelt ist werden verschiedenen Typen unterschieden.

38.2.2.1 - Paketfilter

Bei Paketfiltern werden die Datenpakete auf Ebene 2 bis 4 untersucht. Je nach Parametrierung werden diese Pakete verworfen oder weiter geleitet. Dies kann bei den meisten Routern bereits mit „Bordmitteln“ gemacht werden. In den Zugriffslisten (engl. ACLs Access Control List) können IP-Adressen und Ports definiert werden, die eine Weiterleitung oder Zurückweisung zur Folge haben.

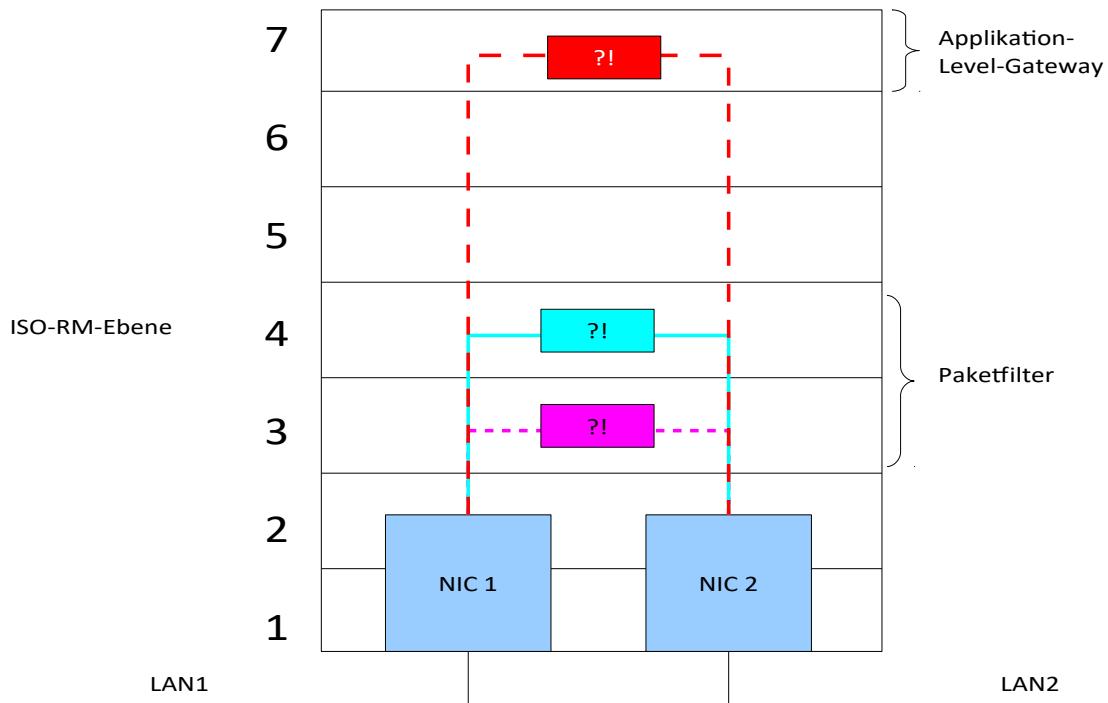


Abbildung 441 : Zuordnung von Paketfiltern zu ISO-RM-Ebenen

38.2.2.2 - Zustandslose Filterung (stateless inspection)

Bei den zustandslosen Paketfiltern kann bei einem Datenpaket nicht darauf eingegangen werden ob die Verbindung vorher ordnungsgemäß aufgebaut wurde. Dies ist natürlich vom verwendeten Protokoll abhängig. Bei TCP wäre es möglich bei UDP nicht. Ein Kontext mit der Zugriffs-Vergangenheit ist nicht herstellbar. Damit können die Pakete einfacher und somit schneller verarbeitet. Die Konfiguration ist statisch und deshalb nicht in der Lage Protokolle zu transportieren, die ihre Ports dynamisch bearbeiten.

38.2.2.3 - Zustandsbehaftete Filterung (stateful inspection)

Hier können, abhängig beim verwendeten Protokoll, die Pakete im Zusammenhang mit der Vergangenheit überprüft werden. Dies ist nur bei verbindungsorientierten Protokollen wie TCP möglich. Datenpakete werden z. B. hier nur weiter geleitet, wenn vorher ein Verbindungsaufbau ordnungsgemäß durchgeführt wurde. Durch diese Vorgehensweise können auch dynamisch agierende Protokolle bearbeitet werden. Die Firewall ist über den Verbindungszustand informiert und handelt danach. Alle Firewalls die mit iptables im Betriebssystem Linux arbeiten sowie die PIX Firewall von Cisco fallen unter diesen Typ. Die Firewall-1 von Checkpoint fällt ebenfalls in diese Klasse.

38.2.2.4 - Proxy Firewall

Hier übernimmt die Firewall die Funktion eines Stellvertreters. Anstelle eines Server tritt die Firewall auf den Plan und übernimmt gegenüber einem externen Client die Funktion des Servers. Gegenüber dem Server übernimmt die Firewall die Funktionen des Clients.

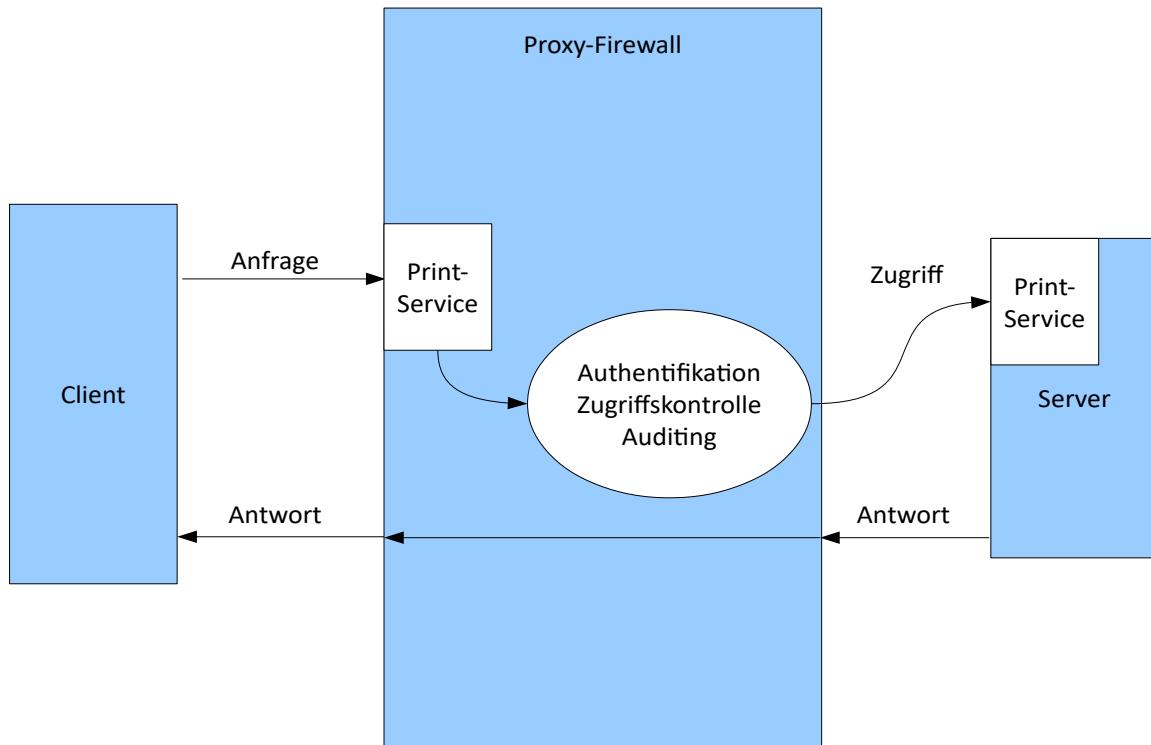


Abbildung 442 : Proxy-Firewall

38.2.2.5 - Application-Level-Gateways

Bei den Application-Level-Gateways sind die Pakete bis zur Ebene 7 des ISO-RM zu bearbeiten. Dies bietet die Möglichkeit applikationsspezifische Eigenheiten zu beachten. Erst damit können Protokolle verwendet werden, die z. B. IP-Adressen im Datenteil austauschen. Eine solche Firewall kann bei FTP zwischen einem PUT- und einem GET-Befehl unterscheiden und ihn zulassen oder unterbinden.

38.2.2.6 - Personal Firewalls

Seit einigen Jahren gibt es genannte Personal Firewalls, die auf PCs installiert werden können. Diese Firewalls sind mittlerweile nicht nur in der Lage den Netzwerk-Verkehr zu überwachen sondern auch z. B. den Start von Programmen und vieles mehr. Seit dem Servicepack 2 hat Windows XP eine solche Firewall in das Betriebssystem integriert.

38.2.3 - Accesslisten

Da Cisco an dieser Stelle eine reichhaltige Auswahl an Möglichkeiten bietet sind die folgenden Beispiele auf das IOS (Betriebssystem von Cisco-Router) zugeschnitten.

38.2.3.1 - Einführung

Mit Zugriffslisten kann der Datenverkehr, über Cisco-Router hinweg, limitiert werden.

Dabei sind folgende Parameter relevant:

- Quell-IP-Adresse
 - Quell- und Ziel-IP-Adresse
 - IP-Protokoll-Typen (TCP, UDP, ICMP)
 - Quell- / Ziel-TCP-Dienste (z. B. Sendmail, Telnet)
 - Quell- / Ziel-UDP-Dienste (z. B. Bootp, Netbios Datagramm)
 - ICMP-Protokoll-Dienste (z. B. Echo..)

Die Verwendung von Zugriffslisten erfolgt in zwei Schritten:

1. Definieren von Zugriffslisten
 2. Zuordnen der Zugriffslisten zu einer Schnittstelle

38.2.3.2 - Definieren von Zugriffslisten

Es gibt, je nach verwendetem Router, unterschiedliche Implementierungen und Versionen die für die Definition von Zugriffslisten welche unterschiedliche Möglichkeiten eröffnen. Dies bedeutet, dass im Einzelfall jeweils zu überprüfen ist, welche Möglichkeiten das zur Verfügung stehende IOS bietet.

Es gibt sowohl benannte als auch nummerierte Zugriffslisten. Die benannten Zugriffslisten werden aufgrund von zugewiesenen Namen unterschieden. Die nummerierten Zugriffslisten werden durch Nummern voneinander unterschieden.

Es gibt verschiedene Arten von nummerierten Zugriffslisten. Die Unterscheidung erfolgt durch die Listen-Nummer, welche im **access-list**-Befehl anzugeben ist.

Listen-Nummernbereich	Bedeutung
1 – 99	Standard-IP-Zugriffsliste
100 – 199, 1000-1999	Erweiterte-IP-Zugriffsliste
700 - 799	MAC-Zugriffsliste
800 – 899	Standard-IPX-Zugriffsliste
900 – 999	Erweiterte IPX-Zugriffsliste

Zugriffslisten bestehen aus einer Folge von Befehlen in denen die Bearbeitung von Paketen erlaubt oder verboten wird.

Eine Zugriffsliste kann mehrere Zeilen (Einträge) enthalten und wird sequentiell abgearbeitet. Sobald die Paket-Parameter mit denen eines Listeneintrags übereinstimmen, wird aufgrund des **permit** oder **deny** Codeworts die weitere Bearbeitung des Pakets durchgeführt oder abgebrochen. Trifft kein Listeneintrag zu, wird das Paket verworfen. Dies trifft natürlich nicht zu, wenn auf eine Schnittstelle keine Zugriffsliste gebunden wurde.

38.2.3.3 - Syntax für eine Standard-Zugriffsliste

access-list [list-number] [**permit|deny**] [source-address] [wildcard-mask] [**log**]

list-number Zugriffslisten-Nummer im Wertebereich von 1–99 (Bezeichnung der Zugriffsliste)

Firewalls

permit	Trifft die Quell-IP-Adresse zu wird das Paket weiter bearbeitet.
deny	Trifft die Quell-IP-Adresse zu wird das Paket verworfen.
source-address	Quell-IP-Adresse oder Quell-IP-Adress-Bereich.
wildcard-mask	Obwohl diese Maske das Aussehen einer Subnetzmaske hat, ist ihre Funktionsweise eine Andere. Sie entspricht einer Platzhalter-/Freigabe-Maske. Mit einer Platzhalter-Maske hat der Administrator die Möglichkeit Adress-Bereiche anzugeben, die entlang der Bit-Grenze binärer Zahlen verlaufen. Kann auch als umgekehrte Subnetzmaske betrachtet werden. 0 bedeutet, dass die Stelle nicht betrachtet werden muss. 1 bedeutet, dass die Stelle relevant ist. Beispiele: 0.0.0.255 entspricht allen Zahlen von 0 – 255 im 4. Oktett 0.0.3.255 entspricht allen Zahlen von 0 - 3 im 3. Oktett und allen Zahlen im 4. Oktett. Entfällt die Wildcard-mask kann in der source-address eine einzelne Quell-IP-Adresse angegeben werden.
log	Mit dem Schlüsselwort log wird ein Eintrag in das Logbuch vorgenommen, falls der Listen-Eintrag mit einem Paket übereinstimmt.
host	Dient zur Definition einer einzelnen Quell-IP-Adresse. Entspricht dem Weglassen der Wildcard-mask.
any	Dient zur Beschreibung von allen möglichen Quell-IP-Adressen. Entspricht einem source-address-Eintrag von 0.0.0.0 mit einem Wildcard-mask-Eintrag von 255.255.255.255

38.2.3.4 - Zuordnung zu einer Schnittstelle

Nachdem die Zugriffsliste definiert wurde, ist sie noch einem Interface zuzuordnen.

Die Zuordnung von Zugriffslisten, kann für eine Schnittstelle in eingehender, als auch in abgehender Richtung, definiert werden.

Damit erfolgt die Paket-Bearbeitung in einem Cisco-Router mit folgenden Schritten

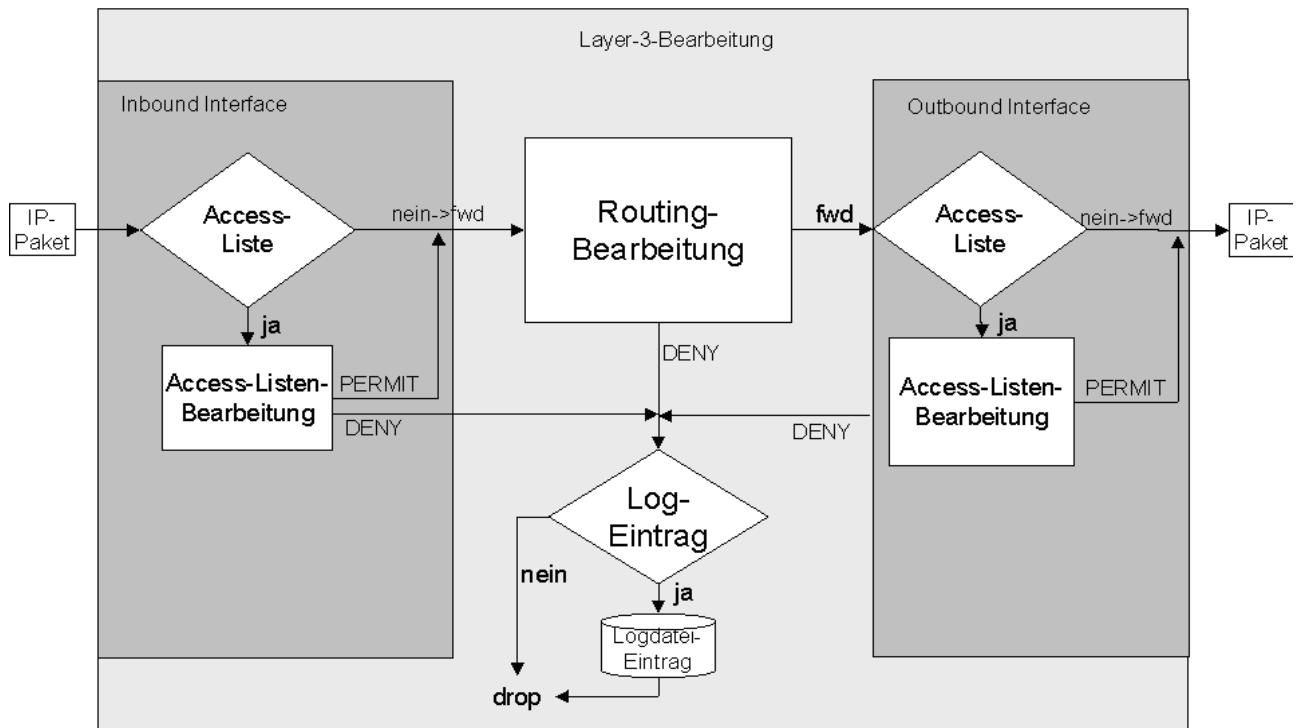


Abbildung 443 : Accesslisten-Bearbeitung

Somit kann es für ein Paket drei Hürden geben, die zu überwinden sind, bis es am Ausgangsinterface ausgegeben wird.

Es ist klar, dass sowohl die Zugriffslisten-Bearbeitung am Eingang und am Ausgang als auch die Routing-Bearbeitung Zeit benötigt. Die Zeitverzögerung ist abhängig von der Performance sowie vom Umfang der Zugriffslisten. Die Zugriffslisten sind deshalb so kurz wie möglich zu halten!

38.2.3.5 - Beispiel-Ablauf:

```

router>en
In Enablemodus gehen
router><enablepasswort>
Enablepasswort eingeben
router#config terminal
In Konfigurationsmodus gehen
router(config)#access list 1 permit 10.20.30.0 0.0.0.255
Zugriffsliste definieren
router(config)#interface fastethernet 0
Interface auswählen
router(config-if)#ip access-group 1 out
Zugriffsliste dem Interface
zuweisen
router(config-if)#^Z
Konfigurationsmodus beenden
router#

```

38.2.3.6 - Bearbeitungsschritte

Ein eingehendes Paket durchläuft bei der Bearbeitung der Zugriffslisten folgende Schritte

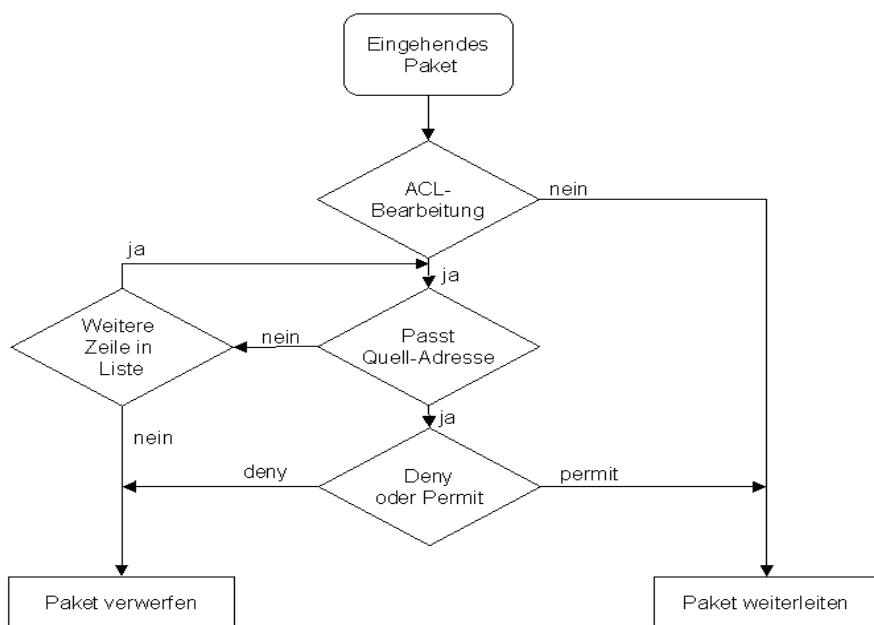


Abbildung 444 : Zugriffslisten-Bearbeitung

38.2.3.7 - Erweiterte Zugriffslisten

Bei den Standard-Zugriffslisten war es nur möglich auf Quell-IP-Adressen zu filtern. Die erweiterten Zugriffslisten ermöglichen es auf Ziel-IP-Adressen, Ports (TCP oder UDP-Ports) und Protokolle (ip, eigrp, gre, igmp, igrp, ipinip, nos ospf, tcp, udp) zu filtern.

Syntax:

```
access-list [list-number] [permit|deny] [protocol | protocol keyword] [source-address source-wildcard] [source port] [destination-address destination-wildcard] [destination port] [log] [options]
```

list-number	Zugriffslisten-Nummer im Wertebereich von 100–199 (Bezeichnung der Zugriffsliste)
permit	Trifft die Paketdefinition zu wird das Paket weiter bearbeitet.
deny	Trifft die Paketdefinition zu wird das Paket verworfen.
source-address	Quell-IP-Adresse oder Quell-IP-Adress-Bereich.
source-wildcard	Obwohl diese Maske das Aussehen einer Subnetzmaske hat, ist ihre Funktionsweise eine andere. Sie entspricht einer Platzhalter/Freigabemaske. Mit einer Platzhaltermaske hat der Administrator die Möglichkeit Adress-Bereiche anzugeben, die entlang der Bit-Grenze binärer zahlen verlaufen. Kann auch als umgekehrte Subnetzmaske betrachtet werden. 0 bedeutet, dass die Stelle nicht betrachtet werden muss. 1 bedeutet, dass die Stelle relevant ist.
Beispiele: 0.0.0.255 entspricht allen Zahlen von 0 – 255 im 4. Oktett 0.0.3.255 entspricht allen Zahlen von 0 - 3 im 3. Oktett und allen Zahlen im 4. Oktett. Entfällt die wildcard-mask kann in der source-address eine einzelne Quell-IP-Adresse angegeben werden.	
source-port	Kann auf unterschiedliche weise definiert werden. Entweder durch die Portnummer wie z. B. 80 für http oder direkt mit dem Namen http.
destination-address	Ziel-IP-Adresse. Kann wie die Quell-IP-Adresse beschrieben werden.
destination-wildcard	Ziel-Wildcard-Maske. Kann wie die source-wildcard-Maske verwendet werden.
log	Mit dem Schlüsselwort log wird ein Eintrag in das Logbuch vorgenommen, falls der Listen-Eintrag mit einem Paket übereinstimmt.
Options	Es gibt eine ganze Reihe von Optionen mit den folgenden Bedeutungen: established es muss das ACK oder RST-Flag gesetzt sein, dann ist das Paket teil einer vorher geöffneten Verbindung

Es gibt noch zwei Schlüsselworte, die ersatzweise für oben genannte Begriffe eingesetzt werden können.

host	Dient zur Definition einer einzelnen Quell-IP-Adresse. Entspricht dem Weglassen der wildcard-mask.
any	Dient zur Beschreibung von allen möglichen Quell-IP-Adressen. Entspricht einem source-address-Eintrag von 0.0.0.0 mit einem wildcard-mask-Eintrag von 255.255.255.255

Es gibt nun weitere Paketeile die zu untersuchen sind. Dadurch wird die Zugriffslisten-Bearbeitung aufwändiger.

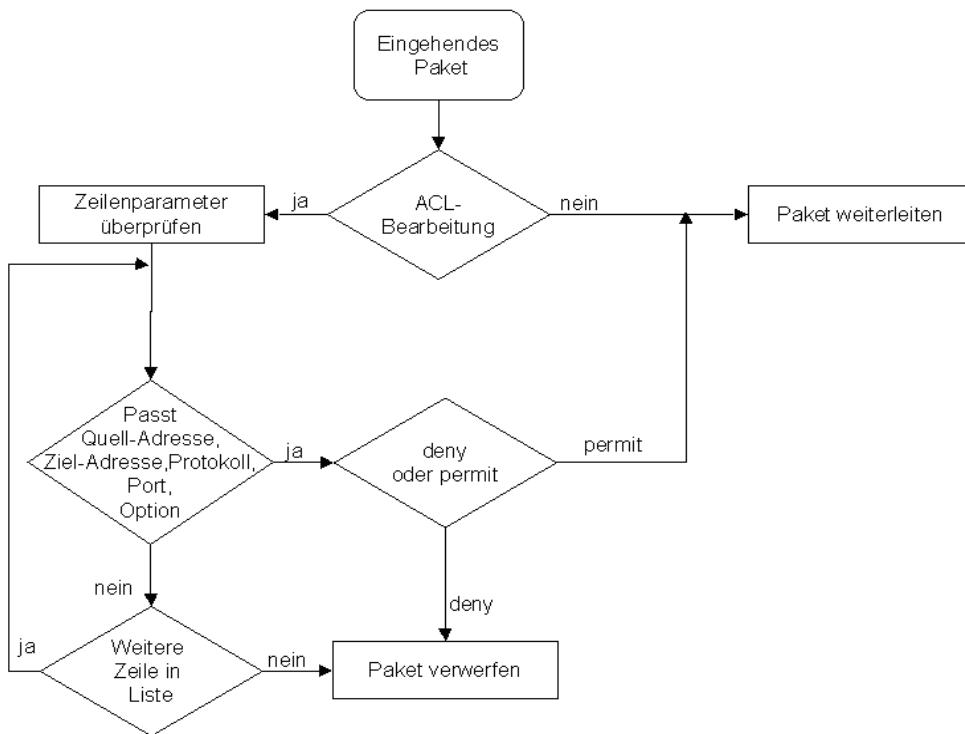


Abbildung 445 : Erweiterte Zugriffslisten-Bearbeitung

38.2.3.8 - Benannte Zugriffslisten

Neben den nummerierten Zugriffslisten gibt es noch die benannten Zugriffslisten. Diese werden anstelle einer Ziffer mit einem Namen beschrieben. Der Name muss mit einem alphanumerischen Zeichen beginnen. Die Namen unterscheiden Groß und Kleinbuchstaben. Es können bis zu 100 Zeichen eingegeben werden. Als gültige Zeichen können verwendet werden:

a-z, A-Z, [], { }, _, -, +, /, \, ., &, \$, #, @, !, und ?

Auch hier gibt es die Aufteilung in Standard- und Erweiterte-Zugriffslisten.

38.2.3.9 - Syntax für benannte Standard Zugriffslisten

ip access-list standard name

name Listenname

Danach folgt eine Aufzählung von erlaubten und verbotenen IP-Quell-Adressen. Die Liste wird mit ^Z abgeschlossen.

Beispiel:

```
router(config)#ip access-list standard otto-darf-nicht      Benannte Liste einleiten
router(config-std-nacl)#deny 10.20.30.40                  IP-Adresse von Otto verbieten
router(config-std-nacl)#^Z                                Abschluss der Liste
router(config)#

```

38.2.3.10 - Syntax für benannte erweiterte Zugriffslisten

ip access-list extended name

name Listenname

Danach folgt eine Aufzählung von erlaubten und verbotenen Paketmerkmalen. Die Liste wird mit ^Z abgeschlossen.

Beispiel:

```
router(config)#ip access-list extended kein-http-mit-otto      Benannte Liste einleiten
router(config-ext-nacl)#deny tcp any host 10.20.30.40 eq www    HTTP mit IP-Adresse von Otto
                                                               verbieten
router(config-ext-nacl)#^Z                                    Abschluss der Liste
router(config)#

```

Um eine benannte standard oder erweiterte Zugriffsliste einer Schnittstelle zuzuordnen, gilt folgende Syntax:

ip-access-group name [in | out]

38.2.3.11 - Dynamische Zugriffslisten

Mit dynamischen Zugriffslisten können temporär begrenzte, Zugriffe erlaubt werden, wenn eine entsprechende Authentisierung erfolgt ist.

Damit ist es einem Administrator möglich mit einer wechselnden IP-Adresse (z. B. über einen ISP) einen Router von zu hause aus zu administrieren.

Die traditionellen Zugriffslisten sind, was die erlaubten oder verbotenen IP-Adressen angeht, statisch. Dies ermöglicht es einem Angreifer durch ip-spoofing über die Zugriffslisten-Begrenzung hinaus zu gelangen!

38.2.3.12 - Reflexive Zugriffslisten

Hierbei ist ein Datenaustausch möglich wenn der Verbindungsauflauf aus einer bestimmten Richtung erfolgt ist. Dies entspricht von der Funktionalität her den zustandsbehafteten Paketfiltern.

38.2.3.13 - Zeit gesteuerte Zugriffslisten

Hier hat der Administrator die Möglichkeit einen zeitlich begrenzten Zugriff auf bestimmte Adressen oder Netzwerke zu ermöglichen.

38.2.3.14 - Ausgabe der Zugriffslisten

Die bereits eingegebenen Zugriffslisten können mit dem Kommando:

show access-lists oder
show ip access-lists

aufgelistet werden.

38.2.3.15 - Überprüfung der Zugriffslisten

debug ...

39 - Netzwerk-Management

39.1 - Einführung

Nachdem die Netzwerke immer größer wurden und die einzelnen Netzwerkgeräte nicht mehr in einem Rahmen, sondern über ein gesamtes Rechenzentrum und später über mehrere Rechenzentren verteilt aufgebaut wurden, entwickelte sich das Management der verschiedenen Bridges und Router als zunehmend schwierig. Es entwickelte sich das geflügelte Wort vom „Management by Turnschuh“, was bedeutet dass die Netzwerk-Betreuer gut zu Fuß sein mussten. In größeren Netzwerken war ein reibungsloser Betrieb nur mit großem, auch personellem Aufwand, zu betreiben.

In Fehlerfällen waren die Ausfallzeiten immens und somit auch die Zeiten in denen ganze Rechenzentren arbeitsunfähig waren. Da Zeit auch Geld ist, wurde hier ein großer Druck auf die Netzwerk-Verantwortlichen ausgeübt.

Es wird die Geschichte erzählt, dass sich ein paar Netzwerk-Betreuer bei einem Ausflug abends gegenseitig ihr Leid klagten und darüber nach sannen, wie man Netzwerkgeräte auf eine einfache Art und Weise fern bedienen kann. Das Ergebnis war ein einfaches Protokoll, welches auf einen Bierdeckel passt und auf dem damals bereits vorhandenen UDP aufsetzt, dem SNMP (Simple Network Management Protokoll). Wegen seiner einfachen Realisierbarkeit wurde SNMP schnell zum de facto Standard.

Parallel dazu wurde von den ISO-Gremien ein allgemein gültiger Standard entwickelt CMIP(Common Management Information Protocol). Allerdings war wegen des langwierigen Normierungs-Verfahrens die Akzeptanz sehr gering da sich SNMP bereits etabliert hatte. Heute bieten nur die großen etablierten Hersteller eine CMIP Unterstützung an.

39.2 - SNMP

Im Protokollstack sitzt SNMP auf IP und UDP auf (Siehe Fehler: Verweis nicht gefunden).

-	SNMP
TCP	UDP
IP	
Ebene 2	
Ebene 1	

Dies bedeutet, dass die Telegramme ohne Quittungsmechanismus gesendet werden. Soll sichergestellt werden, dass Aktionen bestimmt durchgeführt werden, sind entsprechende Telegramme zusätzlich zu senden/empfangen.

39.2.1 - Management-Konsole

Im Normalfall werden mehrere Geräte mit einer Management-Konsole überwacht. An einem dedizierten Gerät wird die Management-Software installiert.

Dies sollte eine leistungsfähige Maschine sein, da das Netzwerk-Management mit einer graphischen Aufbereitung aufwendig zu realisieren ist. Die Management-Konsole greift über SNMP-Telegramme auf die Agenten der zu überwachenden Geräte zu. Die Agenten ihrerseits, verwalten die Geräte. Die erforderlichen Parameter werden in der MIB (Management Information Base) verwaltet. Die MIB ist ein hierarchisch organisierter Speicherbereich innerhalb des Agenten (Siehe MIB-Aufbau). Mit den SNMP-Telegrammen werden die MIB-Werte ausgelesen oder geändert.

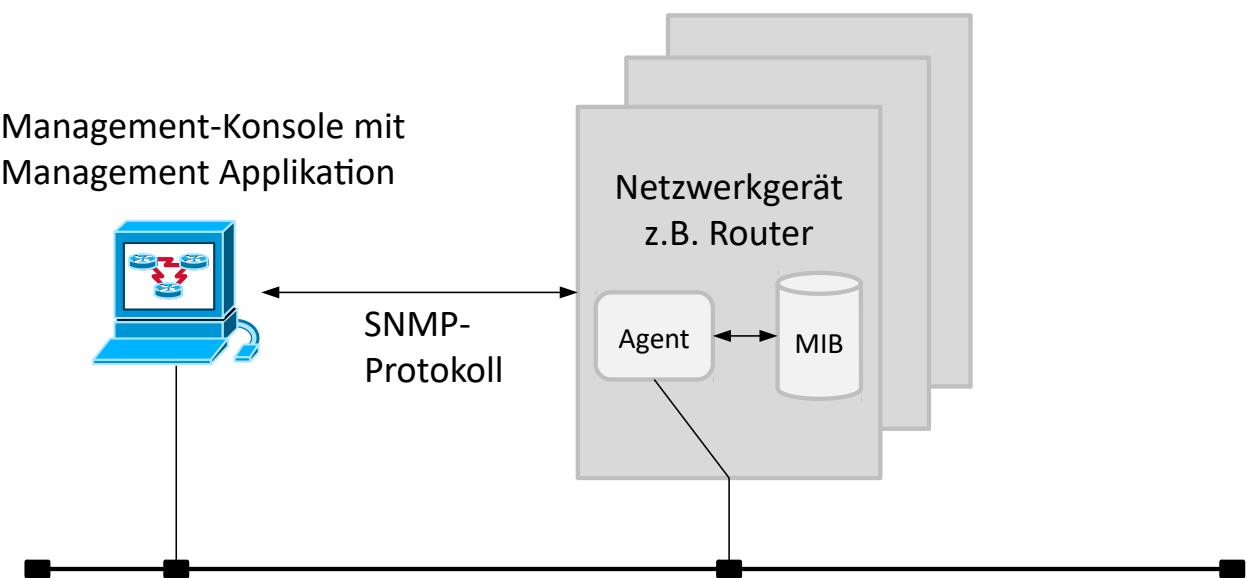


Abbildung 446 : SNMP-Agent

39.2.2 - Zusammenspiel der SNMP-Komponenten

39.2.3 - Proxy-Agent

Bei Geräten, die über keinen SNMP-Agenten, jedoch einen anderen, proprietäre Agenten verfügen, gibt es die Möglichkeit, über einen Proxy-Agenten für dieses Gerät, trotzdem SNMP zu benutzen. Der Proxy-Agent ist ein Softwarepaket, welches auf einem Rechner läuft, der stellvertretend für das Endgerät, die Funktionen des Endgerätes steuert. Hier wird für jedes Gerät, das überwacht werden soll, ein eigener MIB-Bereich im Proxy-Agenten gehalten (Siehe unten). Der Proxy-Agent setzt die proprietären Verwaltungsmechanismen in SNMP-Befehle um und umgekehrt. Die Managementstation interpretiert den Proxy-Agenten so, als ob sie direkt mit dem zu überwachenden Endgerät kommunizieren würden.

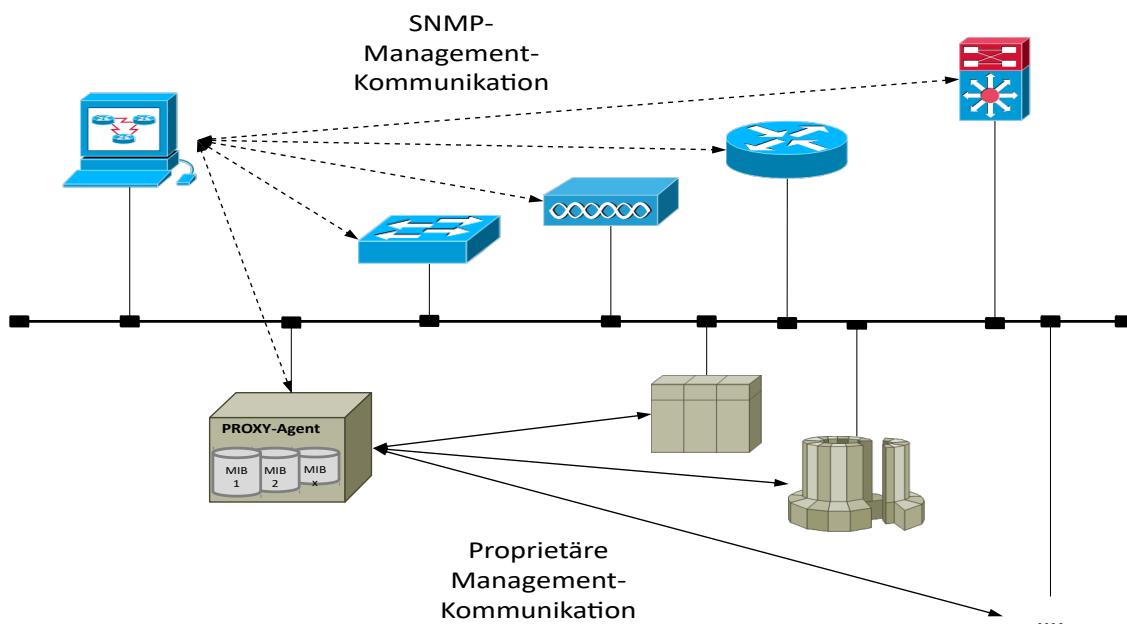


Abbildung 447 : PROXY-Agent

39.2.4 - MIB-Aufbau

Eine MIB (Management Information Base deutsch Kontroll-Informations-Datenbasis), ist ein hierarchisch aufgebauter Speicher. Die Organisation ist in großen Teilen festgelegt.

Es gibt zwei Schreibweisen die einzelnen Verzweigungen zu beschreiben. Entweder mit Ziffern (z. B. .1.3.6.1.2.1.0) oder mit kurzen Bereichs-Bezeichnungen (z. B. .iso.org.dod.internet.mgmt.mib-2.system). Für beide Schreibweisen gilt der Punkt als Trennzeichen zwischen den Bereichen. Die folgende Abbildung zeigt einen Teil daraus.

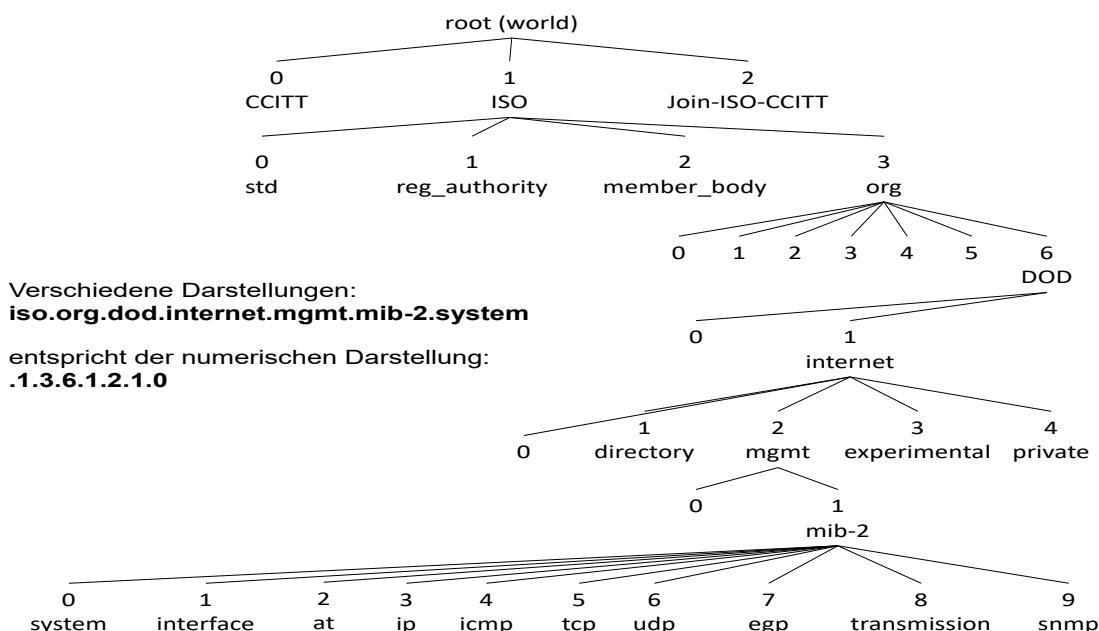


Abbildung 448 : MIB-Aufbau Teil 1

Nur im Private-Bereich (iso.org.dod.internet.private) ist für die verschiedenen Hersteller ein eigener Baum eingerichtet. Dort kann jeder Hersteller seine eigene Informationsstruktur definieren.

Da dies auch ausgiebig gemacht wird, sind die MIBs in ihrem Aufbau unterschiedlich. Dies bedeutet für das Netzwerk-Management-System, dass es alle herstellerspezifischen MIB-Definitionen haben muss, um alle Möglichkeiten der einzelnen Endgeräte ausschöpfen zu können.

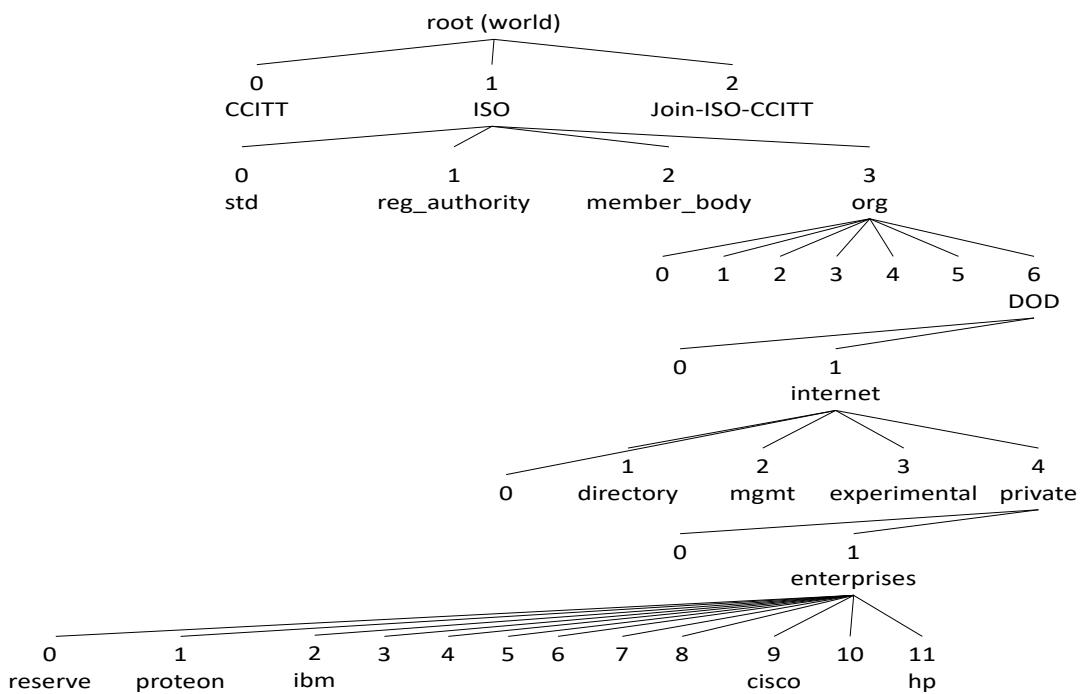


Abbildung 449 : MIB-Aufbau Teil 2

Herstellerspezifische Kennungen unter iso.org.dod.internet.private.enterprises(.1.3.6.1.4.1)

Kennung	Hersteller
0	
1	proteon
2	ibm
9	cisco
11	hp
23	novellMib
119	nec
197	kalpana
353	atmForum
437	grandjunction
494	madge
711	lightstream

39.2.5 - Community-String

Bereits in der Version v1 von SNMP wurde der Community-String oder Community-Name eingeführt.

Er dient dazu, dass sich nur Geräte einer gleichen Gruppe (Community engl. Gemeinde) miteinander unterhalten. Geräte mit unterschiedlichen Community-Namen können nicht miteinander kommunizieren.

Im Allgemeinen gibt es zwei Community-Namen:

- Get-Community-String:
Dient zum Lesenden Zugriff. Hier wird oft public als Voreinstellung verwendet.
- Set-Community-String:
Dient zum Schreibenden Zugriff. Hier wird oft private als Voreinstellung verwendet.

39.2.6 - SNMPv1

In der ersten Version wurden 5 verschiedene Telegramme definiert:

Telegrammbezeichnung	Bedeutung	Richtung	Port
get	Anforderung einer MIB-Variablen	Manager -> Remote-Gerät	161
getnext	Anforderung der lexikographisch nächsten Variablen	Manager -> Remote-Gerät	
response	Antwort auf einen get/getnext-Telegramm	Remote-Gerät -> Manager	
set	Setzen einer MIB-Variablen	Manager -> Remote-Gerät	
trap	Information an den Manager	Remote-Gerät -> Manager	162

Schwachstellen von SNMP in der Version 1

- Jedem Get/Getnext-Telegramm antwortet ein Response-Telegramm. Hiermit können umfangreiche Datenbereiche nicht effizient ausgelesen werden.
- Keine eindeutigen Fehlermeldungen
- Traps erhalten keine Rückmeldung. Somit ist nicht gewährleistet dass sie ihr Ziel erreicht haben.
- Keine Übertragung von komplexen Datenbereichen.
- Keine Kommunikation zwischen verschiedenen Managern
- Keine Mechanismen zur Datensicherheit

Ist beschrieben im RFC1157 und funktioniert innerhalb der Spezifikation SMI (Structure of Management Information)

SMI

Regeln für das Beschreiben von Verwaltungsinformationen mittels ASN.1 (Abstract Syntax Notification One) SMI von SNMPv1 ist in RFC 1155 beschrieben.

39.2.6.1 - Paket-Aufbau unter SNMP

39.2.6.1.1 - Aufbau für Get, Getnext, Response Set

Länge der Nachricht in Bytes		SNMP-Paket-Header
Versionsnummer		
Community-Name		
Typ (get, getnext,..)	PDU- Header	PDU (Protocol Data Unit)
PDU-Länge		
Request-ID		
Fehlerstatus		
Fehler-Index		
Länge PDU-Body	PDU-Body	
Variable Bindung 1		
Variable Bindung 2		
..		
Variable Bindung n		

39.2.6.1.2 - Aufbau für Traps

Länge der Nachricht in Bytes		SNMP-Paket-Header
Versionsnummer		
Community-Name		
Typ (Trap)	PDU- Header	PDU (Protocol Data Unit)
OID des Gerätes, das den Trap generiert		
IP-Adresse des Absenders		
Allgemeine Trap-ID		
Firmenspezifische Trap-ID		
Zeitpunkt des Auftretens des Trap-Ereignisses		
Länge PDU-Body	PDU-Body	
Variable Bindung 1		
Variable Bindung 2		
..		

Variable Bindung n		
--------------------	--	--

39.2.6.1.3 - Aufbau der variablen Bindungen

Größe der variablen Bindung
OID
Datentyp
Wert

39.2.6.2 - Einfache Datentypen

Typ	Wertebereich	Bedeutung
Integer	-2147483648 - +214483647	
Octets	0 - 65535	
Strings		
Object-ID		

39.2.6.3 - Anwendungs-Datentypen

Typ	Wertebereich	Bedeutung
Network-Adr.	32-Bit-IP-Adr.	
Counter	0 - Maxwert	
Gauge	Schleppzeiger	
Time Tick	1/100 Sec. Nach Ereignis	
Opaque	Codierte Zeichenkette	
Integer	Ganze Zahl	
Unsigned integer	Pos. ganze Zahl	

39.2.7 - SNMPv2

Bei der 2. Version wollte man alle Fehler der ersten Version beheben, was dazu führte, dass SNMPv2 von der Industrie als zu komplex abgelehnt wurde. Diese Version konnte sich nicht durchsetzen und wird heute SNMPv2-Classic bezeichnet.

Eine Untermenge der Funktionen von SNMPv2-Classic wurde umgesetzt und ist heute als SNMPv2C auf breiter Basis umgesetzt und in den RFC1901 - RFC1910 beschrieben.

Neu bei SNMPv2C ist:

- Eindeutige Fehlermeldungen
- 64Bit-Zähler für hochfrequente Vorgänge
- Neue Textual Conventions zur Beschreibung von managed Objects

Schwachstellen von SNMP in der Version 2

- Keine Mechanismen zur Datensicherheit

Funktionen von SNMPv2C

Telegrammbezeichnung	Bedeutung	Richtung
get	Anforderung einer MIB-Variablen	Manager -> Remote-Gerät
getnext	Anforderung der lexikografisch nächsten Variablen	Manager -> Remote-Gerät
getbulk	Anforderung großer MIB-Bereiche	Manager -> Remote-Gerät
response	Antwort auf einen get/getnext-Telegramm	Remote-Gerät -> Manager
set	Setzen einer MIB-Variablen	Manager -> Remote-Gerät
inform	Versand bestätigter Meldungen Kommunikation zwischen Managern	Remote-Gerät<-> Manager Manager<-> Manager
trap	Information an den Manager	Remote-Gerät -> Manager

Die Versionen SNMPv2u und SNMPv2* wurden entwickelt um die Sicherheitslücken zu schließen und die Remote-Administration zu ermöglichen. Allerdings blieb diesen Versionen die breite Akzeptanz versagt.

SNMPv2u wurde von IBM bei System View auf AIX sowie auf Agentenseite bei Epilogue und CMU verwendet.
SNMPv2* wurde von SNMP Research, HP, Cisco, und Bay Networks in verschiedenen Geräten eingesetzt.

39.2.8 - SNMPv3

39.2.8.1 - Allgemeines

Die Sicherheitsmechanismen bei SNMP in den beiden ersten Versionen waren so schlecht, dass SNMP für „Security is not my problem“ stand.

Mit der Version 3 wurden sie Sicherheitsmechanismen verbessert. Durch die komplexe Schlüsselverwaltung hat SNMPv3 jedoch noch keine große Verbreitung gefunden.

39.3 - RMON

Obwohl SNMP sich durchgesetzt hat, sind immer noch Schwachpunkte beim Netzwerk-Management auf SNMP-Basis zu verzeichnen.

- Die Polling-Last ist in einem Netzwerk nicht zu unterschätzen.
- Wenn es zu Fehlern kommt, ist der Einsatz von Netzwerk-Analysegeräten wie Sniffer usw. unerlässlich.

Auf Basis von SNMPv1 wurde das RMON (Remote MONitoring; deutsch: ferngesteuert überwachen) entwickelt.

Die Entwicklung fand in mehreren Schritten statt:

RFC1271 RMON für Ethernet

RFC1513 RMON für Token Ring

:

RMON funktioniert wie SNMP über ein Stück Software auf einem Endgerät oder sogar einem eigenständigen Gerät, das in das Netzwerk integriert wird. Allerdings spricht man in diesem Zusammenhang nicht von einem Agenten, sondern von einer Probe; deutsch: Sonde. Diese Probe sammelt Daten und verwaltet sie in einem MIB-Teil. Durch die RMON-Software auf der Management-Station können die gesammelten Daten abgerufen und aufbereitet werden.

Im MIB-Baum wurde RMON unterhalb des MGMT-Knotens angesiedelt.

RMON enthält in seiner ersten Version folgende Klassen

RMON-Klasse	Bedeutung
1	Statistics
2	History
3	Alarms
4	Hosts
5	Host Top10
6	Matrix
7	Filters
8	Capture
9	Events
10	Token Ring

In der Version 2 wurden folgende Klassen angefügt:

RMON-Klasse	Bedeutung
11	Protocol Directory
12	Protocol Distribution
13	Address Map
14	Network Layer Host
15	Network Layer Matrix
16	Application Layer Host
17	Application Layer Matrix
18	User History
19	Probe Configuration
20	Conformance

39.4 - SMON

Speziell für Switches wurden die Grundlagen für die Belange von Switches erweitert und in einer eigenen Struktur festgelegt

39.5 - Netzwerk-Management-Software

39.5.1 - Allgemeines

Viele verschiedenen Hersteller haben Netzwerk-Management-Software auf den Markt gebracht. Mittlerweile hat sich der Markt wieder gelichtet und folgende Produkte sind übrig geblieben.

- HP-OpenView von HP
- Tivoli von IBM
- UNICENTER von CA
- TRANSVIEW von SNI (gibt es mittlerweile nicht mehr)
- NetView von IBM
- SMS von Microsoft
- CiscoWorks von CISCO
- Optivity von NORTEL

Es gibt noch weitere Hersteller. Diese haben aber, was den Marktanteil angeht, keine größere Bedeutung. Die einzelnen Produkte sind nicht für alle gängigen Betriebssysteme verfügbar!

39.5.2 - CiscoView

Dient zur graphischen Ausgabe des Gerätes. Außerdem kann hier, je nach Gerät, eine Vielzahl von Änderungen durchgeführt werden. Z. B. Ändern von VLAN-Portzuordnungen.

39.5.2.1 - Beispiel

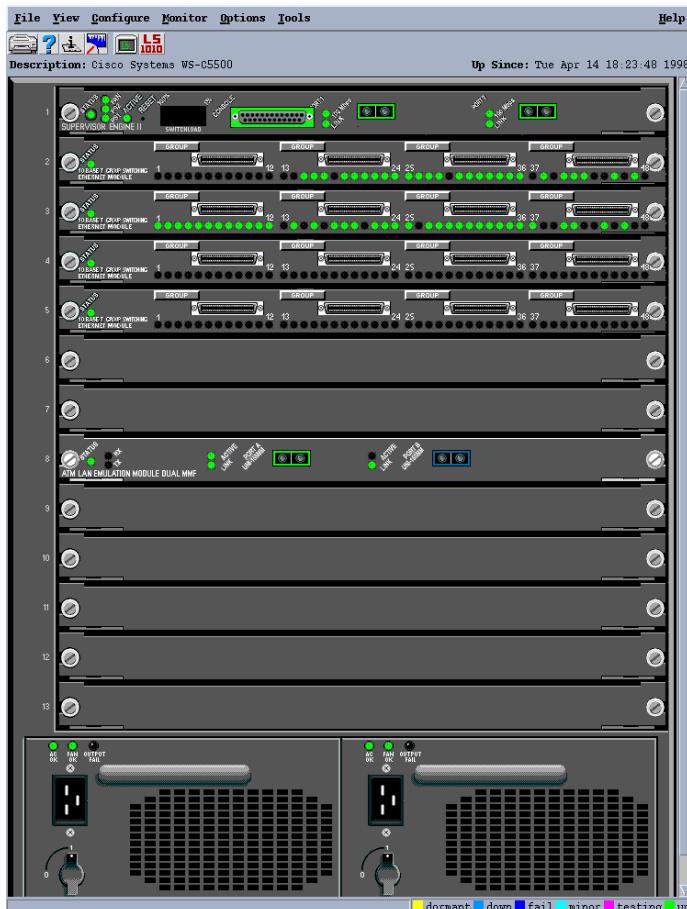


Abbildung 450 : CISCO-View-Beispiel

39.5.2.2 - Bearbeitung

Hardcopies erzeugen

Konfiguration des Gerätes mit graphischen Mitteln. Hier können z. B. VLANs parametriert werden.

Zusätzlich ist ein Monitoring von wichtigen Gerät-Parametern möglich (z. B. CPU-Auslastung, Speicherbelegung, Port-Auslastung)

39.5.3 - VLANDirector

Bietet eine graphische Oberfläche zur Visualisierung und Bearbeitung von VLANs.

39.5.4 - TrafficDirector

Graphische Oberfläche zur Visualisierung der RMON-Daten(Remote MONitoring). Kann sowohl mit Routern als auch mit CISCO Catalyst 5500 (mit Supervisory Modul III) angewendet werden.

39.5.5 - ATMDirector

Bietet eine graphische Oberfläche zur Visualisierung und Bearbeitung von ATM-Verbindungen und Geräten.

40 - Anwendungsprotokolle

40.1 - Einführung

Die unterschiedlichen Applikationen nutzen den TCP/IP-Stack um Daten auszutauschen. Im RFC1700 sind die Protokollnummern sowie die zugehörigen Ports beschrieben.

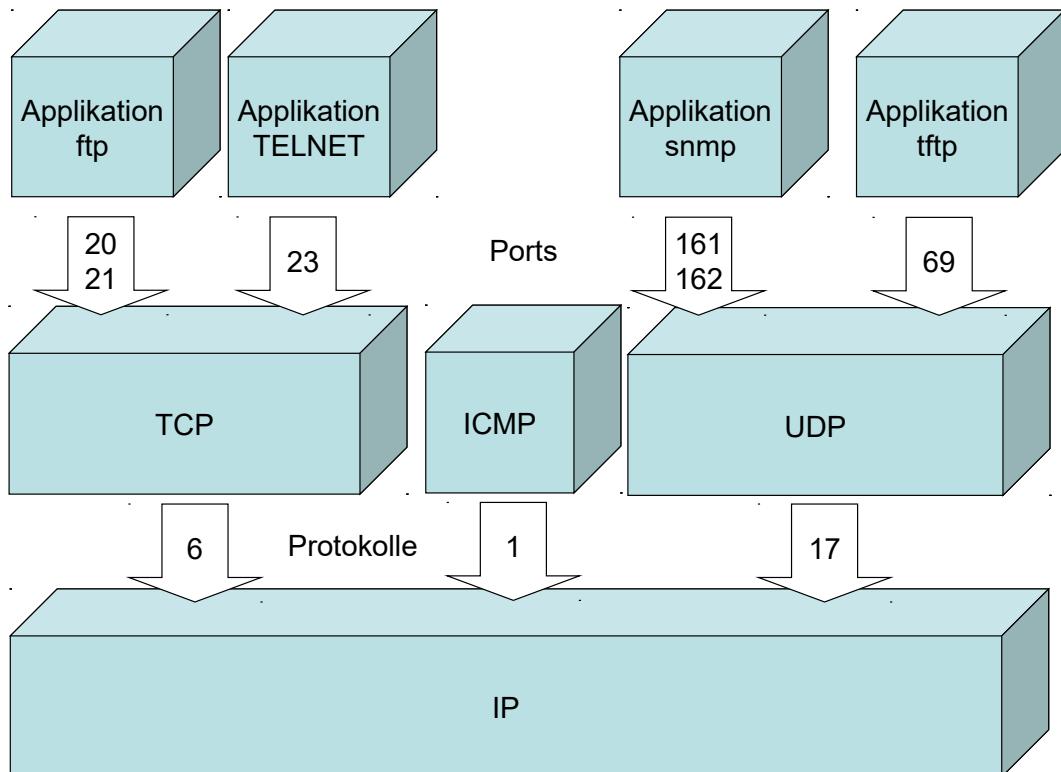


Abbildung 451 : Applikationen -TCP UDP - IP

Auf IP werden die folgenden Protokolle aufgesetzt.

Wert (Dezimal)	Protokoll	Beschreibung
0	-	Reserviert
1	ICMP	Internet Control Message Protocol
6	TCP	Transmission Control Protocol
17	UDP	User Datagram Protocol

Mit TCP oder UDP können die unterschiedlichsten Applikationen Dienste zur Verfügung stellen. Dazu sind im RFC1700 die Ports beschrieben.

Well-Known Ports

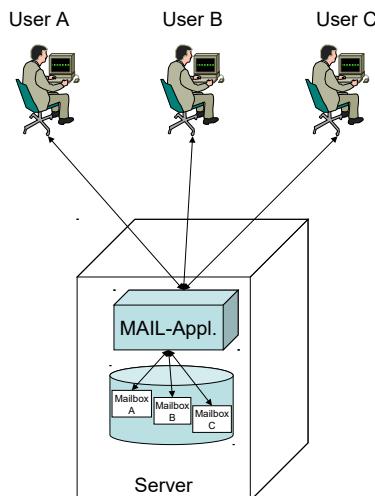
Protokoll	Wert	Service	Beschreibung
echo	7	TCP	Echo
	7	UDP	
daytime	13	TCP	Daytime
	13	UDP	
ftp-data	20	TCP	Filetransfer Protocol, Default Data
ftp	21	TCP	Filetransfer Protocol, Default Control Data
TELNET	23	TCP	Remote Network Terminal
smtp	25	TCP	Simple Mail Transfer
name-server	42	TCP	Host Name Server
	42	UDP	
login	49	TCP	Login Host Server
	49	UDP	
dns	53	TCP	Domain Name Service
bootps	67	TCP	Bootstrap Protocol Server
	67	UDP	
Bootpc	68	TCP	Bootstrap Protocol Client
	68	UDP	
Tftp	69	TCP	Trivial File Transfer Protocol
	69	UDP	
Snmp	161-162	UDP	Simple Network Management Protocol
Print-srv	170	TCP	Network Print Service
	170	UDP	
Talk	517	TCP	Talk
	517	UDP	

40.2 - Electronic Mail (E-Mail)

40.2.1 - Einführung

Neben dem Datentransfer ist der Dialog eine der häufigsten Anwendungen zwischen zwei Personen die mit einem Rechner arbeiten. In den Anfängen der Timesharing-Betriebssysteme konnte hiermit für verschiedenen User ein Informationsaustausch-System zu Verfügung gestellt werden.

Jeder User konnte mit seinem Terminal auf eine Mail-Applikation zugreifen.



Diese Applikation stellte für jeden User ein eigenes Benutzerkonto sowie einen Plattenbereich also eine Mailbox zur Verfügung.

Eine Mail wird als File in der Mailbox für den User verwaltet.

Das Senden einer Mail bedeutet, dass die erstellte Datei der Empfänger-Mailbox zugeordnet wird und in die dortige Verwaltung übergeht.

Abbildung 452 : MAIL - Anfänge

Eine solche Mail-Applikation bietet 4 Grundfunktionen.

- Erstellung Der User editiert eine Datei. Dies ist eine einfache Textverarbeitung
- Sendung Die Applikation legt die erstellte Datei in einer oder mehreren Mailboxen ab.
- Empfangen Der User kann die Dateien in seiner Mailbox lesen
- Speicherung Zur späteren Wiederverwendung kann eine Datei in der Mailbox abgelegt und verwaltet werden.

Auf so einem Ein-Rechner-System können Mails nur zwischen den Usern ausgetauscht werden die auf dieses System einen Zugriff haben. Soll mit den Usern an weiteren Rechnern ein Mailaustausch möglich sein, sind folgende Erweiterungen notwendig:

- I/O-Modul Es ermöglicht den Datenaustausch mit anderen Rechnern über ein Netzwerk (z. B. WAN)
- Mail-Transfer-Logik Sie ist notwendig um die Verwaltung der Mails über mehrere Rechner hinweg (auch Transfersysteme) zu bewerkstelligen.

40.2.2 - Simple Mail Transfer Protocol (SMTP)

Ursprünglich auf UNIX-Systemen implementiert ist es mittlerweile auch auf anderen Plattformen verfügbar. Es ist ein Punkt-zu-Punkt Protokoll und basiert auf dem Client-Server Konzept. SMTP ist im RFC821 beschrieben. Es wird der Port 25 zum bidirektionalen Datenaustausch verwendet.

40.2.2.1 - Ablauf

Der Benutzer der eine Mail senden will startet seine Mail-Applikation und erstellt die Nachricht. Diese wird dem Mail-Prozess übergeben der als Client mit dem Server (Mail-Prozess auf der Empfängerseite) in Kontakt tritt.

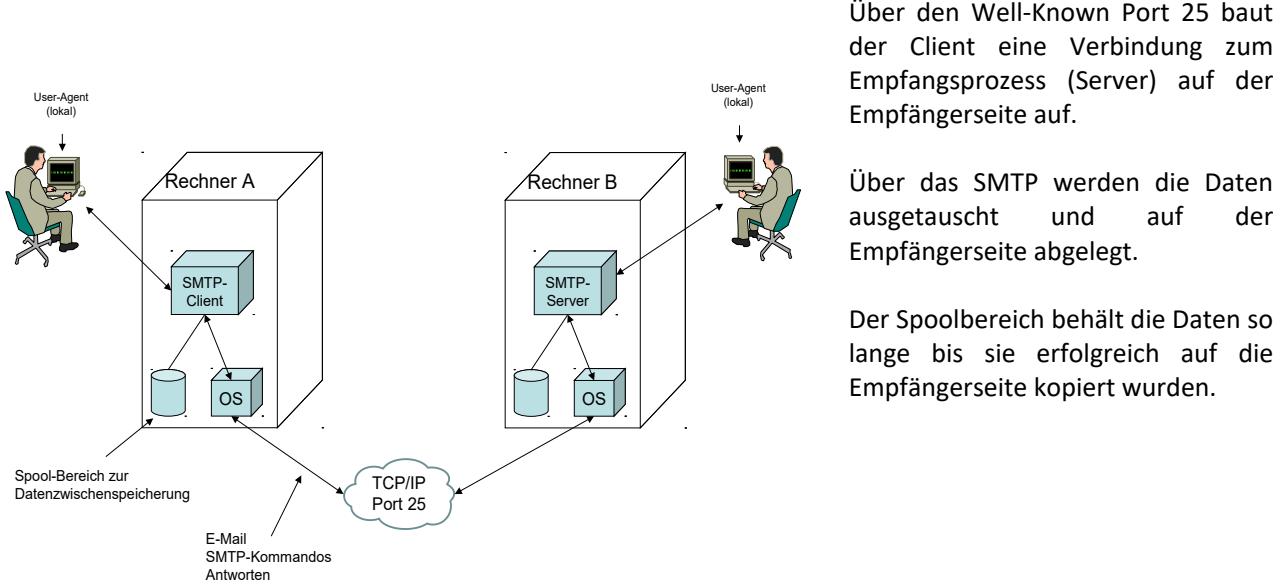


Abbildung 453 : SMTP

40.2.2.2 - E-Mail-Adresse

Eine Mail-Adresse baut sich zum Beispiel otto.huber@firma-xy.com aus aus einer Kombination von Username (Otto Huber) und Domäne (firma-xy.com) auf.

40.2.2.3 - SMTP-Character Code

SMTP verwendet für die Übertragung der Daten den NVT-ASCII Character-Code. Es handelt sich hierbei um einen 7-Bit-ASCII-Code. Damit ist einerseits eine neutrale Datenübertragung sichergestellt. Der Zeichensatz ist jedoch eingeschränkt.

40.2.2.4 - SMTP-Datentransfer

SMTP bedient sich der folgenden Funktionen für die Mail-Übertragung:

➊ Verbindungsaufbau

Über den TCP-Port 25 wird eine Verbindung aufgebaut. Der darauf folgende SMTP-Verbindungsauftbau erfolgt in 4 Schritten

1. Sender öffnet TCP-Verbindung zum Empfänger
2. Empfänger identifiziert sich gegenüber dem Sender
3. Sender identifiziert sich gegenüber dem Empfängers
4. Empfänger akzeptiert Identifikation des Senders.

➋ Mail-Transfer

Jeder Mail-Transfer stellt eine logisch getrennte Transaktion dar. Jede transaktion durchläuft 3 Schritte:
Absender weist sich durch das MAIL-Kommando aus.

Durch ein oder mehrere RCPT-Kommandos werden die Empfänger bestimmt.

Durch das DATA-Kommando wird der Text übertragen

➌ Verbindungsabbau

Erst QUIT-Kommando mit warten auf REPL-Kommand

Danach TCP-Verbindungsabbau

40.2.2.5 - SMTP-Kommandos

Kommando	Bedeutung
SMTP-Hello	Identifikation des Senders (Clients), Verbindungsauftbau
SMTP-Mail	Start des Mail-Prozesses
SMTP-Recipient	Identifikation des Empfängers. Mehrere Empfänger werden durch mehrfache Eingabe des Kommandos angegeben
SMTP-Data	Datentransfer, Transfer-Ende mit <CRLF>.<CRLF>
SMTP-Send	Direktes Senden der Daten an ein Terminal. Ist der User auf der Empfängerseite nicht aktiv wird Reply-Code 450 erzeugt. Das Kommando ist abgeschlossen, wenn die Daten an das Terminal übertragen wurden
SMTP-Send or Mail	Vorzugsweises Senden der Daten an ein Terminal. Ist der User auf der Empfängerseite nicht aktiv werden die Daten in der Mailbox des Empfängers abgelegt. Das Kommando ist abgeschlossen, wenn die Daten an das Terminal oder die Mailbox des Empfängers übertragen wurden
SMTP-Send and Mail	Senden der Daten an ein Terminal und die Mailbox. Das Kommando ist abgeschlossen, wenn die Daten an die Mailbox des Empfängers übertragen wurden
SMTP-Verify	Bestätigung der Benutzer-ID
SMTP-Help	Anforderung von Benutzerinformationen
SMTP-Reset	Abbruch der aktuellen Mailtransaktion
SMTP-Expand	Abfrage von vollständigen Maillisten
SMTP-No-Operation	Es wird lediglich ein OK von der Gegenseite angefordert
SMTP-Quit	Beenden der SMTP-Applikation
SMTP-Turn	Wechseln der Senderichtung. Dies bedeutet der Sender wird zum Empfänger von Mails

40.2.2.6 - SMTP-Replies

Die Antworten auf die Kommandos werden als 3-stellige-Zahlencodes gefolgt von einem Text zurückgegeben. Der Text ist im Gegensatz zur Zahlenfolge nicht immer eindeutig. Jede Stelle des 3stelligenCodes hat eine spezielle Bedeutung:

40.2.2.6.1 - Erste Stelle

- 1yz Vorzeitige positive Bestätigung
- 2yz Positive Abschluss-Bestätigung
- 3yz Zwischenzeitlich positive Bestätigung
- 4yz Vorübergehend negative Abschluss-Bestätigung
- 5yz Permanente negative Abschluss-Bestätigung

40.2.2.6.2 - Zweite Stelle

- x0z Syntaxfehler
- x1z Information
- x2z Verbindung
- x3z Undefiniert
- x4z Undefiniert
- x5z Mail-System

40.2.2.6.3 - Dritte Stelle

Die dritte Stelle dient zur Beschreibung des näheren Sachverhalts.

40.2.2.6.4 - Reply-Tabelle

Reply-Code	Bedeutung
211	System Status, oder Reply auf Help-Kommando
214	Hilfe-Information
220	Rechner bereit für Benutzer
221	Verbindung im Abbau
250	Gewünschte Operation abgeschlossen
251	Benutzer nicht lokal am Rechner, Mail wird weitergeleitet (Pfad)
354	Mail-Eingabe bereit, Beenden der Mail-Eingabe mit <CRLF>.<CRLF>
421	Rechner nicht verfügbar
450	Operation nicht durchgeführt, Mailbox nicht vorhanden
451	Lokaler Fehler, gewünschte Operation abgebrochen
452	Speicher belegt, gewünschte Operation nicht durchgeführt
500	Syntaxfehler, Kommando unbekannt
501	Syntaxfehler bei Kommando oder Parameter
502	Kommando nicht unterstützt
503	Fehler in Kommandofolge
504	Parameter in Kommando nicht unterstützt
550	Kein Zugriff auf Mailbox möglich, Operation nicht durchgeführt
551	Benutzer nicht lokal, Mail weiterleiten an Pfadname
552	Speicher belegt, Operation nicht durchgeführt
553	Speicher belegt, Operation nicht durchgeführt
554	Übermittlung konnte nicht durchgeführt werden

40.2.2.7 - Ablaufbeispiel einer Session

1. Client baut eine Verbindung zum Server (Empfänger) auf
 2. Server antwortet mir Service Ready (220) oder Service not available (421)
3. Sender identifiziert sich mit Hello-Meldung
 4. Der Empfänger antwortet mit seinem Domänen-Namen
5. Client beginnt mit dem eigentlichen Mail-Prozess durch absetzen des MAIL-Kommandos
 6. Server antwortet mit OK (220)
7. Mit dem RCPT-Kommando wird er Empfänger festgelegt
 8. Der Server antwortet mit OK (220) oder Not available. (550)
9. Mit dem Data-Kommando wird der Text übertragen
 10. Der Server antwortet mit Start Mail Input end with <CRLF>.<CRLF> (354)
11. Am Ende Sendet der Client <CRLF>.<CRLF>
12. Der Sender beendet die Session mit dem QUIT-Kommando
 13. Der Server antwortet mit Server Closing (221)

40.2.3 - Post Office Protocol (POP3)

40.2.3.1 - Allgemeines

Dieses Mail-Protokoll wurde im RFC1939 beschrieben. Der Server reagiert auf den TCP-Port 110.

Merkmale:

- Der Client baut nur eine temporäre Verbindung zum Server auf.
- Ein einziges Benutzer-Konto
- Ein einziges Verzeichnis
- Ein einziger Server
- Alle Daten sind als Block auf einmal vom Server abzuholen.

40.2.3.2 - Ablauf

Der Client Rechner, an dem der Benutzer seine Mails lesen will, baut eine Verbindung zum E-Mail-Server auf.

Der Client authentifiziert sich mit Benutzername und Passwort

Der Client fordert vom Server eine Liste mit den eingegangenen Mails an.

Mit dieser Liste kann der Client überprüfen ob neue Mails eingegangen sind.

Die neuen Mails werden daraufhin auf den Client-Rechner kopiert.

Nach erfolgreicher Übertragung werden die Daten in der Regel auf dem Server gelöscht.

Zum Schluss beendet der Client die Verbindung.

Die eigentliche Mail-Verwaltung findet auf dem Client-Rechner statt. Da die Verbindung zum Server nur kurzzeitig bestehen muss, eignet sich dieses Protokoll für Modembenutzer. Eine neue Verbindung wird erst notwendig, wenn neue Mails abgeholt, oder geantwortet werden soll.

40.2.3.3 - POP3-Kommandos

1. Phase

USER	Authentifizierung
PASS	

2. Phase

LIST	Auflisten der Mails
RETR	Abholen der Mails

3. Phase

DELE	Löschen der Mails auf dem Server
STATUS	Abfrage der Mails auf dem Server

Sonstiges

NOOP	
RESET	Reaktivieren einer gelöschten Mail
QUIT	Beenden der Verbindung zum Server

40.2.4 - Multipurpose Internet Mail Extensions (MIME)

Dieser Standard ist im RFC1521 und RFC1522 beschrieben.

Er dient zur Übertragung von Multimedia-Daten:

- Postscript-Dateien
- Binär-Dateien
- Audio-Dateien
- Video-Dateien

Es ist eine Unterstützung der entsprechenden Dateiformate vorhanden.

*.pdf, *.xls,...

40.2.5 - Internet Message Access Protocol (IMAP4)

Dieses Protokoll wird als Nachfolger des POP3 gehandelt. Es ist im RFC2060 beschrieben und eliminiert die Nachteile von POP3.

Teilweises Übertragen von Mails ist möglich.

Teilweises Löschen auf dem Mail-Server ist möglich.

Das Postfach kann von mehreren, nicht gleichzeitig betriebenen Rechnern, angesprochen werden.

Mehrere Verzeichnisse sind möglich. Ein Arbeiten auf mehreren Mailservern ist möglich.

POP3 ist ein Offline-Protokoll. Die Daten werden vom Server abgeholt und dann offline bearbeitet.

IMAP4 ist ein Online-Protokoll. Die Verarbeitung der Mail findet auf dem Server statt.

IMAP4 nutzt TCP der Well-Known Port ist 143.

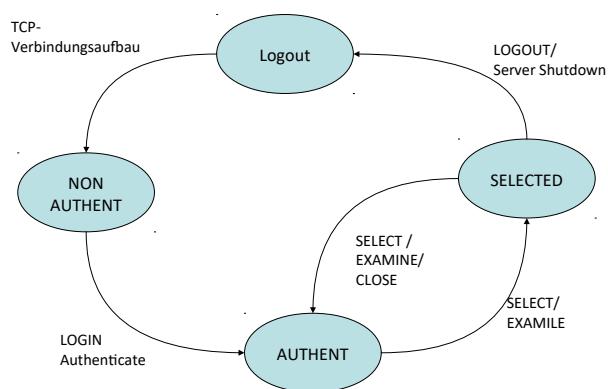


Abbildung 454 : IMAP4-Session-Zustände

Anwendungsprotokolle

Je nach Status sind unterschiedliche Kommandos möglich. Der Aufbau ist folgender:

Requests beginnen mit einem Tag (Buchstaben-Zahlen-Kombination), den der Client bestimmt. Der Server bezieht sich in seiner Antwort auf diesen Tag.

Request-Tag	Kommando	Parameter
A001	SELECT	Inbox

Der Server antwortet mit:

OK
NO
BAD
BYE

Kommandos können verlängert werden. Command Continuation Request Response
In geschweiften Klammern werden die Anzahl der zusätzlichen Oktette angegeben.
Die Bereitschaft für weiteren Text wird mit + angegeben.

Message Attribute / Message Identifikation

Durch eine Message Sequence-Nr. und die Unique Identifier (UID) kann eine Mail eindeutig identifiziert werden.

40.2.6 - Hyper Text Transfer Protocol (HTTP)

Dieses Protokoll dient zur Darstellung von WEB-Seiten also dem Transport von HTML-Seiten die dann vom Browser interpretiert werden.

Es ist in Client-Server-Architektur aufgebaut. Es ist im RFC2068 und RFC2616 beschrieben.

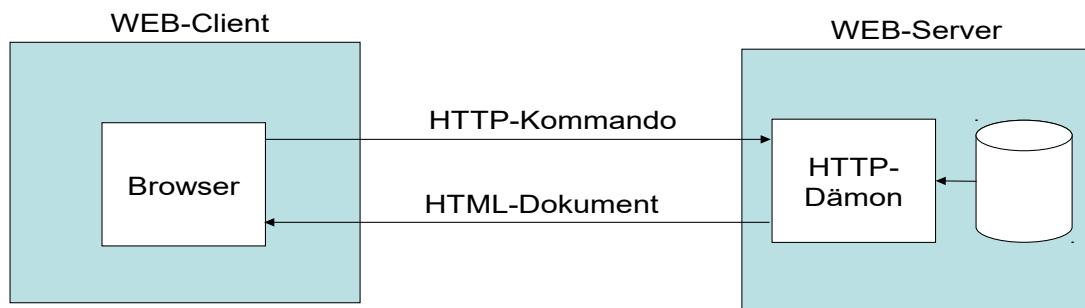
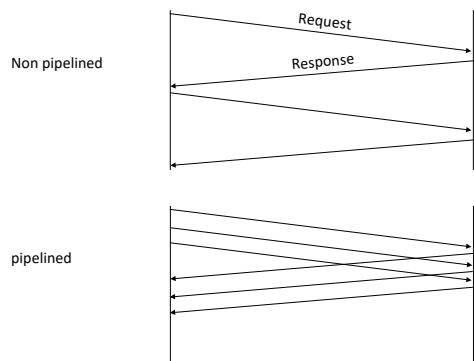


Abbildung 455 : HTTP



Während bei der HTTP-Version 1.0 ein verbindungsloser Charakter zugrunde lag, ist es seit der Version 1.1 möglich mehrere Request und Response-Aktivitäten gleichzeitig durchzuführen.

Abbildung 456 : Pipelining

Anwendungsprotokolle

Dies hat folgende Vorteile:

- Es werden weniger Ressourcen benötigt.
- Mehrere Aufträge können gleichzeitig unabhängig voneinander bearbeitet werden.
- Geringere Netzlast

Beim Internet handelt es sich um weltweit verteiltes Netzwerk, das für die Adressierung ein eigenes Konzept entwickelt hat um auf einzelne Dokumente einen Zugriff ermöglicht. Mit einem Uniform Resource Locator (URL) ist dies möglich.

Eine URL besteht immer aus den folgenden Bestandteilen:

- Protokoll (http, ftp, file)
- Portadresse des Kommunikationsprotokolls (Optional)
- Pfadangabe
- Name des Dokumentes

Beispiel:

`ftp://ftp.nic.de/pub/doc/rfc/rfc1900-1999/rfc1925.txt`

Die Kommunikation zwischen Browser und Server kann unterschiedlich ablaufen.

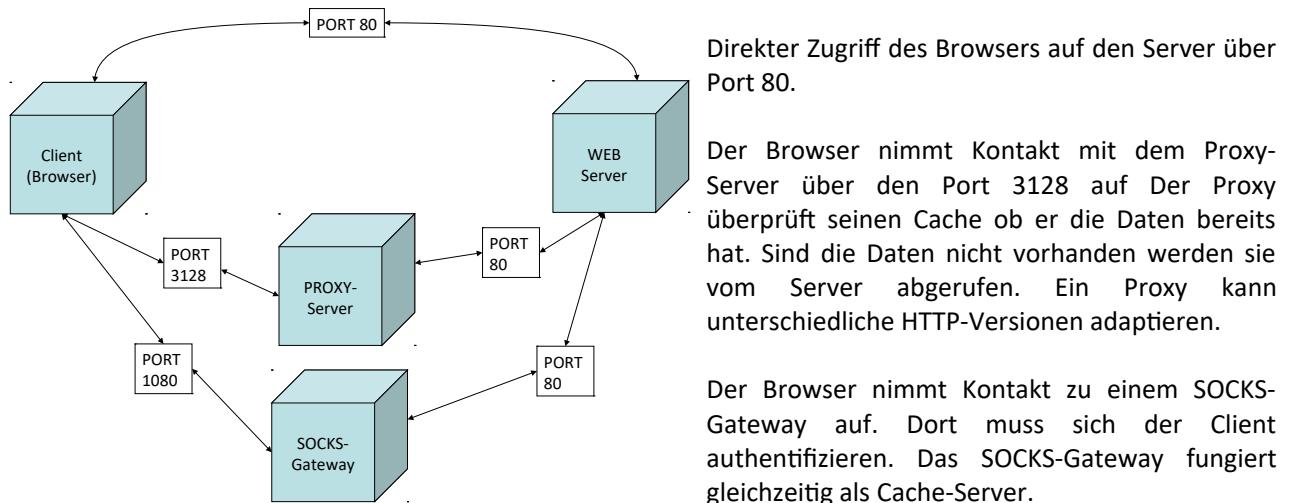


Abbildung 457 : HTTP-Zugriffsmöglichkeiten

40.2.7 - File Transfer Protocol (FTP)

Das FTP ist im RFC959 beschrieben. FTP sitzt auf TCP mit den Ports 20 und 21 auf.

40.2.7.1 - Aufbau

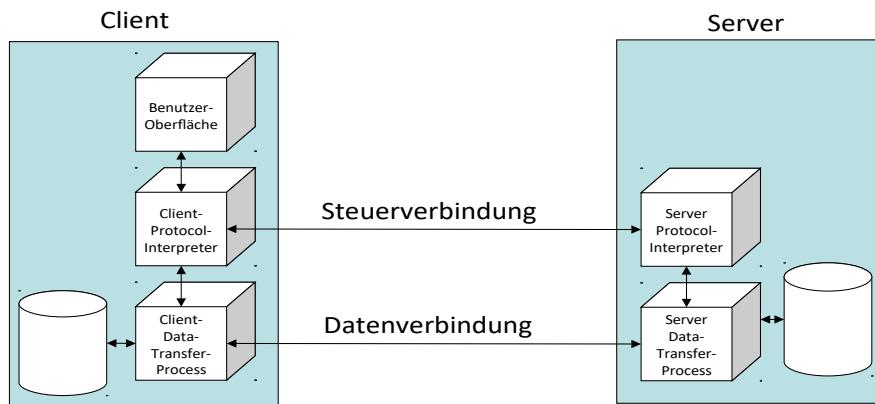


Abbildung 458 : FTP

FTP benutzt für die Steuerverbindung den Port 21 und für den Datenaustausch den Port 20

FTP verfügt über einen großen Befehlssatz. Dabei wird immer vorausgesetzt, dass der Anwender auf dem FTP-Server einen Benutzer-Account und -Verzeichnis hat. Ist dies nicht vorhanden, kann mit dem eingeschränkten Account „anonymous“ gearbeitet werden.

40.2.7.2 - FTP-Befehlssatz

Kommando	Bedeutung
append	Fügt ein lokales File in ein Remote-File ein
ascii	Übertragung erfolgt im ASCII-Format
bell	Es erfolgt ein akustisches Signal nach jedem ausgeführten Kommando
binary	Übertragung erfolgt im Binärformat
bye, quit	FTP beenden
cd	Change Directory im Remote-System
connect, open	Aufbau der Steuerverbindung
delete	Löscht File auf Remote-System
dir, ls	Inhalt des Directoys auf Remote-System ausgeben (ls -l)
get	Transfer eines Files vom Remote-System auf lokales System
lcd	Change Directory im lokalen System
mdelete	Löscht mehrere Files auf Remote-System
mget	Transfer mehrerer Files vom Remote-System auf lokales System
mput	Transfer mehrerer Files vom lokalen System auf das Remote-System
put	Transfer eines Files vom lokalen System auf das Remote-System
pwd	Anzeige des Working Directoys
rename	Ändern des Dateinamens auf Remote-System
rmdir	Löschen eines Remote-Directories
status	Status der FTP-Verbindung ausgeben
user	Sendet Userkennung und Passwort an Remote-System
verbose	Anzeige von Statistiken über Transferrate, Reaktionszeiten
passive	Toggle-Kommando für den Passiv-Modus
proxy	Auswahl eines alternativen Ports
port	Port-Nr. für Datenverbindung, abweichend vom Default

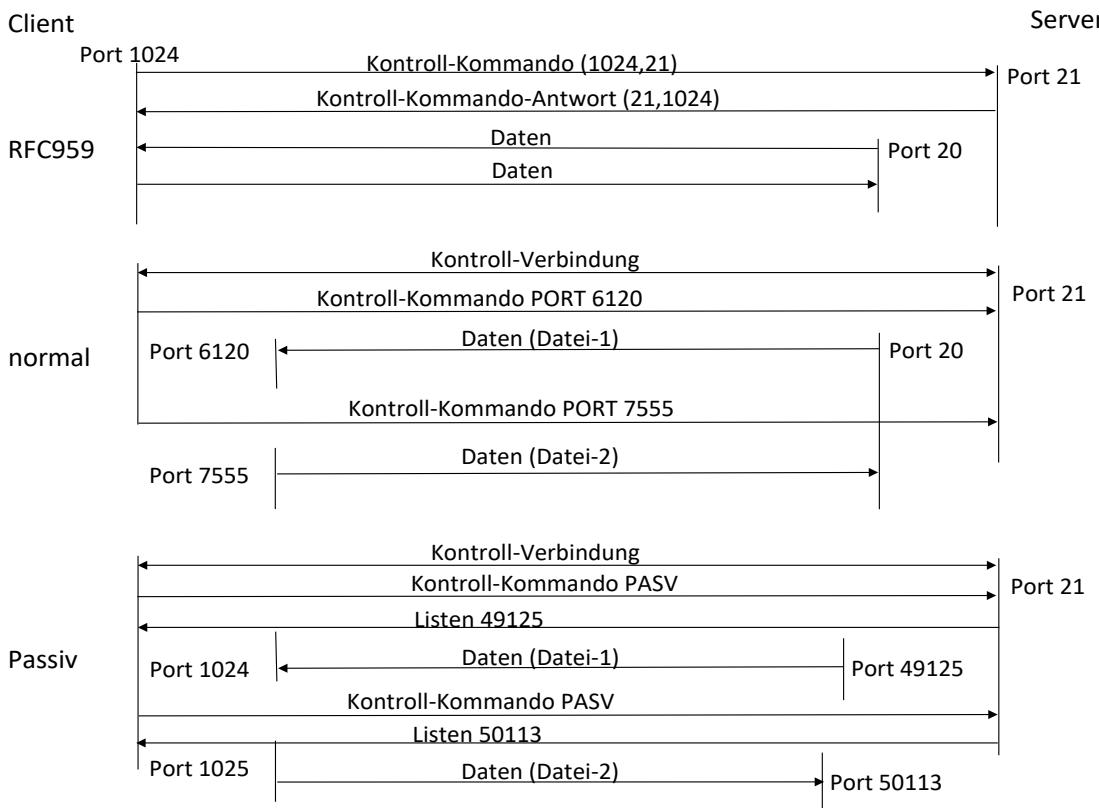


Abbildung 459 : FTP-Portzuweisung

Für jede Datenübertragung wird der Datenkanal neu geöffnet. Beim RFC959 wird davon ausgegangen, dass die Ports sofort wieder frei sind. Dies ist jedoch je nach Implementierung möglich oder nicht der Fall. Ist der Port nicht wieder frei, ist der FTP-Prozess blockiert. Deshalb ist es mittlerweile normal, dass für jede zu übertragende Datei ein neuer Port verwendet wird.

Da bei Firewalls die Port-Information normalerweise nicht ausgewertet wird, ist es möglich, durch das PASV (passiv)-Kommando, den Server aufzufordern mitzuteilen, über welchen Port die Daten ausgetauscht werden sollen. Eine Firewall kann durch Erkennung des PASV und Listen-Kommandos die entsprechende Portnummer für die Datenübertragung freischalten.

40.2.8 - Network Virtual Terminal (Telnet)

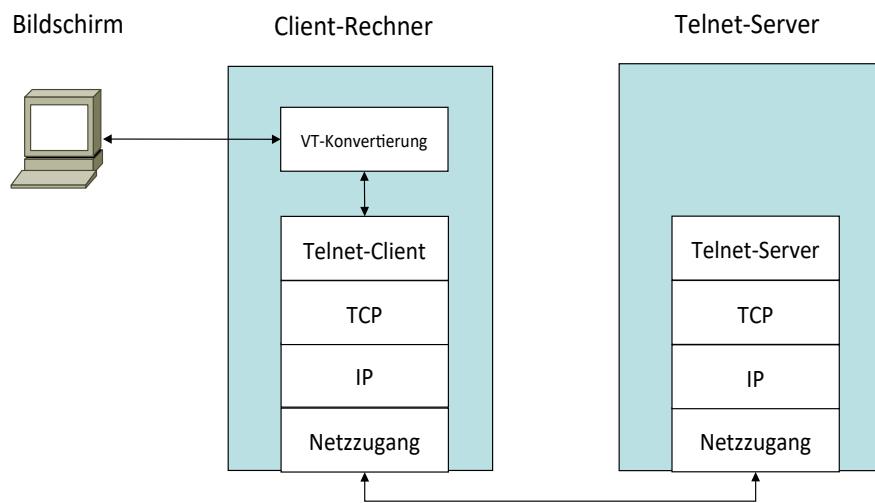


Abbildung 460 : Telnet

Die Möglichkeit von einem Rechner aus mehrere Rechner zu bedienen war seit Anbeginn der Rechnervernetzung eine Grundanforderung. Telnet nutzt TCP zur Datenübertragung. Telnet ist im RFC854 beschrieben. Mit Telnet ist es möglich Rechner unterschiedlicher Hersteller zu bedienen.

Nach dem Verbindungsaufbau wird der Login und das Passwort auf dem Zielrechner abgefragt. Dies geschieht ohne Verschlüsselung. Das heißt, dass die einzelnen Zeichen im Klartext über die Leitung gesendet werden!

41 - IP-Telefonie (Voice over IP (VoIP))

41.1 - Einleitung

Telefonie, so sie wie sie seit langem bekannt ist, setzt ein Leitung-vermitteltes Netzwerk voraus. Mit IP-Telefonie können über ein paketvermittelndes Netzwerk Sprachdaten übertragen werden. Diese Netzwerke sind von ihrem ursprünglichen Design her nicht für die Übermittlung von Sprachdaten ausgelegt. Telefonie erfordert einen gleichmäßigen kontinuierlichen Datenstrom damit die Sprache auf der Empfängerseite verständlich ist. Die paketvermittelnden Netzwerke können von sich aus diese Anforderungen nicht garantieren. Deshalb sind einige zusätzliche Maßnahmen erforderlich, wenn die IP-Telefonie funktionieren soll.

Weiterhin sind zusätzliche Verbindungs-Systeme erforderlich, wenn zusammen mit den Geräten der herkömmlichen Telefonie zusammen gearbeitet werden soll. Hier sind zusätzliche Gateways erforderlich.

Soll dann auch noch das Internet als Transportmittel verwendet werden, sind weitere Maßnahmen notwendig.

41.2 - Historisches

- ➊ 1973 Erste Übertragungen digitaler Sprache im ARPANET mittels Network Voice Protocol (NVP) zwischen PDP11-Rechnern realisiert. Die Standarddatenübertragungsrate bei NVP-II betrug 3.490 kbit/s.
- ➋ 1989 Die Einführung von ISDN durch ITU-T (damals CCITT) ermöglicht das Telefonieren mit höherer Sprachqualität und integriert verschiedene Dienste auf Basis digitaler Datenübertragung. Die Datenübertragungsrate bei ISDN beträgt pro Kanal 64kbit/s.
- ➌ 1992 wurde in Deutschland mit der GSM-Technik (D-Netz) die Datenübertragungsrate von 13kbit/s netto für Sprache ermöglicht. Brutto wurden zu Redundanz-Zwecken 22,8kbit/s übertragen.
- ➍ 1995 Programm des israelischen Unternehmens Vocaltec Communications ermöglicht Internettelefonie im Halbduplexbetrieb.
- ➎ 1996 Beschreibung des Real-Time Transport Protocol in RFC 1889.
- ➏ 1996 Apple-Talk und IP ermöglichen Quick Time - Conferencing (Ton- und Bildkommunikation im Vollduplexbetrieb)
- ➐ 1998 Erstmalige Verabschiedung des ITU-T-Rahmenstandards H.323.
- ➑ 1999 Beschreibung des Session Initiation Protocol (SIP) in RFC 2543.
- ➒ 2002 SIP-Erweiterung in RFC 3261.
- ➓ 2002 Verabschiedung von ITU Q.1912.5 zur Interoperabilität zwischen SIP und ISDN User Part.
- ➔ 2004 Die Software Skype erscheint.

41.3 - Vorteile

- Großes Potential für Kosteneinsparungen.
- Bei Gesprächen von VoIP zu VoIP fallen keine Kosten an.
- Es wird nur eine Infrastruktur / Netzwerk benötigt. Das bisherige Telefonnetz kann entfallen.
- Da das Personal für Daten- und Telefon-Dienstleistungen zusammengelegt werden kann, ergibt sich die Möglichkeit von Personalreduzierungen.
- Teleworker z. b. im Homeoffice können integriert werden. Videokonferenzen sind möglich. Reduzierung von Reise- / Fahrtkosten.
- Telefonnummern sind nicht an Orte gebunden
- Gesprächskopien sind möglich
- Bei VoIP handelt es sich um einen offenen Standard. Dies bietet Möglichkeiten zu vielfältigen Erweiterungen.
- Durch das Konzept der verteilten SIP-Server hat ein Ausfall nur eine Auswirkung auf einen Teilbereich.

41.4 - Nachteile

- Es ist eine ausreichende Bandbreite zur Verfügung zu stellen.
- Es gibt zusätzliche Sicherheitsprobleme. Das Abhören der Leitungen ist einfach. Dies macht evtl. zusätzliche Maßnahmen zur Verschlüsselung erforderlich.
- Es sind spezielle Kenntnisse zum Betrieb der neuen Technologie erforderlich. Dies bedeutet einen zusätzlichen Schulungsaufwand.
- Keine Notrufe möglich.
- Abhängigkeit von Stromversorgung der Endgeräte. Evtl. ist PoE-fähige Hardware erforderlich.
- Bei Ausfall des Netzwerks ist auch die Telefonie betroffen.

41.5 - Aufbau

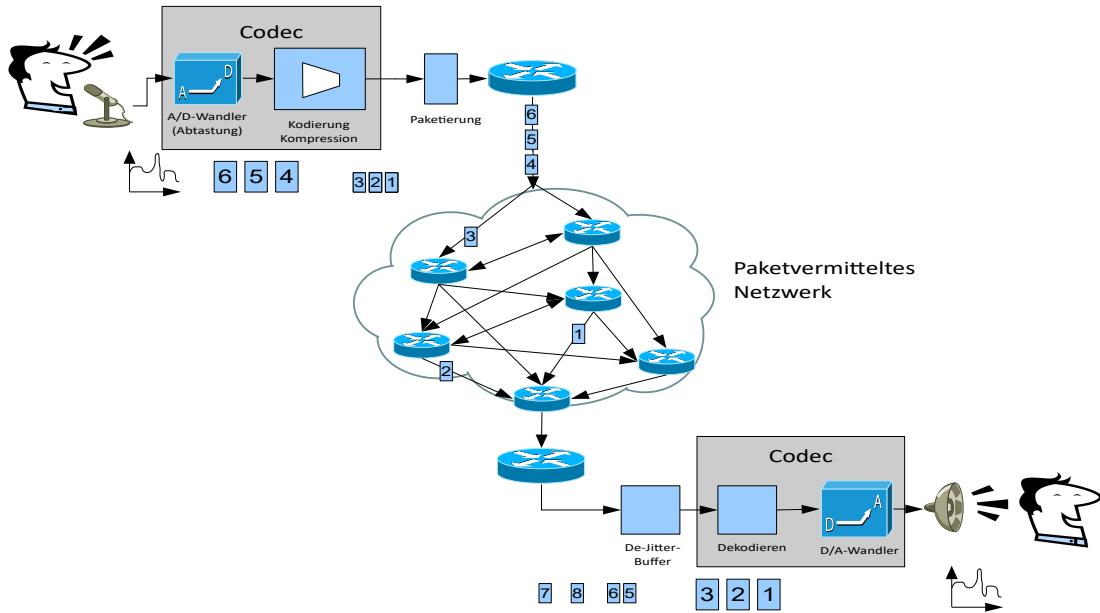


Abbildung 461 : VoIP - Übersicht

Um über ein paketvermitteltes Netzwerk zu telefonieren ist der folgende Aufbau erforderlich.

- ➊ Spracherfassung mit einem Mikrofon
- ➋ Bearbeitung mit einem Codec
 - ➌ Abtasten des zeitkontinuierlichen Sprachsignals mit einem A/D-Wandler.
Damit wird das Signal in eine digitale Form gebracht.
 - ➍ Kodierung.
 - ➎ Komprimierung
- ➏ Paketierung
- ➐ Übertragung über ein paketvermitteltes Netzwerk. Hierzu gehörender Verbindungsauflaufbau mittels einer Signalisierung und der Austausch der Sprachinformation.
- ➑ Auf der Empfängerseite erfolgt die Bearbeitung mit einem De-Jitter-Buffer. Da die Pakete mit unterschiedlichen zeitlichen Verzögerungen eintreffen und evtl. vertauscht oder verloren gegangen sind, werden sie in einem De-Jitter-Buffer sortiert und mit gleichen Zeitabständen an den Codec weiter gegeben
- ➒ Bearbeitung in einem Codec
 - ➓ Dekodierung.
 - ➔ Umwandlung des digitalen Signals in ein zeitkontinuierliches Sprachsignal
- ➕ Ausgabe des Sprachsignals mit einem Lautsprecher

41.5.1 - Spracherfassung mit einem Mikrofon

Wie zu Zeiten des Telefonersfinders Alexander Graham Bell wird die Sprache mit einem Mikrofon in ein elektrisches analoges zeitkontinuierliches Signal umgeformt

41.5.2 - Bearbeitung mit einem Codec

Je nach erforderlicher Sprachqualität stehen unterschiedliche Codecs zur Verfügung. Je besser die Sprachqualität, desto größer ist natürlich die zu übertragende Datenmenge. Bei ISDN wird Sprache in Sampeln von 8Bit/Bytes zerlegt und pro Sekunde 8000 Mal abgetastet. Dies ergibt eine Datenrate von 64 Kbit/s.

Codec	Benötigte Netto-/Bruttobandbreite	Bemerkung
G.711a, G.711u	64 kbit/s / 87,2 kbit/s	Von ISDN verwendeter Codec. Wird von allen Clients unterstützt A-law oder μ-law Kompression (schwach)
G.722	48, 56 oder 64 kbit/s	
G.723.1 ACELP	5,6 kbit/s / 16,27 kbit/s	Hohe Verbreitung bei Hardwaretelefonen. Kaum Verbreitung bei Softwaretelefonen aufgrund von Patentproblemen. Hohe Kompression bei akzeptabler Sprachqualität
G.726	16 kbit/s / 39,2 kbit/s	
G.726	24 kbit/s / 47,2 kbit/s	
G.726	32 kbit/s / 55,2 kbit/s	
G.726	40 kbit/s / 63,2 kbit/s	
G.728	16 kbit/s / 31,5 kbit/s	
G.729	8 kbit/s / 31,2 kbit/s	
GSM	13 kbit/s	Von Mobiltelefonen der zweiten Generation verwendeter Codec Hohe Verbreitung bei Softwaretelefonen. Hohe Resistenz gegen Bitfehler. Ordentliche Kompression und Sprachqualität
iLBC	15,2 kbit/s / 27kbit/s	Der „Internet Low Bitrate Codec“ wurde speziell für das Internet entwickelt und ist im RFC3951 beschrieben. Vermutlich von Skype verwendeter Codec. Hohe Verbreitung bei Softwaretelefonen. Hohe Resistenz gegen verlorene Packete. Die Kompression und Sprachqualität vergleichbar mit GSM.
Speex	Variabel: 2 bis 44 kbit/s	Von Xiph.org (OGG/Vorbis) entwickelter, neuer Codec. Hohe Verbreitung bei Softwaretelefonen. Bessere Sprachqualität oder höhere Kompression (je nach Einstellung) als GSM und iLBC

41.5.3 - Paketierung

Die Daten werden in Pakete von 20 – 240 Byte aufgeteilt.

41.5.4 - Datenübertragung über ein paketvermittelndes Netzwerk

Zwischen den Endgeräten ist vor der Datenübertragung zuerst eine Verbindung aufzubauen bevor eine Datenübertragung (Telefonat) stattfinden kann. Dazu ist eine Signalisierung erforderlich, damit die Telefonnummern in IP-Adressen umgesetzt werden und die Verbindungsparameter wie z. B. die verwendeten Codecs festgelegt werden können.

41.5.5 - Signalisierungsprotokolle

Für den Verbindungsaufbau zur Telefon-Gegenstelle wird ein Signalisierungsprotokoll verwendet. Derzeit gibt es die folgenden Signalisierungsprotokolle:

- SIP (Session Initiation Protocol IETF beschrieben im RFC 3261)
SIP ist an HTTP angelehnt und somit leicht zu integrieren. Nutzt TCP, UDP und IP. Kann auch für Telefon-Konferenzen oder Netzwerkspiele genutzt werden.
- SIPS (Session Initiation Protocol over SSL beschrieben im RFC 3261)
- H.323 (ITU-T)

Dieses Protokoll kann auch als „ISDN über IP“ bezeichnet werden. H.323 ist nur für Telefonie gedacht.

Von ITU-T sehr stark normiert. H.323 ist Protokollfamilie:

- H.225.0 (Setup)
- H.235 (Sicherung und Authorisierung)
- H.245 (Telefonie)
- H.450 (weitere Leistungmerkmale z.B. von ISDN)
- Q.931 (Signalisierung)
- Sprachcodec ist G.711

Als Alternative steht OpenH323 (MPL) zur Verfügung.

- IAX – Inter-Asterisk eXchange protocol
- ISDN over IP – ISDN/CAPI-basierendes Protokoll
- Skinny Client Control Protocol von Cisco ≠ SCCP (Q.71x von ITU-T)
- Jingle XMPP Protokoll-Erweiterung (Google Talk)
- MiNET von Mitel
- MGCP und MeGaCo (Media Gateway Control Protocol H.248 ist eine Gemeinschaftsproduktion von ITU-T und IETF)

41.5.5.1 - SIP**41.5.5.1.1 - Dialoge**

SIP stellt mehrere Dialoge zur Verfügung um zwischen zwei Teilnehmern (User Agent) eine Sitzung zu verwalten. Wie bei HTTP bestehen die Dialoge aus Requests des User Agent Client und Responses des User Agent Servers.

41.5.5.1.2 - SIP Requests:

Request	Beschreibung
Invite	Sitzungsaufbau. Dieser Request entspricht der Signalisierung wenn beim angerufenen das Telefon klingelt
Acknowledge	Bestätigung der Verbindung
Bye	Einer der beiden Gesprächspartner beendet das Gespräch
Cancel	Verbindungsabbruch
Options	Übertragung von Zusatzinformationen des Anwenders
Register	Übergabe der Standort-Informationen des Clients an den Server. Damit kann der Client angerufen werden.

41.5.5.1.3 - Responses von SIP:

Kennung	Bedeutung
1	Anruf erfolgt
100	Verbindung wird hergestellt (Trying)
180	Verbindung etabliert, warten auf Gegenseite (Ringing)
181	Der Anruf wird zu einem anderen Bestimmungsort umgeleitet
182	Die Gegenstelle ist zur Zeit nicht verfügbar, weist den Anrufer aber nicht zurück, sondern stellt ihn in die Warteschleife
200	OK
300	Die Rufnummer führt zu mehreren Zielen. Es erfolgt eine Auswahlmöglichkeit
305	Das Anruftziel ist nur über einem Proxy-Server erreichbar
400	SIP-Syntaxfehler bei der Verbindungsaufnahme
404	Die Gegenstelle teilt mit, dass das Anruftziel nicht existiert
485	Das Anruftziel ist vieldeutig. Der SIP-Server kann mehrere Möglichkeiten nennen
500	Interner Server-Fehler
501	Das SIP-Gateway unterstützt die angeforderte Aktion nicht
504	Timeout beim Warten auf eine anderen Server überschritten

600	Besetzt
603	Die Gegenseite weist den Anruf ab
604	Die Gegenseite existiert nicht im angegebenen SIP-Netz
605	Der Session Aufbau wurde ohne weitere Begründung nicht akzeptiert

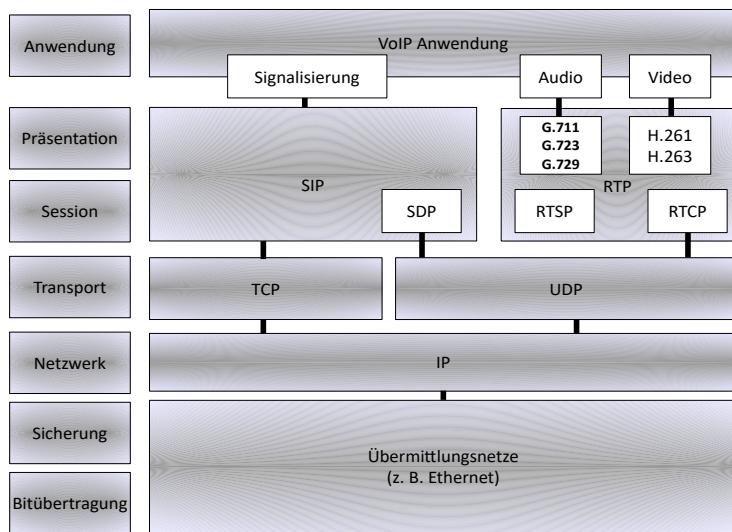


Abbildung 462 : SIP-Protokollstack

Das Session Initialisation Protocol ist das modernere der beiden aktuellen Signalisierung-Protokolle.

Eigentlich ist es nur ein kleiner Teil des so genannten SIP-Protokoll-Stacks.

Zum Protokollstack gehören die folgenden Protokolle dazu:

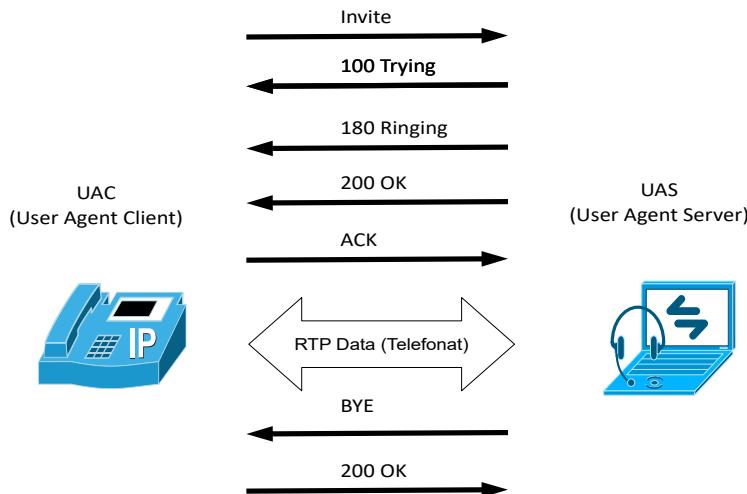
SDP - Session Description Protocol

RTSP - Realtime Streaming Protocol

RTCP - Realtime Control Protocol steuert RTP.

RTP - Realtime Transport Protocol wird für die kontinuierliche Datenübertragung genutzt.

41.5.5.1.4 - Verbindungsauflaufbau



SIP basiert wie HTTP auf dem Client Server Prinzip.

Bei SIP wird der Anrufende als UAC (User Agent Client) und der Angerufene als UAS (User Agent Server) bezeichnet.

Prinzipiell können die Sitzungen auch direkt zwischen den Clients abgehandelt werden.

Abbildung 463 : SIP direkte Verbindung

Da die Clients jedoch nicht immer zur Verfügung stehen und auch nicht immer die gleiche IP-Adresse haben werden sie in einem SIP-Server verwaltet. Dazu meldet sich jeder Client beim SIP Server an.

Dieser Server kann mehrere Funktionen abdecken. Er fungiert als Proxy zum Aufbau der Verbindung, als Registrar zur Verwaltung der Telefonnummern und als Location Server zur Auflösung der Namen in IP-Adressen (ähnlich DNS).

Der SIP Server kann in zwei unterschiedlichen Modi betrieben werden:

- ➊ Im Redirect Mode
- ➋ Im Proxy-Mode

41.5.5.1.5 - SIP im Redirect-Mode

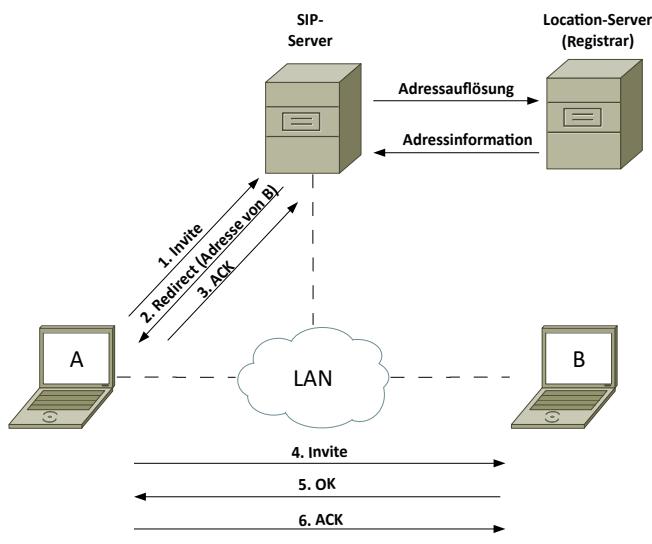


Abbildung 464 : SIP-Redirect-Mode

gehalten.

Wird eine Verbindung zu einer Gegenstelle aufgebaut ist zuerst der Standort der Gegenstelle zu ermitteln.

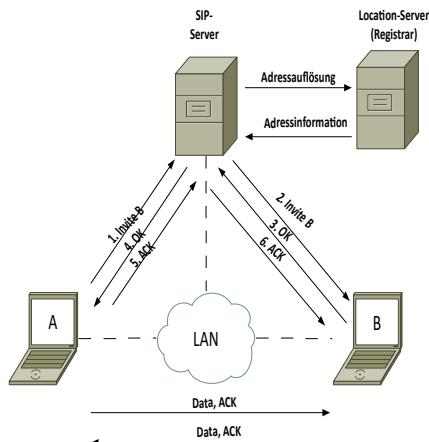
Dazu bedient sich der rufende Client des SIP-Servers. Der SIP-Server greift auf den SIP-Registrar zu um den Standort (IP-Adresse) des Ziel-Clients herauszufinden. Der SIP-Registrar funktioniert dabei wie ein DNS-Server.

SIP-Proxy und SIP-Registrar sind oft auf einem Server untergebracht.

Die Antwort geht zurück an den Client der dann die Verbindung mit der Gegenstelle aufbaut.

Die eigentliche Telefonverbindung wird dann direkt vom Client-A mit dem Client-B

41.5.5.1.6 - SIP im Proxy-Mode

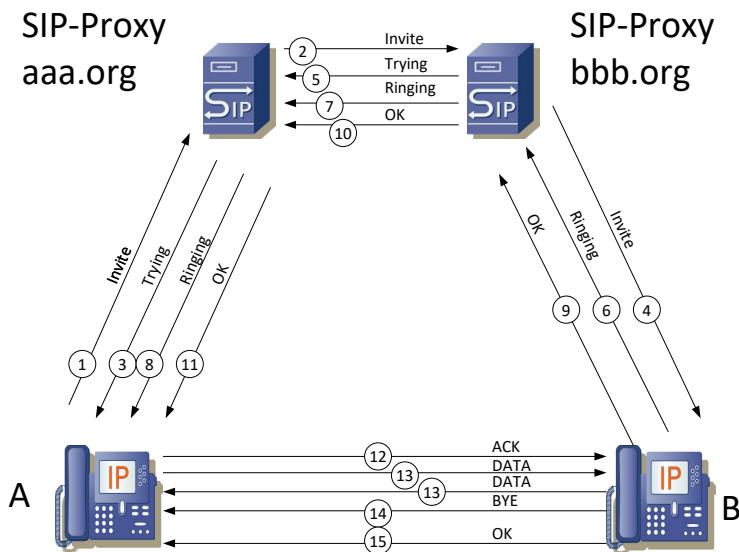


Hierbei wird die Verbindung zur Gegenstelle vom Proxy aufgebaut.

Diese Variante empfiehlt sich wenn über das Internet telefoniert werden soll da dann der Proxy Server mit einer international gültigen IP-Adresse ausgestattet werden kann.

Die eigentliche Telefonverbindung wird dann, wie beim Redirect-Mode, direkt vom Client-A mit dem Client-B gehalten.

Abbildung 465 : SIP-Proxy-Mode



Erfolgt der Verbindungsaufbau über zwei SIP-Server entsteht das so genannte SIP-Trapez.

Hierbei werden 2 SIP-Server im Proxy-Mode betrieben.

Abbildung 466 : SIP-Trapez

41.5.6 - ENUM

Mit einem ENUM-fähigen Telefon oder Provider kann jeder, der eine SIP-Adresse besitzt, per SIP angerufen werden.

ENUM steht für **E164 Number Mapping**. Damit ist die Umsetzung einer Telefonnummer in eine Adresse im URI-Format gemeint.

Die bei E164 verwendeten Nummern haben den folgenden Aufbau:

1 – 3 Stellen CC = Country Code

15 Stellen NDC = National Distribution Code + SN = Subscriber Number.

Die bei SIP verwendeten Adressen werden im URI-Format (wie bei E-Mails oder www-Adressen) geschrieben.

- ➊ Unverschlüsselte SIP-Verbindung: `sip:user@domain`
- ➋ Verschlüsselte Verbindung: `sips:user@domain`

Allerdings ist die Telefonnummer hierbei in das URI-Format zu überführen. Dabei wird folgendermaßen vorgegangen:

1. Telefonnummern: +49(711)12345
2. Zeichen löschen: 4971112345
3. Rückwärts schreiben: 5432111794
4. Punkte einfügen: 5.4.3.2.1.1.7.9.4
5. Domain anfügen: 5.4.3.2.1.1.7.9.4.e164.arpa

Derzeit gibt es drei globale Verzeichnisse für die Umsetzung in das E164-Format:

- ➊ e164.arpa: Offizielles Verzeichnis (arpa steht in diesem Zusammenhang für Address and Routing Parameter Area)
- ➋ e164.org: Von einer NPO getragenes, alternatives Verzeichnis
- ➌ e164.info: Spezielles Verzeichnis für VoIP-Anbieter

41.5.7 - Verzögerung - Laufzeit

Für die (Sprach-)Qualität ist die Zeit der Gesamtverzögerung (delay) zwischen dem Sprechen des Senders und dem Hören des Empfängers (Ende-zu-Ende-Verzögerung) ausschlaggebend.

Laufzeitverzögerungen entstehen während der unterschiedlichen Bearbeitungsschritte vom Sender bis zum Empfänger.

Die größten Verzögerungszeiten entstehen also beim Transport der Pakete durch das Netzwerk besonders in Routern, die zwischen unterschiedlichen Medien Daten austauschen, Switches, die im Store & Forward Modus arbeiten sowie Firewalls und Proxys. Die Verzögerung in den Codecs ist von der Rechenleistung abhängig. Allerdings sind diese Zeiten eher marginal. Eine Verzögerung sollte 150 ms nicht überschreiten. Eine Verzögerung unter 150 ms ergibt eine sehr gute Sprachqualität. Ab einem Delay von 250 ms wird ein Gespräch bereits negativ beeinflusst. Mit bis zu 400 ms gilt ein Gespräch noch als akzeptabel. Eine Verzögerung ab 400 ms ist als deutliche Gesprächspause hörbar. Bei kurzen Verzögerungen entsteht ein Echo. Bei größeren Verzögerungen hört man den anderen Teilnehmer noch, obwohl er schon zu Ende gesprochen hat. Das führt dazu, dass man dem Gesprächspartner zu oft ins Wort fällt. Dieses Problem kennt man bei Mobilfunkgesprächen, wenn der Empfang einseitig schlecht ist. Dann kommt es zu unangenehmen Verzögerungen und Unterbrechungen.

41.5.8 - Laufzeit mit Ping messen

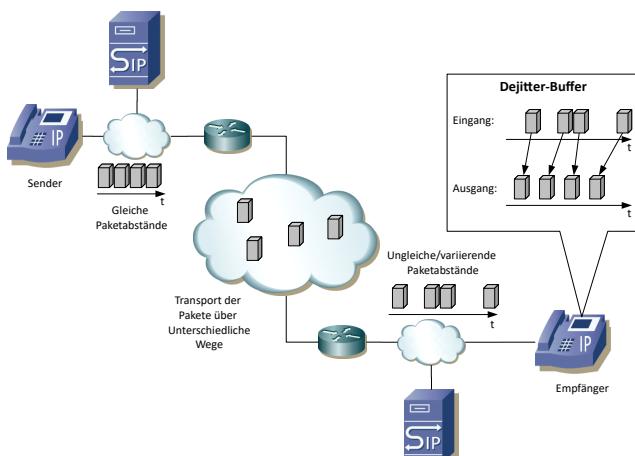
Um Verzögerungen auf einer Übertragungsstrecke zu messen, bietet sich der Ping-Befehl an. Er wird in einem CLI (command Line Interface (unter Windows z. B. DOS-Box) eingegeben und dient als grobe Abschätzung.

Dabei muss man beachten, dass der Ping die Gesamtverzögerung von Hinweg und Rückweg (Round-Trip-Time, RTT) misst. Sprachdaten dagegen werden jeweils nur in eine Richtung übertragen und enden beim Empfänger. Der Wert, den Ping liefert, muss somit halbiert werden. Da der Hin und der Rückweg sich voneinander unterscheiden können und Ping die Zeiten nicht trennen kann, ist diese Vorgehensweise nur ein Näherungswert.

Um die Messung mit Ping trotzdem einigermaßen realistisch zu gestalten muss die Paketgröße von Ping entsprechend eingestellt werden. Geht man von der Kodierung mit G.711 und 20 ms Sprachdaten pro Paket aus, dann entspricht das 160 Byte (64 kB/s x 0,02 s). Hinzurechnen muss man noch 40 Byte für den IP/UDP/RTP-Header-Anteil. Der Ping sollte also 200 Byte pro Paket verschicken, was dieser Befehl per Voreinstellung nicht macht.

Unter Windows würde das Ping-Kommando demnach **ping -l 200 -t {Hostname}** lauten. Durch das Attribut -t wird der Ping so lange wiederholt, bis die Tastenkombination Strg + C gedrückt wird. Unter Linux würde das Ping-Kommando **ping -s 200 {Hostname}** lauten.

41.5.9 - Jitter



Bei der Übertragung von Datenpaketen gibt es unterschiedliche Verzögerungen bei der Laufzeit. Die Schwankungen in der Laufzeit werden als Jitter bezeichnet und führen zu einer schlechten Sprachqualität.

Um das zu vermeiden, bedient man sich eines De-Jitter-Buffers. Der De-Jitter-Buffer speichert eingehenden Datenverkehr zwischen, um so ungleichmäßigen, wiederholten oder fehlerhaften Datenfluss auszugleichen.

Die Datenpakete, die mit unterschiedlichen Abständen eintreffen werden zwischengespeichert und mit etwas größeren, als den ursprünglichen Zeitabständen weiter geleitet.

Abbildung 467 : De-Jitter-Buffer

41.5.10 - Paketverluste - Packet Loss

Paketverluste treten z. B. bei Überlastung des Netzwerks auf, da das bei der Übertragung von VoIP-Sprachdaten verwendete UDP keinen Schutz gegen Paketverlust garantiert. Da ein Sprachpaket nur etwa 20 bis 30 ms an Sprache (etwa eine Silbe) enthält ist es unsinnig, ein solches Paket zu wiederholen. Dies ist auch, sofern das nicht zu häufig auftritt, tolerierbar. Sobald jedoch aufeinanderfolgende Pakete verloren gehen, führt das dazu, dass ganze Wörter oder Satzbestandteile fehlen.

Unter "Packet Loss" wird die prozentuale Menge verlorengegangener Datenpakete bei der Datenübertragung verstanden. Normalerweise liegt dieser Wert bei unter einem Prozent. Ein Datenverlust von bis zu 5% kann durch ein Codec ausgeglichen werden, da er nicht bemerkt wird.

41.5.11 - QoS (Quality of Service) / ToS (Type of Service)

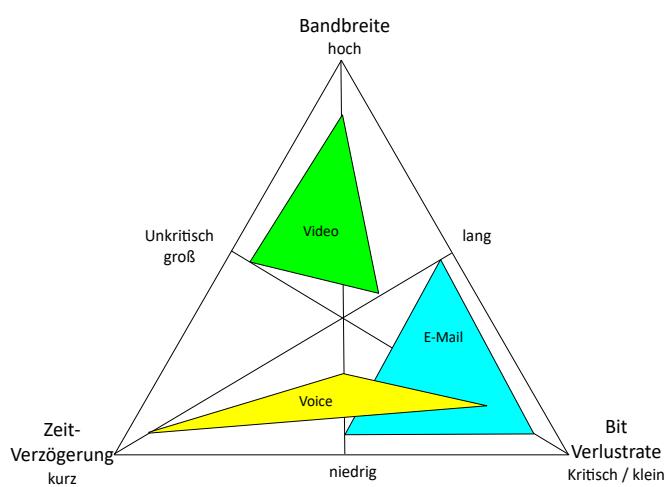


Abbildung 468 : Qualitätsanforderung von VoIP

Um von der Netzwerk-Seite die Probleme einzugrenzen wird versucht, die bereits vorhandenen Möglichkeiten, bei der Datenübertragung zu optimieren.

Es ist ein entsprechender Kompromiss aus Bandbreite, Zeitverzögerung und Bit-Verlustrate zu erzielen.

Dazu kann das 8 Bit große Feld ToS im IP-Header verwendet werden.

Die ersten 3 Bits werden der IP-Precedence zugeordnet. Dadurch ergeben sich die gleichen 8 Priorisierungs-Gruppen wie bei IEEE802.1q und IEEE802.1p

Die nächsten 3 Bits werden zusammen mit den Bits der IP-Precedence zur zum DSCP (Diffserve Code Point) zusammengefasst.

Die Möglichen Kombinationen sind folgende:

000 000 = Best Effort

101 000 = Expedited Flow (VoIP stream)

101 110 = Expedited Forwarding (VoIP stream)

Die letzten beiden Bits sind ungenutzt.

41.6 - Zusammenfassung

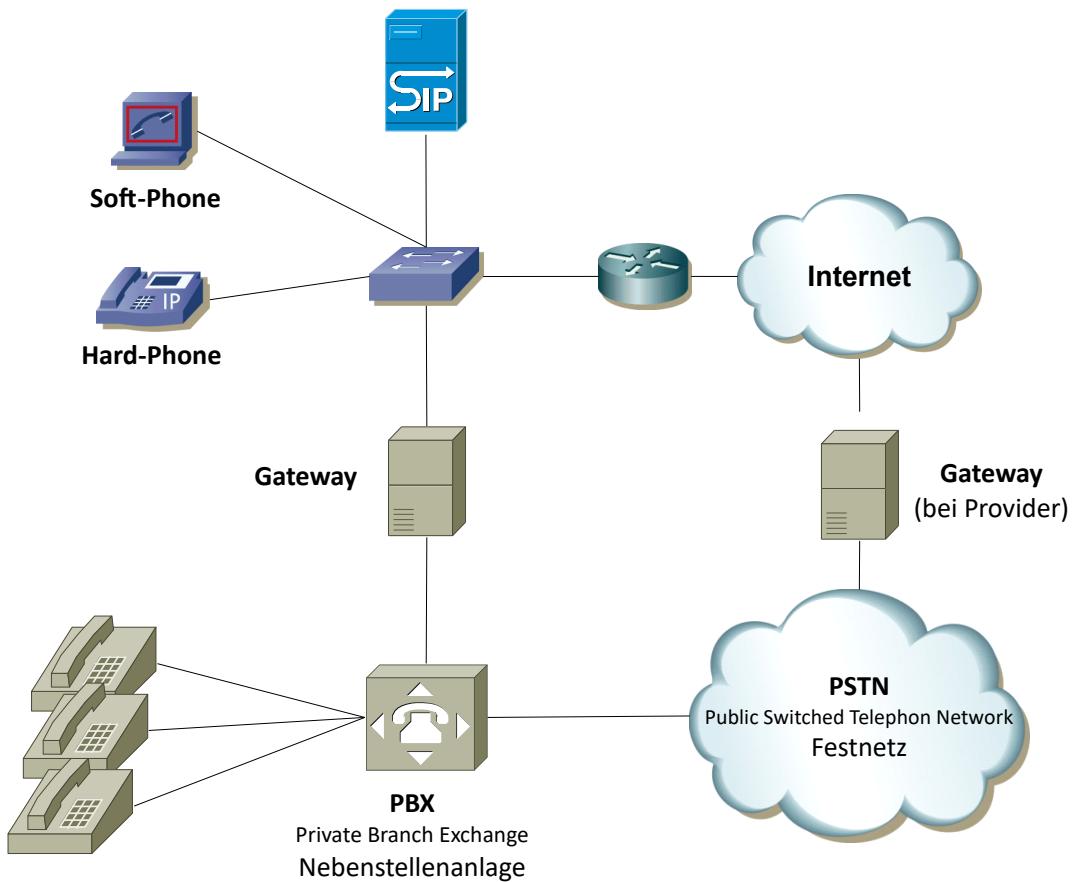


Abbildung 469 : Kopplung von Telefonanlage und VoIP

Die Verbindung von herkömmlichen Telefon-Anlagen mit einer VoIP-Welt kann über Gateways erfolgen. Diese können entweder lokal selbst betrieben werden, oder man verwendet eine Gateway das durch einen Provider zur Verfügung gestellt wird.

41.7 - Quellen

www.wikipedia.org

www.elektronik-kompendium.de

www.abis-freiburg.de

TCP/IP GE-PACKT

Mathias Hein, Michael Reisner

mitp-Verlag 2001 ISBN 3-8266-0803-8

TCP/IP

Mathias Hein

mitp-Verlag 2001 ISBN 3-8266-4094-2

Der Netzwerk Insider

ComConsult Research

42 - Anhang

42.1 - MAC-Adr. – Hersteller-Zuordnung

Erste 3 Byte (Hex)	Abkürzung	Hersteller
00000C	CISCO	Cisco
000020	DIAB	Data Industrier AB
000022	Visual	Visual Technology
00002A	TRW	TRW
00005A	S&K	Schneider and Koch
000065	NetGen	Network General
000093	Protn	Proteon
00009F	AmeStr	Ameristar Technology
0000A9	NetSys	Network Systems
0000AA	Xerox	Xerox machines
0000B3	CIMLnk	CIMlinc
0000C0	WesDig	Western Digital
0000DD	Gould	Gould Computers
000102	BBN-a	BBN Internal Use (not registered)
001700	Kabel	Kabel
005004	3Com	3Com 3C90x - Netzwerkkarte
00DD00	Ungera	Ungermann-Bass
00DD01	Ungerb	Ungermann-Bass
020406	BBN-b	BBN Internal Use (not registered)
020701	Intrln	Interlan UNIBUS/QBUS machines Apollo
02608C	3Com	3Com PC Type card IBM PC Imagen
02CF1F	CMC	CMC board Masscomp Silicon Graphics
080001	CV-Sun	
080002	Bridge	A Bridge Comm Server
080003	ACC	
080004		
080005	Symbol	Symbolics LISP Machine
080006	Siemns	Siemens AG
080007		
080008	BBN-c	BBN
080009	HP	Hewlett Packard

Erste 3 Byte (Hex)	Abkürzung	Hersteller
08000A	Nestar	Nestar Systems
08000B	Unisys	Unisys
08000C	ICL	ICL
08000D	AT&T	AT & T
08000E	ExIn-a	Excelan controller
08000F	NSC	NSC
080010		
080014		
080017		
08001A	DG-a	Data General
08001B	DG-b	Data General
08001E	Apollo	Apollo Workstations
080020	Sun	Sun Workstations
080022	NBI	NBI
080025	CDC	CDC
080028	TI	Texas Instruments
08002B	DEChw	DEC Hardware Address
80036	Interg	Intergraph CAE stations
80039	Spider	Spider Systems
80041	DCA	DCA
80047	Sequent	Sequent
80049	Univat	Univation
08004C	Encore	Encore
08004E	BICC	BICC Data Networks
08005A	IBM	International Business Machines
80067	Comdes	Comdesign
80068	Ridge	Ridge
80069	SilGrf	Silicon Graphics
08006E	ExIn-b	Excelan Controller
80075	Dde	Danish Data Elektronik A/S
08007C	Vitlnk	Vitalink Bridge
80089	Kinetk	Kinetics Apple Talk Ethernet Interface
08008B	Pyrmid	Pyramid

42.2 - Sonstige MAC-Adress-Zuordnungen

MAC-Adr.	Abkürzung	Hersteller
09002B00000F	DEC LAT MCst	DECServer (LAT) Multicast
09002B010001	DECBridgeHello	DECs LANBridge Multicast
09002B	DEC MC	Other DEC Multicasts
AA000	DECN	DECNet
AB0000010000	DEC MOP Mcst	DEC MOP Dump/Load Assist
AB0000020000	Dnet ID Mcst	DEC MOP System ID Multicast
AB0000030000	DnetHello MC	Decnet Hello Multicast
AB0000040000	Dnet Routemc	Decnet Router Multicast
AB000401	DEC LAVC	DEC Local Area Vax Cluster Multicast
AB000	DNTMC	Other Decnet Multicasts
FFFFFFFFFFFF	Broadcast	Main Broadcast Address

42.3 - Ethernet Typ-Kennungen

Typ	Kennung (hex)
AppleTalk	809B
DEC	600x
DEC LANbridge	8038
Excelan	8010
HP Probe	8005
Loopback	9000
Novell IPX	8137
TCP/IP	08xx
IP	0800
ARP	0806
XNS	0600
ISO	<= 05F6 (<1526 dez)

42.4 - Portnummern-Zuordnungen TCP -und UDP-Ports

Funktion	Protokoll	Portnummer
Reserviert	-	0
Nicht zugewiesen	-	01.04.88
RJE (Remote Job Entry)	TCP	5
ECHO (Echo)	TCP	7
DISCARD (Discard)	TCP	9
DAYTIME (Daytime)	TCP	13
QUOTE (Quote of the day)	TCP	17
CHARGEN (Character Generator)	TCP	19
FTP-Data (Filetransfer Default Data)	TCP	20
FTP (Filetransfer Control)	TCP	21
TELNET (Telnet)	TCP	23
SMTP (Simple Mail Transfer Protocol)	TCP	25
NSW-FE (NSW User System FE)	TCP	27
MSG-ICP (MSG ICP)	TCP	29
MSG-AUTH (MAG Authentification)	TCP	31
DSP (Display Support Protocol)	TCP	33
any private printer server	TCP	35
TIME (Time)	TCP	37
RLP (Recource Location Protocol)	TCP	39
GRAPHICS (Graphics)	TCP	41
NAMESERVER (Host Name Server)	TCP	42
NICNAME (Who is)	TCP	43
MPM-FLAGS (MPM-Flags Protocol)	TCP	44
MPM-SND (MPM default send)	TCP	46
NI-FTP (NI-FTP)	TCP	47
LOGIN (Login Host Protocol)	TCP	49
DOMAIN (Domain _Name Server)	TCP	53
ISI-GL (ISI Graphics Language)	TCP	55
Any private Terminal	TCP	57
Any private file service	TCP	59
NI-MAIL (NI-Mail)	TCP	61
VIA-FTP (VIA Systems FTP)	TCP	63
TACACS-DS (TACACS Database Service)	TCP	65
BOOTPS (Bootstrap Protocol Server)	TCP	67

Anhang

Funktion	Protokoll	Portnummer
BOOTPC (Bootstrap Protocol Client)	TCP	68
TFTP (Trivial File Transfer Protocol)	TCP	69
NETRJS-! (Remote Job Service)	TCP	71
NETRJS-“ (Remote Job Service)	TCP	72
NETRJS-§ (Remote Job Service)	TCP	73
NETRJS!\$ (Remote Job Service)	TCP	74
FINGER (Finger)	TCP	79
HTTP	TCP	80
MIT-ML-DEV (MIT ML Device)	TCP	83
MIT-ML-DEV (IT ML Device MIT ML)	TCP	83
Any private terminal link	TCP	87
SU-MIT-TG (SU/MIT Telnet Gateway)	TCP	89
MID-DOV (MIT Dover Spooler)	TCP	91
DCP (Device Control Protocol)	TCP	93
SUPDUP (SUPDUP)	TCP	95
SWIFT-RVF (Swift Remote Virtual F.)	TCP	97
TACNEWS (TAC News)	TCP	98
METAGRAM (Metagram Relay)	TCP	99
HOSTNAME (NIC Host Name Server)	TCP	101
ISO-TSAP (ISO-TSAP)	TCP	102
X400 (X400)	TCP	103
X400-SND (X400-SND)	TCP	104
CSNET-NS (MailboxName-Server)	TCP	105
RTELNET (Remote Telnet Service)	TCP	107
POP2 (Post-Office-Protocol 2)	TCP	109
SUNRPC (SUN Remote Procedure Calls)	TCP	111
AUTH (Authentification Service)	TCP	113
SFTP (Simple Mail Transfer Protocol)	TCP	115
UUCP-PATH (UUCP-Path-Service)	TCP	117
NNTP (Network News Transfer Protocol)	TCP	119
NTP (Network Time Protocol)	TCP	123
LOCUS-MAP (Locus PC- Interface)	TCP	125
LOCUS-MAP (Locus PC- Interface)	TCP	125
PWDGEN (Pathword Generator Protocol)	TCP	129
CISCO-FNA (Cisco FNATIVE)	TCP	130
CISCO-TNA (Cisco TNATIVE)	TCP	131

Funktion	Protokoll	Portnummer
CISCO-SYS (Cisco SYSMAINT)	TCP	132
STATSRV (Statistics Service)	TCP	133
INGRES-Net (INGRES-NET-Service)	TCP	134
LOC-SRV (Location Service)	TCP	135
PROFILE (PROFILE Naming System)	TCP	136
NETBIOS-NS (NETBIOS-Name-Server)	TCP	137
NETBIOS-DGM (NETBIOS-Datagram-Server)	TCP	138
NETBIOS-SSN (NETBIOS-Session-Server)	TCP	139
EMFIS-DATA (EMFIS-Data Service)	TCP	140
EMFIS-CNTL (EMFIS-Control Service)	TCP	141
BL-IDM (Britton-Lee IDM)	TCP	142
RCP (Remote Copy)	TCP	514
Browser-Dienst (Computer-Suchdienst)	UDP	137,138
DHCP-Lease	UDP	67,68
DHCP-Manager (Administration des DHCP-Servers)	TCP	135
Verzeichnisreplikation	UDP,TCP	138(UDP),139(TCP)
DNS-Administration	TCP	139
DNS-Namensaflösung	UDP	53
Ereignisanzeige	TCP	139
Zugriffe auf den Datei-Server	TCP	139
Anmeldesequenz	UDP,TCP	137,138(UDP) 139(TCP)
Net Logon-Dienst	UDP	138
Validierung von Zugriffen bereits angemeldeter Benutzer im Netzwerk	UDP,TCP	137,138(UDP), 139(TCP)
Systemmonitor	TCP	139
PPTP	TCP	1723 (IP-Protokoll 47)
Drucken	UDP,TCP	137,138(UDP) 139(TCP)
Registry-Editor	TCP	139
Server-Manager	TCP	139
Vertrauenstellungen und erforderliche Kommunikation zwischen vertrauten Servern	UDP, TCP	137,138(UDP), 139(TCP)
Benutzer-Manager	TCP	139
Windows-NT-Diagnose	TCP	139
Schere Windows-NT-Kommunikationskanäle beispielsweise für den Anmeldeprozeß	UDP, TCP	137,138(UDP, 139(TCP))
WINS-Replikation	TCP	42

Anhang

Funktion	Protokoll	Portnummer
WINS-Manager	TCP	135
SNMP	UDP	161
SNMP-Trap	UDP	162
WINS-Registrierung	TCP	137

42.5 - AWG-Tabelle

AWG bedeutet American Wire Gauge

AWG-Wert	Durchmesser in mm	Querschnitt mm ²	Widerstand W/km	I bei 3A/mm ² in mA
46	0,04	0,0013	13700,00	3,8
44	0,05	0,0020	8750,00	6
42	0,06	0,0028	6070,00	9
41	0,07	0,0039	4460,00	12
40	0,08	0,0050	3420,00	14
39	0,09	0,0064	2700,00	19
38	0,10	0,0078	2190,00	24
37	0,11	0,0095	1810,00	28
	0,12	0,0110	1520,00	33
36	0,13	0,0130	1300,00	40
35	0,14	0,0150	1120,00	45
	0,15	0,0180	970,00	54
34	0,16	0,0200	844,00	60
	0,17	0,0230	757,00	68
33	0,18	0,0260	676,00	75
	0,19	0,0280	605,00	85
32	0,20	0,0310	547,00	93
30	0,25	0,0490	351,00	147
29	0,30	0,0710	243,00	212
27	0,35	0,0960	178,00	288
26	0,40	0,1300	137,00	378
25	0,45	0,1600	108,00	477
24	0,50	0,2000	87,50	588
	0,55	0,2400	72,30	715
	0,60	0,2800	60,70	850
22	0,65	0,3300	51,70	1A

AWG-Wert	Durchmesser in mm	Querschnitt mm ²	Widerstand W/km	I bei 3A/mm ² in mA
	0,70	0,3900	44,60	1,16A
	0,75	0,4400	38,90	1,32A
20	0,80	0,5000	34,10	1,51A
	85,00	0,5700	30,20	1,70A
19	0,90	0,6400	26,90	1,91A
	0,85	0,7100	24,30	2,12A
18	1,00	0,7800	21,90	2,36A
	1,10	0,9500	18,10	2,85A
	1,20	1,1000	15,20	3,38A
16	1,30	1,3000	13,00	3,97A
	1,40	1,5000	11,20	4,60A
	1,50	1,8000	9,70	5,30A
14	1,60	2,0000	8,54	6,0A
	1,70	2,3000	7,57	6,7A
13	1,80	2,6000	6,76	7,6A
	1,90	2,8000	6,05	8,5A
12	2,00	3,1000	5,47	9,4A

42.6 - Verwendete mathematische Zuordnungen

42.6.1 - Logarithmen

$\log(x) = \log_{10}(x) = \lg(x)$ = Logarithmus zur Basis 10

$\log_n(x) = \ln(x)$ = Logarithmus zur Basis e

$\log_2(x) = \text{Id}(x)$ = Logarithmus zur Basis 2

43 - Literaturhinweise

Zur weiteren Vertiefung der Themen können die folgenden Bücher genutzt werden.

Titel	Author	Verlag	ISBN	Preis
Internetworking	Petra Borowka	Datacom Buchverlag	3-89238-141-0	96.-
Handbuch Netzwerk-Technologien	M.Ford H. Kim Lew S.Spanier T. Stevenson	CISCO PRESS	3-8272-2034-3	99.95
High Speed Internetworking	Anatol Badach Erwin Hoffmann Olaf Knauer	ADDISON WESLEY	3-8273-1232-9	79.90
Meßtechnik für Computernetze	Jörg Holzmann Jürgen Plate	Richard Pflaum Verlag	3-7905-1504-3	29.80
LAN Praxis lokaler Netze	D.H. Traeger A. Volk	Teubner Verlag	3-519-06189-9	56.-
Rechnernetze	W.E. Proebster	Oldenburg Verlag	3-486-24540-6	68.-
Fast Ethernet	Othmar Kyas	International Thomson Publishing	3-8266-4029-2	79.-
Glossar Netzwerktechnologie	Hans-Peter Boell	Heise Verlag	3-88229-032-3	?
Troubleshooting TCP/IP	Mark A. Miller	Heise Verlag	3-88229-029-3	?
TCP/IP-Praxis	Mark A. Miller	Heise Verlag	3-88229-071-4	?
Computernetzwerke	Andrew S. Tanenbaum	Prentice Hall	3-8272-9536-X	99,95
TCP/IP Illustrated Volume I	W. Richard Stevens	ADDISON WESLEY	9-780201-633467	105

Im Test explizit gegebene Literaturhinweise werden im Literaturverzeichnis beschrieben

Literaturverzeichnis

- Scherff-GCN-2010:** Scherff, Jürgen, Grundkurs Computernetzwerke, 2010 ISBN: 978-3-8348-0366-5
- HELÖ-NATE-2000:** Herter, Eberhard / Lörcher, Wolfgang, Nachrichtentechnik Übertragung-Vermittlung-Verarbeitung, 2000 ISBN: 3-446-21405-4
- BOS-EIDN-2012:** Bossert, Martin, Einführung in die Nachrichtentechnik, 2012 ISBN: 978-3-486-70880-6
- RFC-791:** Postel, Jon Internet Protocol , 1981
- RFC-4632:** Fuller, V. Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan, 2006
- RFC-5798:** Nadas, Ed. Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6, 2010
- BOR-NT-2002:** Borowka, Petra, Netzwerk-Technologien, 2002 ISBN: 3-8266-4093-4
- IEEE802.3ad:** ,
- IEEE802.1AX-2020:** Haddock, Stephen / Rouyer, Jessy Standard for Local and Metropolitan Area Networks – Link Aggregation, 2020
- NI-2001-02:** Borowka, PetraLink Aggregation, 2001

44 - Abbildungsverzeichnis**Abbildungsverzeichnis**

Abbildung 1: Internet-Gremien.....	3
Abbildung 2: Bereiche der IP-Adressvergabe.....	6
Abbildung 3: CE-Kennzeichen.....	7
Abbildung 4: RFC-Lebenszyklus.....	10
Abbildung 5: Einordnung der Netztechnik in die Ebenen der Wirtschaft.....	13
Abbildung 6: Informationssysteme.....	14
Abbildung 7: Einsortierung von Informationen in Wissen.....	15
Abbildung 8: Bandbreitenbedarf über der Zeit.....	16
Abbildung 9: Terminal-Netzwerk.....	19
Abbildung 10: Client-Server und Peer-to-Peer-Systeme.....	19
Abbildung 11: E-Commerce-Beispiel.....	20
Abbildung 12: Kommunikationssystem.....	21
Abbildung 13: Kommunikationsformen.....	23
Abbildung 14: Verkehrsarten.....	24
Abbildung 15: Betriebsarten der Nachrichtenübertragung.....	25
Abbildung 16: Beispiele für Broadcast- und Punkt-zu-Punkt-Netzwerke.....	26
Abbildung 17: Übertragungskonzept von Point-to-Point-Netzen.....	27
Abbildung 18: Netz-Zugangsarten.....	28
Abbildung 19: Verbindungstypen von Rechnernetzen.....	31
Abbildung 20: Gegenüberstellung: Nachrichtenvermittlung vs. Paketvermittlung.....	32
Abbildung 21: Datagramm-Verfahren.....	32
Abbildung 22: Paket-Verfahren.....	32
Abbildung 23: Elektromagnetisches Spektrum.....	33
Abbildung 24: Funkwellenausbreitung.....	34
Abbildung 25: Mikrowellenausbreitung.....	34
Abbildung 26: ISM-Bänder in Deutschland und USA.....	35
Abbildung 27: Unterscheidung von Anwendungsfällen (LEO / MEO / GEO).....	36
Abbildung 28: Satellitenkommunikation.....	37
Abbildung 29: IRIDIUM-Satelliten.....	37
Abbildung 30: Kommunikationsvermittlung bei Satelliten.....	38
Abbildung 31: Starlink-Orbitalebene.....	38
Abbildung 32: Starlink-Abdeckung in erster Stufe. Quelle: Business Insider.....	39
Abbildung 33: VSAT.....	39
Abbildung 34: Cubesat Quelle: Wikipedia.....	39
Abbildung 35: Dienstesicht.....	41
Abbildung 36: Protokollsicht.....	41
Abbildung 37: Grundelemente einer Kommunikations-Architektur.....	44
Abbildung 38: Interaktionen zwischen Schichten.....	45
Abbildung 39: Schnittstellen-Übergabe.....	46
Abbildung 40: Bestandteile von Referenzmodellen.....	47
Abbildung 41: Dienste / Primitive.....	48
Abbildung 42: Primitive bei verbindungsorientierter Kommunikation.....	49
Abbildung 43: Primitive bei verbindungsloser Kommunikation.....	50
Abbildung 44: Globale und lokale Signifikanz.....	51
Abbildung 45: SAP-Zugriff erlaubt / nicht erlaubt.....	52
Abbildung 46: ISO-RM-Übersicht.....	53
Abbildung 47: Beispiel: Header der Ebene 1 bei Ethernet.....	55
Abbildung 48: Beispiel: Ermittlung der Frame-Check-Sequence bei Ethernet.....	56
Abbildung 49: Kommunikation auf Ebene2.....	57
Abbildung 50: MAC-Adress-Zuweisung zum Frame.....	57
Abbildung 51: Beispiel: Umwandlung von LSB in MSB bei Ethernet.....	61

Abbildung 52: Framebearbeitung in Abhangigkeit von der Ziel-MAC-Adresse.....	61
Abbildung 53: Routing.....	63
Abbildung 54: Routing uber Netzwerk-Grenzen hinweg.....	64
Abbildung 55: Klassifizierung von Signalen.....	66
Abbildung 56: Abtastung mit $f_A > 2B$	67
Abbildung 57: $f_A = 2B$	68
Abbildung 58: $f_A < 2B$	68
Abbildung 59: Zeit-kontinuierliches Signal.....	69
Abbildung 60: Abtastintervall.....	69
Abbildung 61: Zeit- und wert-diskrete Abtastung.....	69
Abbildung 62: Quantisierungsrauschen.....	70
Abbildung 63: Baudrate / Symbolrate / Schritt.....	70
Abbildung 64: Ubertragungsgeschwindigkeit.....	71
Abbildung 65: Aliasing1-Zeitbereich.....	72
Abbildung 66: Aliasing1 - Frequenzbereich.....	72
Abbildung 67: Aliasing2 Zeitbereich.....	73
Abbildung 68: Aliasing2 - Frequenzbereich.....	73
Abbildung 69: Darstellungsmoglichkeiten von Sinus-Signalen.....	74
Abbildung 70: Fourier-Synthese (Teil-1).....	76
Abbildung 71: Fourier-Synthese (Teil-2).....	78
Abbildung 72: Fourier-Synthese (Teil-3).....	79
Abbildung 73: Message-Cube.....	82
Abbildung 74: Multiplex-Verfahren.....	83
Abbildung 75: Zeitmultiplex.....	83
Abbildung 76: Frequenzmultiplex.....	84
Abbildung 77: Gleichstrom-Anteil.....	85
Abbildung 78: Ubertragung uber das offentliche Telefonnetz.....	85
Abbildung 79: 4-Draht-Verbindung.....	87
Abbildung 80: Gabelumschalter.....	87
Abbildung 81: Bruckenschaltung.....	87
Abbildung 82: Takt-Ruckgewinnung-1.....	88
Abbildung 83: Takt-Ruckgewinnung-2.....	88
Abbildung 84: Scrambling - Descrambling.....	89
Abbildung 85: Rahmen-Ausrichtung.....	89
Abbildung 86: Prambel.....	90
Abbildung 87: Asynchrone Datenubertragung.....	90
Abbildung 88: Nachrichten-Ebene.....	95
Abbildung 89: Kanal.....	96
Abbildung 90: Kodierungsarten.....	97
Abbildung 91: Codebam einer prifixfreien und einer nicht prifixfreien Codierung.....	98
Abbildung 92: Huffmann-Codierung.....	102
Abbildung 93: Huffmann-Codierung (Graphisch).....	103
Abbildung 94: Ermittlung des Paritatsbits.....	104
Abbildung 95: Code-Wrfel.....	106
Abbildung 96: Fehlererkennung mit Paritatsbits bei zweidimensionaler Paritat.....	107
Abbildung 97: CRC-Berechnung.....	108
Abbildung 98: CRC-Berechnungsbeispiel.....	109
Abbildung 99: CRC-Bearbeitung auf der Empfangerseite.....	110
Abbildung 100: Zweistufige Leitungskodierung.....	112
Abbildung 101: NRZ-Wire-Codes.....	114
Abbildung 102: Biphasic und Manchester-Codierung.....	115
Abbildung 103: Ternary-Wire-Codes.....	117
Abbildung 104: Ideales Signal.....	118
Abbildung 105: Wahrscheinlichkeitsverteilung eines Signals.....	118
Abbildung 106: Zusammenhang zwischen BER und SNR.....	119
Abbildung 107: Augenmuster.....	120
Abbildung 108: Geschlossenes Auge bei einer zweistufigen Leitungscodierung.....	120

Abbildungsverzeichnis

Abbildung 109: Offenes Auge bei einer zweistufigen Leitungscodierung.....	120
Abbildung 110: Modulation - Demodulation.....	121
Abbildung 111: Modulationsarten.....	123
Abbildung 112: Signale der Modulation.....	124
Abbildung 113: Demodulation.....	125
Abbildung 114: 50%-Modulation.....	126
Abbildung 115: 100%-Modulation.....	126
Abbildung 116: Übermodulation.....	127
Abbildung 117: Frequenzmodulation (FM).....	128
Abbildung 118: Komplexe Ebene bei der unipolaren Übertragung.....	128
Abbildung 119: Signalverlauf der unipolaren Übertragung.....	128
Abbildung 120: Komplexe Ebene bei der bipolaren Übertragung (BPSK).....	129
Abbildung 121: Signalverlauf der bipolaren (BPSK) Übertragung.....	129
Abbildung 122: Komplexe Ebene bei der orthogonalen Übertragung.....	130
Abbildung 123: Signalverlauf einer orthogonalen Übertragung.....	130
Abbildung 124: Komplexe Ebene bei der Übertragung von 4-ASK.....	131
Abbildung 125: Signalverlauf einer 4-ASK-Übertragung.....	131
Abbildung 126: Signalverlauf einer 4FSK-Übertragung.....	132
Abbildung 127: Komplexe Ebene bei der Übertragung von QPSK.....	132
Abbildung 128: Signalverlauf einer QPSK-Übertragung.....	132
Abbildung 129: QPSK.....	133
Abbildung 130: Komplexe Ebene bei der Übertragung von 16QAM.....	134
Abbildung 131: Signalverlauf einer 16QAM-Übertragung.....	134
Abbildung 132: 64-QAM.....	134
Abbildung 133: Pulsmodulation.....	135
Abbildung 134: Spektrallinien bei PAM.....	136
Abbildung 135: PCM.....	137
Abbildung 136: Differenz-Modulation.....	138
Abbildung 137: Stromkreis.....	140
Abbildung 138: Ausschnitt aus Stromkreis.....	140
Abbildung 139: Magnetisches und elektrisches Feld.....	140
Abbildung 140: Leitungs-Ersatzschaltbild.....	141
Abbildung 141: Ermittlung des Wellenwiderstandes.....	142
Abbildung 142: Wellenausbreitung.....	145
Abbildung 143: Reflexion.....	146
Abbildung 144: Magnetfeld um Leiter.....	149
Abbildung 145: Induktion.....	149
Abbildung 146: Link-Definitionen.....	150
Abbildung 147: Wirkprinzip der Twisted-Pair-Leitungen.....	151
Abbildung 148: NEXT / FEXT.....	152
Abbildung 149: NEXT-Messung.....	153
Abbildung 150: Dämpfung / attenuation.....	155
Abbildung 151: Dämpfungsmessung.....	156
Abbildung 152: a, NEXT, ACR.....	157
Abbildung 153: ACR-Messung.....	158
Abbildung 154: PSNEXT / PSFEXT.....	159
Abbildung 155: PSACR-Messung.....	160
Abbildung 156: ELFEXT.....	161
Abbildung 157: PSELFEXT-Messung.....	162
Abbildung 158: Propagation Delay.....	163
Abbildung 159: Propagation Delay-Skew.....	164
Abbildung 160: HDTDR-Messung.....	165
Abbildung 161: HDTDX-Messung.....	166
Abbildung 162: RL-Messung.....	167
Abbildung 163: Alien-Crosstalk.....	168
Abbildung 164: Split Pairs bei RJ45-Stecker-Belegung.....	169
Abbildung 165: Richtige Verdrahtung bei Twisted Pair-Leitungen mit RJ45-Steckern.....	169

Abbildung 166: Verlauf in dB über der Frequenz.....	173
Abbildung 167: Zugriffsverfahren.....	174
Abbildung 168: Pure ALOHA - Kollisionen.....	175
Abbildung 169: Kollision (Kritische Zeit).....	176
Abbildung 170: Pure Aloha Datendurchsatz.....	177
Abbildung 171: Slotted ALOHA.....	178
Abbildung 172: CSMA-Verfahren.....	179
Abbildung 173: Zugriffsverfahren im Vergleich.....	180
Abbildung 174: Keine Kollisionserkennung bei Full-Duplex.....	181
Abbildung 175: Kollisionserkennung bei Half-Duplex.....	181
Abbildung 176: Zusammenhang zwischen Signallaufzeit und Netzwerk-Dimensionen.....	182
Abbildung 177: Mindestpaketgröße um Kollisionen zu erkennen.....	183
Abbildung 178: Kanalzugriff.....	185
Abbildung 179: Frei-Token.....	187
Abbildung 180: Token-Ring: Teilnehmer.....	187
Abbildung 181: Unbeteiligte Stationen leiten die Daten weiter.....	187
Abbildung 182: Empfänger kopiert die Daten und ändert Token.....	187
Abbildung 183: Daten werden auf dem Ring weiter geleitet.....	187
Abbildung 184: Lese-Information wird zum Sender weiter geleitet.....	188
Abbildung 185: Nach erfolgreicher Übertragung erzeugt der Sender ein freies Token.....	188
Abbildung 186: Topologiformen.....	190
Abbildung 187: Physikalische und logische Topologie.....	192
Abbildung 188: Ring-Topologie mit äußerer Stern-Struktur.....	194
Abbildung 189: Symmetrische Leitungen.....	196
Abbildung 190: Unsymmetrische Leitungen.....	197
Abbildung 191: Yellow-Cable.....	198
Abbildung 192 – Cheapernet-Kabel.....	199
Abbildung 193 – Twin-Koaxial-Leitung.....	200
Abbildung 194: Symmetrische-Twin-Koax-Leitung.....	200
Abbildung 195: Sternvierer.....	201
Abbildung 196: Twisted-Pair-Leitung.....	201
Abbildung 197: UTP-Kabel.....	202
Abbildung 198: STP-Kabel.....	202
Abbildung 199: PiMF.....	202
Abbildung 200: SSTP/SFTP-Kabel.....	203
Abbildung 201 - Lichtbrechung.....	209
Abbildung 202 – Dämpfungsverlauf bei verschiedenen Wellenlängen.....	210
Abbildung 203 – Refexion der Lichtstrahlen in Glasfaser.....	211
Abbildung 204 – Multimode-Faser.....	212
Abbildung 205 – Brechungsindex-Verlauf bei Multimodefaser.....	212
Abbildung 206 – Gradianten-Faser.....	213
Abbildung 207 – Brechungsindex-Verlauf bei Multimodefaser.....	213
Abbildung 208 – Monomode-Faser.....	214
Abbildung 209 – Brechungsindex-Verlauf bei Monomode-Faser.....	214
Abbildung 210: Einstrahlverhalten.....	215
Abbildung 211: Übersicht Einzelfasern.....	216
Abbildung 212: Glasfaser-Zugofen.....	220
Abbildung 213: Spleissvorgang.....	221
Abbildung 214: Spleissbox.....	221
Abbildung 215: Single-Strand-Verbindung.....	224
Abbildung 216: Bauformen: PC/SPC/UPC - APC.....	227
Abbildung 217: Pigtail.....	230
Abbildung 218: LWL SC-SC-Patchleitung.....	230
Abbildung 219: Ältestes noch erhaltenes Bild von Ethernet.....	232
Abbildung 220: Aufbau eines Pakets mit 10 Mbps auf Ebene 1.....	233
Abbildung 221: Manchester-Kodierung.....	233
Abbildung 222: 10 Mbps Coaxialkabel-Varianten.....	234

Abbildungsverzeichnis

Abbildung 223: 10Base5.....	235
Abbildung 224: 10Base2.....	236
Abbildung 225: Eliminierung von Störungen durch Verdrillung.....	237
Abbildung 226: Link Integrity Test (LIT) / Normal Link Pulse (NLP).....	237
Abbildung 227: Pin-Numerierung einer RJ45-Buchse.....	238
Abbildung 228: Crossover-Verbindung.....	238
Abbildung 229: Straight-Through-Verbindung.....	238
Abbildung 230: Ausdehnung von 10Base-T mittels FOIRL.....	240
Abbildung 231: Einführung neuer Sublayer für 100 Mbps.....	242
Abbildung 232: Umwandlung von Bytes in Nibbles.....	242
Abbildung 233: MII-D-Subminiatur-Stecker.....	243
Abbildung 234: Übergang von der Manchester-Codierung zu MLT-3.....	244
Abbildung 235: 100 Mbps-Ethernet-Paket.....	246
Abbildung 236: NLP und FLP mit dem Basic Link Codewort.....	247
Abbildung 237: Pause-Frame.....	250
Abbildung 238: Extension-Frame und Burst-Limit.....	254
Abbildung 239: GMII-Einführung.....	256
Abbildung 240: Nutzung von allen 4 Adernpaaren in beiden Richtungen bei Gigabit-Ethernet.....	259
Abbildung 241: Bausteine der 1000Base-T-PHY.....	260
Abbildung 242: Beeinflussung des Signals durch die Leitungsdämpfung.....	261
Abbildung 243: Erhöhung des Abstandes durch gerade und ungerade Symbole.....	262
Abbildung 244: Zuordnung von Y auf gerade und X auf ungerade Symbole.....	262
Abbildung 245: Um 45 ° gedreht und in normale und inverse Symbole unterteilt.....	263
Abbildung 246: Trellis-Diagramm.....	266
Abbildung 247: Trellis-Diagramm von 1000Base-T.....	266
Abbildung 248: Brückenschaltung mit Hybridfunktion für ein Adernpaar.....	267
Abbildung 249: Sublayer bei 10 Gigabit-Ethernet.....	271
Abbildung 250: WWDM-Verfahren bei 10GBase-LX4.....	274
Abbildung 251: STH-Rahmen mit STM-1-Struktur.....	276
Abbildung 252: 10Gigabit-Ethernet Payload Envelope mit Path Overhead innerhalb eines STM.....	277
Abbildung 253: 4X-Buchsen (wie sie auch bei InfiniBand verwendet werden (Quelle: Wikipedia)).....	279
Abbildung 254: 4X-Stecker (Quelle: DELL).....	279
Abbildung 255: DSP-Funktionen bei 10GBase-T.....	280
Abbildung 256: 2D-DSQ-128 Symbole.....	281
Abbildung 257: Auswahl eines Signalraumpunktes bei DSQ128.....	282
Abbildung 258: Bildung der LDPC-Frames.....	283
Abbildung 259: Sublayer der 40/100 Gigabit Lösungen.....	288
Abbildung 260: Mini Multilane 10 Gbps 12X.....	289
Abbildung 261: MPO-Stecker (Quelle: Lindy).....	290
Abbildung 262: MPO-Stecker-Optionen für 100GBase-SR10.....	290
Abbildung 263: Timeline der Ethernet-Entwicklungen.....	293
Abbildung 264 – Barrel-Stecker (N-Stecker).....	299
Abbildung 265 – SUB-D-Stecker/Buchse.....	300
Abbildung 266 - RJ11-Stecker.....	301
Abbildung 267 – RJ12-Stecker.....	302
Abbildung 268 – RJ45-Stecker.....	302
Abbildung 269: GG45 (Quelle KSI).....	306
Abbildung 270: GG45 im CAT 5 und 6-Modus (Quelle: LANmark).....	306
Abbildung 271: GG45 im CAT7 Modus (Quelle: LANmark).....	306
Abbildung 272: TERA-Stecker (Quelle Fa. Siemon).....	307
Abbildung 273 – RJ21-Stecker (TELCO-Stecker).....	308
Abbildung 274 – IBM-Typ-I-Stecker für IVS.....	308
Abbildung 275: Strukturierte Verkabelung.....	311
Abbildung 276: Hierarchische Verkabelungsstruktur.....	314
Abbildung 277 – Backbone.....	315
Abbildung 278: PoE-Endspan-Phantomspeisung.....	319
Abbildung 279: PoE-Endspan-Spare-Pairs.....	320

Abbildung 280: PoE-Midspan.....	321
Abbildung 281: SDH.....	325
Abbildung 282SDH-Rahmen.....	326
Abbildung 283: DQDB.....	327
Abbildung 284: Paketvermittelnde Datennetze.....	328
Abbildung 285: Frame Relay Netz-Aufbau.....	329
Abbildung 286: ISDN-Schnittstellen.....	331
Abbildung 287: S0-Bus-Aufbau.....	332
Abbildung 288: So-Bus (kurz).....	333
Abbildung 289: S0-Bus (erweitert).....	334
Abbildung 290: S0-Bus (Punkt zu Punkt).....	335
Abbildung 291: interner / externer S ₀ -Bus.....	336
Abbildung 292: S0-Rahmenaufbau.....	337
Abbildung 293: Modifizierter AMI-Code.....	337
Abbildung 294: S2M-Rahmen.....	339
Abbildung 295: DSL-Frequenzbereiche.....	342
Abbildung 296ADSL-Aufbau.....	343
Abbildung 297: MPLS-Tag.....	345
Abbildung 298: MPLS-Domäne.....	346
Abbildung 299: Paketweiterleitung unter MPLS.....	347
Abbildung 300: MPLS-Dienste.....	348
Abbildung 301: MPLS-Übersicht.....	348
Abbildung 302 : Störung im Repeater-Netz.....	352
Abbildung 303: Local- und Remote-Repeater.....	353
Abbildung 304 : Repeater im ISO-RM.....	354
Abbildung 305 : Rahmen-Bearbeitung in Brücken.....	356
Abbildung 306 : Brücken im Netzwerk.....	358
Abbildung 307 : Brücken im ISO-RM.....	359
Abbildung 308 : Brücken-Schleifen.....	360
Abbildung 309 : Spanning-Tree-Ablauf 1.....	363
Abbildung 310 : Spanning-Tree-Ablauf 2.....	364
Abbildung 311 : Spanning-Tree-Ablauf 3.....	366
Abbildung 312 : Spanning-Tree-Ablauf 4.....	367
Abbildung 313 : Spanning-Tree-Ablauf 5.....	368
Abbildung 314: Spanning-Tree-Ablauf 6.....	369
Abbildung 315 : Spanning-Tree-Ablauf 7.....	370
Abbildung 316 : Spanning-Tree – Port-Zustände.....	371
Abbildung 317 : RSTP-Root-Ermittlung.....	372
Abbildung 318 : RSTP-Designated-Bridge-Ermittlung.....	373
Abbildung 319 : RSTP Root- / Designated- / Edge-Port.....	374
Abbildung 320 : IEEE-802.1w.....	376
Abbildung 321 : RSTP Rapid Transition.....	377
Abbildung 322 : RSTP Request und Reply.....	378
Abbildung 323 : RSTP Verarbeitung der TCN-Meldungen.....	380
Abbildung 324 : Layer-2-Switch im Netzwerk.....	383
Abbildung 325 : Layer-2-Switch im ISO-RM.....	383
Abbildung 326 : Layer-3-Switch im Netzwerk.....	384
Abbildung 327 : Layer-3-Switch im ISO-RM.....	385
Abbildung 328 : Layer-4-Switching.....	386
Abbildung 329: 1 zu 1 - Verbindungen bei Switches.....	387
Abbildung 330: Klassische 3stufige Hierarchie.....	387
Abbildung 331: Leaf-Spine-Architektur.....	388
Abbildung 332 : Router verbinden Netzwerke.....	391
Abbildung 333 : Router-Anschlussmöglichkeiten.....	392
Abbildung 334 : Router im ISO-RM.....	393
Abbildung 335 : Routing-Beispiel.....	396
Abbildung 336 : Ein Gateway verbindet Netze unterschiedlicher Protokolle.....	399

Abbildungsverzeichnis

Abbildung 337 : Gateway im ISO-RM.....	400
Abbildung 338 : Collision/Broadcast-Domain.....	401
Abbildung 339 : Leitungsvermittlung.....	403
Abbildung 340 : Speichervermittlung.....	404
Abbildung 341 : Signalisierung.....	405
Abbildung 342 : Flusskontrolle.....	406
Abbildung 343 : Übertragungswiederholung.....	407
Abbildung 344 : Stop and Wait.....	408
Abbildung 345 : Fenstertechnik.....	409
Abbildung 346 : Zusammenfassung von Quittungen.....	410
Abbildung 347 : Go back n.....	411
Abbildung 348 : Selective Repeat.....	412
Abbildung 349: Transfermodi.....	413
Abbildung 350: Kommunikationsprinzipien.....	414
Abbildung 351 : Protokoll-Übersicht.....	415
Abbildung 352 : Aufbau eines Rahmens auf der Leitung.....	416
Abbildung 353 : Ethernet-Formate.....	417
Abbildung 354 : Aufbau-LLC-Frame.....	420
Abbildung 355 : Unterschiede-RFC894/RFC1042.....	422
Abbildung 356 : Protokoll_Abhängigkeiten.....	423
Abbildung 357 : FDDI-Ring.....	425
Abbildung 358: Beispiel: CIDR Teil-1.....	432
Abbildung 359: Beispiel: CIDR Teil-2.....	433
Abbildung 360 : Beispiel für Subnetting.....	435
Abbildung 361 : Beispiel für Subnetting 2.....	437
Abbildung 362: IP-Adress-Vergabe.....	439
Abbildung 363: Einfachere Darstellung eines IP-Netzwerks mitsamt den Teilnehmern.....	440
Abbildung 364 : Umsetzung der Multicast-ID in IP-Adresse.....	447
Abbildung 365 : Network-Address-Translation.....	452
Abbildung 366 : Umsetzung der IP-Adressen bei NAT.....	453
Abbildung 367 : SIP_Trapez.....	455
Abbildung 368 : NAT Full Cone.....	456
Abbildung 369 : NAT Restricted Cone.....	457
Abbildung 370 : NAT Port Restricted Cone.....	458
Abbildung 371 : NAT Symmetric Cone.....	459
Abbildung 372 : NAT TURN.....	462
Abbildung 373 : ARP-Datenaufbau.....	463
Abbildung 374 : ARP-Ablauf.....	464
Abbildung 375 : RARP-Ablauf.....	465
Abbildung 376 : PROXY-ARP.....	466
Abbildung 377 : UNARP.....	467
Abbildung 378 : DHCP unter WINDOWS.....	469
Abbildung 379 : DHCP-Zustände.....	471
Abbildung 380 : ICMP-Timestamp.....	480
Abbildung 381 : Generische Top-Level-Domains (gTLDs).....	484
Abbildung 382: DNS-Auflösung: Iterativ vs. Rekursiv.....	486
Abbildung 383 : DNS-Namensauflösung.....	487
Abbildung 384 : DDNS.....	493
Abbildung 385 : Letzte IPv4-Adressen.....	494
Abbildung 386 : Scope.....	498
Abbildung 387 : MAC- EUI-64 Konvertierung.....	501
Abbildung 388 : Kommunikationstypen.....	502
Abbildung 389: Format der Subnet-Router-Anycast-Adresse.....	502
Abbildung 390: Format von Anycast-Adressen.....	503
Abbildung 391 : Dual Layer - Dual Stack.....	515
Abbildung 392 : Verbindmöglichkeiten bei Dual-Stack-Technik.....	515
Abbildung 393 : Tunnelverfahren.....	516

Abbildung 394 : ISATAP-Tunnelaufbau.....	517
Abbildung 395 : Translation-Technik.....	517
Abbildung 396 : Teredo.....	518
Abbildung 397 : 6 to 4.....	518
Abbildung 398: VRRP: Wirkungsbereich.....	521
Abbildung 399: IP-Adress Owner.....	523
Abbildung 400: VRRP: Anwendung der Priorität.....	524
Abbildung 401: VRRP: Verwendung einer zusätzlichen VIP.....	526
Abbildung 402: HSRP / VRRP.....	528
Abbildung 403: VRRP: Anwendungsbeispiel-1.....	531
Abbildung 404: VRRP: Anwendungsbeispiel-2.....	532
Abbildung 405: VRRP: Anwendungsbeispiel-3.....	533
Abbildung 406 : IP-Adress-Lifetime.....	538
Abbildung 407 : DHCPv6-Ablauf.....	539
Abbildung 408 : Microsegmentierung.....	540
Abbildung 409 : VLANs.....	541
Abbildung 410: Unterschied zwischen portbasierten und tagged VLANs.....	542
Abbildung 411: VLAN-Bearbeitung am Accessport.....	543
Abbildung 412 : Dynamische VLANs.....	545
Abbildung 413 : Übergang vom LAN zum VLAN.....	546
Abbildung 414 : Ausgangszustand.....	547
Abbildung 415 : Zuordnung der Geräte zu 2 IP-Netzwerken.....	547
Abbildung 416 : Auftrennung in VLANs.....	548
Abbildung 417 : Routing zwischen den VLANs.....	548
Abbildung 418 : TCP-Verbindungsstati.....	562
Abbildung 419 : TCP-Open/Close.....	563
Abbildung 420 : TCP-Half-Close.....	566
Abbildung 421 : TCP simultaneous open.....	568
Abbildung 422 : TCP simultaneous close.....	569
Abbildung 423 : TCP Sliding Window.....	571
Abbildung 424 : TCP-Datenübertragungsbeispiel.....	572
Abbildung 425 : TCP Urgent-Mode.....	575
Abbildung 426: TCP-Slow-Start.....	576
Abbildung 427 : RIP - Routing Updates.....	582
Abbildung 428 : Wegfall einer Route.....	583
Abbildung 429 : OSPF Areas.....	586
Abbildung 430 : Verbindung autonomer Systeme bei OSPF.....	588
Abbildung 431 : OSPF-Topologie-1.....	589
Abbildung 432 : OSPF 2.....	590
Abbildung 433 : OSPF 3.....	592
Abbildung 434 : IGMP-Datenaustausch.....	599
Abbildung 435: Link Aggregation.....	601
Abbildung 436: Einfügen der LAC.....	604
Abbildung 437 : Eine Firewall trennt Rechnernetze.....	606
Abbildung 438 : Dual-Homed Firewall.....	607
Abbildung 439 : Screened-Host Firewall.....	608
Abbildung 440 : Screened-Subnet Firewall.....	609
Abbildung 441 : Zuordnung von Paketfiltern zu ISO-RM-Ebenen.....	610
Abbildung 442 : Proxy-Firewall.....	611
Abbildung 443 : Accesslisten-Bearbeitung.....	614
Abbildung 444 : Zugriffslisten-Bearbeitung.....	615
Abbildung 445 : Erweiterte Zugriffslisten-Bearbeitung.....	617
Abbildung 446 : SNMP-Agent.....	621
Abbildung 447 : PROXY-Agent.....	622
Abbildung 448 : MIB-Aufbau Teil 1.....	623
Abbildung 449 : MIB-Aufbau Teil 2.....	624
Abbildung 450 : CISCO-View-Beispiel.....	633

Abbildungsverzeichnis

Abbildung 451 : Applikationen -TCP UDP - IP.....	635
Abbildung 452 : MAIL - Anfänge.....	637
Abbildung 453 : SMTP.....	638
Abbildung 454 : IMAP4-Session-Zustände.....	646
Abbildung 455 : HTTP.....	648
Abbildung 456 : Pipelining.....	648
Abbildung 457 : HTTP-Zugriffsmöglichkeiten.....	649
Abbildung 458 : FTP.....	650
Abbildung 459 : FTP-Portzuweisung.....	652
Abbildung 460 : Telnet.....	653
Abbildung 461 : VoIP - Übersicht.....	656
Abbildung 462 : SIP-Protokollstack.....	660
Abbildung 463 : SIP direkte Verbindung.....	661
Abbildung 464 : SIP-Redirect-Mode.....	662
Abbildung 465 : SIP-Proxy-Mode.....	662
Abbildung 466 : SIP-Trapez.....	663
Abbildung 467 : De-Jitter-Buffer.....	665
Abbildung 468 : Qualitätsanforderung von VoIP.....	665
Abbildung 469 : Kopplung von Telefonanlage und VoIP.....	666

45 - Stichwortverzeichnis

Stichwortverzeichnis

1 Gbps.....	55	Adressbuch.....	360
1-persistent CSMA.....	179	Adressbuchverwaltung.....	360
10 Gbps.....	55	Adressierung.....	56, 427, 442
10 Mbps.....	55, 317	ADSL.....	340f.
100 Mbps.....	55	Aging-Mechanismus.....	360, 395
1000 Mbps.....	317	Aktionen.....	15
1000Base-CX.....	206	ALG.....	461
1000Base-LX.....	206	Aliasing-Effekt.....	67
1000Base-SX.....	206	Alien Crosstalk.....	168
1000Base-T.....	206, 302f.	All-Hosts-Group.....	600
1000Base-TX.....	8	All-Hosts-Group-ID.....	600
100Base-Fx.....	205	AllSPFRouters.....	593
100Base-Sx.....	205	Alphabet.....	91
100Base-T.....	303	Alternate Port.....	375
100Base-T2.....	8, 205	AMI-NRZ.....	116
100Base-T4.....	205, 303	AMI-RZ.....	116
100Base-Tx.....	302	Amplitude.....	123
100Mbps.....	425	Amplitude Shift Keying.....	123
100VGAnyLAN.....	8, 303	Amplitudenmodulation.....	123
10Base-F.....	204	Amplitudenumtastung.....	123
10Base-T.....	204, 302f.	Analoges Signal.....	72f.
10Base2.....	199, 204	Anforderungen an eine Datenübertragung.....	92
10Base5.....	198, 204, 300	Anhang.....	669
10Broad36.....	204	Anpassung.....	147
10GBase-T.....	206, 303	Anschlussdosen.....	333f.
16-QAM.....	132	ANSI.....	2
2-Draht.....	87	Antworten.....	421
2MSL Timer.....	579	Anwendungs-Ebene.....	65
4-Draht.....	87	Anwendungsebene.....	64
4PSK.....	133	Any-to-Any-Kommunikation.....	455
a/b-Wandler.....	331, 336	Anycast.....	24
Abgetastetes Signal.....	72f.	API.....	556
Ableitung.....	141	APIPA.....	474
Ableitungsbelag.....	141	Apple Talk.....	394
abortive release.....	567	Application Layer Gateway.....	461
Abschlusswiderstand.....	146, 165, 334	Application-Layer.....	65
Abtastfrequenz.....	66	Applikation.....	635f.
Abtastintervall.....	70	ARP.....	422
Abtastrate.....	72f.	ARP-Request.....	474
Abtasttheorem.....	67	Reply.....	466
Abtastung.....	66, 73	Request.....	463, 466
Abtastwert.....	81	Response.....	463
AC0.....	421	ARP-Reply.....	528
AC1.....	421	ARP-Request.....	528
Access-Modus.....	543	ARQ.....	407
ACK.....	186, 408, 570, 576	AS.....	586
Acknowledge.....	408	ASCII.....	65
ACR.....	157	ASIC.....	382
Active Close.....	579	ASK.....	123
Adaptive Deltamodulation.....	138	Asynchrone Datenübertragung.....	90
Adjacency.....	594f.	Asynchroner Transfer-Mode.....	413
ADM.....	138	ATM.....	195, 229, 327f.
Administration.....	549	ATMDirector.....	634

Stichwortverzeichnis

attenuation.....	155	Bridges.....	356
AU.....	327	British Standard.....	6
Augenmuster.....	120	Broadband.....	8
AUI.....	55	Broadcast. 24, 26f., 356f., 360, 429, 442, 444, 541, 549, Schnittstelle.....	580
AUI-Stecker.....	300	Adresse.....	439
Ausbreitungsgeschwindigkeit.....	148, 209	All Subnets Directed.....	445
Ausbreitungskonstante.....	143f., 148	Limited.....	445
Auto Partitioning.....	354	Net Directed.....	445
Automatic Private IP Addressing.....	474	Subnet Directed.....	445
Automatic Repeat Request.....	407	Broadcast-Domain.....	401, 541
Autonomes System.....	586	Broadcast-Netzwerken.....	26
B-ISDN.....	325	Broadcastdomain.....	401, 540, 544
B2B.....	20	Brücken.....	356
B2C.....	20	Brücken-ID.....	361
Backbone.....	315	Brücken-Port.....	361
Backbone-Netze.....	425	Brückenschaltung.....	87
Backoff Time.....	185	BS.....	6
Backoff-Timer.....	186	Bündelader-Kabel.....	217
Backup Port.....	375	Bündelfaserkabel.....	217
Backup-Router.....	593	Bündelung.....	339
BAKT.....	331	Business-to Consumer.....	20
Balun.....	197	Business-to-Business.....	20
BAN.....	29	Byte.....	92
Bandbreite.....	81, 85, 92, 540	C.....	141
Barrel-Stecker.....	299	C'.....	141
Baud.....	70	C2C.....	20
Baud-Rate.....	92	Cache-Server.....	649
Bezeichnungscodes.....	218f.	Campusnetzwerk.....	28
Bezugserde.....	196	Carrier Sense.....	232
BGP.....	394, 586	Carrier Sense Multiple Access.....	179
Bi-Phase.....	112	CAT.....	171
Biphase-Codierung.....	115	CAT3.....	171
Biphase-L.....	115	CAT4.....	171
Biphase-M.....	115	CAT5.....	171
Biphase-S.....	115	CAT6.....	171
BISDN-RM.....	45	CAT6a.....	171
Bit.....	92, 133	CAT6e.....	171
Bit-Übertragungsrate.....	92	CAT7.....	171
Bitfehler.....	407	CAT8.....	171
Bitfehlerrate.....	118, 154, 331	Category.....	171
Bitmuster.....	416	CBDS.....	327
Bitstrom.....	89	CCITT.....	2, 328
Bitübertragungs-Schicht.....	55	ccTLD.....	4
BLC.....	247	CDDI.....	425
Blocking Mode.....	375	Channel-Link.....	150
BNC-Stecker.....	298	Cheapernet-Cable.....	199
Bonding.....	339	Checksum.....	449
BOOTP.....	468	CIR.....	329
Bootstrap Protocol Client.....	636	CISC.....	357
Bootstrap Protocol Server.....	636	CiscoView.....	633
Border Gateway Protocol.....	586	Client-Prozess.....	19
BPDU.....	361, 375	Client-Server-Modell.....	18f.
BR.....	593	CMIP.....	620
Breakout-Kabel.....	217	Code.....	92
Brechungsindex.....	213	Codierung.....	97
Brechzahl.....	209	Collapsed Backbone.....	315

Collision Avoidance.....	185	Deadlock.....	578
Collision Detection.....	232	Decoder.....	89
Collision Free.....	207	DEE.....	2, 21
Collision Window.....	183	Default Route.....	396
Collision-Domain.....	401	Default-Gateway.....	395f., 474
Collisiondomain.....	401, 540	Default-VLAN.....	544
Community-String.....	625	Default-Wert.....	373
Configuration-BPDU.....	361	Dekompression.....	65
Confirm.....	49f.	Deltamodulation.....	138
Consumer-to-Consumer.....	20	Demodulation.....	85, 121
Contention Window.....	185	Demultiplexer.....	324
Control.....	418	Deprecated-Lifetime.....	538
Corporate Network.....	28	Descrambling.....	89
Country Code TLD.....	4	Designated Bridge.....	373
CRC.....	426, 428	Designated Port.....	374f.
Error.....	382	Designated Router.....	593
CRC-Generatorpolynome.....	110	Designierte Brücke.....	362
CSMA.....	179	Designierter Port.....	362
CSMA/CA.....	185	Destination.....	449
CSMA/CD.....	8, 56, 181, 207, 232, 381	Destination unreachable.....	395
Cut-Through.....	382	Destination-Service-Access-Point.....	418
Cut-Through (Collision-Free).....	382	DHCP.....	440, 469, 474
CW.....	185	ACK.....	470f.
CWND.....	576	Client.....	470f.
D-Kanal.....	330, 338	Discover.....	471
DAD.....	538	NAK.....	471
Dämpfung.....	149, 155, 157, 352	Offer.....	471
Dämpfungskonstante.....	148	Relay-Agent.....	469
Dämpfungsverlauf.....	210	Release.....	471
Dämpfungswert.....	221	Request.....	470f.
DARPA.....	45	Server.....	470f.
DARPA-Modell.....	415	Zustände.....	471
Darstellungs-Schicht.....	65	DHCP-Reply-Nachricht.....	539
Data Communication Equipment.....	21	DHCP-Request.....	474
Data Terminating Equipment.....	21	DHCP-Request-Nachricht.....	539
Data-Link-Layer.....	56	DHCP-Server.....	474
Database-Description-Pakete.....	594	DHCPv6.....	538
Datagramme.....	32	Dialog-Kontrolle.....	65
Datagramme,.....	427	Dibit.....	132
Daten.....	15, 18	Dienst.....	52
Daten Übertragungseinheit.....	21	Dienste-Primitive.....	48
Daten-Endeinrichtung.....	21	Differential Manchester.....	116
Datendurchsatz.....	177	Differenz Puls Code Modulation.....	138
Datenkanäle.....	330	Differenz-Pulsecode-Modulation.....	138
Datenquelle.....	21	DIFS.....	185f.
Datensenke.....	21	Digitalsignalmultiplexer.....	324
Datenstation.....	22	DIN.....	2
Datenübertragung.....	18	DIN EN 50090.....	312
Datenübertragungsfehler.....	51	DIN EN 50173.....	312
Datenübertragungsrate.....	317	DISC.....	421
Datenverbund.....	30	Discarding Mode.....	375
Daytime.....	636	Dispersion.....	211, 213
DBP.....	5	DIX.....	418
DC Loop Resistance.....	167	DIX-Gruppe.....	233
DCE.....	21, 328	DLSAP.....	419
DCF Inter Frame Spacing.....	185	DM.....	138, 421
DD.....	597	DNS.....	4, 65, 440, 483

Stichwortverzeichnis

Autoritative Server.....	485	EN 50173.....	6, 309, 311
Country-Code.....	484	EN 50173-1.....	309, 311
Domain-Namensraum.....	483	EN 50173-1:2002.....	312
FQDN.....	484	EN 50173-2.....	312
Fully Qualified Domain Name.....	484	EN 50173-3.....	312
lookup.....	483	EN 50173-4.....	312
Nameserver.....	483	EN 50173-5.....	312
Network Information Center.....	484	EN 50174.....	309
NIC.....	484	EN 50174-1.....	309
Nicht autoritative Server.....	485	EN 50174-2.....	309
Resolver.....	483	EN 50174-3.....	309
Resource Records.....	488	EN 50310.....	309
Resource Records Format.....	488	EN 50346.....	309
Resource Records Typen.....	489	Endgerät.....	319
reverse lookup.....	483	Endgeräte.....	333f.
TLD.....	484	Endspan-Versorgung.....	319f.
Top-Level-Domain.....	484	Entity.....	47
Zone.....	484	Entropie.....	93, 97
DoD-RM.....	45	Entscheidungsgehalt.....	94
Domain Name Service.....	483, 636	Entscheidungsinhalt.....	93
DPCM.....	138	Entschlüsselung.....	65
DQDB.....	8, 327	Erde.....	196
DR.....	593	Ersatzschaltbild.....	141f.
Dreistufige Leitungscodierung.....	112	Erweiterter Passiver Bus.....	334
DSAP.....	418	ESCON-Stecker.....	229
DSL-Modem.....	22	Etagenverkabelung.....	313
DTE.....	21, 328	Ethernet.....	195, 540
DÜE.....	2, 21	Disparity.....	257
duplex.....	87	IEEE-802.3u.....	242
Duplexkabel.....	217	IEEE-802.3x.....	250
Duplicate Address Detection.....	538	Jam-Signal.....	182
Durchschnittlicher mittlerer Informationsgehalt.....	93	Media Independent Interface.....	242
Dynamische Routing-Einträge.....	395	NLP.....	237, 247
Dynamisches Adressbuch.....	360	Normal Link Pulse.....	237
Dynamisches DNS.....	461	Reconciliation-Layer.....	242
E-Bits.....	338	Ethernet II.....	422
E-Commerce.....	18, 20	Ethernet V2.....	418
E-Mail-Adresse.....	639	Exponential Backoff.....	185
E2000 Stecker.....	228	Extended RIP.....	580
Eastbound.....	556	Extended Unique Identifier.....	538
EBCDIC.....	65	Externer und interner SO-Bus.....	336
Echo.....	636	Fano Bedingung.....	98
Echokanal.....	338	FAQ's.....	12
Echounterdrückung.....	342	Far End Crosstalk.....	152
ECMA.....	5	Faserbrüche.....	222
Edge Port.....	375	FC-Stecker.....	228
Egress-Router.....	347	FDDI.....	195, 229, 315, 381, 425
EIA.....	6	Fehler-Erkennung und -Korrektur.....	406
EIA / TIA.....	6	Fehlerarten.....	406
EIA/TIA 568A.....	170	Fehlerbehandlung.....	406
EIA/TIA 568B.....	170	Fenster-Größe.....	578
EIGRP.....	394	Fenstergröße.....	410
Einleitung.....	351	Fern-Nebensprechen.....	152
elektrisches Feld.....	140	FEXT.....	152, 159, 203
ELFEXT.....	161	Fiber Connector.....	228
Empfangs-Folgenummer.....	420	file.....	649
EN.....	7	File Transfer Protocol.....	650

Filetransfer Protocol.....	636	Full Duplex.....	207
Filter.....	358	Full-Duplex.....	65, 181
Final ACK.....	579	Full-Duplex-Betrieb.....	169
Firewall.....	652	Fundamentalfrequenz.....	112, 116
Flags.....	449	Fünfstufige Leitungscodes.....	112
FLP.....	247	Funk.....	55
Flusskontrolle.....	65, 406, 578	Funktionsverbund.....	30
FO.....	5	FYI.....	12
Forwarder.....	556	G.....	141
Forwarding Mode.....	375	G.711.....	2
Fragment Offset.....	449	G'.....	141
Fragmentation.....	62	G2C.....	20
Fragmentierung.....	427	Gabelschaltung.....	87
Frame Relay.....	344	GAN.....	29
Frame-Formate.....	420	Gateway Load Balancing Protocol.....	521
Frame-Relay.....	329	Gateways.....	399
Frequency Shift Keying.....	123	Gebäudeverkabelung.....	313
Frequenz.....	33, 123, 155	Geflechtschirm.....	202f.
Frequenz-Multiplex.....	84, 342	Generic Top Level Domains.....	4
Frequenzmodulation.....	123	geroutete Protokolle.....	62
Frequenzumtastung.....	123	Geschwindigkeit.....	92
Frequenzzuteilung.....	35	Get-Community-String.....	625
FRMR.....	421	GLBP.....	521
FSK.....	123	Gleichstrom-Anteil.....	85
FSMA-Stecker.....	227	Gleichstrom-Schleifenwiderstand.....	167
ftp.....	649	Globale Signifikanz.....	51
FTP.....	65, 650	GMII.....	55
anonymous.....	650	Go back n.....	411
append.....	651	Go back N.....	407
ascii.....	651	Goverment-to-Consumer.....	20
bell.....	651	Gradienten-Faser.....	212f.
binary.....	651	Graphenbaum.....	592
bye.....	651	Group-Switch-Modul.....	355
cd.....	651	Gruppen-Adresse.....	599
connect.....	651	Gruppen-Zugehörigkeit.....	600
delete.....	651	H.323.....	2
dir.....	651	Halbduplex-Betrieb.....	25
get.....	651	Half Duplex.....	207
lcd.....	651	Half-Duplex.....	65, 181
ls.....	651	Hallo-Paket.....	361
mdelete.....	651	HDB3.....	116
mget.....	651	HDSL.....	340f.
mput.....	651	HDTDR.....	165
open.....	651	HDTDX.....	166
passive.....	651	HDTDX-Messung.....	169
port.....	651	Header.....	64
proxy.....	651	Header Checksum.....	428
put.....	651	Heimnetzwerk.....	28
pwd.....	651	HELLO-Pakete.....	593
quit.....	651	HELLO-Protocol.....	595
rename.....	651	Herstellung.....	220
rmdir.....	651	Hochlauf.....	580
status.....	651	Hochverfügbare Systeme.....	17
Steuerverbindung.....	650	Host.....	598f.
user.....	651	Host Name Server.....	636
verbose.....	651	host unreachable.....	577
Full Cone.....	456	Host-Adressen.....	436

Stichwortverzeichnis

Host-Route-Eintrag.....	395	Informationstechnik.....	13
Hot Standby Router Protocol.....	521	Infrarotübertragung.....	36
HSRP.....	394, 521	Innenwiderstand.....	317
HTML-Seite.....	648	Installationshinweise.....	439
http.....	649	Instanz.....	47, 52
HTTP.....	648	Integrated Services Digital Network.....	330
Hub.....	355, 540	Integrität.....	92
Huffmann-Codierung.....	100	Inter Frame Gap.....	183
Hyper Text Transfer Protocol.....	648	Inter Packet Gap.....	183
I-Frames.....	420	Interface.....	599
I.430.....	2	Interior Gateway Protocol.....	586
I.431.....	2	Internet Control Message Protocol.....	428, 635
IAB.....	3, 9	Internet Group Managing Protocol.....	598
IANA.....	3, 447	Internet Message Access Protocol.....	646
IBM.....	229	Internet Service Provider.....	28
IBM Data-Connector.....	424	Internet-Gremien.....	3
IBM-Typ-1-Kabel.....	424	Intervall.....	178
IBM-Verkabelungssystem.....	424	IP.....	62, 394
ICANN.....	4	Adress-Klassen.....	429
ICI.....	45	Adresse.....	439
ICMP.....	395, 428, 475, 635	CIDR.....	430
ICMPv6.....	534	Classless-inter-Domain-Routing.....	430
ID.....	449	Default Gateway-IP-Adresse.....	439
IDC.....	424	Experimentelle Adressen.....	429
IEC.....	5	Flusskontrolle.....	428
IEEE.....	8	Header Checksum.....	428
IEEE-802.....	8	Host.....	439
IEEE-802.10.....	546	Host-Teil.....	429
IEEE-802.16.....	327	IPv4-Adresse.....	429
IEEE-802.1q.....	543, 546	Multicasts.....	429
IEEE-802.1t.....	372	Netzwerk-Teil.....	429
IEEE-802.2.....	419	IP.....	427
IEEE-802.3.....	233, 418, 422	IP-Adresse.....	63, 585
IEEE-802.3af.....	317	IP-Host-Adresse.....	63
IEEE-802.3u.....	242	IP-Netzwerk-Adresse.....	63, 593
IESG.....	3	IP-Protokoll.....	32
IETF.....	461, 586	IP-Protokoll.....	63
IFG.....	183	IP-Protokoll-Feld.....	598
IGMP.....	598	IP-Telefone.....	317
IGMP-Meldungen.....	598	ipconfig /all.....	474
IGMP-Query.....	600	IPG.....	183
IGMP-Report.....	600	IPSec.....	454
IGP.....	586	IPX.....	62, 394
IGRP.....	62, 394	IPX/SPX.....	418
IHL.....	448	ISDN.....	330
IMAP4.....	646	ISDN-Dienste.....	330
Indication.....	49	ISDN-Schnittstellen.....	331
Induktion.....	149	ISDN-Telefon.....	336
Induktivität.....	141	ISL.....	546
Induktivitätsbelag.....	141	ISM-Bänder.....	35
Information.....	93	ISO.....	2, 7
Informationen.....	15, 600	7-Schicht-Modell.....	427
Informationsgehalt.....	93	Brücke im ISO-RM.....	359
Informationskanal.....	21	RM.....	356
Informationsmenge (I).....	82	ISO-8802.....	8
Informationsquelle.....	21, 96	ISO-Referenzmodell.....	415
Informationssysteme.....	14	ISO-RM.....	45

ISO/IEC 11801.....	311	LC-Stecker.....	228
ISOC.....	3	Learning Mode.....	375
ISP.....	28	Least Significant Bit.....	417
IT.....	13	LED.....	215
ITU.....	2	LEDs.....	210
ITU-D.....	2	Leerlauf.....	147
ITU-R.....	2	Leistung.....	317
ITU-T.....	2, 328	Leistungsklassen.....	322
IVM.....	424	Leistungsverbund.....	30
Jam-Signal.....	181	Leitung.....	140
John Tyndall.....	208	Leitungsabschnitt.....	142
Jumbo-Frames.....	183	Leitungsanomalien.....	165
Kabel.....	140	Leitungscodierung.....	324
Kabelfernsehen.....	327	Leitungslänge.....	165
Kanal.....	83, 96	Leitungsunterbrechung.....	170
Kanalkapazität.....	81, 408	Leitungsvermittlung.....	31, 402f.
Kapazität.....	92, 141, 317	Length.....	449
Kapazitätsbelag.....	141	Lichtgeschwindigkeit.....	33, 148
Keepalive Timer.....	579	Lichtwellenleiter.....	55
Kernglas.....	216	Lichtwellenübertragung.....	36
Klassen.....	171	33 - Link Aggregation.....	601
Koaxialkabel.....	324	LAC.....	604
Koaxkabel.....	198	LACP.....	602, 604
Kodierung.....	55	LACPDU.....	602
Kollision.....	175, 178f., 181, 540	LAG.....	601
Kollisionserkennung.....	338	Link Aggregation Control Protocol.....	602
Kommandos.....	421	Link Aggregation Control Protocol Data Unit.....	602
Kommunikationsmodelle.....	18	Link Aggregation Control.....	604
Kommunikationssatelliten.....	36	Link Integrity Test.....	237
Kompression.....	65	Link Local Scope.....	498
Kontrollfunktionen.....	421	Link State Data Base.....	591
Konvergenzzeit.....	582, 584	Link-Definitionen.....	150
Kosten.....	92, 591	Link-Längen.....	223
Kostentabelle.....	592	Link-LED.....	237
Kraft-Millan-Ungleichung.....	98	Link-Local-All-Nodes-Multicast-Address.....	504
Kredit.....	409	Link-State-Algorithmus.....	587
Kupfer.....	55	Link-State-Updates.....	594
Kurzer Passiver Bus.....	333	Listen-Kommando.....	652
Kurzschluss.....	147, 170	Listening Modus.....	375
L.....	141	LIT.....	237
L'.....	141	LLC.....	8, 419, 426
LA.....	601	Typ 1.....	419
Labeling.....	131	Typ 2.....	419
LAN.....	28f.	Typ 3.....	419
Länge.....	426	Local Area Network.....	28
Längenrestriktionen.....	215	Logical Link Control.....	419
Längsparitätsbits.....	107	Login.....	653
Längswiderstand.....	142	Login Host Server.....	636
LASER.....	215	Lokale Brücken.....	359
Laserdioden.....	210	Lokale Signifikanz.....	51
Lastverteilung.....	30	Long Collisions.....	181
LAT.....	394	longest Match.....	396
Late Collisions.....	181	LSB.....	65, 417
Laufzeit.....	148, 164, 212	LSDB.....	591, 595
Layer-3-Switch.....	384	LSU.....	594
Layer2-Switches.....	383	Lucent Connector.....	228
Layer3-Switch.....	548	LWL.....	55, 425

Stichwortverzeichnis

LWL-Faserklassen.....	223	Ingress-Router.....	346
MAC-Adresse.....	56, 357, 360f., 373, 463, 465, 467, 543	Label Distribution Protocol.....	346
MAC-Layer.....	174	Label Switched Path.....	345f.
Magnetfeld.....	140, 149	Label-Edge-Router.....	346
MAN.....	8, 29, 327	LDP.....	346
Management-VLAN.....	549	LER.....	346
Managementstation.....	549	Longest-Prefix-Matching.....	344
Manchester.....	116	LSP.....	345, 347
Mantelglas.....	216	LSR.....	346
Maschine-Maschine-Kommunikation.....	23	MP-BGP.....	349
Maximale Ausdehnung eines Netzwerks.....	183	PE.....	349
Maximale Brückenanzahl.....	358	Penultimate Hop Popping.....	347
Maximallänge eines Frames.....	183	PHP-Router.....	347
Maximum segment lifetime.....	579	RFC5462.....	345
Maximum Segment Size.....	578	Swap-Operation.....	347
Media Independent Interface.....	242	VRF.....	349
Media-.....	352	MSB.....	65, 88, 417, 424f.
Media-Converter.....	355	MSL.....	579
Media-Independent -Interface.....	55	MSS.....	578
Media-Konverter.....	355	MSS,.....	576
Medien-Zugriff.....	56	MSTP.....	372
Medien-Zugriffs-Verfahren.....	26	MT-RJ Stecker.....	229
Mehrwertige Leitungscodes.....	112	Multi Protocol Label Switching.....	344
Mensch-Maschine-Kommunikation.....	23	Multicast.....	24, 26f., 356f., 442, 584, 593
Mensch-Mensch-Kommunikation.....	23	Adressen.....	361
Message Cube.....	82	Multicast-API.....	599
Messung.....	222	Multicast-Gruppe.....	599
Metronetz.....	327	Multicast-ID.....	446
Metropolitan Area Networks.....	327	Multicasting.....	598
MIB.....	623	Multimode LWL.....	207
MIC-Stecker.....	229, 425	Multimode-Faser.....	216
Microsegmentierung.....	540	Multimode-Fasern.....	212
MIDCOM.....	461	Multiple Access.....	232
Midspan-Versorgung.....	321	Multiple Spanning Tree.....	372
MII.....	55	Multiple Token.....	188
Mikrowellen.....	34	Multiplexing.....	65, 83, 406f.
MIME.....	645	Multiplexrahmen.....	324
Minimale Frame-Länge.....	183	Multiport-Brücken.....	359
mit Source Routing Transparent Bridging.....	381	Multipurpose Internet Mail Extensions.....	645
Mitgliedschaft.....	599	N-CONNECT.c.....	48
MLT3.....	112	N-CONNECT.confirm.....	48
MLT3.....	116	N-CONNECT.i.....	48
Mode.....	211	N-CONNECT.indication.....	48
Mode-Conditioning Kabel.....	215	N-CONNECT.r.....	48
Modem.....	22, 85, 343	N-CONNECT.request.....	48
Modenfilter.....	215	N-CONNECT.response.....	48
Modifizierter AMI-Code.....	337	N(R).....	420
Modulation.....	55, 85, 121, 342	N(S).....	420
Modulationsverfahren.....	123	Nachbarschaftsbeziehungen.....	593
Monomode-Fasern.....	214	Nachricht.....	96
Most Significant Bit.....	417	Nachrichten.....	18
MPLS.....	32, 344	Nachrichten-Ebene.....	95
BGP.....	349	Nachrichtenvermittlung.....	32
CE.....	349	NACK.....	412
Egress-Router.....	346	Nagle-Algorithmus.....	574
FEC.....	344	Nah-Nebensprechen.....	149, 152, 157
Forwarding Equivalence Class.....	344	NAPT.....	454

NAT.....	452, 454	P2P.....	20
NAT-Tabelle.....	455	PA-Slots.....	327
Near End Crosstalk.....	152	Padding.....	449
Nebensprechen.....	166	Paket.....	32, 63
Negativ-Stopfverfahren.....	324	Paket-Transfer-Mode.....	413
Net-Route-Eintrag.....	395	Paketvermittlung.....	402, 404
NetBEUI.....	394	Paketvermittlungsnetz.....	328
NetBIOS.....	394	Paketverwaltung.....	412
netstat.....	600	PAM.....	135
Network Address Translation.....	454	PAN.....	29
Network and Port Address Translation.....	454	Passwort.....	653
Network Interface Controller.....	22, 415	PASV.....	652
Network Print Service.....	636	PAT.....	454
network unreachable.....	577	Patchkabel.....	230
Network Virtual Terminal.....	653	PCI.....	45
Network-Layer.....	62	PCM.....	2, 137
Netzwerk-Adresse.....	436	PD.....	317
Netzwerk-Komponenten.....	351	PDH.....	324, 330
Netzwerke.....	63	PDM.....	135
Netzwerksicherheit.....	549	PDU.....	45
NEXT.....	149, 152, 158f., 203	Peer.....	52
NEXT, FEXT.....	152	Peer-to-Peer.....	20
NFS.....	65, 579	peer-to-peer-commuication.....	45
NIC.....	22, 415	Peer-to-Peer-Kommunikation.....	455
Nicht routbare Protokolle.....	394	Peer-to-Peer-Modell.....	18, 20
Nicht-persistentes CSMA.....	180	Peferred-Lifetime.....	538
Node Local Scope.....	498	Permanent-Link.....	150
Northbound.....	556	Persist Timer.....	578
NOVELL.....	418	Pfadkosten.....	361, 373
NRZ.....	113	PFM.....	135
NRZ-L.....	113	Phantomspeisung.....	319
NRZ-M.....	113	Phase.....	123
NRZ-S.....	113	Phase II.....	418
NT.....	331	Phase Shift Keying.....	123
NT1.....	331	Phasenkonstante.....	148
NT2.....	331	Phasenmodulation.....	123
NTBA.....	22, 331f., 336	Phasenumtastung.....	123
NTPM.....	331	PHP.....	347
Nullpegel.....	338	Physical-Layer.....	55
NVP.....	163	Physical-Media-Dependent.....	55
Nyquist-Frequenz.....	66	Piggybacking-Verfahren.....	410
Nyquist-Grenze.....	66	Pigtail.....	221, 230
Nyquist-Kriterium.....	66, 72	PiMF.....	202
ODTR.....	222	Pinbelegung.....	322
Offline-Protokoll.....	646	Plesiochrone Digitale Hierarchie.....	324
Oktett.....	88	PMD.....	55
Online-Protokoll.....	646	PoE.....	317
Open Shortest Path First.....	586	Poison Reverse.....	584
Optical Time Domain Reflectometer.....	222	Poisson-Verteilung.....	176
Optionen.....	428	Pop-Operation.....	345
Options.....	449	POP3.....	644, 646
orderly release.....	567	POP3-Kommandos.....	645
OSI.....	394	Port.....	598
OSI-Modell.....	7	Port Address Translation.....	454
OSI-RM.....	7	Port Restricted Cone.....	458
OSPF.....	62, 394f., 586	Port-ID.....	361
p-persistent CSMA.....	180	Port-Priorität.....	373

Stichwortverzeichnis

Portdichte.....	300	QAM.....	133
Positiv-Null-Negativ-Stopfverfahren.....	324	QoS.....	8
Positiv-Stopfverfahren.....	324	QPSK.....	133
Post Office Protocol.....	644	Quadrature Amplitude Modulation.....	133
POTS.....	342	Quadrature Phase Shift Keying.....	133
Power over Ethernet.....	8, 317	Qualität.....	92
Power Sourcing Equipment.....	317	Quantisierung.....	81
Power Sum FEXT.....	159	Quantisierungsrauschen.....	70
Power Sum NEXT.....	159	Quaternäre Leitungscodes.....	112
Powered Device.....	317	Querleitwert.....	142
PPM.....	135	Querparitätsbits.....	107
Präambel.....	90, 417, 426	Query.....	600
Präambel-Bytes.....	417	Quinäre Leitungscodes.....	112
Präambelfelder.....	416	Quittung.....	407, 409, 411
Presentation-Layer.....	65	Quittungen.....	428
Primärverkabelung.....	313	R.....	141
Primary Rate Interface.....	339	R'.....	141
Primitive.....	48	RA.....	538
Priorisierung.....	543, 549	Radiofunk.....	34
Privacy Extensions.....	538	Rahmenübertragungszeit.....	176
Probe.....	630	Rapid Reconfiguration Spanning Tree.....	372
Probe-Segment.....	579	Rapid Spanning Tree.....	8
Promiscuous Mode.....	356	RARP.....	422
Propagation Delay.....	163	Request.....	465f.
Propagation Delay Skew.....	164	Server.....	465
Protocol.....	449	Rauschen.....	81, 118
Protokoll.....	44	RDNSS.....	538
Protokoll-Funktionen.....	402	Reassemblierung.....	427
Protokoll-Stack.....	22	Reassembling.....	62
Protokollbindungen.....	423	Receive Not Ready.....	421
Protokolle.....	52, 62, 635	Receive Ready.....	420
Protokollnummer.....	635	Recursive DNS Server.....	538
Proxy.....	649	Redundanz.....	94, 360
Proxy-Agenten.....	622	Referenz-Netzwerke.....	450
PROXY-Server.....	466	Referenzmodelle.....	45
Prüfschleifen.....	331	Reflexion.....	146, 209
PSACR.....	160	Reflexionsfaktor.....	147
PSE.....	317	REJ.....	420
PSELFEXT.....	162	Reject.....	420
PSFEXT.....	159	Relevanz.....	94
PSK.....	123	Remote Network Terminal.....	636
PSNEXT.....	159	Remote-Brücken.....	359
Pulsamplitudenmodulation.....	135	Repeater.....	352, 355
Pulsdauermodulation.....	135	Repeater-Regeln.....	354
Pulse Code Modulation.....	137	Request.....	49, 581, 585
Pulsfrequenzmodulation.....	135	Response.....	49f., 581, 585
Pulsmodulation.....	135	Restricted Cone.....	457
Pulsphasenmodulation.....	135	Return Loss (RL).....	167
Pulsweitenmodulation.....	135	RFC 1247.....	586
Punkt-zu-Punkt-Netzwerk.....	27	RFC 1918.....	450
Punkt-zu-Punkt-Verbindung.....	335	RFC 2328.....	586
Pure ALOHA.....	175	RFC-Bezugsquellen.....	12
Push-Operation.....	345	RFC-Lebenszyklus.....	10
PWM.....	135	RFC's.....	9
Q.920/21.....	2	RFC1521.....	645
Q.930/31.....	2	RFC1522.....	645
QA-Slots.....	327	RFC1700.....	635f.

RFC1939.....	644	SAN.....	29
RFC2060.....	646	SAP.....	45, 47, 52, 419
RFC2068.....	648	SC-Stecker.....	228
RFC2616.....	648	Schicht.....	64
RFC792.....	475	Schichtenanzahl.....	41
RFC821.....	638	Schmelztechnik.....	220
RFC854.....	653	Schnittstelle.....	63
RFC959.....	650, 652	Schrägenschliff.....	228
RG58.....	199	Schritt.....	70, 96
RG59B.....	199	Schrittgeschwindigkeit.....	96
RG62A.....	199	Scrambling.....	89, 354
RG8A/U.....	198	Screened shielded TP.....	203
Ringstruktur.....	424f.	SDH.....	325, 330
RIP.....	62, 394f., 580, 587	SDN.....	550
RIP Version 1.....	580	SDSL.....	340f.
RIP Version 2.....	584	SDU.....	45
RIPE.....	6	Seitenbänder.....	136
RISC.....	357	Sekundärverkabelung.....	313
RJ11-Stecker.....	301	Selbstlernmodus.....	357, 360
RJ12-Stecker.....	302	Selective Reject ARQ.....	412
RJ45.....	300, 317	Selective Reject Automatic Repeat Request.....	407
RJ45-Stecker.....	302	Selective Repeat.....	412
Rlogin.....	579	Sende-Folgenummer.....	420
RMON.....	630	Sequenznummer.....	412
RNR.....	421	Server-Prozess.....	19
Root Bridge.....	372	Service-Access-Point.....	47
Root Port.....	375	Service-Provider.....	47
Root-Bridge.....	362	Service-User.....	47
Root-Path.....	362	Session-Layer.....	65
Root-Path-Cost.....	362	Set-Community-String.....	625
Routebare Protokolle.....	394	SFD.....	90, 418, 426
Routen.....	62	Shared Media.....	174
Router.....	62, 64, 343, 427, 580, 586	Short Inter Frame Spacing.....	185
Router-Advertisement-Nachricht.....	538	Shortest Path First.....	593
Router-Advertisements.....	538	Sicherheit.....	92
Router-ID.....	593	Sicherungs-Schicht.....	56
Router-Priorität.....	593	SIFS.....	185f.
Router-Solicitation-Nachricht.....	538	Signal.....	96
Routing-Protokolle.....	62	Signal zu Rausch-Verhältnis.....	81
Routing-Tabelle.....	62ff., 395	Signalisierung.....	405, 420
Routing-Tabellen.....	595	Signalkanal.....	330
Routingprotokolle.....	394f., 580, 586	Signallaufzeit.....	182
RR.....	420	Signalstärke.....	81
RS232.....	300	Silly Window Syndrome.....	578
RSTP.....	372	Simple Mail Transfer.....	636
RSTP Port Modi.....	375	Simple Mail Transfer Protocol.....	638
RTT.....	183	Simple Network Management Protocol.....	636
Ruhesignal.....	338	Simplex.....	65
Rundfunksysteme.....	33	Simplex-Betrieb.....	25
RZ.....	113	Simplexkabel.....	217
S-Frames.....	420	Single Bit.....	132
S0.....	2	Single-Point of Failure.....	360
S0-Rahmen.....	337	Single-Point-of-Failure.....	593
S0-Rahmenaufbau.....	337	SingleMode LWL.....	207
S2M.....	2, 339	Singlemode-Faser.....	216
SABME.....	421	SIP_Trapez.....	455
Sammelquittung.....	410	SIP-Trapez.....	455

Stichwortverzeichnis

Site Local Scope.....	499	Standortverkabelung.....	313
Sitzungs-Schicht.....	65	Start Frame Delimiter.....	90
SLAAC.....	538	Start of Authority.....	485
Sliding Window.....	407, 409	Start-Frame-Delimiter.....	418
Slot.....	83, 178	Start-Rahmen-Begrenzer.....	90
Slotted ALOHA.....	178	Stateful Address Autoconfiguration.....	539
Slow Start.....	576	Stateless Address Autoconfiguration.....	538
SLSAP.....	419	Statische Routing-Einträge.....	395
SMDS.....	327	Statisches Adressbuch.....	360
SMTP.....	65, 638	Sternkoppler.....	355
SMTP-Kommandos.....	640	Steuerkanal.....	405
SNAP.....	418	Stop and Wait.....	407f.
SNMP.....	65, 620	Stop-and-Wait.....	65
SNMP-Agenten.....	622	Stopfbits.....	324
SNMPv2-Classic.....	629	Störabstand.....	149, 154
SNMPv2*.....	629	Store-And-Forward.....	382
SNMPv2C.....	629	Store-and-Forward-Net.....	328
SNMPv2u.....	629	STP.....	202, 375
SNMPv3.....	630	Straight Tip.....	227
SNR.....	119, 149, 154, 570	Strom.....	317
SOA.....	485	Stromversorger.....	317
SOA-Resource-Record.....	491	Strukturierte Verkabelung.....	309
SOCKS-Gateway.....	649	Stufenindex.....	212
Software Defined Networks.....	550	Stufenindexfaser.....	212ff.
Solicitation-Nachricht.....	539	STUN.....	460
SONET.....	325	SUB-D-Stecker.....	300
Source.....	449	Subnet Access Protocol.....	418
Source Routing Transparent Bridging.....	381	Subnetmask.....	396, 439
Source-Quench.....	576	Subnetmaske.....	585
Source-Routing-Brücken.....	381	Subnetzmask.....	441
Source-Service-Access-Point.....	418	Subnetzmaske.....	580, 584
Southbound.....	556	Switch.....	540
Spanning Tree.....	8	Switching Hub.....	355
Spanning-Tree-Algorithmus.....	361	Switching-Verfahren.....	382
Spare-Pairs.....	319	SWS.....	578
Speichervermittlung.....	31, 402	Symbol.....	96, 133
Speichervermittlungsnetz.....	328	Symmetric Cone.....	459
Spektrum.....	72	Symmetrische Leitungen.....	196
Spektrum der Pulsmodulation.....	136	Synchrone Übertragung.....	88
SPF.....	593	Synchroner Transfermodus.....	413
SPF-Baums.....	595	Synchronisation.....	55, 89
Spleiss.....	222	Synchronisationsbit.....	337
Spleissbox.....	221, 230	Synchronisationspunkte.....	65
Spleissverbindung.....	221	Systeme.....	83
Split Horizon.....	584	TA-Adapter.....	331
Split Pairs.....	169	Tagging.....	8
Splitter.....	340, 343	Takt-Rückgewinnung.....	55, 88ff., 112
Sprachübertragung.....	81	Taktimpuls.....	88
SPT.....	361	Talk.....	636
SRB.....	381	TCP.....	65, 410, 558f., 635f., 646, 650, 653
SRT.....	381	ACK.....	560, 564f.
SSAP.....	418	Acknowledgement-Number.....	560
SSH.....	454	delayed ACK.....	570
SSL.....	454	Destination-Port.....	560
SSTP/SFTP.....	203	EOF.....	565
ST-Stecker.....	227	FIN.....	565
standards.....	1	FLAGS.....	560

FIN.....	560	Token Ring.....	8, 187, 195, 302, 304, 424
PSH.....	560	Token-Ring.....	381
RST.....	560	Token-Zugriffsverfahren.....	187
SYN.....	560	Topologie.....	189f.
URG.....	560	Topologie-Vergleich.....	195
im ISO-RM.....	559	TOS.....	428, 448
ISN.....	564	TrafficDirector.....	634
MSS.....	564	Trägersignal.....	121
NODELAY.....	574	Transceiver.....	22
Options.....	561	Transmission Control Protocol.....	635
End of option list.....	561	Transport-Layer.....	65
MSS.....	561	Transport-Schicht.....	65
No option.....	561	Traversal-Problem.....	455
Timestamp.....	561	Tribit.....	132
Window Scale Factor.....	561	Triggered Updates.....	584, 587
RST.....	567, 579	Trivial File Transfer Protocol.....	636
Sequence –Number.....	560	Trunk.....	546
Sequenznummer.....	570	Trunk-Modus.....	543
Source-Port.....	560	TTL.....	345, 428, 449, 579
SYN.....	564, 567	TURN.....	462
TCP-Timer.....		Twin-Koax-Kabel.....	200
2MSL Timer.....	579	Twisted Pair.....	201
Keepalive Timer.....	579	Twisted-Pair-Kabel.....	425
Persist Timer.....	578	Typ.....	426
Retransmission Timer.....	577	Typ- / Längen-Feld.....	543
TIME-WAIT.....	579	TYP-N-Stecker.....	299
Urgent-Mode.....	575	Typen.....	419
Verbindungsabbau.....	565	U-Frames.....	421
Verbindungsaufbau.....	563	UA.....	421
TCP-Timer.....	577	UADSL.....	340
TCP/IP.....	418	Überblick.....	174
TCP/IP - RM.....	45	Übertragungswiederholung.....	407
TCP/IP-Stack.....	635	Überwachungskamera.....	317
TE.....	331	Ubiquitous Computing.....	18, 20
TE1.....	331	UDP.....	65, 454, 558f., 620, 635f.
TE2.....	331	UDP im ISO-RM.....	558
Technisches Übertragungskonzept.....	26	UFTP.....	202
Telnet.....	579, 653	UI.....	421
Temperatur.....	317	UID.....	647
Terminal-Netz.....	18	Umtastung.....	123
Terminal-Systeme.....	19	UNARP.....	467
ternäre Codes.....	112	Unicast.....	24, 26f., 356f., 442
Ternary-Wire-Codes.....	116	Uniform Resource Locator.....	649
Tertiärverkabelung.....	313	Unique Globally Scope.....	499
TEST.....	421	Unique Local Scope.....	499
Testschaltung.....	317	Universal Plug'n'Play.....	461
TIA.....	6	Unshielded-TP-Kabel.....	202
TIA 568A.....	303	Unsymmetrische Leitungen.....	197
TIA 568B.....	303	Update.....	584
Time To Live.....	428	UPnP.....	461
Timeout.....	407, 411f.	URL.....	649
Timer.....	65, 407, 411f., 587	User Datagram Protocol.....	635
Timer-Intervall.....	583	UTP.....	202
TK-Anlage.....	336	V.24.....	2, 300
TLD.....	4	V.34.....	342
Token.....	207	Valid-Lifetime.....	538
Token Bus.....	8, 187	Value Added Network.....	28

Stichwortverzeichnis

VAN.....	28	WAN.....	29, 328
Variable Length of Subnet Mask.....	584	WEB-Server.....	455
VCSEL.....	215	Wegeentscheidung.....	396
VDSL.....	340f.	Wegentscheidung.....	62, 64
Verbindungslose Übertragung.....	402	Weitverkehrsnetze.....	328
Verbindungslose-Kommunikation.....	65	Well-Known Ports.....	636
Verbindungsloser Dienst.....	32	Wellenlänge.....	33, 210
Verbindungsorientierte.....	402	Wellenwiderstand.....	142, 144, 165
Verbindungsorientierte-Kommunikation.....	65	Westbound.....	556
Verbindungsorientierter Dienst.....	32	Western-Stecker.....	301
Verbindungsstati.....	562	Wide Area Networks.....	328
Verbindungstyp.....	31	Widerstand.....	141
Verbraucher.....	317	Widerstandsbelag.....	141
Verdrillung.....	164	Wiederholung.....	65, 175
Verfügbarkeits-Verbund.....	17, 30	Wiederholungen.....	428
Verkehrsarten.....	24	Window Size.....	410
Vermittlung.....	402	Window-Probe-Paket.....	578
Vermittlungs-Schicht.....	62	Window-Size.....	571, 578
Vermittlungssysteme.....	31	Windowing.....	65
Verschlüsselung.....	65	Wire-Map-Fehler.....	169
Version.....	448	Wissen.....	15
Versorgungsspannung.....	317	WLAN-Accesspoint.....	317
Vertical Cavity Surface Emitting Laser.....	215	X-Windows.....	454
VfrsDx.....	5	X.21.....	2
Vierstufige Leitungscodierung.....	112	X.25.....	2, 328
Virtual Router Redundancy Protocol.....	521	X.28.....	328
virtueller Pfad.....	32	X.29.....	328
Virtuelles LAN (VLAN).....	540	X.3.....	328
Virtuelles Privates Netzwerk.....	28	X.31.....	328, 333f.
VLAN.....	8, 395	X.75.....	328
VLAN Tagging.....	543	xDSL.....	340
VLAN-ID.....	543	XGMII.....	55
VLANDirector.....	634	XID.....	421
VLMS.....	584	XWINDOWS.....	65
VMPS.....	544	Yellow-Cable.....	198
VoIP.....	455	Zeichen.....	15, 96
Vollduplex-Betrieb.....	25	Zeit-Multiplex.....	83, 325, 337
Vollduplex-Verbindung.....	342	Zeitschlitz.....	83, 178
VPN.....	28, 460	Zugangsprozedur.....	338
VRRP.....	521	Zugehörigkeit.....	94
Default Gateway.....	522	Zugverfahren.....	220
IP Adress-Owner.....	523	Zuverlässigkeit.....	92
Prioritätszuordnung.....	524	Zweidimensionale Parität.....	107
VIP.....	522	Zweidrahtleitung.....	324
Virtuelle Router ID.....	522	ZWR.....	331
VR.....	522	Zyklenfreiheit.....	360f.
VRID.....	522		44
VRRP-Router.....	522		

46 - Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
4G	Mobilfunktechnik	Mobilfunk 4. Generation (LTE)
5G	Mobilfunktechnik	Mobilfunk 5. Generation
Φ	Einheiten	Phase
λ	Einheiten	Lambda für Wellenlänge [in m]
π	Konstante	3.14159265359
ω	Einheiten	Kreisfrequenz (= $2\pi f$)
	Abtastung	Amplitude
A	Modulation	Amplitude
	DNS-Protokoll	IPv4-Adresse eines Hosts
AA	WLAN	Authenticator Address
AAA	Security	Authentication, Authorization and Accounting
AAAA	DNS-Protokoll	IPv6-Adresse eines Hosts
a	Leitungsmessung	Attenuation (Dämpfung)
ABR	OSPF	Area Border Router
	Schaltungstechnik	Alternating Current (Wechselstrom)
AC	Kommunikation	Anycast
	WLAN	Access Category
ACI	WLAN	Access Category Index
ACK	Protokolle	Acknowledge (pos. Quittung)
ACL	Security	Access Control List
ACR	Leitungsmessung	Attenuation to Crosstalk Ratio
AD	Strukturierte Verkabelung	Anschluss Dose
ADM	Modulation	Adaptive Delta Modulation
ADSL	WAN	Asymmetric Digital Subscriber Line
AES	Security	Advanced Encryption Standard
AES-CCM	Security	Advanced Encryption Standard CTR/CBC MAC
AFC	WLAN	Automatic Frequency Control
AGC	WLAN	Automatic Gain Control
AH	IPSec	Authentication Header
AICCU	Protokolle	Automatic IPv6 Connectivity Client Utility
AIFS	Mediumzugriff	WLAN: Arbitration Inter Frame Space (für QoS)
AID	WLAN	Association-ID
ALG	Firewalls	Application Level Gateway
AM	Modulation	Amplituden Modulation
AMI-NRZ	Wire-Coding	Alternate Mark Inversion Non Return to Zero
AMI-RZ	Wire-Coding	Alternate Mark Inversion Return to Zero
AMP	Systeme	Amplifier (Verstärker)
ANSI	Normierung	American National Standards Institute
AP	WLAN	Access Point
	Spanning Tree	Alternate Port
APC	LWL-Stecker	Angled Physical Contact
API	Software	Application Programming Interface
APIPA	Protokolle	Automatic Private IP Addressing

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
ARQ	Protokolle	Automatic Repeat Request
ARP	Protokolle	Address Resolution Protocol
AS	OSPF	Autonome System
ASBR	OSPF	Autonome System Boundary Router
ASCII	Kodierung	American Standard Code for Information Interchange
ASIC	Hardware	Application Specific Integrated Circuit
ASN.1	Management	Abstract Syntax Notification One
ATIM	WLAN	Ad-hoc Traffic Indication Map Announcement Traffic Indication Message
ATM	Kommunikationsarchitektur	Asynchronous Transfer Mode
ATU	WAN	ADSL Terminal Unit (ADSL-Modem)
AU	MAN	DQDB-Access Unit
AUI	Schichtenmodell	Attachment Unit Interface
AWG	Verkabelung	American Wire Gauge
AXTALK	Leitungsmessung	Alien Crosstalk
B	Datenübertragung	Bandwidth
BA	WAN	ISDN Basis Anschluss
	WLAN	Block ACK
BAKOM	Normierung	Bundesamt für Kommunikation (Schweiz)
BAKT	WAN	ISDN: Basisanschuß-Konzentrator
BAN	Netzwerke	Body Area Network
BAPT	Normen	Bundesamt für Post und Telekommunikation
BAR	WLAN	Block ACK Request
BC	Kommunikation	Broadcast
BD	Strukturierte Verkabelung	Building Distributor
	Kommunikation	Broadcast Domain
BDSG	Gesetze	Bundes Daten Schutz Gesetz
BEC	Channel-Coding	Backward Error Correction
BER	Datenübertragung	Bit Error Rate
BF	WLAN	Beamforming
BFWA	WLAN	Broadband Fixes Wireless Access
BGP	Protokolle	Border Gateway Protocol
BIP	WLAN	Broadcast / Multicast Integrity Protocol
BIT	Zahlendarstellung	Binary Digit
BLC	Ethernet	Basic Link Codewort
Bluetooth SIG	Stamndard-Gremium	Bluetooth Special Interest Group
BNC	Stecker	Bayonet Neill Concelman
Bnetza	Normierung	Bundes Netzagentur
BO	WLAN	Back Off
BOOTP	Protokolle	Bootstrap Protocol
BOT	WLAN	Back Off Time
BP	Spanning Tree	Blocking Port
BPDU	Brücken /Switches	Bridge-PDU (zur Bearbeitng des Spanning Trees)
BPSK	Modulation	Binary Phase Shift Keying

Abkürzung	Bereich	Ausgeschrieben
BR	OSPF	Backup Router
BRA	WAN	ISDN: Basic Rate Access
BRI	WAN	ISDN: Basic Rate Interface
BRPIFS	Mediumzugriff	WLAN: Beam Refinement Protocol IFS
BS	Normierung	British Standard
BSI	Normierung	British Standards Institution
BSS	WLAN	Basic Service Set
BSSID	WLAN	Basic Service Set ID
BSR	WLAN	Buffer Status Report
BSRP	WLAN	Buffer Status Report Poll
BUP	Spanning Tree	Backup Port
C	Abtastung	Kanalkapazität [in Bit/s]
	Schaltungstechnik	Kapazität [in Farad (F)]
C'	Schaltungstechnik	Kapazitätsbelag [in Farad (F)]
c	Einheiten	Lichtgeschwindigkeit [299792km/s]
CA	WLAN	Collision Avoidance
CAN	Topologien	Controller Area Network (siehe auch CAN-Bus)
CAT	Verkabelung	Category
CBC	Security	Cipher Block Chaining
CBDS	MAN	DQDB: Connectionless Broadband Data Service
CBW	WLAN	Channel Bandwidth
CC	DNS-Protokoll	Country Code
CCA	Mediumzugriff	Clear Channel Assessment
CCITT	Normierung	Comité Consultatif International Télégraphique et Téléphonique
CCK	Modulation	Complementary Code Keying
CCM	Security	CTR / CBC-MAC
CCMP	Security	CCM Protocol
	Mediumzugriff	Collision Detection
CD	Strukturierte Verkabelung	Campus Distributor
	Kommunikation	Collision Domain
CDDI	Netzwerke	Copper Distributed Data Interface
CDM	Multiplextechnik	Code Division Multiplex
CDMA	Multiplextechnik	Code Division Multiplex Access
CE	WAN	MPLS: Customer Edge Device
CEN	Normierung	Comité Européen de Normalisation
CENELEC	Normierung	Europäisches Komitee für elektrotechnische Normung
CEPT	Normierung	Conference Européenne des Administrations des Postes et des Télécommunications
CF	WLAN	Contention Free
CFP	WLAN	Contention Free Period
CGMII	Ethernet	100 Gigabit Media Independent Interface
CIDR	Routing	Classless Inter Domain Routing
CIR	WAN	Frame Relay: Committed Information Rate
CLI	Geräteschnittstellen	Command Line Interface
CMIP	Management	Common Management Information Protocol
CN	Mobile IP	Corresponding Node

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
COA	Mobile IP	Care Of Address
COBOL	Programmiersprache	Common Business Oriented Language
CODEC	Abtastung	Codierung Decodierung (Einheit)
CP	Verkabelung	Consolidation Point
CPU	Rechnerarchitektur	Central Processing Unit
CR	Steuerzeichen	Carriage Return
CRC	Channel-Coding	Cyclic Redundancy Check
CRLF	Steuerzeichen	Carriage Return Line Feed
CS	Mediumzugriff	Carrier Sense
CSMA	Mediumzugriff	Carrier Sense Multiple Access
CSMA/CA	Mediumzugriff	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Mediumzugriff	Carrier Sense Multiple Access with Collision Detection
CSMA/CR	Mediumzugriff	Carrier Sense Multiple Access with Collision Resolution
CTR	WLAN	Counter
CTS	WLAN	Clear To Send
Cu	Werkstoff	Kupfer
CW	Mediumzugriff	Collision Window (bei CSMA/CD) Contention Window (bei CSMA/CA)
CWND	TCP	Congestion Window (Überlast Fenster)
D	Abtastung	Dynamic (= Sendeleistung / Rauschleistung = P_S / P_N)
DA	WLAN	Destination Address
DAD	ICMPv6	Duplicate Address Detection
DARPA	Ethernet und Protokolle	Defence Advanced Research Projects Agency
db	Einheit	Dezibel
DBPSK	Modulation	Differential Binary Phase Shift Keying
DC	Schaltungstechnik	Gleichstrom (direct current)
DCE	Übertragungstechnik	Data Communication Equipment
DCF	Medienzugriff	WLAN: Distributed Coordination Function
DD	OSPF-Protokoll	Database Description
DDE	Schichtenmodell	Dienst-Daten-Einheit
DDNS	Protokolle	Dynamic Domain Name Service
DECT	Funktechnik	Digital Enhanced Cordless Telecommunications
DEE	Übertragungstechnik	Daten End Einrichtung
DEI	VLAN	Drop Eligible Indicator
DF	Protokolle	Dont Fragment (Flag)
DFS	WLAN	Dynamic Frequency Selection
DG	Netzwerke	Default Gateway
DHCP	Protokolle	Dynamic Host Configuration Protocol
DIFS	Mediumzugriff	Distributed coordination function Inter Frame Space
DIN	Normierung	Deutsches Institut für Normung
DISC	Protokolle	Disconnect
DL	WLAN	Down Link
DLL	Schichtenmodell	Data Link Layer
DM	Modulation	Delta-Modulation
	Protokolle	Disconnect Mode
DME	Ethernet	Differential Manchester Encoding

Abkürzung	Bereich	Ausgeschrieben
DMG	WLAN	Directional Multi Gigabit
DMZ	Security	De-Militarisierte Zone
DNAT	Protokolle	Destination Network Address Translation
DNS	Protokoll Service	Domain Name Service
DP	Spanning Tree	Designated Port
DPB	Normierung	Deutsche (Bundes) Post
DPCM	Modulation	Differenz Puls Code Modulation
DQDB	MAN	Distributed Queue Dual Bus
DR	OSPF	Designated Router
DSAP	Ethernet	Destination Service Access Point
DS	WLAN	Distribution System
DSL	WAN	Digital Subscriber Line
DSP	Prozessoren	Digital Signal Processor
DSSS	Modulation	Direct Sequence Spread Spectrum
DTE	Übertragungstechnik	Data Termination Equipment
DTIM	WLAN	Delivery Traffic Indication Map
DÜE	Übertragungstechnik	Daten Übertragungs Einrichtung
DVMRP	Protokolle	Distance Vector Multicast Routing Protocol
EAP	Security	Extensible Authentication Protocol
EAPoL	Security	EAP over LAN
EBCDIC	Kodierung	Extended Binary Coded Decimal Interchange Code
ECC	Normierung	Electronic Communication Commission
ECMA	Normierung	European Computer Manufacturers Association
EDCA	QoS	WLAN: Enhanced Distributed Channel Access
EDCAF	Mediumzugriff	WLAN: Enhanced Distribution Channel Access Function
EGP	Protokolle	Exterior Gateway Protocol
EHF	Frequenzbereich	Extremely High Frequency (10 – 1 mm / 30 – 300 GHz)
EIA	Normierung	Electronic Industries Alliance
EIFS	Mediumzugriff	WLAN: Extended IFS
EIGRP	Protokolle	Enhanced Interior Gateway Routing Protocol
EIRP	Antennentechnik	Equivalent Isotropically Radiated Power
EIV	WLAN	Extended IV
EIVID	WLAN	EIV Identiy
ELFEXT	Leitungsmessung	Equalized Level Far End X-Talk
EN	Normierung	Europäische Norm
ENP	Ethernet	Extended Next Page
EOF	TCP	End of File
EOL	Dateien	End of Line
EP	Spanning Tree	Edge Port
EPROM	Hardware	Erasable Programable Read-Only-Memory ERMES (European Radio Messages System)
ERMES	Frequenzbereiche	European Radio Messages System
ERP	WLAN	Extended Rate PHY
ERP-OFDM	WLAN	Extended Rate PHY Orthogonal Frequency Division Multiplex
ERP-PBCC	WLAN	Extended Rate PHY Packet Binary Complementary Code

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
ESP	IPSec	Encapsulation Security Payload
ESS	WLAN	Extended Service Set
ETSI	Normierung	European Telecommunications Standard Institute
EUI	MAC-Adressformat	Extended Unique Identifier
EWC	WLAN	Enhanced Wireless Consortium
f	SI-Einheiten	Frequenz [in 1/s]
FA	Mobile IP	Foreign Agent
FAQ	Normierung	Frequently Asked Questions
FC	LWL-Stecker	Fiber Connector
FCC	Normierung	Federal Communications Commission (USA)
FCS	Channel-Coding	Frame Check Sequence
FD	Datenübertragung	Full Duplex
	Strukturierte Verkabelung	Floor Distributor (Etagen Verteiler)
FDD	WLAN	Frequency Division Duplex
FDDI	Netzwerke	Fiber Distributed Data Interface
FDM	Multiplextechnik	Frequency Division Multiplex
FDMA	Multiplextechnik	Frequency Division Multiplex Access
FEC	Channel-Coding	Forward Error Correction
	WAN	MPLS: Forwarding Equivalence Class
FER	Channel Coding	WLAN: Frame Error Rate
FEXT	Leistungstheorie	Far End Crosstalk
FFT	Math. Verfahren	Fast Fourier Transformation
FIN	TCP	Finalize (Flag)
FLP	Ethernet	Fast Link Pulse
FHSS	Modulation	Frequency Hopping Spread Spectrum
FM	Modulation	Frequency Modulation
FO	Normierung	Fernmelde Ordnung
FOIRL	Ethernet	Fiber Optic Inter Repeater Link
FPGA	Hardware	Field Programmable Gate Array
FPK	WLAN	Fast Packet Keying
FQDN	DNS-Protokoll	Fully Qualified Domain Name
FRMR	Protokolle	Frame Reject
FSPL	WLAN	Free Space Path Loss
FT	Math. Verfahren	Fourier Transformation
FTP	Protokolle	File Transfer Protocol
	Verkabelung	Foiled Twisted Pair
FTTB	Verkabelung	Fiber to the Building (LWL-Anschluss bis in ein Gebäude)
FTTC	Verkabelung	Fiber to the Curve (LWL-Anschluss bis zum Straßenrand)
FTTD	Verkabelung	Fiber to the Desk (LWL-Anschluss bis zum Schreibtisch)
FTTH	Verkabelung	Fiber to the Home (LWL-Anschluss bis in die Wohnung)
FYI	Normierung	For Your Information
G	Schaltungstechnik	Ableitung
G'	Schaltungstechnik	Ableitungsbelag
GAA	MAC-Adressformat	Global Administrated Address
GAN	Netzwerke	Global Area Network
GCR	WLAN	Groupcast with Retries

Abkürzung	Bereich	Ausgeschrieben
GEO	Satellitenorbit	Geostationary Earth Orbit
GF	WLAN	Green Field
GFSK	Modulation	Gaussian Frequency Shift Keying Modulation
GG	Stecker	GigaGate (Stecker für 10 GB-Ethernet)
GGP	Protokolle	Gateway to Gateway Protocol
GI	WLAN	Guard Interval
GLBP	Protokolle	Gateway Load Balancing Protocol
GMII	Ethernet	Gigabit Media Independent Interface (1000Mbps)
GPS	Positionsbestimmung	Global Positioning System
GRPS	Mobilfunktechnik	General Packet Radio Service
GSM	Mobilfunktechnik	Global System for Mobile Communications
GTKSA	WLAN	Group Temporal Key Security Association
GUA	IPv6	Global Unique Address
H ₀	Informationstheorie	Entscheidungsinhalt [in Bit / Symbol]
HA	Mobile IP	Home Agent
HBA	Hardware	Fiber Channel: Host Bus Adapter
HCF	Mediumzugriff	WLAN: Hybrid Coordination Function
HD	Datenübertragung	Half Duplex
HDB3	Wire-Coding	High Density Bipolar (mit 3 Pegeln)
HDLC	Protokolle	High Level Data Link Control
HDSL	WAN	High Bit Rate Digital Subscriber Line
HDTDR	Leitungsmessung	High Definition Time Domain Reflectometry
HDTDX	Leitungsmessung	High Definition Time Domain Crosstalk
HE	WLAN	High Efficiency (Präfix für Begriffe bei IEEE802.11ax)
HEC	WLAN	Head Error Control (Field)
HF	Frequenzbereich	High Frequency (100 – 10 m / 3 – 30 MHz)
	WLAN	WLAN-Sendeeinheit
HR	WLAN	High Rate
HSPA	Mobilfunktechnik	High Speed Packet Access
HSRP	Protokolle	Hot Standby Router Protocol
HT	WLAN	High Throughput (Präfix für Begriffe bei IEEE802.11n)
HTC	WLAN	High Throughput Capabilities
HTML	Programmiersprache	Hyper Text Markup Language
HTTP	Protokolle	Hyper Text Transfer Protocol
Hz	SI-Einheiten	Herz [in 1/s]
	Informationstheorie	Informationsmenge [in Bit]
I	Schaltungstechnik	Informationsgehalt [in Bit / Symbol]
		Strom [in Ampere]
IAB	Normierung	Internet Architecture Board
IANA	Normierung	Internet Assigned Numbers Authority
IAPP	WLAN	Inter Access Point Protocol
IBSS	WLAN	Independent Basic Service Set
ICANN	Verwaltungsgremium	Internet Corporation for Assigned Names and Numbers
ICI	Schichtenmodell	Interface Control Information
ICMP	Protokolle	Internet Control Message Protocol
ICV	WLAN	Integrity Check Value

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
ID	Allgemein	Identifikation
IDC	Stecker	IBM Data Connector
IDS	Security	Intrusion Detection System
IE	WLAN	Information Element
IEC	Normierung	International Electrotechnical Commission
IEEE	Normierung	Institute of Electrical and Electronics Engineers
IESG	Internet-Verwaltungsgremium	Internet Engineering Steering Group
IETF	Verwaltungsgremium	Internet Engineering Task Force
IFT	Math. Verfahren	Inverse Fourier Transformation
IFFT	Math. Verfahren	Inverse Fast Fourier Transformation
IFG	Mediumzugriff	Inter Frame Gap (siehe auch IFS)
IFS	Mediumzugriff	Inter Frame Space
IGMP	Protokolle	Internet Group Managing Protocol
IGP	Protokolle	Interior Gateway Protocol
IGRP	Protokolle	Interior Gateway Routing Protocol
IGTKSA	Security	Integrity Group Temporal Key Security Association
IHL	Protokolle	Inter Header Length
IMACD	IT-Betrieb	Insert / Move / Add / Change / Disposal
IMAP4	Protokolle	Internet Message Access Protocol Version 4
IoT	Begriffe	Internet of Things
IP	Protokolle	Internet Protocol
IpnG	Protokolle	IP next Generation (-> IPv6)
IPv6	Protokolle	Internet Protocol Version 6
IPG	Mediumzugriff	Inter Packet Gap (siehe auch IFS)
IPSec	Security	IP Security
IPX	Protokolle	Internetwork Packet Exchange
IrDA	Datenübertragung	Infrared Data Association
IRSG	Verwaltungsgremium	Internet Research Steering Group
IRTF	Verwaltungsgremium	Internet Research Task Force
ISATAP	Protokolle	Intra-Site Automatic Tunnel Addressing Protocol
ISDN	WAN	Integrated Services Digital Network
ISI	WLAN	Symbolinterferenz
ISM	Frequenzbereiche	Industrial, Scientific und Medical
ISN	TCP	Initialisierungs Sequenznummer
ISO	Normierung	International Organisation for Standardization
ISOC	Internet-Verwaltungsgremium	Internet Society
ISP	Internet	Internet Service Provider
IT	Begriffe	Informationstechnik
ITU	Normierung	International Telecommunications Union
IV	WLAN	Initialisierungs Vector
IVS	Verkabelung	IBM-Verkabelungs-System
KID	WLAN	Key Identity
L	Schaltungstechnik	Induktivität

Abkürzung	Bereich	Ausgeschrieben
L'	Schaltungstechnik	Induktivitätsbelag
LA	Verkabelung	Link Aggregation
LAC	Verkabelung	Link Aggregation Control
LACP	Verkabelung	Link Aggregation Control Protocol
LACPDU	Verkabelung	Link Aggregation Control Protocol Data Units
LAG	Verkabelung	Link Aggregation Group
LAN	Netzwerke	Local Area Network
LASER	Bauteil	Light Amplification by Stimulated Emission of Radiation
LAT	Protokolle	Local Area Transport (Protocol) in DECnet
LBIFS	Mediumzugriff	WLAN: Long Beamforming IFS
LC	LWL-Stecker	Lucent Connector
LDP	WAN	MPLS: Label Distribution Protocol
LDPC	Channel Coding	Low Density Parity Check
LED	Bauteil	Light Emitting Diode
LEO	Satellitenorbit	Low Earth Orbit
LER	WAN	MPLS: Label Edge Router
LF	Frequenzbereich Steuerzeichen	Low Frequency (10 – 1 km / 30 – 300 kHz) Line Feed
LFAP	Protokolle	Lightweight Flow Accounting Protocol
LIT	Ethernet	Link Integrity Test
LLA	IPv6	Link Local Address
LLC	Schichtenmodell	Logical Link Control
LME	WLAN	Layer-Management-Entitys
LOS	Funktechnik	Line Of Sight
LSB	Bit-Numerierung	Least Significant Bit
LSDB	OSPF	Link State Data Base
LSP	WAN	MPLS: Label Switched Path
LSR	WAN	MPLS: Label Switched Router
LSU	OSPF	Link State Update
LTE	Mobilfunktechnik	Long Term Evolution
LTf	WLAN	Long Training Field
LWL	Medium	Licht-Wellen-Leiter
MAC	Schichtenmodell	Medium Access Control
MA-L	MAC-Adressformat	MAC Address Large
MA-M	MAC-Adressformat	MAC Address Medium
MA-S	MAC-Adressformat	MAC Address Short
MAN	Netzwerke	Metropolitan Area Network
MAP	WLAN	Mesh Access Point
MBIFS	Mediumzugriff	WLAN: Medium Beamforming IFS
MBSS	WLAN	Mesh Basic Service Set
MBWA	Mobilfunktechnik	Mobile Broadband Wireless Access (IEEE 802.20)
MC	Kommunikation	Multicast
MCF	Mediumzugriff	WLAN: Mesh Coordination Function
MCS	Drahtlose Netzwerke	Modulation Coding Scheme
MDI	Ethernet	Media Dependent Interface

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
MDIX	Ethernet	Media Dependent Interface Crossed
MEO	Satellitenorbit	Medium Earth Orbit
MF	Frequenzbereich	Medium Frequency (1000 – 100 m / 0,3 – 3 MHz)
MIB	Management	Management Information Base
MIC	Security	WLAN: Message Integrity Code
MIDCOM	Protokolle	Middlebox Communication
MII	Ethernet	Media Independent Interface (100Mbps)
MIME	Protokole	Multipurpose Internet Mail Extensions
MIMO	WLAN	Multiple Input Multiple Output
MISO	WLAN	Multiple Input Single Output
MLMA	Mediumzugriff	Multi-Level Multi-Access
MLME	WLAN	MAC Layer Management Entity
MLT3	Wire-Coding	Multiple Level Transmit (mit 3 Pegeln)
MM	LWL	Multi Mode (Faser)
MP	WLAN	Mesh (Access) Point
MPBGP	WAN	Multi Protocol Border Gateway Protocol
MPDU	WLAN	MAC Protocol Data Unit
MPLS	Protokolle	Multi Protocol Label Switching
MPP	WLAN	Mesh Portal (Access) Point
MRC	WLAN	Maximal-Ration Combining
MS	WLAN	Multiple Sounding (Multiple Beamforming)
MSB	Bit-Numerierung	Most Significant Bit
MSDU	WLAN	MAC Service Data Unit
MSL	TCP	Maximum Segment Lifetime
MSN	WAN	ISDN: Multiple Subscriber Number
MSOH	Ethernet	Multiplex Section Overhead
MSS	TCP	Maximum Segment Size
MSTP	Spanning Tree	Multiple Spanning Tree
MTU	Protokolle	Maximum Transfer Unit (Size)
MU	WLAN	Multi User
MX	DNS-Protokoll	Mail Exchange
NA	Protokolle	Network Address
NACK	Protokolle	Negative (No) Acknowledge
NAPT	Protokolle	Network and Port Address Translation
NAT	Protokolle	Network Address Translation
NAV	WLAN	Network Allocation Vector
N _{BPSC}	WLAN	Number of Bits Per Sub Carrier
N _{CBPS}	WLAN	Number of Coded Bits Per OFDM-Symbol
NCC	Verwaltungsgremium	Network Coordination Center
N _{DBPS}	WLAN	Number of Data Bits Per OFDM-Symbol
NDP	WLAN	Null Data Packet
Protokolle	Protokolle	Neighbour Discovery Protocol
NetBEUI	Protokolle	NetBIOS Extended User Interface
NetBIOS	Protokolle	Network Basic Input/Output System
NEXT	Leitungstheorie	Near End Crosstalk

Abkürzung	Bereich	Ausgeschrieben
NFS	Protokolle	Network File System Network File Service
NIC	Normierung	Network Information Center
NIC	Hardware	Network Interface Controller
NIST	Normierung	National Institute of Standards and Technology
NLP	Ethernet	Normal Link Pulse
NLOS	WLAN	Non Line of Sight
NNTP	Protokolle	Network News Transfer Protocol
NP	Ethernet	Next Page
NRZ	Wire-Coding	Non Return to Zero
NRZ-L	Wire-Coding	Non Return to Zero Land
NRZ-M	Wire-Coding	Non Return to Zero Mark
NRZ-S	Wire-Coding	Non Return to Zero Space
NSD	WLAN	Anzahl Subcarrier für Daten
NSYM	WLAN	Anzahl der OFDM-Symbole
NTBA	WAN	ISDN: Network Termination Basis Anschluss
NTBBA	WAN	ISDN: Network-Termination-Breitband Anschluss
NTP	Protokolle	Network Time Protocol
NTPM	WAN	ISDN: Network Termination Primary Multiplex
NVP	Leitungsmessung Protokolle	Nominal Velocity of propagation (Nenn-Ausbreitungsgeschwindigkeit) Network Voice Protocol
OBSS	WLAN	Overlapping Basic Service Set
OFDM	Modulation	Orthogonal Frequency Division Multiplex
OFDMA	Modulation	Orthogonal Frequency Division Multiple Access
OID	Management	Object Identification
OS	Rechnersysteme	Operating System (Betriebssystem)
OSI	Normierung	Open Systems Interconnection
OSPF	Protokolle	Open Shortest Path First
OSPF-IGP	Protokolle	OSPF als IGP konfiguriert
OUI	MAC-Adressformat	Organizationally Unique Identifier
P	Einheiten	Power (dt.: Leistung) Wahrscheinlichkeit (probability)
PAD	Protokolle	Padding (Füller)
PAM	Modulation	Puls Amplitude Modulation
PAN	Netzwerke	Personal Area Network
PASV	FTP	Passive Kommando
PAT	Protokolle	Port Address Translation
PBCC	WLAN	Packet Binary Convolutional Code
PBSS	WLAN	Personal BSS
PBX	Telephony	Private Branch Exchange (Nebenstellenanlage)
PC	Begriffe WLAN	Personal Computer Point Coordinator
PCF	Medienzugriff	WLAN: Point Coordination Function
PCI	Schichtenmodell	Protocol Control Information
PCO	WLAN	Phased Coexistence Operation
PCP	WLAN	PBSS Control Point

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
	VLAN	Priority Code Point (Benutzer-Prioritätsinformation)
PD	PoE	Powered Device
PDE	Schichtenmodell	Protokoll Daten Einheit
PDH	Multiplextechnik	Plesiochrone Digitale Hierarchie
PDM	Modulation	Pulsdauermodulation
PDU	Schichtenmodell	Protocol Data Unit
PE	WAN	MPLS: Provider Edge Device
PER	WLAN	Packet Error Rate
PFM	Modulation	Puls-Frequenzmodulation
PHY	Schichtenmodell	Physikalische Ebene / Schnittstelle
PIFS	Mediumzugriff	Point Coordiantion Function Inter Frame Space
PiMF	Verkabelung	Pair in Metal Foil
PLCP	Schichtenmodell	Physical Layer Convergence Protocol
PLME	WLAN	Physical Layer Management Entity
PLS	Ethernet	Physical Line Signaling
PLW	WLAN	PSDU Length Word
PM	Modulation	Puls Modulation
PMA	Ethernet	Physical Medium Attachment
PMD	Ethernet	Physical Medium Dependent
PMF	WLAN	Protected Management Frames
PMK	Security	WLAN: Pairwise Master Key
PMO	Ethernet	Multi Path Push On (LWL-Stecker)
PMX	WAN	ISDN: Primärmultiplex-Anschluss
PoE	Ethernet	Power over Ethernet
POH	Ethernet	Path Overhead
POTS	WAN	Plain Old Telephone Service
PPDU	WLAN	Physical Protocol Data Unit
PPM	Modulation	Puls-Phasenmodulation
PPK	Security	WLAN: Per Packet Key
PRA	WAN	ISDN: Primary Rate Access
PRBS	Ethernet	Pseudo Random Binary Sequenz
PRF	Zufallszahlen	Pseudo-Random Function
PRI	WAN	ISDN: Primary Rate Interface
PRNG	Zufallszahlen	Pseudo-Ramdom Number Generator
PSACR	Leitungsmessung	Power Sum Attenuation to Crosstalk Ratio
PSE	PoE	Power Sourcing Equipment
PSF	WLAN	PLCP Signaling Field
PSH	TCP	Push (Flag)
PSI	Schichtenmodell	Protokoll Steuer Information
PSFEXT	Leitungsmessung	Power Sum Far End Crosstalk
PSNEXT	Leitungsmessung	Power Sum Near End Crosstalk
PSELFEXT	Leitungsmessung	Power Sum Equalized Level Far End Crosstalk
PSTN	Telephony	Public Switched Telephone Network (Öffentliches Telefonnetz)
PSK	Modulation	Phase Shift Keying
POP3	Protokolle	Post Office Protocol Version 3

Abkürzung	Bereich	Ausgeschrieben
PPP	Protokolle	Point-to-Point Protocol
PSACR	Leitungsmessung	Power Sum Attenuation Crosstalk Ratio
PSDU	Schichtenmodel	PLCP Service Data Unit
PSF	WLAN	PLCP Signaling Field
PSFEXT	Leitungsmessung	Power Sum Far End X-Talk
PSNEXT	Leitungsmessung	Power Sum Near End X-Talk
PTR	DNS-Potokoll	Pointer (für Reverse Lookup)
PWM	Modulation	Puls-Weitenmodulation
QAM	Modulation	Quadrature Amplitude Modulation
QAP	WLAN	Quality of Service Access Point
QBSS	WLAN	Quality of Service Basic Service Set
PTK	Security	WLAN: Pairwise Temporal Key
PTKSA	Security	WLAN: Pairwise Temporal Key Security Association
QAM	Modulation	Quadrature Amplitude Modulation
QAP	WLAN	QoS AP
QBSS	WLAN	QoS BSS
QoS	Protokolle	Quality of Service
QPSK	Modulation	Quadrature Phase Shift Keying
QSTA	WLAN	QoS STA
OSPF	Protokolle	Open Shortest Path First
R	Informationstheorie	Redundanz [in Bit / Symbol]
	Schaltungstechnik	Widerstand
r	Leitungstheorie	Reflexionsfaktor
R'	Schaltungstechnik	Widerstandsbelag
RA	ICMPv6	Router Advertisement
RADIUS	Security	Remote Authentication Dial in User System
RARP	Protokolle	Reverse Address Resolution Protocol
RBUFCAP	WLAN	Receive Buffer Capability
RC4	Security	Rivet Cipher 4
RD	Ethernet	Running Disparity
RDNSS	ICMPv6	Recursive Domain Name Service Server
RegTP	Normierung	Regulierungsbehörde für Telekommunikation und Post
REJ	Protokolle	Reject
RF	Ethernet	Remote Fault
RFC	Normierung	Request for Comments
RIFS	Mediumzugriff	WLAN: Reduced IFS
RIP	Protokolle	Routing Information Protocol
RIPng	Protokolle	Routing Information Protocol next Generation
RIPE	Verwaltungsgremium	Réseaux IP Européens
RIR	Verwaltungsgremium	Regional Internet Registry
RJ	Stecker	Registered Jack
RL	Leitungsmessungen	Return Loss
RM	Schichtenmodelle	Referenz Modell (z. B. ISO OSI-RM mit 7 Schichten)
RMON	Management	Remote MONitoring
RNR	Protokolle	Receive Not Ready

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
RP	Spanning Tree	Root Port
RPC	Software	Renmote Procedure Call
RR	Pprotokolle	Receive Ready
Rservices	Protokolle	Remote Services
RSN	Security	WLAN: Robust Security Network
RSOH	Ethernet	Regenerator Section Overhead
RSSI	WLAN	Received Signal Strength Indication
RST	TCP	Reset (Flag)
RSTP	Spanning Tree	Rapid Reconfiguration Spanning Tree
RSVP	WAN	MPLS: Resource Reservation Protocol
RTS	WLAN	Request To Send
RTR	Normierung	Rundfunk und Telekom Regulierungs-GmbH (Österreich)
RTT	Mediumzugriff	Round-Trip-Time
RTO	TCP	Retransmission Timeout
RU	WLAN	Resource Unit
RX	Datenübertragung	Receive / Receiver
RZ	Wire-Coding	Return to Zero
s	Einheiten	Sekunde
SABME	Protokolle	Set Asynchronous Balanced Mode Extended
SAE	Security	WLAN: Simultaneous Authentication of Equals
SAN	Netzwerke	Storage Area Network
SAP	Schichtenmodelle	Service Access Point
SBIFS	Mediumzugriff	WLAN: Short Beamforming IFS
SC	LWL-Stecker	Subscriber Connector
SDE	Schichtenmodelle	Schnittstellen Daten Einheit
SDH	Multiplextechnik	Synchronous Digital Hierarchy
SDM	Multiplextechnik	Space Division Multiplex
SDMA	Multiplextechnik	Space Division Multiplex Access
SDN	Netzwerke	Software Defined Networks
SDSL	WAN	Symmetric Digital Subscriber Line
SDU	Schichtenmodell	Service Data Unit
SFD	Ethernet	Start Frame Delimiter
SHF	Frequenzbereiche	Super High Frequency (10 – 1 cm / 3 – 30 GHz)
SIFS	Mediumzugriff	Short Inter Frame Space
SIG	Normierung	Bluetooth: Special Interest Group
	WLAN	Signanlisierungs-Feld
SIIT	Protokolle	Stateless IP/ICMP Translator
SIMO	WLAN	Single Input Multiple Output
SIP	Protokolle	Session Initiation Protocol
SISO	WLAN	Single Input Single Output
SLAAC	IPv6	Stateless Address Auto Configuration
SLRC	Mediumzugriff	WLAN: Station long retry count
SM	LWL	Single Mode (Faser)
	Protokolle	Subnet Mask
SME	WLAN	Station Management Entity
SMDS	MAN	DQDB: Switched Multi-Megabit/Metropolitan Data Service

Abkürzung	Bereich	Ausgeschrieben
SMI	Management	Switch of Management Information
SMON	Management	Switch MONitoring
SMTP	Protokolle	Simple Mail Transfer Protocol
SNAP	Protokolle	Subnet Access Protocol
SNAT	Protokolle	Source Network Address Translation
SNMP	Protokolle	Simple Network Management Protocol
SNR	Datenübertragung	Signal to Noise Ratio
SOA	DNS-Protokoll	Start Of Authoroty
SOHO	Anwender	Small Office Home Office
SONET	Multiplextechnik	Synchronous Optical Network Technology
SPC	LWL-Stecker	Super Physical Contact
SPF	OSPF	Shortest Path First
SPT	Brücken / Switches	Spanning Tree
SPX	Protokolle	Sequenced Packet Exchange
SRB	Routing	Source Routing Brücken
SRD	WLAN	Short Range Device
SRT	Brücken	Source Route Transparent Bridging
SS	WLAN	Spatial Stream Single Sounding (Einfaches Beamforming) Single Stream
SSAP	Ethernet	Source Service Access Point
SSB	Modulation	Single Side Band
SSD	Hardware	Solid State Disk
SSH	Security	Secure Shell
SSL	ProtokSecurityolle	Secure Socket Layer
SSRC	Mediumzugriff	WLAN: Station short retry count
SSTP	Verkabelung	Screened Shielded Twisted Pair
ST	LWL-Stecker	Straight Tip
STA	WLAN	Station
STBC	WLAN	Space-Time Block Coding
STF	WLAN	Short Training Field
STK	Security	WLAN: STSL transient Key
STKSA	Security	WLAN: STSL transient Key Security Association
STP	Verkabelung	Shielded Twisted Pair
STM	Ethernet	Synchronous Transport Module
STSL	WLAN	Station To Station Link
STUN	Protokolle	Simple Traversal of User Datagramm Protocol
SU	WLAN	Single User
SWS	TCP	Silly Window Syndrome
SYN	TCP	Synchronise (Flag)
T	Einheiten Abtastung Einheit	Periodendauer [in s] Abtastintervall Time
TBTT	WLAN	Target Beacon Transmission Times
TC	IPv6 WLAN	Traffic Class Traffic Category

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
	Spanning Tree	Topology Change
TCI	VLAN	Tag Control Identifier
TCP	Protokolle	Transmission Control Protocol
TDD	WLAN	Time Division Duplex
TDM	Multiplextechnik	Time Division Multiplex
TDMA	Multiplextechnik	Time Division Multiplex Access
Telnet	Protokolle	Network Virtual Terminal
TETRA	Frequenzbereich	Trans European Trunked Radio
TFTP	Protokolle	Trivial File Transfer Protocol
THF	Frequenzbereich	Tremendously High Frequency (10 -1 µm / 0,3 – 3 THz)
THP	Ethernet	Tomlinson Harashima Precoder
TIA	Normierung	Telecommunication Industries Association
TIC	Protokolle	Tunnel Information and Control Protocol
TID	WLAN	Traffic Identifier
TIM	WLAN	Traffic Indication Map
TK	Begriffe Security	Telekommunikation WLAN: Temporal Key
TKIP	Security	WLAN: Temporal Key Integrity Protocol
TL	Protokolle	Typ / Längen (Feld)
TLD	DNS	Top Level Domain
TO	Verkabelung Protokolle	Terminal Outlet (Anschlussdose) Timeout
ToS	Protokolle	Type of Service
TP	Verkabelung	Twisted Pair
TPC	WLAN	Transmission Power Control
TPID	VLAN	Tag Protocol Identifier
TR	Topologie	Token Ring
TS	WLAN	Traffic Stream
TSF	WLAN	Timing Synchronisation Function
TTL	Protokolle	Time-To-Live
TTAK	Security	WLAN: TKIP-mixed transmit address and key
TU	WLAN	Time Unit
TURN	Protokolle	Traversal Using Relays around NAT
TX	Datenübertragung	Transmit / Transmitter
TXOP	WLAN	Transmit Opportunity
TXVECTOR	WLAN	Transmit Vector
UADSL	WAN	Universal Asymmetric Digital Subscriber Line
UC	Kommunikation	Unicast
UDP	Protokolle	User Datagram Protocol
U	Schaltungstechnik	Spannung
UA	Protokolle	Unnumbered Acknowledgement
U-NII	Funkfrequenzbereiche	Unlicenced National Information Infrastructure
UFTP	Verkabelung	Unshielded Foiled Twisted Pair
UHF	Frequenzbereich	Ultra High Frequency (10 – 1 dm / 0,3 – 3 GHz)
UI	Protokolle	Unnumbered Information
UL	WLAN	UP Link

Abkürzung	Bereich	Ausgeschrieben
ULA	IPv6	Unique Local Address
UMTS	Mobilfunktechnik	Universal Mobile Telecommunications System
UPC	LWL-Stecker	Ultra Physical Contact
UPnP	IPv6	Universal Plug'n'Play
URG	TCP	Urgent (Flag)
URI	WWW	Uniform Resource Information
URL	WWW	Uniform Resource Locator
URN	WWW	Uniform Resource Name
UT	Zeit	Universal Time
UTP	Verkabelung	Unshielded Twisted Pair
UWB	Funktechnik	Ultra Wide Band
v	Einheit	Geschwindigkeit (velocity)
VAN	Begriffe	Value Added Network
VCSEL	Bauteil	Vertical Cavity Surface Emitting Laser
VDS	Virtualisierung	Virtual Distributed Switch (über mehrere Hosts verteilt)
VDSL	WAN	Very High Bit Rate Digital Subscriber Line
VftsDx	Normierung	Verordnung für den Fernschreib- und Datexdienst
VHF	Frequenzbereich	Very High Frequency (10 – 1 m / 20 – 300 MHz)
VHT	WLAN	Very High Throughput Präfix für Begriffe bei IEEE802.11ac
VID	VLAN	VLAN-Identifier
VIP	VRRP-Protokoll	Virtuelle IP (Adresse)
VLAN	Netzwerke	Virtuelles Local Area Network
VLSM	Protokolle	Variable Length of Subnet Mask
VM	Virtualisierung	Virtual Machine
VMTP	Protokolle	Versatile Message Transaction Protocol
VoIP	Protokolle	Voice over IP
VoWLAN	WLAN	Voice over WLAN
VPN	Netzwerke	Virtual Private Network
VR	Virtualisierung	Virtual Reality
	VRRP-Protokoll	Virtual Router
VRF	WAN	MPLS: Virtual Routing and Forwarding Instances
VRID	VRRP-Protokoll	Virtuelle Router ID
VRRP	Protokolle	Virtual Router Redundancy Protocol
VSAT	Satellitentechnologie	Very Small Aperture Terminal
VSS	Virtualisierung	Virtual Standard Switch (auf Host begrenzt)
VTEP	Virtualisierung	Virtual Tunnel End Point
VXLAN	Virtualisierung	Virtual Extensible VLAN
WAN	Netzwerke	Wide Area Network
WDS	WLAN	Wireless Distribution System
WECA	WLAN	Wireless Compatibility Alliance
WEP	Security	WLAN: Wired Equivalence Privacy
WEPplus	WSecurityLAN	WLAN: Wired Equivalence Privacy Erweiterung von HP
Wi-Fi	WLAN	Wireless Fidelity
WIS	Ethernet	WAN Interface Sublayer
WLAN	Netzwerke	Wireless Local Area Network

Abkürzungsverzeichnis

Abkürzung	Bereich	Ausgeschrieben
WMAN	Netzwerke	Wireless Metropolitan Area Network
WIMAX	Netzwerke	Worldwide Interoperability for Microwave Access
WIN	TCP	Window Size
WPA	Security	WLAN: Wi-Fi Protected Access
WPAN	Netzwerke	Wireless Personal Area Network
WS	TCP	Window Size
WWAN	Netzwerke	Wireless Wide Area Network
WWi_SE_	WLAN	World-Wide Spectrum Efficency
WWW	Begriffe	World Wide Web
XDSL	WAN-Protokolle	Unspezifiziertes DSL
XID	Protokolle	Exchange Identifier
XLGMII	Ethernet	40 Gigabit Media Independent Interface
XML	Programmieren	Extensible Markup Language
Z _w	Leistungstheorie	Wellenwiderstand
ZWR	WAN	ISDN: Zwischenregenerator