Daten-kommunikation

Zusammenfassung

HTA Horw

Rainer Meier
Käserei
6288 Schongau
skybeam@skybeam.ch

Klasse: 4
2002 - 2006

2005-09-12

1. Inhaltsverzeichnis

1. Inhaltsverzeichnis 2
2. Schichtenmodelle 6
2.1. OSI Modell 6
2.2. TCP/IP Modell 6
2.3. Encapsulation 7
2.4. Protokolle 7
2.4.1. Schicht 1 / Physical 7
2.4.2. Schicht 2 / Data Link 7
2.4.3. Schicht 3 / Network 7
2.4.4. Schicht 4 / Transport 8
2.4.5. Schicht 5 / Session 8
2.4.6. Schicht 6 / Presentation 8
2.4.7. Schicht 7 / Application 8
2.5. Protokollfamilien 8
3. TCP/IP 9
3.1. IPv4 Header 9
3.1.1. Version 9
3.1.2. Internet Header Length (IHL) 9
3.1.3. Service Type (TOS) 9
3.1.4. Total Length 10
3.1.5. Identification 10
3.1.6. Flags 10
3.1.7. Fragment Offset 10
3.1.8. Time-to-Live (TTL) 10
3.1.9. Protocol 10
3.1.10. IP-Header Checksum 10
3.1.11. IP Source Address 10
3.1.12. IP Destination Address 10
3.1.13. Options 10
3.1.14. Padding 11
3.2. IPv4-Adressierung 11
3.2.1. Klassen 11
3.2.2. Private Adressen 11
3.2.3. Subnetting 11
3.2.4. Netzwerkadresse 11
3.2.5. Broadcast-Adresse 12
4. Internet Control Message Protocol (ICMP) 13
5. TCP Protokoll 15
5.1. Verbindungsaufbau 15

5.2. Verbindungsabbau ... 15
5.3. Header-Format ... 16
5.3.1. Source/Destination Port ... 16
5.3.2. Sequence Number ... 16
5.3.3. Acknowledgement Number ... 16
5.3.4. Data Offset ... 17
5.3.5. Reserved ... 17
5.3.6. Control Flags ... 17
5.3.7. Window Size ... 17
5.3.8. Checksum ... 17
5.3.9. Urgent Pointer ... 17
5.3.10. Options ... 17
5.3.11. Padding ... 17
6. UDP Protokoll ... 18
7. NAT/PAT ... 18
8. DHCP ... 19
9. CIDR ... 20
10. IPv6 ... 21
10.1. Adressierung ... 21
10.2. Header ... 22
11. Routing und Routingprotokolle ... 23
11.1. IP Routing-Algorithmus ... 23
11.2. Routing-Methoden ... 23
11.3. Multiprotocol Label Switching (MPLS) ... 24
11.4. Distanz Vektor Routing ... 24
11.4.1. Routing Information Protocol (RIP) ... 25
11.4.2. Interior Gateway Routing Protocol (IGRP) ... 25
11.5. Link State Routing-Protokolle ... 25
11.5.1. Open shortest Path First (OSPF) ... 25
11.6. Border Gateway Protocol (BGP) ... 26
12. Multicasting ... 27
12.1. Internet Group Management Protocol (IGMP) ... 27
12.2. Cisco Group Mangement Protocol (CGMP) ... 27
13. Ethernet ... 28
13.1. Link Layer (Layer 2) ... 28
13.2. Physikalische Medien ... 28
13.3. IEEE 802.3 / Ethernet Verfahren (CSMA/CD) ... 28
13.4. Ethernet Frame ... 28
13.5. Hubs ... 29
13.6. Switches ... 29

13.6.1. Cut-Through ... 29
13.6.2. Store-And-Forward ... 29
13.6.3. Fragment-Free ... 30
13.7. Spanning-Tree Protocol IEEE 802.1 ... 30
13.7.1. Regeln zur Bestimmen der Root-Bridge ... 30
13.7.2. Bestimmen des Root-Ports ... 30
13.7.3. Bestimmen der Designated-Bridge für jedes LAN: ... 31
14. VLAN ... 32
15. WLAN (IEEE 802.11) ... 32
15.1. Link Layer ... 32
15.1.1. Physikalische Eigenschaften ... 32
15.2. IEEE 802.11a ... 32
15.3. IEEE 802.11b ... 32
15.4. IEEE 802.11g ... 32
15.5. Ethernet-Verfahren (CSMA/CA) ... 33
15.6. Sicherheit ... 33
15.6.1. SSID ... 33
15.6.2. MAC-Filterung ... 33
15.6.3. Wired Equivalent Privacy (WEP-Verschlüsselung) ... 33
15.6.4. Wi-Fi Protected Access (WPA) ... 34
16. WAN Technologien ... 35
16.1. Integrated Services Digital Network (ISDN) ... 35
16.2. Modem ... 35
16.3. Digital Subscriber Line (DSL) ... 35
16.4. Frame Relay ... 36
16.5. Asynchronous Transfer Mode (ATM) ... 36
16.5.1. QoS ... 36
16.5.2. Virtuelle Verbindungen ... 36
16.5.3. Architektur ... 37
17. PPP ... 38
18. Computer Telophony Integration (CTI), VoIP ... 39
18.1. Architektur ... 39
18.2. VoIP - Voice over IP ... 39
18.3. Protokolle und Standards ... 39
18.3.1. H.323 (Voice over IP) ... 40
18.3.2. VoIP/POTS Integration ... 40
18.3.3. Resource ReSerVation Protocol (RSVP) ... 41
18.3.4. Differentiated Services (DiffServ) ... 41
19. Netzwerkmanagement ... 42
19.1. Simple Network Management Protocol (SNMP) ... 42

19.1.1. Netzwerk-Management 42
19.1.2. MIB - Management Information Base 42
19.2. SNMPv2 43
19.3. ASN.1 43
19.4. Remote Monitoring (RMON) 43
20. Sicherheit 44
20.1.1. Filterbasierte Firewalls 44
20.1.2. Proxybasierte Firewalls 44
20.2. VPN & IpSec 44
20.3. SSL 45
21. Abbildungsverzeichnis 47
22. Tabellenverzeichnis 47
23. Index 48

2. Schichtenmodelle

Es gibt zwei Schichtenmodelle die heute von Bedeutung sind:

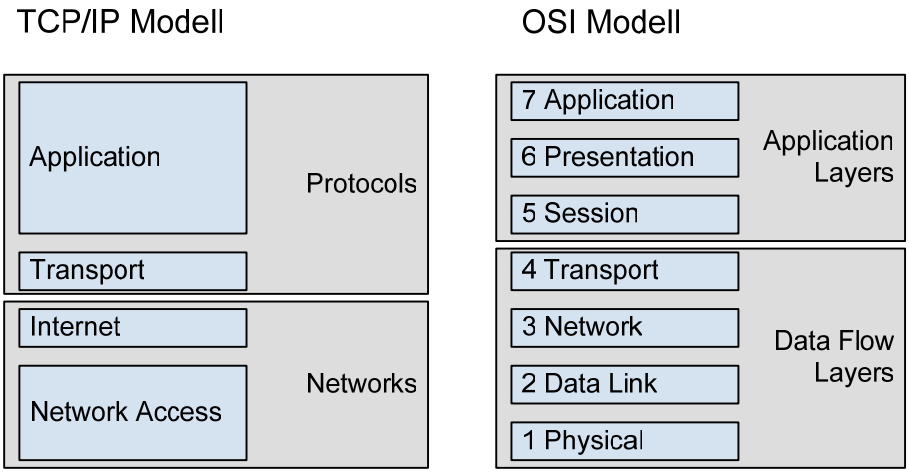


Abbildung 1 Schichtenmodelle

2.1. OSI Modell

Die Daten durchlaufen der Reiche nach die Schichten von oben nach unten auf der Sender Seite bzw. von unten noch oben auf der Empfänger Seite. Die Schichten sind dabei folgendermassen gegliedert:

Tabelle 1 OSI-Schichten

Schicht	Bezeichnung	Beschreibung
Schicht 7	Application	In der Anwendungsschicht sind Anwendungsprotokolle wie HTTP, FTP, SMTP und NNTP.
Schicht 6	Darstellungsschicht	Umwandlung von Kodierungen, Formaten und Kryptografie. Standardisieren von Datenstrukturen
Schicht 5	Session	Organisiert die Verbindungen zwischen den Endsystemen. Sicherung über Check Points um verlorengegangene Verbindungen wieder aufnehmen zu können.
Schicht 4	Transportschicht	Zuordnung der Datenpakete zu Anwendungen (z.B. TCP Ports). Sicherung der Übertragung.
Schicht 3	Netzwerk	Logische Adressierung der Endgeräte (Vermittlung). Steuert die zeitlich und logisch getrennte Kommunikation.
Schicht 2	Sicherungsschicht, Link	Sichert die Übertragung auf dem Übertragungsmedium. Funktionen zur Fehlererkennung, Fehlerbehebung und Datenflusskontrolle. Hier findet auch die physikalische Adressierung statt.
Schicht 1	Bitübertragung	Definiert elektrische, mechanische und funktionale Schnittstellen zum Übertragungsmedium. Das Übertragungsmedium selbst ist kein Bestandteil dieser Schicht.

2.2. TCP/IP Modell

Diese Modell definiert nur 4 Schichten. Diese lassen sich logisch gesehen den ISO-Schichten zuordnen:

Tabelle 2 TCP/IP Schichten

Schicht	Daten-Typ	Protokoll	OSI-Schichten

Application	Nachricht	HHTP, SMTP, Telnet, FTP	7, 6, 5
Transport	Segment	TCP, UDP	4
Internet	Datagramm (Paket)	IP	3
Network Access	Bit	TP, Coax, Fiber, Stecker	2, 1

2.3. Encapsulation

Wenn eine Applikation Daten verschickt werden diese Schicht für Schicht nach unten geschickt. Dabei werden die Daten jeweils mit einem Erweiterungsheader versehen und somit „eingepackt“. Dies nennt man Encapsulation.

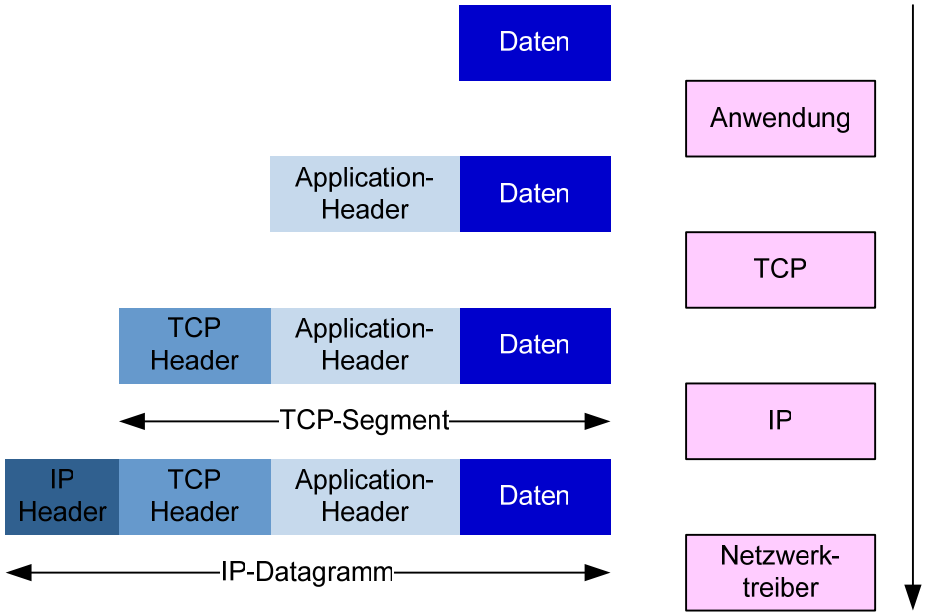


Abbildung 2 Encapsulation

2.4. Protokolle

Hier sollen ein paar wichtige Protokolle aufgelistet werden.

2.4.1. Schicht 1 / Physical

Ethernet, X.21, EIA-232/RS-232, EIA-422, EIA-485

2.4.2. Schicht 2 / Data Link

Ethernet, Token Ring LLC/MAC, X.75, V.120, HDLC, FDDI, PPP, ATM

2.4.3. Schicht 3 / Network

IPv4, IPv6, ICMP, ARP

ARP: Das Adress Resolution Protokoll wird verwendet um IP-Adressen nach MAC-Adressen aufzulösen. Werden Daten an ein Ethernet-Gerät geschickt, muss zur Adressierung die MAC-Adresse bekannt sein. Dazu wird ein ARP-Request mit der IP-Adresse des Rechners an die Broadcast-MAC-Adresse geschickt. Der Host mit der gesuchten IP-Adresse sendet dann einen ARP-Reply mit seiner MAC-Adresse zurück. Die so gefundenen Adresspaare können im ARP-Cache zwischengespeichert werden.

2.4.4. Schicht 4 / Transport

TCP: Stellt einen virtuellen Kanal zwischen zwei Endpunkten einer Netzwerkverbindung her.

UDP: Minimales, verbinungsloses Protokoll. UDP ist nicht auf Zuverlässigkeit ausgelegt.

2.4.5. Schicht 5 / Session

ISO-8326, Connection Oriented Session Service

ISO-8327, Connection Oriented Session Protocol

2.4.6. Schicht 6 / Presentation

ISO 8823, COPP - Connection Oriented Presentation Protocol

ISO 8824, ASN.1

2.4.7. Schicht 7 / Application

http, HTTPS, SMTP, DNS, FTP, NTP, UUCP, NNTP, SSH, IRC, SILC, SNMP, SIP, SDP, RTP, Telnet, Gopher, IMAP, Finger, POP-3, LDAP...

2.5. Protokollfamilien

Ein zusammenhängendes System von aufeinander aufbauenden Protokollen wird Protokollfamilie genannt.

- TCP/IP
- UDP/IP
- IPX/SPX
- NetBEUI
- SMB
- CIFS

3. TCP/IP

Die TCP/IP Protokollfamilie ist wohl die am weitesten verbreitete überhaupt.

3.1. IPv4 Header

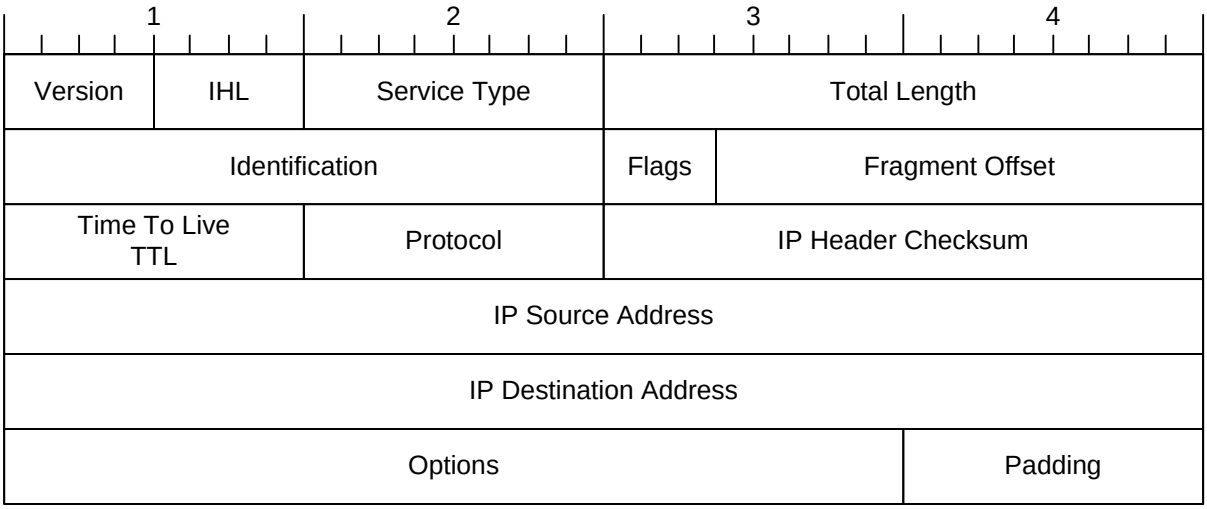


Abbildung 3 IPv4 Header

3.1.1. Version

Legt die verwendete Version de IP-Headers fest

3.1.2. Internet Header Length (IHL)

Wird wegen der variablen Länge Optionsfeldes fest und wird in 32-bit Einheiten festgelegt.

3.1.3. Service Type (TOS)

Definiert die Dienste eines IP-Datagramms. Anhand dieses Feldes können Pakete klassifiziert werden.

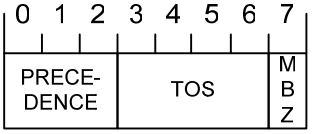


Abbildung 4 IP TOS Feld

Mit Hilfe der drei Precedence Bits werden im IP-Protokoll die in den IEEE 802.1q und 802.p-Standard definierten acht Priorisierungsgruppen (0-7) abgebildet.

Die TOS-Flags sind wie folgt aufgebaut:

1000, minimize delay

0100, maximize throughput

0010, maximize reliability

0001, minimize monetary cost

0000, normal service

Das OSPF Routing-Protokoll verwendet die selben Flags um die Datenströme zu klassifizieren, allerdings wird das TOS-Feld dann binär gelesen und anderst interpretiert.

3.1.4. Total Length

Gesamtlänge des Datagramms einschlisslich des IP-Headers und des Datenteils in Anzahl Oktetten. Die Maximalllänge von 65535 Oktetten werden von den meisten Netzen und Netzknoten nicht verarbeitet. Eine Länge von 576 Oktetten muss aber verarbeitet werden können.

3.1.5. Identification

Kennwert zur Zuordnung von Fragmenten zu einem Datagramm. Die Nummer wird im Normalfall durch eine höhere Schicht (z.B. TCP) vergeben und als Parameter an IP übergeben.

3.1.6. Flags

Bit 0: Reserviert, muss auf 0 gesetzt sein

Bit 1: (DF) Don't fragment (0: Fragmentierung unmöglich, 1: Fragmentierung möglich)

Bit 2: (MF) 0: Letztes Fragment, 1: Es folgen weitere Fragmente

3.1.7. Fragment Offset

Gibt die Lage der Fragmentdaten relativ zum Anfang des Datenblocks im ursprünglichen Datagramm an (als ein vielfaches von 8 Bytes). Beim ersten Fragment ist der Wert immer 0.

3.1.8. Time-to-Live (TTL)

Verbleibende Lebensdauer eines Datagrammes. Router verkleinern diesen Wert beim Weiterleiten. Erreicht er 0 wird das Packet verwofen.

3.1.9. Protocol

Definiert das Protokoll der nächsthöheren Schicht. Gültige Werte sind z.B. ‚1' (ICMP), ‚6' (TCP), ‚8' (EGP) oder ‚17' (UDP).

3.1.10. IP-Header Checksum

Prüfsumme des Headers (nur für den Header, nicht für die Daten). Jeder Router muss die Checksumme neu berechnen, da durch Veränderung des TTL-Feldes die Checksumme verändert wird.

3.1.11. IP Source Address

Enthält die Absender-Adresse.

3.1.12. IP Destination Address

Enthält die Zieladresse.

3.1.13. Options

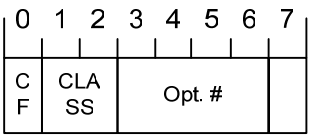


Abbildung 5 IP Optionen

CF: Legt fest, ob die Optionen beim Fragmentieren in jedes Fragment kopiert werden müssen.

CLASS:

00, Kontrolle

01, reserviert

10, Debugging

11, reserviert

Die Optionsnummer gibt den Typ der Option an und signalisiert auch das Ende der Optionen.

3.1.14. Padding

Das Packet wird mit Füllzeichen (‚00') aufgefüllt um sicherzustellen, dass es immer im 32-bit Format endet.

3.2. IPv4-Adressierung

IP-Adressen sind 32-bit Adressen, die zur besseren Lesbarkeit meist in punktierter Dezimalschreibweise mit 4 Oktetten geschrieben wird.

Beispiel:

```
11000000.10101000.00000001.00000001 (binär)
192.168.1.1 (dezimal)
```

3.2.1. Klassen

Klasse	Prefix	Netz-anteil (bits)	Host-anteil (bits)	Erste Adresse	Letzte Adresse	Netze	Hosts/Netz
A	0_2	7	24	1.0.0.0	127.255.255.255	2^7-2 =126	2^{24}-2 =16777214
B	10_2	14	16	128.0.0.0	191.255.255.255	2^{14}-2 =16382	2^{16}-2 =65534
C	110_2	21	8	192.0.0.0	223.255.255.255	2^{21}-2=2097150	2^8-2= 254

Abbildung 6 IP-Klassen

Zusätzlich gibt es noch die D-Klasse. Dabei handelt es sich um Multicast-Adressen im Bereich 224.0.0.0 – 239.255.255.255. Die noch fehlenden E-Klasse Adressen (240.0.0.0 – 254.255.255.255) sind reserviert.

Das gesamte 127.0.0.0 A-Klasse-Netz hat eine Spezielle funktion (localhost).

3.2.2. Private Adressen

Einige Adressbereiche sind sogenannte „private" Netze. Diese Adressen werden im Internet nicht geroutet. Somit können sie in lokalen Netzen nach Belieben verwendet werden und selbst bei einer versehentlichen Internet-Verbindung entstehen keine Adresskonflikte.

10.0.0.0 bis 10.255.255.255 (A-Klasse)

172.16.0.0 bis 172.31.255.255 (B-Klasse)

192.168.0.0 bis 192.168.255.255 (C-Klasse)

3.2.3. Subnetting

Durch verwendung von Subnetz-Masken kann ein Netz weiter in kleinere Netze aufgeteilt werden. So ist es kaum sinnvoll 16777214 Hots in einem einzigen A-Klasse-Netz zu verwalten. Dazu wird die Netzmaske um weitere Bits erweitert.

3.2.4. Netzwerkadresse

Die Netzwerkadresse kann errechnet werden indem man die Netzmaske logisch UND-verknüpft mit der IP-Adresse:

```
192.168.  1.240 -> 1100 0000 . 1010 1000 . 0000 0001 . 1111 0000
255.255.255.128 -> 1111 1111 . 1111 1111 . 1111 1111 . 1000 0000 (UND)
192.168.  1.128 -> 1100 0000 . 1010 1000 . 0000 0001 . 1000 0000
```

3.2.5. Broadcast-Adresse

Die Broadcast-Adresse eines Netzes kann bestimmt werden indem man die Netzmaske invertiert und mit der IP-Adresse logisch ODER-verknüpft:

```
255.255.255.128 -> 1111 1111 . 1111 1111 . 1111 1111 . 1000 0000 (INVERT)
  0.  0.  0.127 -> 0000 0000 . 0000 0000 . 0000 0000 . 0111 1111
192.168.  1.240 -> 1100 0000 . 1010 1000 . 0000 0001 . 1111 0000 (ODER)
192.168.  1.255 -> 1100 0000 . 1010 1000 . 0000 0001 . 1111 1111
```

4. Internet Control Message Protocol (ICMP)

ICMP ist ein Layer 3 Protokoll und wird für die Übermittlung von Fehler- und Informationsmeldungen verwendet. ICMP wird in IP-Pakete verpackt (Protocol-Feld: 1).

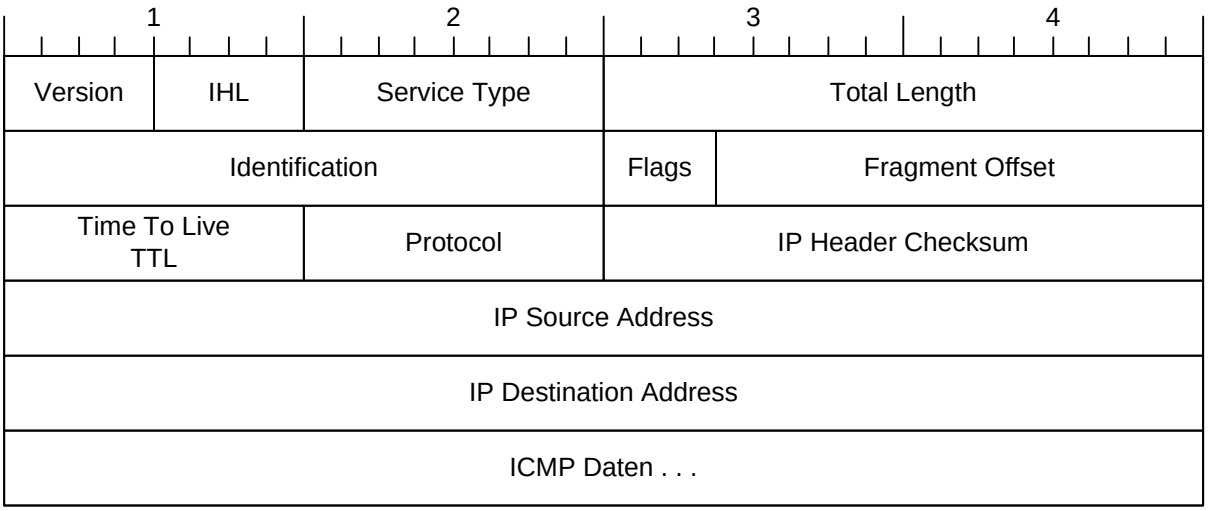


Abbildung 7 IP Header mit ICMP Daten

Hier einige ICMP-Header-Formate:

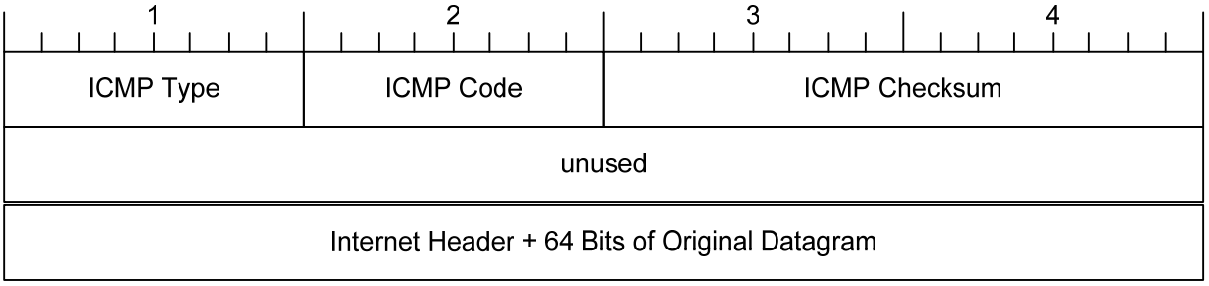


Abbildung 8 ICMP Destination Unreachable

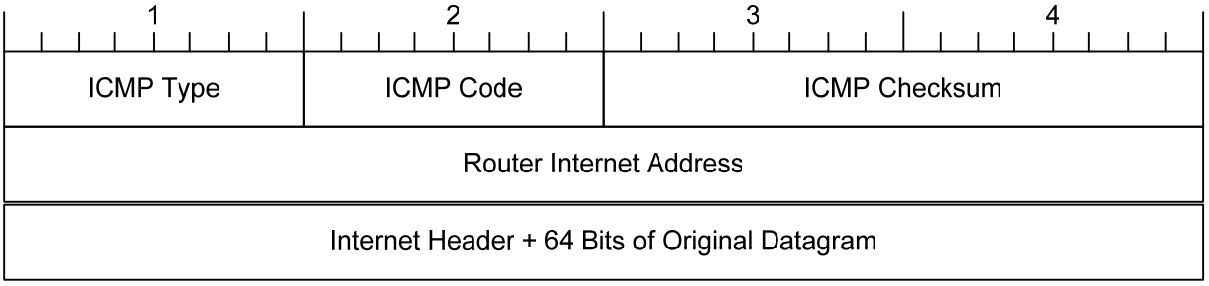


Abbildung 9 ICMP Redirect

Hier die Erläuterung der ICMP Type und Code Felder:

Typ	Code	Bedeutung
0	0	Echo reply (Ping)
3	0	Destination network unreachable
3	1	Destination host unreachable
3	2	Destination protocol unreachable
3	3	Destination port unreachable

3	4	Dont' fragment set and fragmentation needed
3	5	Source route not available
3	6	Destination network unknown
3	7	Destination host unknown
4	0	Source quench
5	0	Umleitung aller Datagramme über ein bestimmtes Netz
5	1	Umleitung aller Datagramme über einen bestimmten Router
5	2	Umleitung aller Datagramme für einen bestimmten Service-Typ und Netz
5	3	Umleitung aller Datagramme für einen bestimmten Service-Typ und Rechner
8	0	Echo request (Ping)
9	0	Route advertisement
10	0	Route discovery
11	0	TTL expired (traceroute)
11	1	Reassembly timer expired (Maximale Zeit für die Fragmentierung überschritten)
12	0	Bad IP header
13	0	Timestamp request
14	0	Timestamp reply
15	0	Information request (erfragen der Netzadresse)
16	0	Information reply
17	0	Address format request (länge der Subnet-Maske)
18	0	Address format reply

Abbildung 10 ICMP Codes

5. TCP Protokoll

TCP ist ein verbindungsorientiertes Protokoll und bietet damit eine zuverlässige Verbindung an.

Aufgaben des TCP-Protokolles:

- Prüfung des Datenflusses auf Fehler
- Sortieren der ankommenden Segmente
- TCP Header entfernen und Weitergabe an die Anwendung
- Verbindungsabbau

TCP bietet ein zuverlässiges, verbindungsorientiertes Protokoll um eine Verbindung aufzubauen, Daten auszutauschen und die Verbindung wieder abzubauen.

5.1. Verbindungsaufbau

Der Verbindungsaufbau geschieht nach folgendem Schema.

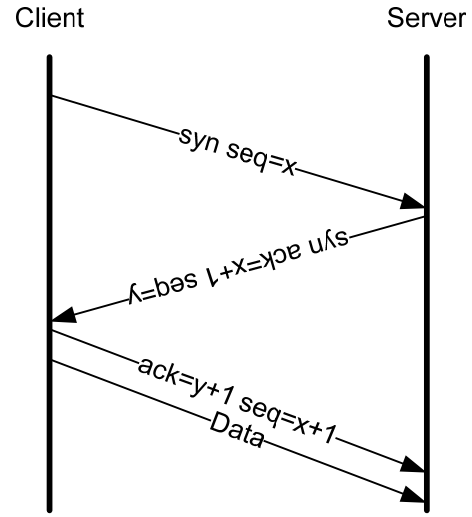


Abbildung 11 TCP 3-way Handshake

5.2. Verbindungsabbau

Wie bei jedem sauberen Verbindungsorientierte Protokoll findet natürlich auch bei TCP ein sauberer Verbindungsabbau statt.

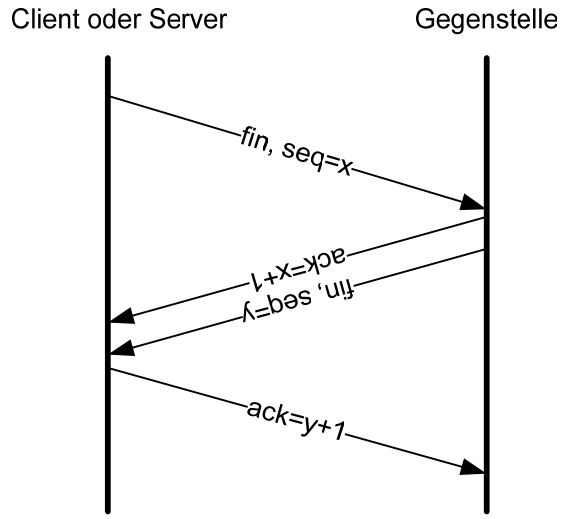


Abbildung 12 TCP Verbindungsabbau

5.3. Header-Format

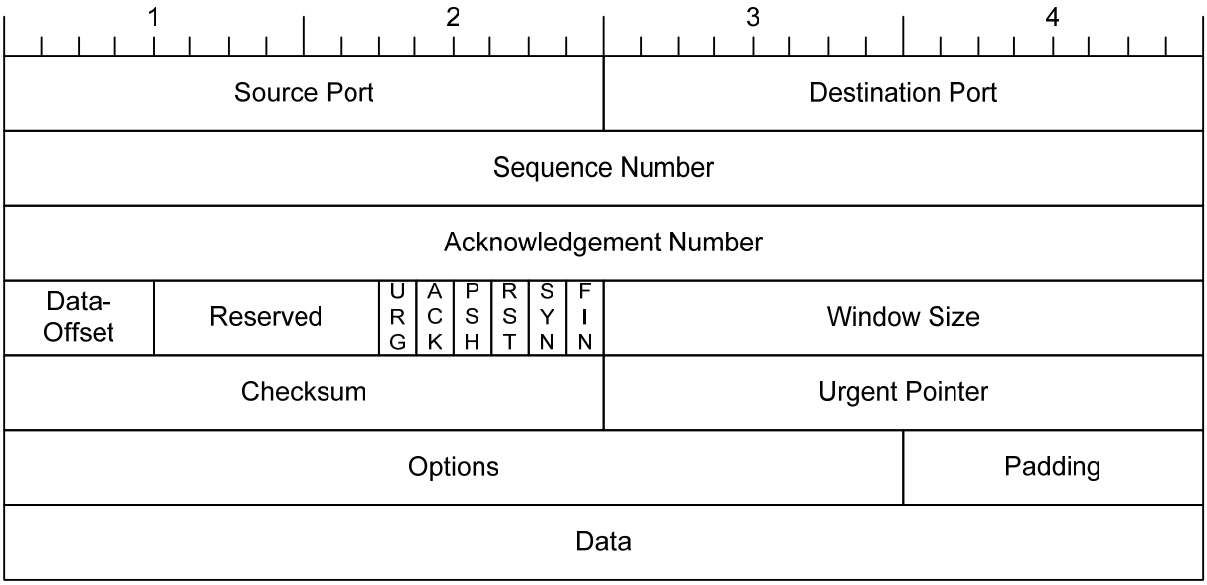


Abbildung 13 TCP-Header

5.3.1. Source/Destination Port

Beschreibt Absender-Port auf den die Antwort gesendet werden soll bzw. den Ziel-Port auf den die Pakete gesendet werden.

5.3.2. Sequence Number

Wird zur Flusskontrolle verwendet. Basiert auf einer fortlaufenden Nummerierung der Daten-Bytes. Die Sequenznummer steht für das erste Byte im Datenpaket.

5.3.3. Acknowledgement Number

Wird zur Flusskontrolle verwendet. Durch diese Nummer bestätigt der Empfänger dem Sender alle empfangenen Daten und zeigt gleichzeitig an, welche Sequenznummer als nächstes erwartet wird.

5.3.4. Data Offset

Gibt die Anzahl 32-bit Worte im TCP-Header an (also die Position an der die Daten beginnen). Dies ist wegen der variablen Länge des Optionen-Feldes nötig.

5.3.5. Reserved

Reserviert für zukünftige Anwendungen

5.3.6. Control Flags

Flags zum Aufbau, Beenden und Aufrechterhaltung von Verbindungen.

Urgent Pointer (URG): Markiert Vorrangdaten und zeig an, dass das Urgend Pointer-Feld beachtet werden muss.

Acknowledgement (ACK): Bestätigt den Empfang von Daten.

Push (PSH): Teilt dem Empfänger mit, dass die Daten sofort an das höhere Protokoll weitergegeben werden müssen. Bei der Übertragung von Telnet-Parametern wird der Push-Mechanismus immer verwendet.

Reset (RST): Der Sender will die Verbindung beenden.

Synchronisation (SYN): Eine Verbindung soll synchronisiert werden.

Final (FIN): Die Verbindung ist endgültig abgebaut, keine weiteren Daten folgen.

5.3.7. Window Size

Dient zur Flusskontrolle (Sliding-Window-Algorithmus).

5.3.8. Checksum

Die Prüfsumme wird aus dem TCP-Header und einem 96-Bit Pseudo-Header gebildet.

5.3.9. Urgent Pointer

Wird als positives Offset der Sequenznummer angegeben und markiert das Ende eines Datenblockes, der mit höherer Dringlichkeit verarbeitet werden muss.

5.3.10. Options

Hier können weitere Service-Optionen angefügt werden. Die Länge hängt von den übermittelten Optionen ab

5.3.11. Padding

Füllinformationen damit der Header ein mehrfaches von 32-bit lang wird.

6. UDP Protokoll

UDP verfügt nur über minimale Protokollmechanismen mit denen die Daten zwischen Kommunikationspartnern übermittelt werden. UDP garantiert im Gegensatz zu TCP keine Ende-zu-Ende Kontrolle. Dies hat den Vorteil, dass UDP einfach ist, wenig Overhead mit sich bringt und wenig Rechenzeit benötigt.

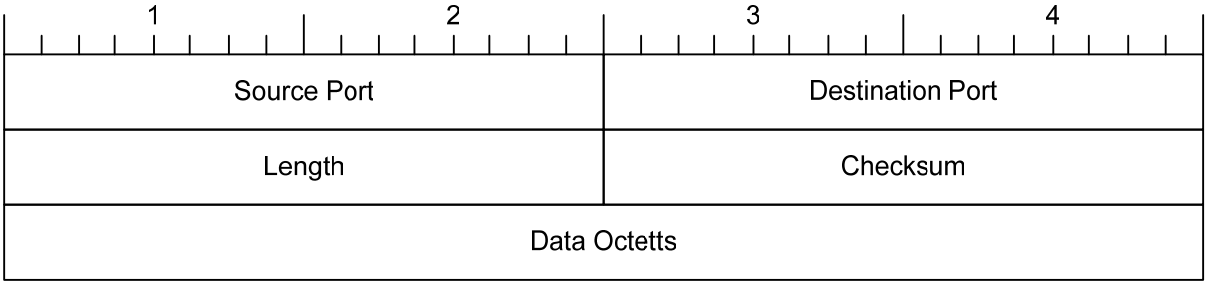


Abbildung 14 UDP-Header

Die Felder sind selbsterklärend. Speziell ist, dass die Prüfsumme optional ist und auch auf 0 gesetzt werden kann was soviel bedeutet wie ‚nicht berechnet'.

7. NAT/PAT

NAT steht für Network Adress Translation. NAT-Router können bei passierenden Paketen die Quell- oder Zieladresse ersetzen. Man unterscheidet zwischen Source-NAT (die Quelladresse wird ersetzt) und Destination-NAT (die Zieladresse wird ersetzt).

Ein Beispiel:

Die Internen PC's PC1 und PC2 verwenden die privaten IP-Adressen 192.168.1.2 und 192.168.1.3. Diese können im öffentlichen Netz nicht verwendet werden. Beim Netzübergang ins Internet kann ein NAT-Router diese Adressen im IP-Paket durch eine öffentliche IP ersetzen (z.B. 138.188.2.50) → Source-NAT. Antworten des angesprochenen Zielrechners werden dann natürlich an das NAT-Gerät geschickt. Dieses weiss aber anhand der Ziel-IP im Paket an welchen Internen Host es weitergeleitet werden muss.

Der Nachteil liegt auf der Hand. Man benötigt für jede interne Adresse eine externe, da jeder Host auf eine eigene öffentliche IP umgesetzt werden muss.

Diese Beschränkung wird durch PAT (Port Adress Translation) aufgehoben. Das Verfahren wird auch NAPT (Network Adress Port Translation) oder Masquerading genannt. Über PAT kann ein ganzes Netzwerk hinter einer einzigen (oder auch mehreren) IP-Adresse ‚versteckt' werden. Jedes Paket das den Router passiert wird verändert. Die Quell-Adresse wird durch die externe IP-Adresse des Routers ersetzt und der Absender-Port wird ersetzt. Zusätzlich führt der Router dann eine Liste (die NAT-Tabelle) in der die Ports mit den lokalen IP-Adressen verknüpft werden.

Für aussenstehende Geräte sieht es dann so aus als würde der PAT-Router alle Pakete versenden und antworten natürlich auf die entsprechende Absender-Adresse und den eingetragenen Source-Port.

Kommt ein Paket beim Router an vergleicht er den eingetragenen Port in der Tabelle und kann somit per PAT-Tabelle die IP-Adresse ausfindig machen an welche das Antwort-Paket weitergeleitet werden muss. Das Paket wird dabei nochmals verändert.

Tabelle 3 PAT/NAPT/Masquerading Tabelle

Destination	Outgoing Port	Internal IP	Internal Port
138.188.2.50	24033	192.168.1.2	5380
138.188.2.50	30150	192.168.1.10	8563

Durch diese Tabelle kann der Router feststellen an wen ein eintreffendes Paket weitergeleitet werden muss. Trifft eine Antwort auf Port 30150 vom Absender 138.188.2.50 ein so wird das Paket an

192.168.1.2:5380 weitergeleitet. Trifft vom gleichen Absender eine Antwort auf Port 30150 ein so wird das Paket auf 192.168.1.10:8563 weitergeleitet.

Die Tabelle wird dynamisch aufgebaut. Sendet ein interner Host ein Paket an einen externen so wird ein entsprechender Eintrag erzeugt. Der Outgoing Port auf dem Router kann frei gewählt werden (sofern er natürlich nicht schon belegt ist). Alle weiteren Felder können aus dem Paket entnommen werden.

Eigenarten von PAT:

Mit PAT-Routing ist es nicht möglich Pakete direkt zu einem internen Host zu schicken, da Verbindungen immer nur von innen nach aussen aufgebaut werden können. Wird ein Paket von aussen an den Router geschickt und es existiert kein entsprechender Eintrag in den Tabellen so wird das Paket verworfen.

Um trotzdem einen direkten Verbindungsaufbau von aussen her zu erlauben ist es bei den meisten Routern möglich statische Portforwardings einzurichten. Dabei werden Pakete an bestimmte Ports des Routers immer an eine fest definierte IP-Adresse weitergeleite.

Diese Eigenart kann störend sein wenn Verbindungen von aussen nach innen erwünscht oder gar benötigt werden. Beispielsweise wird beim FTP-Protokoll eine zweite Datenverbindung für den Dateitransfer erstellt. Diese Verbindung wird dynamisch aufgebaut und benutzt zu allem Übel auch noch dynamisch zugewiesene Ports. Im FTP Aktiv-Modus wird die Verbindung vom Server auf den Client erstellt, was bei einem dazwischengeschalteten PAT-Router natürlich fehlschlägt, da dieser nicht weiss an wen er das Paket weiterleiten soll. Um dieses Problem zu umgehen wurde der Passive-Modus eingeführt, bei der auch die Daten-Verbindung vom Client initialisiert wird. Dies hilft aber nur, solange der Server nicht hinter einem PAT-Router steht oder gar beide Teilnehmer, dann würden beide Modi versagen.

Abhilfe bieten da nur PAT-Router mit Stateful Packet Inspection. Diese müssen dann bis auf Layer 7 arbeiten und die entsprechende Server-Client Kommunikation analysieren. Dadurch wird es dann möglich die ankommenden Pakete richtig zu interpretieren und auch entspreched weiterzuleiten. Dies ist aber sehr aufwändig und teuer.

8. DHCP

Das Dynamic Host Configuration Protocol dient zum automatischen Konfigurieren von Netzwerk-Hosts. Dazu schickt ein Client eine DHCPDISCOVER Nachricht und wartet auf eine Antwort. Darauf kann ein DHCP-Server eine DHCPOFFER Nachricht schicken. Der Client entscheidet sich dann für eine der erhaltenen Offerten und sendet eine DHCPREQUEST Nachricht an diesen Server. Dieser quittiert dies mit einer DHCPACK Nachricht.

DHCP kann nicht nur zur Zuweisung von IP-Adressen verwendet werden. Auch weitere Parameter wie Subnetz-Maske, Gateway, DNS-Server, DNS-Prefix usw. können darüber konfiguriert werden.

9. CIDR

Classless Interdomain Routing (CIDR) beschreibt einen Versuch die Routing-Tabellen in Backbones zu verkleinern. Das Problem dabei ist, dass es nur funktioniert wenn viele zusammenhängende Netze an einem Interface erreichbar sind. Durch geschickte Wahl der Subnetz-Maske können ganze Netz-Gruppen auf einmal adressiert werden.

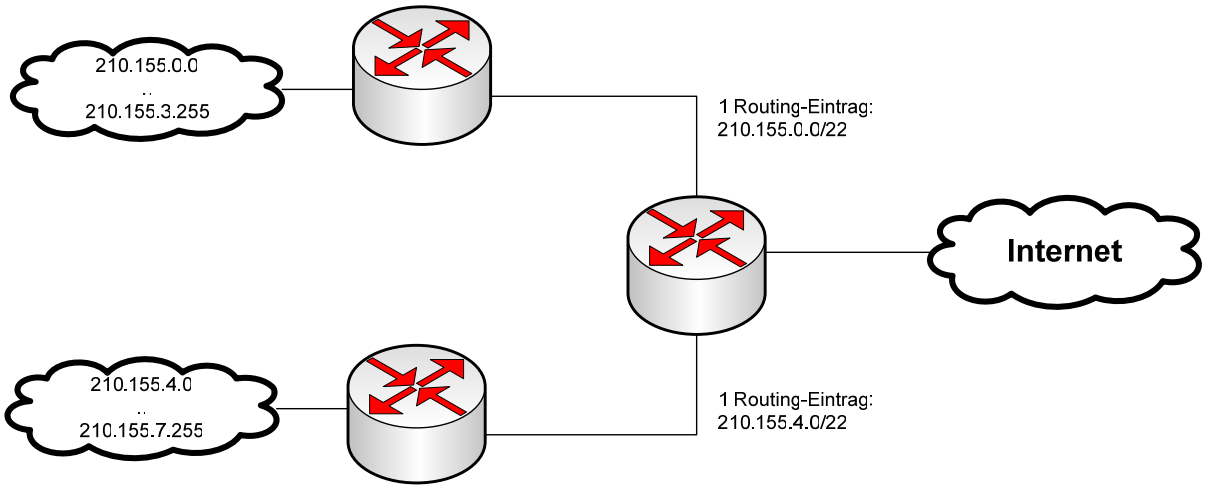


Abbildung 15 CIDR Routing (Supernetting)

10. IPv6

Die auffälligste Neuerung auf den ersten Blick sind die 128-bit langen Adressen die in 16-bit grossen Hexadezimalen Zahlen dargestellt werden die durch Doppelpunkt voneinander getrennt werden. Um die Adressen weiter zu verkürzen können Folgen von 0 durch zwei Doppelpunkte abgekürzt werden. Somit wird die Schreibweise für die Localhost-Adresse sogar kürzer als bei IPv4:

```
::1
```

10.1. Adressierung

IPv6-Adressen werden nicht mehr in Klassen eingeteilt sondern in sogenannte Adress-Typen:

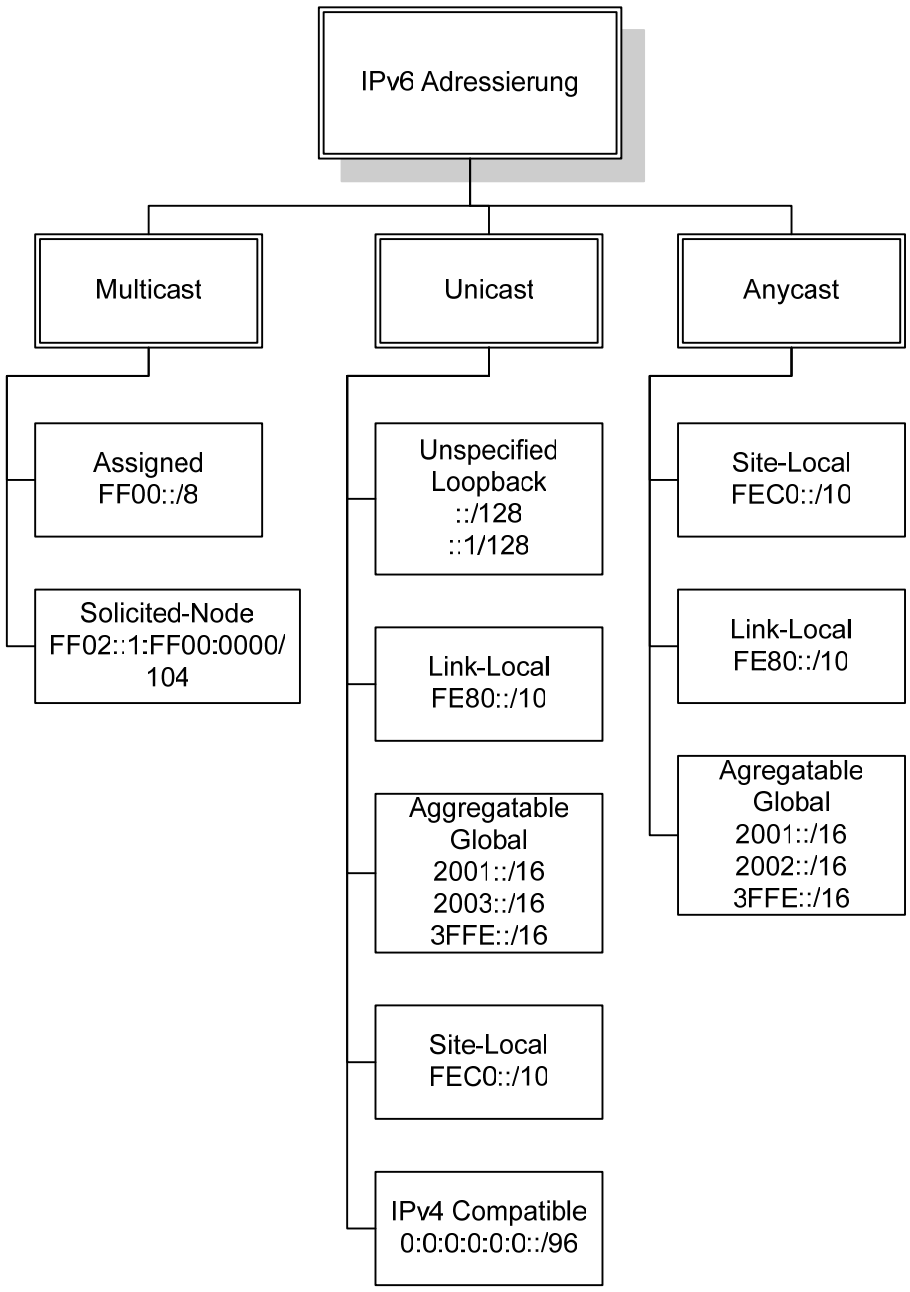


Abbildung 16 IPv6 Adress-Typen

10.2. Header

Der IPv6 Header ist trotz der 4 mal so langen Adressen nur doppelt so lange. Dies dank der Tatsache, dass die häufig unbenutzten Felder des IPv4 Headers konsequent entfernt wurden. Dafür können viel einfacher neue Optionen eingefügt werden.

Wichtige Änderungen gegenüber IPv4:

- Keine Prüfsummen mehr im Header (Fehlerkontrolle durch TCP)
- Fragmentierung durch Sender, nicht mehr durch das Protokoll selbst
- Keine Subnetz-Adressierung mehr
- Host- und Netzadresse eines Netzknotens kann automatisch generiert werden

11. Routing und Routingprotokolle

11.1. IP Routing-Algorithmus

Der Folgende Algorithmus muss von jedem IP-Fähigen Gerät implementiert werden. Nicht nur von Routern.

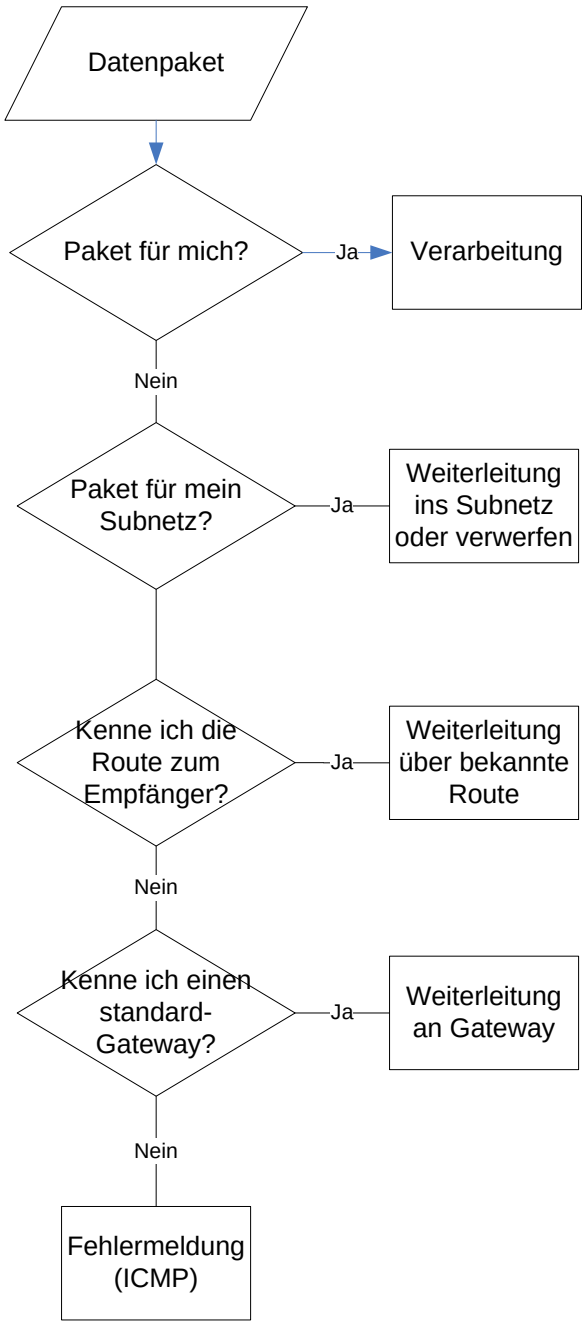


Abbildung 17 IP Routing Algorithmus

11.2. Routing-Methoden

- Statisches Routing, unabhängig von Kosten, Zustand und Geschwindigkeit der Verbindungen.
- Distance Vector Routing-Protokolle: Versenden von Teilen der Routing-Tabelle (Distance-Vector Tabelle) an die Nachbar-Router. Die einzelnen Rouoter kennen nicht die vollständige Topologie (nur Next Hop Infomrationen).

- Link State Routing-Protokolle: Versenden von Link State Advertisements an alle Router innerhalb eines Bereiches. Vollständige, identische Topologie-Information in allen beteiligten Routern.

11.3. Multiprotocol Label Switching (MPLS)

MPLS arbeitet unterhalb der IP-Schicht und kann das Routing deutlich beschleunigen. Dies geschieht indem den Paketen Labels hinzugefügt werden. Anhand dieser Labels kann dann ein Paket weitergeleitet werden (Paket Switching). Switching ist im Gegensatz zu Routing hardware-basierend und dadurch viel schneller da die Pakete auch nicht bis auf Layer 3 ausgepackt werden müssen um das Ziel festzustellen.

MPLS stellt QoS zur Verfügung und unterstützt IP, ATM und Frame Relay und ist unabhänig zu Layer 2 und 3 des Schichtenmodells.

Funktionsweise:

- Sobald ein Paket ein MPLS-Netzwerk betritt wird die Zieladresse (bzw. Weg zum Ziel) und das entsprechende Label dazu in der Routingtabelle gesucht
- Alle Hops im MPLS-Netzwerk suchen nun ihrerseits das nächste Ziel und das neue Label

Ein MPLS-Netzwerk besteht aus Label Edge Routern (LER) und Label Switch Routern (LSR). Die Switch Router leiten dabei Pakete innerhalb des Netzes weiter und die LER stehen am Netzübergang (Eintritts- und Austrittspunkt). Die LER verbinden das MPLS-Netzwerk mit ATM, Frame Relay, Ethernet...).

Über das Label Distribution Protocol (LDP) wird der Pfad durch das Netzwerk erstellt und die Ressourcen reserviert. Der Label Switch Path (LSP) spezifiziert den Pfad durch das MPLS-Netzwerk durch hop-by-hop Routing oder explizites Routing.

Ablauf einer MPLS-Verbindung:

- Zuerst wird der Label Switch Path zwischen den beiden end-Routern aufgebaut. Der Aufbau dieses LSP ist Topologie-Abhängig und kann beispielsweise über IGP oder BGP erfolgen. Ausserdem gibt es Request-basierende Methoden die mit speziellen, dynamischen Signalisierungsprotokollen arbeiten
- Jeder Router auf dem Weg schreibt die Route in die Label Information Base (LIB). Dadurch wird ein verbindungsorientierter Weg zwischen den zwei LER erstellt (LSP)

Vorteile von MPLS:

- Sehr schnelle Paket-Weiterleitung
- Bandbreiten-Reservierung
- Protokollunabhängi
- Prioritäten können vergeben werden
- VPN Funktion (MPLS Tunneling)
- Traffic Engineering
    - Effiziente Verteilung auf verfügbare Ressourcen
    - Kontrollierter Gebrauch von Ressourcen
    - Schnelle Reaktion auf eine Änderung der Netztopologie

11.4. Distanz Vektor Routing

Distance-Vector Routing-Protokolle funktionieren nach dem Prinzip “Teile deinen Nachbarn mit, wie du die Welt siehst”. Einige Distance-Vector Routing-Protokolle. Dabei werden teile der Routing-Tabelle (Distance-Vector Tabelle) an die Nachbar-Router verschickt.

Die Router haben dabei keine vollständigen Topologie-Informationen

11.4.1. Routing Information Protocol (RIP)

Ein dynamisches Routing-Protokoll welches UDP verwendet und mit dem Distanz-Vektor-Algorithmus arbeitet. RIP verwendet als Metrik nur den Hop-Count.

Die Router tauschen untereinander die Distance-Vector Tabellen der jeweiligen Nachbarn aus. Passiert ein RIP-Paket ein Router so erhöht dieser die Metrik um eins (für sich selbst) und leitet das Paket weiter. Erreicht die Metrik 15 so wird das Paket verworfen (z.B. wenn das Paket im Kreis läuft). Dies nennt man „Counting to Infinity".

RIP ist nur für kleinere Netze (maximal 15 Hops) geeignet. Ausserdem verursacht es recht hohe Netzlast bei grossen Netzen. Weitere Einschränkungen sind schlechte Subnetz-Unterstützung und fehlende Authentifizierung. RIP wird immer mehr von OSPF abgelöst.

RIP2 Erweiterungen:

- Unterstützung variabler Subnetzmasken
- Unterstützung von CIDR/Supernetting
- Unterstützung eines authentifizierten Austauschs von Routing-Informationen

11.4.2. Interior Gateway Routing Protocol (IGRP)

Cisco-proprietäres Distanz-Vektor Routing-Protokoll. Wird von Routern innerhalb von autonomen Systemen verwendet.

Der Maximale Hop-Count beträgt 255. Routing-Metriken sind die zur Verfügung stehende Bandbreite, die Verzögerung (Latency) die Zuverlässigkeit und die Auslastung. Standardmässig wird die Metrik aus Bandbreite und Verzögerung gebildet.

EIGRP ist der von Cisco bevorzugte Nachfolger von IGRP und kombiniert die Vorteile von Distanz-Vektor Routing-Protokollen mit denen von Link-State Routing-Protokollen. EIGRP kann auf Layer-3 Protokollen aufsetzen und kann insbesondere bei Netzänderungen diese schnell erkennen und die Routen anpassen.

11.5. Link State Routing-Protokolle

Verschiedene Metriken werden verwendet. Jeder Knoten weiss wie er seine direkt verbundenen Nachbarn erreichen kann (hat aber keine komplette Sicht über das Gesamte Netzwerk). Die Informationen werden über sogenannte LSP ausgetauscht. Diese beinhalten die folgenden Informationen:

- ID des Knotens, der das LSP erzeugt hat.
- Eine Liste der direkt verbundenen Nachbarn mit den Kosten der Verbindungsleitung
- Eine Sequenznummer. Falls ein Knoten ein LSP mit einer kleineren Kennung erhält muss dieser LSP älter sein und kann verworfen werden.
- Lebensdauer für dieses Paket.

Link-State Routingprotokolle tauschen nur die jeweiligen Änderungen und nicht immer ihre gesamten Routing-Informationen aus.

11.5.1. Open shortest Path First (OSPF)

Ist ein dynamisches Routing-Protokoll innerhalb eines autonomen Systems. OSPF verwendet die Kosten als Metrik und kann bei gleichen Kosten lastverteilt arbeiten.

Vorteile:

- Für grosse Netzwerke geeignet.
- Status wird meist aus mehreren Kriterien berechnet.
- Benutzt einfache Authentifizierung.
- Setzt kurze Datagramme ein.

- Realisiert Lastverteilung.
- Kennt grobe Sicht durch „zuverlässiges Fluten“ (verteilen der Link-State Pakete an alle Knoten).
- Hello Pakete prüfen, ob Nachbar noch erreichbar ist.

11.6. Border Gateway Protocol (BGP)

BGP ist ein Protokoll für das Routing zwischen mehreren Autonomen Systemen (AS). BGP arbeitet nach dem sogenannten Distance-Path-Algorithmus (nicht zu verwechseln mit dem Distance-Vector Algorithmus) und basiert auf External Gateway Protocol (EGP), hat aber einige Vorteile:

- Verwendung von alternativen Routen zw. Zwei Domänen bzw. AS
- Kann Endlosschleifen Vermeiden und erkennen
- Nur bei Updates werden Meldungen verschickt
- Retransmission

12. Multicasting

Multicast dient zum Übertragen eines Datenstromes an n Emfänger. Als Transport-Protokoll wird UDP verwendet.

Einige Eigenschaften:

- Unidirektional
- Kein Feedback
- Kein TCP!
- Keine Fehlerkorrektur
- Keine Congestion Control
- Pakete können doppelt ankommen
- Pakete könne verloren gehen
- Pakete können in falscher Reihenfolge ankommen

12.1. Internet Group Management Protocol (IGMP)

Ist eine Erweiterung von IP um IP-Multicasting zu ermöglichen. IGMP wird von IP wie ein Protokoll der höheren Schicht behandelt, ist aber selber ein Layer-3 Protokoll. IGMP verwaltet dynamische Gruppen. Die Verwaltung findet in den Routern statt. Damit IGMP funktioniert müssen alle Router zwischen Sender und Empfänger IGMP unterstützen.

Die Router fragen im Netz durch sogenante „Host Membership Queries“ nach Mitgliedern einer Gruppe. Die Hosts antworten mit einem „Host Membership Report“.

12.2. Cisco Group Mangement Protocol (CGMP)

Bei VLANs sorgt das für die Kommunikation zwischen Routern und LAN-Switches aktivierte CGMP dafür, dass die IP-Multicast-Pakete nicht zu allen Switch-Ports eines VLAN (wie für Multicast-Pakete sonst allgemein üblich) gesendet werden, sondern nur zu den Switch-Ports, an denen sich mindestens ein IP-Multicast Teilnehmer befindet.

13. Ethernet

Ethernet ist die am weitesten verbreitete physikalische Netzwerkstruktur für kleinere bis mittelgrosse Netze/Netzabschnitte.

13.1. Link Layer (Layer 2)

Setzt auf dem Physical Layer auf und fasst die Daten zu sogenannten Frames zusammen. Zur Adressierung werden 48-bit lange MAC-Adressen benutzt. Ausserdem wird auf diesem Layer eine Flusskontrolle (Flow Control) implementiert. Ausserdem findet eine Error Detection (CRC) und Error Correction (ECC) statt.

13.2. Physikalische Medien

- 10Base5: 10Mbps, Koaxial-Kabel (Thick Ethernet), Bustopologie, max. 500m, Abschlusswiderstände (50 Ohm), 100 Geräte pro Segment, max. 50m pro Stichleitung.
- 10Base2: 10Mbps, Koaxial-Kabel (Thin Ethernet), Bustopologie, max. 185m, Abschlusswiderstände (50 Ohm), 30 Geräte pro Segment.
- 10BaseT, 10Mbps, Twisted Pair Kabel (UTP), Sterntopologie über Hubs/Switches, max. 100m zwischen Hub und Host, 802.3i
- 100BaseT, 100Mbps…
- 1000BaseT, 1000Mbps…

13.3. IEEE 802.3 / Ethernet Verfahren (CSMA/CD)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) bezeichnet ein Verfahren bei dem mehrere Geräte auf das selbe physikalische Medium zugreifen und dabei Kollisionen entdecken können. Dazu hören die Geräte das Medium ab und warten auf ein Freiwerden (Carrier Sense). Dann beginnen die Geräte zu senden und hören dabei auf Kollisionen (Collision Detection). Tritt eine Kollision auf wird ein sogenanntes JAM-Signal gesendet. Das Paket muss dann erneut gesendet werden. Häufige Kollisionen beeinflussen bei stark belasteten Netzwerken die Perofrmance.

Der Round Trip Delay (RTD) entspricht der Summe aller Verzögerungen auf dem Hin- und Rückweg eines Signals. Die Signallaufzeit beschränkt auch die maximale Ausdehnung des Netzes. Sind diese zu lang kann nicht mehr sichergestellt werden, dass eine Kollision auch erkannt werden kann bzw. es ist möglich, dass eine Station am gegenüberliegenden Ende des Netzes zu senden beginnt weil das Signal noch nicht angekommen ist und somit eine Kollision auftritt. Der entfernte Rechner kann unter Umständen die Kollision dann auch gar nicht mehr erkennen.

13.4. Ethernet Frame

Ethernet ist ein paketvermittelndes Netzwerk. Die übermittelten Pakete werden Frames genannt:

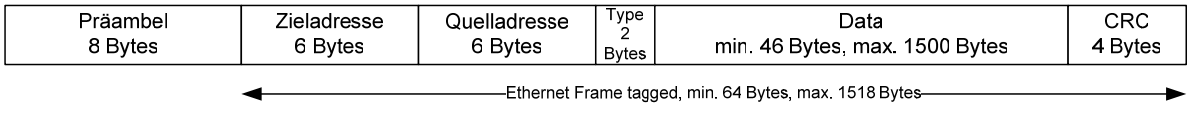


Abbildung 18 Ethernet Version 2.0 Frame

Die Felder erfüllen folgende Funktion:

- Alternierende Bitfolge von 8 Bytes um Geräte auf eine eingehende Übertragung vorzubereiten. Das abschliessende, letzte Byte endet zwei binären 1.
- Ziel- und Quell- MAC Adresse. Identifiziert das Ziel bzw. die Quelle.
- Type Feld: Identifiziert das Protokoll der nächsthöheren Schicht (z.B. 0x0800 = IPv4, 0x0806 = ARP, 0x86DD = IPv6).

- Data: Enthält die Nutzdaten. Sind diese kleiner als 46 Byte muss ein PAD-Feld angehängt werden.
- CRC: Prüfsumme über das gesamte Ethernet-Frame

Beim Einsatz von VLAN's kommt das sogenannte Tagged-Frame zum Einsatz:

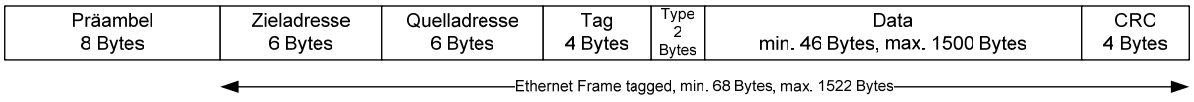


Abbildung 19 Ethernet Version 2.0 Tagged-Frame

Dieser Frame-Typ beinhaltet zusätzlich noch ein 4 Bytes langes Tag Feld welches das Frame einem VLAN zuordnet.

13.5. Hubs

Hubs werden verwendet um eine Sterntopologie aufzubauen. Dabei nimmt ein Hub Übertragungen auf einem Port entgegen und sendet sie an alle anderen Ports weiter.

Dabei gibt es aktive und passive Hubs. Die aktiven Hubs werden auch als Multiport-Repeater bezeichnet, da sie die Signale beim Weiterleiten aktiv verstärken.

Beim Aufbau einer Netzwerktopologie ist auf die 5-4-3-Regel zu achten: Innerhalb eines Übertragungsweges zwischen zwei beliebigen Endstationen dürfen maximal fünf Kabelsegmente auftauchen, also höchstens vier Repeater eingestzt sein. Von den fünf Segmenten dürfen maximal drei mit Endstationen versehen sein.

13.6. Switches

Switches sind „intelligente Hubs". Anstatt alle Datenpakete auf alle Ports zu schicken merken sich die Switches anhand der MAC-Adressen welche Geräte an einem Port angeschlossen sind und leiten die Pakete nur an diesen weiter. Dadurch wird auch an jedem Switch-Port eine eigene Collision-Domain erzeugt.

Wichtige Kenndaten für einen Switch sind die Grösse des ARP-Caches (um sich die angeschlossenen Geräte merken zu können), die interne Bandbreite (Backplane) und die Latenz.

Die Backplane-Geschwindigkeit gibt an wie viele „Ströme" der Switch maximal verarbeiten kann. Ist es möglich zwischen jeweils zwei Ports in beiden Richtungen die Volle Übertragungsrate auszunutzen spricht man von einem non-blocking Switch.

Es gibt dabei unterschiedliche Switching-Verfahren wie Cut-Through, Store-and-Forward, Adaptive-Cut-Through und FragmentFree-Cut-Through.

Im folgenden werden einige Verfahren erklärt.

13.6.1. Cut-Through

Der Switch analysiert bereits die Ethernet-Frames, bevor sie vollständig eingetroffen sind. Hat er die Ziel-Adresse identifiziert wird das Frame schon am Ziel-Port ausgegeben. Die Latenz, die Verzögerungszeit zwischen Empfangen und Weiterleiten eines Frames ist äusserst gering.

Das Cut-Through-Verfahren verzichtet auf die vollständige Analyse der Frames, wobei fehlerhafte oder beschädigte Frames unerkannt bleiben und ungehindert weitergeleitet werden. Obwohl dieses Verfahren sehr schnell ist, kann es auch zu einer Belastung des Netzwerkes führen, weil defekte Ethernet-Frames nochmals übertragen werden müssen.

13.6.2. Store-And-Forward

Der Switch speichert das Ethernet-Frame und leitet es erst weiter nachdem es vollständig angekommen ist. Somit werden ungültige und defekte Frames gar nicht erst weitergeleitet. Der Nachteil liegt dabei natürlich in einer erhöhten Latenzzeit.

13.6.3. Fragment-Free

Eine selten genutzte Variante ist das so genannte Fragment-Free-Switching. Es arbeitet wie Cut-through, nur dass es die Daten erst weiterleitet, wenn die ersten 64 Byte des Pakets fehlerlos angekommen sind. Der Grund für dieses Verfahren ist, dass die meisten Fehler und alle regulären Kollisionen innerhalb dieses Zeitfensters auftreten.

13.7. Spanning-Tree Protocol IEEE 802.1

Das Ziel dieses Protokolles ist die Verhinderung von Schlaufen auf Layer 2 Ebene in LANs.

Durch zwei oder mehrfache Verbindungen im geswitchten Ethernet können doppelte Frames entstehen. Diese können mehrfach beim Empfänger ankommen.

Spanning-Tree spannt das physikalische Netzwerk zu einem logischen Baum auf, in dem zu jedem Ziel nur ein einziger Weg existiert. Die Switches bzw. Bridges kommunizieren in einem Netzwerk mit Hilfe von BPDUs (Bridge Protocol Data Unit). Diese Konfigurationspakete werden als Multicast-Frames an die MAC-Adresse 01-80-C2-00-00-10 geschickt. Diese Frames werden alle 2 Sekunden an die nächst tiefer gelegene Station (Bridge oder Switch) übermittelt. Auf diese Weise werden parallele Strecken erkannt und die optimale Strecke ermittelt. Man spricht dann von Prioritäten bzw. Wegkosten, die die Datenrate und Entfernung berücksichtigt. Ports mit nichtbevorzugten Strecken werden dann deaktiviert.

Fällt die bevorzugte Strecke aus, bleibt auch das BPDU-Frame aus, was zu einer Reorganisation des Netzwerkes führt. Bei komplizierten Verschachtelungen wird der Baum (Spanning Tree) neu berechnet, was zu einer Verzögerung von bis zu 30 Sekunden oder mehr dauern kann. Erst danach kann auf der redundanten Strecke die Übertragung fortgesetzt werden.

13.7.1. Regeln zur Bestimmen der Root-Bridge

Nach dem Aufstarten (power-up):

- Alle Anschlüsse sind im Blocking Status und jede Bridge versucht Root Bridge zu werden durch aussenden von Konfiguration-BPDUs
- Bridge mit kleinstem Wert der Bridge-ID wird Root-Bridge

Bridge-ID: Prioritätsfeld und Teil der MAC-Adresse des Ports mit kleinster Adresse.

Bei der Initialisierung geht jede Bridge davon aus, dass sie Root- Bridge ist.

Austausch der IDs erfolgt über regelmässig gesendete Konfiguration-BPDUs.

Nach der Bestimmung der Root Bridge:

Aussenden von Konfigurations-BPDUs wird exklusiv durch die Root-Bridge ausgelöst.

Konfiguration-BPDUs enthalten folgende Informationen:

- welche Bridge ist gerade Root
- welche Anschlusskosten existieren zur Root-Bride (Root-Path-Cost)
- Die Bridge-ID und Anschluss-ID der sendenden Bridge

13.7.2. Bestimmen des Root-Ports

- Erkennt eine Bridge, dass sie nicht Root-Bridge ist, so muss sie einen Anschluss in Richtung Root-Bridge bestimmen.
- Berechnung der Pfadkosten zur Root-Bridge (Bestimmung der tiefsten Pfadkosten zur Root-Bridge)
    - Berechnung basiert auf der Summe der Root-Path-Costs (welche aus den empfangenen BPDUs gelesen werden) und die Portkosten des Interfaces, durch welche das BPDU empfangen wurde. Die Portkosten werden dem BPDU addiert und das BPDU wird über alle anderen Ports weitergeschickt.
    - Übertragungsgeschwindigkeit kann als Kostenfaktor dienen (1000/xMbps)

- Selektion des Ports mit den geringsten Kosten, Dieser Anschluss wird der Root-Port. Bei gleichen Kosten entscheidet die Port-ID (Anschlussnummer), tiefer bedeutet besser!

Eine Designated Bridge wird für jedes LAN Segment bestimmt

13.7.3. Bestimmen der Designated-Bridge für jedes LAN:

Ein Netz kann mehrere Root-Ports besitzen. Es wird derjenige mit den geringsten Kosten als Designated-Port des LANs gewählt, also mit den tiefsten Root-Path-Cost an ihrem Root-Port.

Die Bridge wird damit zur Designated Bridge. Sind zwei oder Mehr Wege gleich „teuer“ so entscheidet die Bridge-ID. Es gewinnt die Bridge mit der tiefsten ID.

14. VLAN

VLANs können physikalische Ethernet-Netzwerke in mehrere logische Netzwerke aufteilen. VLANs arbeiten auf Layer 3 und können die Vorteile von Switching und Routing vereinen. Bleibt der Verkehr innerhalb des VLANs wird nur geswitcht. Um in ein anderes VLAN zu gelangen wird geroutet. Man spricht auch von Layer-3 Switches.

Dies hat insbesondere den Vorteil, dass auch mehrere Broadcast-Domänen entstehen, da inter-VLAN-Traffic über einen Router weitergeleitet wird.

Um mehrere VLANs unabhängig voneinander über ein einziges physikalisches Medium transportieren zu können wurde 802.1q definiert (siehe Ethernet Frame). Dazu werden 4 Bytes zum VLAN-Tagging in den Ethernet-Header eingefügt. Diese werden dazu verwendet um ein Paket eindeutig einem VLAN zuordnen zu können. Verlässt das Frame das VLAN so kann das Tag wieder entfernt werden um ein Ethernet Version 2.0 Frame zu erhalten.

15. WLAN (IEEE 802.11)

Dieser Standard definiert drahtlose Netzwerke mit lokaler Ausdehung (Haushalt, Bürogebäude, Firmenkomplex o.ä.).

15.1. Link Layer

15.1.1. Physikalische Eigenschaften

Bei der Spezifikation des physischen Protokolls sind die Eigenschaften der Übertragung über die Luftschnittstelle zu berücksichtigen. Das gilt besonders für mögliche Störungen.

Nach dem Standard IEEE 802.11 kann die Datenübertragung (und dem entgegenwirken der Störungen) mit verschiedenen physikalischen Medien durchgeführt werden. Zwei dieser Verfahren senden mit elektromagnetischen Wellen und benutzen ein Frequenzsprungverfahren (frequency hopping, FHSS) bzw. ein Direct-Sequence-Verfahren (DSSS), welche abhängig von den Örtlichkeiten mehrere Kilometer überbrücken können. Ein drittes Verfahren basiert auf Infrarottechnik, die bis zu 10 m übertragen kann. Dabei müssen Sender und Empfänger nicht aufeinander ausgerichtet sein oder klare Sichtverbindung herrschen. Diese Technik kann allerdings nur innerhalb von Räumen eingesetzt werden.

FHSS erlaubt den gleichzeitigen Betrieb mehrere Systeme im selben Frequenzbereich. Dabei sorgt es für eine faire Verteilung des Übertragungsmediums. Das Prinzip des Frequency Hopping besteht darin, dass sowohl Sender als auch Empfänger die Trägerfrequenz nach einer festgelegten Abfolge wechseln.

Aus diesem Grunde wurde die physikalische Schicht in zwei Schichten unterteilt, von denen die untere medienabhängig (PMD: physical media dependent), die darüber liegende medienunabhängig ist (PLCP: physical layer convergent protocol).

15.2. IEEE 802.11a

Funkt im 5GHz Bereich mit maximal 54Mbit/s brutto und benutzt eine Frequenzbereich von 455MHz unterteilt in 19 Kanäle (nicht überlappend). In der Schweiz ist diese Technik nur sehr begrenzt nutzbar, da das 5GHz Band für den Militärischen Bereich reserviert ist.

15.3. IEEE 802.11b

Funkt im lizenzfreien 2.4GHz Band mit maximal 11Mbit/s brutto. Da insbesondere Bluetooth-Geräte und Mikrowellenherde auch im selben Frequenzband arbeiten kann es zu vermehrten Störungen kommen.

15.4. IEEE 802.11g

Funkt im lizenzfreien 2.4 GHz Band mit maximal 54Mbit/s brutto.

15.5. Ethernet-Verfahren (CSMA/CA)

Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) ist ein Verfahren um Kollisionen auf einem gemeinsamen Medium zu verhindern. Diese Verfahren wird bei der WLAN-Übertragung eingesetzt, da ein Collision-Detection Mechanismus nicht immer realisierbar ist. Dazu müsste die Netzwerkkarte während der Übertragung das Medium überwachen, was bei WLAN nicht immer möglich ist.

Aus diesem Grunde wird eine „listen before talk“ Methode implementiert. Dadurch lassen sich Kollisionen nicht ganz verhindern aber doch minimieren. Wegen der begrenzten Signalausbreitung kann es zu Effekten wie „versteckten“ oder „ausgelieferten“ Endgeräten kommen.

Bei CSMA/CA wird daher durch den "Inter-Frame Space" (IFS, die Zeit zwischen zwei Datenpaketen) eine Möglichkeit für einen prioritätsabhängigen Zugriff mit Kollisionsvermeidung geschaffen.

Möchte ein Gerät Daten versenden, so ist u.a. folgender Ablauf möglich:

Zuerst wird das Medium abgehört. Ist das Medium für die Dauer eines IFS frei, wird gesendet

Ist das Medium belegt, wird auf einen freien IFS gewartet und zur Kollisionsvermeidung zusätzlich um eine zufällige Backoff-Zeit verzögert. Wird das Medium während der Backoff-Zeit von einer anderen Station belegt, bleibt der Backoff-Timer so lange stehen

Eine andere Möglichkeit ist die Adress-Abitrierung, welche z.B. beim CAN-Bus verwendet wird. Um das Problem der "versteckten" oder "ausgelieferten" Endgeräte zu beseitigen, existiert eine RTS/CTS-Erweiterung für CSMA/CA. Dabei muss die sendewillige Station den Kanal durch ein RTS-Paket reservieren. Der Empfänger bestätigt diese Reservierung mit einem CTS-Paket. Anschliessend ist ein sofortiges Senden der Daten möglich. Andere Stationen speichern die Belegungsdauer, die im RTS- und CTS-Paket gesendet wurde, und senden während dieser Zeit keine Daten.

Zudem besteht in drahtlosen Systemen keine realistische Möglichkeit, Kollisionen zu erkennen. Ein CSMA/CD-Algorithmus wie beim Ethernet nach 802.3 ist daher nicht möglich.

Deswegen muss bei der drahtlosen Übertragung nach 802.11 der ordnungsgemässe Empfang eines Rahmens quittiert werden. Die Versendung der Quittung (Acknowledgement - ACK) erfolgt nach einer Wartezeit, die man als Short Interframe Space (SIFS) bezeichnet. Dieser SIFS ist kürzer als der DIFS, so dass die Bestätigung nicht die Wartezeiten der normalen Datenübermittlung einhalten muss. Durch die kürzere Wartezeit erhalten die Quittungsrahmen eine höhere Priorität als die normalen Datenpakete.

15.6. Sicherheit

WLAN Netze implementieren einige Sicherheitsmechanismen. Da es sich um Drahtlose Netzwerke handelt ist es besonders leicht Daten abzugreifen. Aus diesem Grunde ist eine Verschlüsselung der Übertragungsstrecke besonders wichtig.

15.6.1. SSID

Die SSID ist nicht wirklich ein Sicherheitsmerkmal, da sie im Klartext übertragen wird und eigentlich nur dazu dient das Netz zu identifizieren.

Einige Geräte können die Übertragung der SSID in den Broadcast-Meldungen unterbinden. Dies ist aber nicht empfehlenswert, da einige Endgeräte damit nicht klarkommen. Ausserdem erhöht dies nicht die Netzwerksicherheit da die Daten immer noch unverschlüsselt übertragen werden.

15.6.2. MAC-Filterung

Die Filterung nach MAC-Adressen mag auf den ersten Blick eine sichere Methode zu sein nur vertrauenswürdige Benutzer zur Kommunikation freizugeben. In der Praxis lässt sich eine MAC-Adresse aber auch fälschen. Ausserdem behept es nicht das Problem, dass die Daten unverschlüsselt übermittelt werden und von jedem abgehört werden können.

15.6.3. Wired Equivalent Privacy (WEP-Verschlüsselung)

WEP arbeitet mit dem RC4 Algorithmus zu Verschlüsselung. Es sind Schlüssellängen von 64bit oder 128bit möglich. WEP ist nicht mehr als sicher zu betrachten da abzüglich der 24bit des

Initialisierungsvektors noch eine Verschlüsselung mit 40 bzw. 104bit bleibt. Können genügend Daten abgehört werden so ist es möglich den Schlüssel zu bestimmen (im Normalfall ca. 4'000'000 Pakete). Bei gut ausgelasteten Netzwerken kann das bereits nach ca. 5-15 Minuten der Fall sein.

Ein weiterer Nachteil von WEP ist, dass der Schlüssel geteilt wird. Wird dieser kompromittiert müssen alle Access-Points und Clients auf einen neuen Schlüssel umgestellt werden. Ausserdem bietet der Algorithmus selbst nicht genügend Sicherheit.

15.6.4. Wi-Fi Protected Access (WPA)

WPA bietet basierend auf dem Tomporal Key Integrity Protokol (TKIP) zusätzlichen Schutz durch dynamische Schlüssel. Ausserdem bietet es zur Authentifizierung PSK (Pre-Shared-Keys) oder Extensible Authentication Protocol (EAP) über 802.1x an.

Der Initialisierungsvektor ist hier 48bit lang. Ausserdem wurden weitere Mechanismen implementiert um Integrität der Pakete zu prüfen.

Da der Verschlüsselungsalgorithmus RC4 als gebrochen gilt wurde die Erweiterung von WPA (WPA2) entwickelt welche mit dem AES-Standard arbeitet.

16. WAN Technologien

Hier werden Technologien zur Datenfernübertragung (DFÜ) erläutert.

16.1. Integrated Services Digital Network (ISDN)

ISDN ist ein internationaler Standard für den Zugang in ein digitales Telekommunikationsnetz. Es nutzt die bestehenden Kupferkabel zur Kommunikation (Zweidrahtleitungen). Durch ein Zeitmultiplex-Verfahren werden mehrere Kanäle zur Verfügung gestellt die unabhängig für Daten und Telefon-Dienste genutzt werden können.

Ein ISDN Basisanschluss bietet zwei Nutzkanäle mit je 64kbit/s Datenübertragungsrate. Zusätzlich wird für die Signalisierung der Sogenannte D-Kanal mit 16kbit/s zur Verfügung gestellt.

Zusätzlich ist es möglich mehrere Kanäle durch „Kanalbündelung“ zusammenzuschalten und somit beispielsweise einen Virtuellen 128kbit/s schnellen Kanal zur Verfügung zu stellen (2x64kbit/s).

16.2. Modem

Ein Modem (zusammengesetztes Wort aus Modulator/Demodulator) dient dazu, digitale Daten in für eine vorhandene analoge Leitung geeignete Signale umzuwandeln und auf der anderen Seite wieder in digitale Daten zurückzuwandeln. Die dafür verwendete Modulation ist auf die analoge Leitung abgestimmt.

Mit einem Modem werden digitale Daten durch Modulation eines analogen Signals über analoge Kommunikationsnetze (Telefonnetz, Kabel-TV), Standleitungen und per Funk übertragen. Am anderen Endpunkt der Kommunikation werden die digitalen Daten durch Demodulation aus dem analogen Signal wieder zurückgewonnen.

16.3. Digital Subscriber Line (DSL)

Der Begriff DSL wurde ursprünglich für den Basisanschluss von ISDN verwendet. Mit der Verfügbarkeit von digitalen Signalprozessoren mit sehr hoher Rechenleistung wurden dann auch viel höhere Datenübertragungsraten möglich. Diese wurden hauptsächlich für Standleitungen eingesetzt.

Spätere Standards nach xDSL (ADSL, HDSL, SDSL, VDSL, UADSL) bieten vor allem immer höhere Datenübertragungsraten. Da mit erhöhtem Datendurchsatz auch die Anforderungen an das Übertragungsmedium (Kupferkabel) und die Störanfälligkeit steigt ist die Leitungslänge für die Übertragungsstrecke stark begrenzt. Es gibt aber auch xDSL Verfahren, die speziell auf lange Leitungswege optimiert sind.

Da die meisten heutigen xDSL-Verfahren im Frequenzbereich über derjenigen der klassischen Telefoniedienste arbeiten kann z.B. eine ADSL-Internetverbindung permanent aktiv sein und trotzdem kann telefoniert werden.

Tabelle 4 DSL-Technologien

Technologie	HDSL	SDSL	ADSL	VDSL	ISDN
Max. Datenrate (Downstream)	1.544Mbps 2.048Mbps	1.544Mbps 2.048Mbps	Bis 8Mbps	Bis 51.84Mbps	0.064Mbps 0.128Mbps
Max Datenrate (Upstream)	1.544Mbps 2.048Mbps	1.544Mbps 2.048Mbps	Bis 1Mbps	Bis 2.3Mbps	0.064Mbps 0.128Mbps
Max. Leitungslänge	4km	3km	5.5km	Datenraten bei 0.3km	-
Benötigte Adernpaare	2 bei 1.544M 3 bei 2.048M	1	1	1	1
Frequenzbereich	~240kHz	~240kHz	~1MHz	~30MHz	120kHz

Anwendungen	T1-Standleitungen	WAN/LAN, Ersatz für T1	Internet, Intranet	WAN/LAN, Multimedia, HTV	Telefonie, Daten, Fax

16.4. Frame Relay

Eine WAN Technologie. Frame Relay ist eine Datenübertragungstechnik, die ursprünglich als Datenzubringerdienst für ISDN entwickelt wurde. In Europa werden häufig die Basistationen des GSM-Netzes über Frame Relay angebunden. Aber auch Netzbetreiber bieten Frame Relay Verbindungen als billigere Alternative zu einer Standleitung an.

Frame Relay multiplext wie X.25 beziehungsweise das Datex-P-Netz die Datenströme verschiedener Sende- beziehungsweise Empfangsstationen nach statistischen Gesichtspunkten über eine Leitung und unterstützt dabei Geschwindigkeiten zwischen 56 kBit/s und 45 Mbit/s. Wegen seiner hohen Ähnlichkeit zu X.25 ist es eigentlich dessen Weiterentwicklung mit der Fähigkeit zu höherer Übertragungsgeschwindigkeit.

Häufig wird Frame Relay mit einer garantierten Übertragungsgeschwindigkeit (CIR von Committed Information Rate) und einer kurzzeitigen Überschreitung der Übertragungsgeschwindigkeit (EIR von Extendet Information Rate) angeboten.

Eine Gemeinsamkeit mit X.25 ist, dass Frame Relay ebenfalls verbindungsorientiert ist. Für jeden Teilnehmer wird eine eigene virtuelle Verbindung aufgebaut.

Ein wesentlicher Unterschied zu X.25 besteht in den Fehlerkorrekturmechanismen. X.25 wurde ursprünglich zur Übertragung von Daten über Telefonleitungen entwickelt, die selten bessere Fehlerraten als 1:10.000 haben. Deswegen hat X.25 aufwendige Mechanismen zur Korrektur von Fehlern und zur wiederholten Übertragung verfälschter Datenblöcke. Frame Relay hat diese Mechanismen nicht.

Frame Relay ist eine effektive Datenübertragungstechnik für Datenströme, die eine konstante Bitrate haben wie zum Beispiel digitale Sprache. Für Datenübertragungen mit stark wechselndem Verkehrsprofil oder auch für Multimedia ist sie nicht besonders gut geeignet. Trotzdem wird sie wegen der geringen Kosten gerne für die Verbindung von LANs über Weitverkehrsstrecken verwendet. Die Fehlerrate ist dann aber in Lastsituationen deutlich spürbar.

Frame Relay wurde entwickelt, um eine effiziente Ausnutzung der existierenden technischen Ressourcen zu ermöglichen. Der Anbieter kann allen Kunden in Summe mehr Übertragungskapazität anbieten als ihm zur Verfügung steht, da die meisten Kunden nicht immer 100 Prozent ihrer "Leitung" ausnützen. In manchen Marktsegmenten bekam Frame Relay deswegen einen schlechten Ruf - da einige Anbieter in Summe deutlich mehr Bandbreite verkauften als zur Verfügung stand.

Frame Relay wird zunehmend von ATM und Produkten die auf IP basieren ersetzt. Besonders Virtuelle Private Netze übernehmen zunehmend als noch billigere Alternative das Marktsegment von Frame Relay.

16.5. Asynchronous Transfer Mode (ATM)

ATM ist eine Technologie, bei der der Datenverkehr in kleine Pakete (bei ATM "Zellen" genannt) mit fester Länge (53 byte) encodiert wird. Die Zellen-Technik hat im Vergleich zu Übertragungstechniken mit variabler Paketgrösse (v.a. Ethernet) den Vorteil, dass die Pakete geswitcht und nicht geroutet werden und so effizienter weitergeleitet werden können.

16.5.1. QoS

ATM bietet Garantie hinsichtlich der effektiven Bitrate, Delay und Jitter.

16.5.2. Virtuelle Verbindungen

ATM beruht auf Verbindungen, die nur für eine bestimmte Zeit geschaltet werden. Dies spiegelt sich im Konzept der Virtual Paths (VPs) und Virtual Circuits (VCs) wider. Jede ATM-Zelle hat einen 8 bzw. 12 Bit langen Virtual Path Identifier (VPI) und einen Virtual Circuit Identifer (VCI) von 16 bit in ihrem Header. Während diese Zellen das ATM-Netzwerk passieren, wird das Switching durch Änderung der VPI/VCI-Werte erreicht. Obwohl die VPI/VCI-Werte also nicht notwendigerweise von einem Ende der

Verbindung zum anderen gleich bleiben, entspricht dies dem Konzept einer Verbindung, da alle Pakete mit gleichen VPI/VCI-Werten den gleichen Weg nehmen (im Gegensatz zu IP, wo ein Paket sein Ziel über eine andere Route erreichen könnte als vorhergehende und nachfolgende Pakete).

Virtuelle Verbindungen haben auch den Vorteil, dass man sie als Multiplexing-Layer für unterschiedliche Services (Sprache, Frame Relay, IP, SNA etc.) benutzen kann, die sich dann eine gemeinsame ATM-Verbindung teilen können, ohne sich gegenseitig zu stören.

16.5.3. Architektur

Für verschiedene Datentypen (QoS Klassen) gibt es bei ATM verschiedene sogenannte Adaption Layers (AAL). Der AAL übernimmt die Daten-Segmentation bzw. Zusammenfassung und kann mit dem Internet Transport-Layer verglichen werden.

Der ATM Network Layer ist für das Cell-Switching/Routing zuständing.

Der Physical Layer schliesslich für die Übertragung.

Die folgenden Versionen des AAL Layers sind abhängig von der Dienstklasse verfügbar:

- AAL0: Zellen ohne nähere Bedeutung
- AAL1: Für CBR (Constant Bit Rate) Dienste, z.B. Circuit Emulation
- AAL2: Für VBR (Variable Bit Rate) Dienste, z.B. Video/Audio Streaming
- AAL5: Für Daten (z.B. IP Datagramme)

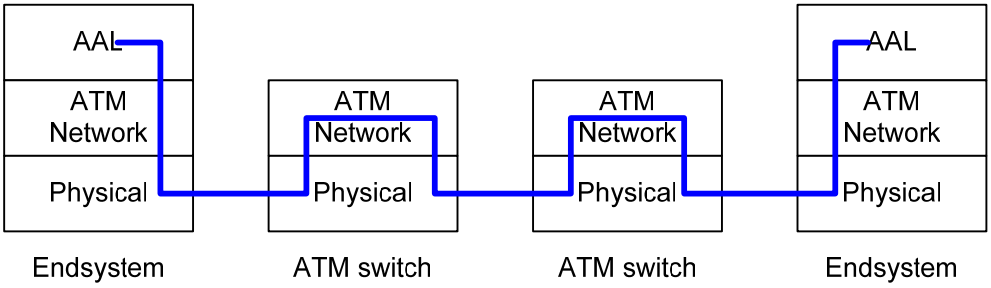


Abbildung 20 ATM Switching

17. PPP

Das Point-to-Point Protocol bzw. Punkt-zu-Punkt-Protokoll (PPP) ist ein Protokollzum Verbindungsaufbau über Wählleitungen (zumeist über Modem oder ISDN). Es ermöglicht die Übertragung verschiedenster Netzwerkprotokolle (z.B. IP, IPX, AppleTalk...).

Damit ein Layer 3 Protokoll ein WAN Link über eine Dialup oder Standleitung traversieren kann muss es via ein Data-Linklayer Protokoll encapsuliert werden.

PPP ist so ein Data-Link Protokoll, welches Router –zu-Router und Host-zu-Netzwerk über synchrone und asynchrone Verbindungen zulässt.

PPP unterstützt folgende grundlegenden Features:

- Dynamic address allocation
- CHAP/PAP authentication
- Multilink PPP: Lastverteilung (Loadbalancing) über mehrere, synchrone oder asynchrone, Leitungen ermöglicht, beispielsweise über ISDN- Verbindungen.
- Callback
- Authentifizierung (PAP, CHAP): PAP sendet das Passwort als Klartext. Durch einen strategisch günstig plazierten Paketsniffer könnte diese dies aufgefangen und dekodiert werden.

Nachteile:

- Keine Error Korrektur/Recovery
- Keine Flusskontrolle
- Auslieferreihenfolge immer OK.

18. Computer Telophony Integration (CTI), VoIP

CTI bedeutet so viel wie computerunterstütztes Telefonieren. Darunter ist die Kopplung zwischen der klassischen Telekommunikation und der Datenverarbeitung an einem Computerarbietsplatz zu verstehen.

Die einfachste Form der Integration ist der Verbindungsaufbau/Abbau über den Computer. Im Optimalfall ersetzt der Computer auch das Telefon.

Die konsequente Erweiterung dieser Anwendung kommt im Zusammenhang mit CRM(Customer Relationship Managment). Hier wird anhand der, vom Anrufer, übermittelten Rufnummer zum vorher bestimmten Sachbearbeiter verbunden. Der Sachbearbeiter bekommt zeitgleich auf seinem Computer die Kundendaten angezeigt und kann sich im Vorfeld eines Gesprächs auf den Kunden einstellen.

Spielen alle Faktoren in der Technik und in der Organisation zusammen, so ist eine hohe Kundenbindung und Mitarbeiterauslastung erreichbar.

18.1. Architektur

Die CTI-Architektur definiert die Art und Weise, wie die Technik der Telekommunikation und die Technnik in der Datenverarbeitung miteinander gekoppelt wird.

Hierbei wird zwischen First-Party-Telephony(Desktop-CTI) und Third-Party-Telephony(Host-CTI) unterschieden.

18.2. VoIP - Voice over IP

In Internet-Telefonie wurde bereits darüber berichtet, wie sich das Internet als Alternative zum klassischen Festnetz oder Mobilfunknetz als Kommunikationsmedium nutzen lässt. Zwar nutzt das Internet auch das Festnetz als Übertragungsmedium, es stellt sich jedoch als Dienst dar. Internet-Telefonie setzt als Anwendung auf diesen Dienst auf.

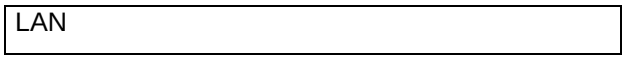
Das paketorientierte Internet-Protokoll (IP) geht wesentlich ressourcenschonender mit dem zu Verfügung stehenden Übertragungsmedium um. So lässt sich über eine IP-gesteuerte Leitung, abhängig vom Codec, mehr Verbindungen (virtuell) realisieren als über eine Festnetz-Leitung.

Für ein Telefongespäch in entsprechender Qualität, muss ein bestimmtes Frequenzspektrum gewährleistet sein. Man spricht vom sogenannten Fernsprechkanal. In diesem Fernsprechkanal wird die Sprache isochron (gleich lang andauernd) übertragen.

18.3. Protokolle und Standards

Einheitliche Standards bei der Sprachübertragung über IP sind bisher dünn gesäht. Setzt man auf die Produkte eines einzigen Herstellers, so hat man keine Probleme. Versucht man jedoch die Produkte unterschiedlicher Hersteller zur Zusammenarbeit zu bewegen, stellen sich einem einige Hürden in den Weg.

<table>
<tr><th colspan="2">Call Control</th><th>Audio</th><th>Video</th></tr>
<tr><td colspan="2" rowspan="2">SIP
H.323
H.245
Q.931
RAS
H.225.0
H.450</td><td>G.711
G.722
G.728
G.723
G.729</td><td>H.261
H.263</td></tr>
<tr><td colspan="2">RTP
RTCP</td></tr>
<tr><td>TCP</td><td colspan="3">UDP</td></tr>
<tr><td colspan="4">IP</td></tr>
</table>



18.3.1. H.323 (Voice over IP)

Der Standard H.323 hat seinen Ursprung als Protokoll für die Videokommunikation über TCP/IP. Dazu wurde die Protokollfamilie rund um H.323 entwickelt. Die internationale Normung durch ITU-T war bereits 1996.

Innerhalb von H.323 sind die Protokolle H.225.0(Setup), Q.931(Signalisierung), H.245(Telefonie) und H.450(weitere Dienste und Leistungmerkmale) definiert. Über H.323 sind auch Gateway- und Gatekeeper-Funktionen definiert. Über das Gateway wird der Übergang in andere Sprachnetze ermöglicht. Der Gatekeeper regelt das Bandbreitenmanagment und die Umsetzung von der symbolischen Adresse in die IP-Adresse.

Viele IP-Telefone haben Probleme beim Erkennen des Endes einer eingetippten Rufnummer(Aufgrund der Art der Vermittlung). Das Overlap Sending sendet die Rufnummer während des Eintippens. So kann der Gatekeeper das Ende schneller erkennen und zügig die Verbindung herstellen. Die Anrufinformationen sind in einem Binärcode geschrieben. Haben sich zwei Endgeräte auf einen Codec geeinigt, dann erfolgt die Sprachübertragung über das Realtime Transport Protocol(RTP). Das RAS-Protokoll ist ein Verfahren zur Anmeldung von Endgeräten, Verbindungsanforderungen und Bandbreitenzuteilung(Registration Admission Status).

Wenn die Verbindung aufgebaut ist, übernimmt das H.245 mit einem Handshaking-Verfahren die Arbeit. Dabei werden Audio- und Videocodecs für Sprach- und Videokompression auf Verfügbarkeit geprüft. Als Sprach-Codecs sind die in der Tabelle weiter oben aufgeführten Standards enthalten. Aber nur der G.711-Codec ist als Muss definiert. Alle anderen Codecs können von den Herstellern in ihre Produkte implementiert werden.

Aufgrund der Komplexität sind beim Betrieb von VoIP-Produkten unterschiedlicher Hersteller Tests und Feinabstimmungen notwendig. Ungünstige Konstellationen schliessen einen gemeinsamen Betrieb aus.

18.3.2. VoIP/POTS Integration

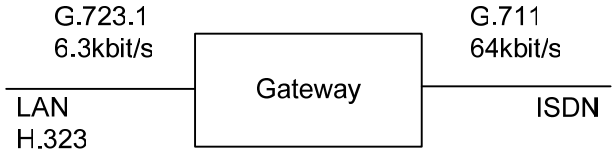


Abbildung 21 VoIP-Gateway/Gatekeeper mit H.323

Das VoIP-Gateway ist für den Auf- und Abbau der Sprachkanäle zwischen dem H.323-LAN und dem Telefonnetz zuständig. Dabei wird der Sprachverkehr vom IP-Codec G.723.1(8,3 kBit/s) auf G.711(64 kBit/s) umgesetzt.
Das Gateway kann entfallen, wenn keine Verbindung zum klassischen Telefonnetz erforderlich ist. Auf der einen Seite ist das Gateway mit dem LAN verbunden. Auf der anderen Seite ist das Gateway über mehrere ISDN-B-Kanäle mit dem Telefonnetz verbunden. Das Gateway ist der Netzwerk-/Systemknoten, der für den Jitter-Puffer, die Laufzeitoptimierung, Echo-Unterdrückung und andere Verfahren zur Verbesserung von Quality-of-Service(QoS) zuständig ist.
Das Kernstück des PSTN/IP-Gateways ist der Gatekeeper(Torwächter). Er ist die Schnittstellenfunktion des H.323-Standards und dient der Emulation des PSTN-Verbindungsaufbaus zwischen Endgerät über das IP-Netz. Der Gatekeeper übernimmt die...

- ...Anrufsteuerung(Signalisierung) und die dafür notwendigen Übersetzung von IP-Adresse in PSTN-Rufnummer bzw. umgekehrt. Die Steuerungsfunktionen sind im H.225 festgelegt.
- ...Signalisierung auf den Teilnehmeranschlussleitungen zum Auf- und Abbau von Verbindungen(Q.931).
- ...Umwandlungen des synchronen Datenstroms, aus dem PSTN, in IP-Pakete.

18.3.3. Resource ReSerVation Protocol (RSVP)

Das Resource ReSerVation Protocol (kurz RSVP) ist eines der wichtigsten Signalisierungsprotokolle im Internet Protocol-Stack ab der neuen Version 6 des Internet-Protokolls (IPv6). Es erlaubt Empfängern ausserhalb einer Multicast-Gruppe, deren Dienstanforderungen festzulegen. Damit können für bestimmte Anwendungen, z. B. für die Übertragung von Video-Streams bestimmte Bandbreiten für einzelne Verbindungen reserviert werden. In der bisher verwendeten Version 4 des Internet-Protokolls sind solche Garantien nicht vorgesehen, was im Beispiel der Video-Streams zu ruckelnden Bildern führen kann.

RSVP kann auch für die Reservierung der Dienstgüte (QoS, Quality of Service) bei Unicast-Übertragungen benutzt werden. Eine solche Reservierung wird wie folgt aufgebaut:

Der Sender schickt eine spezielle Nachricht zum Empfänger, die RSVP Path Message. Damit wird ein möglicher Pfad vom Sender zum Empfänger ermittelt.

Die dabei passierten Router werden protokolliert und so dem Empfänger mitgeteilt. Entlang diesen Pfades schickt der Empfänger dann eine weitere Nachricht, die RSVP Reservation Message. Diese enthält eine sogenannte Flussspezifikation, die die Anforderungen für die Reservierung beschreibt.

Die Router auf dem Weg reservieren die Ressourcen entsprechend dieser Flussspezifikation oder schicken eine Fehlermeldung zurück. Kommt die RSVP Reservation Message beim Sender an, kann dieser sich auf die Reservierungen verlassen und gemäss der Spezifikation senden.

18.3.4. Differentiated Services (DiffServ)

DiffServ ist in den RFCs 2474 und 2475 beschrieben und ist ein Quality of Service (QoS) Verfahren zur Priorisierung von IP-Datenpaketen.

Ein herkömmliches IP-Netzwerk unterscheidet nicht zwischen verschiedenen Anwendungen, die im Netzwerk unterwegs sind. Dem Risiko von Engpässen wurde bislang deshalb durch Bereitstellung grosser (und teurer) Kapazitäten begegnet. Durch das neue Verfahren wird jedes IP-Paket zur Feststellung der Paketwichtigkeit geprüft.

Im Gegensatz zu anderen QoS Verfahren (wie IntServ mit RSVP) wird die Priorität eines IP-Paketes bereits vom Sender bestimmt. Die Router auf dem Weg zum Empfänger entscheiden allein anhand dieser Angabe über die bevorzugte Weiterleitung zum Empfänger.

DiffServ nutzt zur Signalisierung der Priorität das schon vorhandene Type of Service (ToS) Byte im IP-Header des IPv4 oder das Class Field im IP-Header des IPv6-Protokolls. Zur Abgrenzung gegenüber dem früheren ToS bzw. Class-Field wird das Byte dann als Differentiated Services Code Point (DSCP) bezeichnet.

19. Netzwerkmanagement

Unter Einschränkung auf Komponenten eines Kommunikationsnetzes spricht man von Netzwerkmanagement. Werden gesamte verteilte Systeme verwaltet, so handelt sich dabei um Systemmanagement.

19.1. Simple Network Management Protocol (SNMP)

Das SNMP ist ein Protocol zur Verwaltung und Steuerung von Netzwerken. Es ist für den Transport von Management-Informationen, Status- und Statistikdaten zwischen den einzelnen Netzwerkkomponenten und einem Management-System zuständig.

Bei der Einführung von TCP/IP wurde kurzfristig SNMP verwendet und sollte durch ein OSI-konformes Protokoll ersetzt werden. SNMP setzt sich jedoch innerhalb kürzester Zeit durch. Die Anpassung an die Anforderungen von OSI waren jedoch zu umfangreich und wurden ausgesetzt. Stattdessen wurde kurzerhand SNMP, SMI und MIB zum offiziellen Standard erklärt. Deshalb muss in allen verwaltbaren Netzwerk-Komponenten SNMP, SMI und MIB implementiert sein.

19.1.1. Netzwerk-Management

Mit zunehmender Tendenz werden immer mehr Anwendungen aus der Informations- und Kommunikationstechnik in die betrieblichen Arbeitsabläufe integriert. Dadurch entstehen immer grössere und komplexere Netzwerke, an die immer mehr Anwendungen und Benutzer angeschlossen werden. Um Probleme und Störungen in einem Netzwerk frühzeitig erkennen und beseitigen zu können sind Elemente erforderlich, die ein Netzwerk verwalten und beobachten können. An dieser Stelle setzen Netzwerk-Management-Systeme an. Diese Systeme werden allgemein unter der Bezeichnung Netzwerk-Management-Technologie (NMT) zusammengefasst.

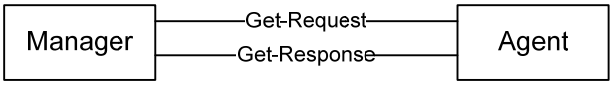


Abbildung 22 SNMP Manager und Agent

Die Architektur von SNMP trennt zwischen dem Manager, den Agenten, den Verwaltungsinformationen und dem Verwaltungsprotokoll. Der Manager ist eine Anwendung auf einem speziell dafür vorgesehenen Computer. Die Software integriert verschiedene Diagnosewerkzeuge, Filtermöglichkeiten, grafische Darstellung von Fehlermeldungen und Netztopologien uvm. Die Agenten sind die einzelnen Netzwerk-Komponenten. Sie führen die Management-Funktionen aus. Die Verwaltungsinformationen sind Informationen über das Netzwerk, der Konfiguration, dem Aufbau und den statistischen Daten. Das Verwaltungsprotokoll ist SNMP selber. Es tauscht die Verwaltungsinformationen und Daten zwischen dem Manager und den Agenten aus.

Der Ablauf zwischen Manager und Agenten ist immer der selbe. Der Manager schickt einen Request an den Agenten. Dieser führt den Befehl aus (z.B. Konfigurationsänderungen) und schickt einen Response zurück. Dieses Verfahren wird Polling genannt. Weiterhin existieren Trabs, die einen Agenten dazu veranlassen unvorhergesehene Ereignisse an den Manager zu melden. Viele gleichzeitig versendete Traps können jedoch zur Überlastung des Managers führen. Deshalb sind Traps nur bei kritischen Ereignissen empfehlenswert. Um eine unnötige Netzwerkbelastung zu vermeiden findet der Datenaustausch von SNMP über UDP statt.

19.1.2. MIB - Management Information Base

Die mit SNMP übertragenen Informationen und Daten müssen irgendwo abgelegt und gespeichert werden. Die MIB ist mit einer Datenbank vergleichbar. In ihr werden hauptsächlich diese Daten gespeichert. Die Daten werden in Form von Objekten strukturiert in einer Art Baum abgelegt. Wegen den Bedürfnissen des Netzwerk-Managements wurde die Standard-MIB durch Erweiterungen angepasst. Daraus ergab sich die MIB II.

Wegen der steigenden Komplexität wurde SNMP und MIB durch die RMON-MIB (Remote Monitoring) erweitert.

19.2. SNMPv2

SNMPv1 hat nur IP, TCP und UDP unterstützt. Zudem gab es Sicherheitsprobleme, da die Messages per Klartext übermittelt wurden. Weitere Probleme:

- lesen grosser Tabellen von Managed Objects sehr langsam
- Traps sind unbestätigt, so dass Ereignisse verloren gehen können
- die erste Version der MIB beschreibt nur eine beschränkte Zahl von Datentypen
- es wurde keine inter-Agent-Kommunikation spezifiziert
- die Fehler in Responses sind nicht aussagekräftig definiert

Mit SNMPv2 kann SNMP auch auf andere Protokolle, wie z. B. IPX, Appletalk und weitere OSI-Protokolle, eingesetzt werden. Neben den verbesserten Sicherheitsfunktionen, Werkzeugen zur Verwaltung verteilter Netze ist es auch möglich mehrere Manager untereinander kommunizieren zu lassen.

19.3. ASN.1

Abstract Syntax Notation One ist ein ISO-Standard, der unter anderem eine Darstellung für Daten definiert, die über ein Netzwerk zu senden sind. Ihr Hauptzweck ist der, Daten, deren Strukturen und Inhalte auf zwei verschiedenen Systemen oft sehr unterschiedlich dargestellt werden, einheitlich zu spezifizieren. Um diese über ein Netzwerk zu übertragen, benötigt man Regeln, nach denen die formal beschriebenen Datenstrukturen serialisiert werden. Diese werden Basic Encoding Rules (BER) genannt.

19.4. Remote Monitoring (RMON)

- Überwachung / Verkehrsstatistik von Netzwerkbereichen durch Paketuntersuchung.
- Agent/Monitor führt kontinuierlich Diagnose und Performancetests durch, sofern seine Ressourcen ausreichen.
- Datensammlung auch in Netzbereichen, die der Manager normalerweise nicht erreicht.

20. Sicherheit

Eine Firewall ist ein speziell programmierter Router, der zwei oder mehrere physikalische Netzewrke verbindet. Die Firewall leitet Pakete von einem Netzwerk zu einem andern weiter, dabei aber diese Pakete filtert. Um diese Regeln festzulegen werden so genannte Policy verwendet: Policies sind eine Beschreibung, welche Kontrollmechanismen wie eingesetzt werden sollen, beispielsweise welche Dienste in welchen Richtungen wie authentifiziert werden müssen.

Es gibt zwei grobe Kategorien von Firewalls:

- Filterbasierte und
- Proxy-basierende

20.1.1. Filterbasierte Firewalls

Filterbasierte Firewalls unterhalten eine Tabelle von Adressen, die weitergeleitet werden oder nicht. Diese Tabelle besteht aus einem 4-Tupel, welches die IP-Adresse und die TCP- bzw. UDP-Port-Nummer der Quelle und des Ziels enthält. Das sieht in etwa so aus:

<192.12.13.14, 1234, 128.7.6.5, 80>

Probleme von Paketfiltern:

- Risiko von „Löchern“
- Permit-Deny Entscheide bei jedem Paket sehen z.B. TCP-Verbindung nicht
- Adressfälschung (Spoofing) wird nicht immer entdeckt, ebenso Manipulationen am IP-Header
- Benutzerauthentifikation kaum möglich
- nicht verwendbar bei Protokollen ohne feste oder dynamisch zugeteilte Portnummern (z.B. FTP)

20.1.2. Proxybasierte Firewalls

Ein Proxy scheint für eine Server der Client, für den Client der Server zu sein. Wird z.B. ein HTTP-Proxy in der Firewall bereitgestellt, so kann dieser entscheiden, ob die Anfrage z.B. an einen firmeninternen Webserver zugelassen wird oder nicht. Würde eine filterbasierte Firewall verwendet, so könnte man nur den Port 80 weiterleiten oder nicht oder man könnte festlegen, welche IP-Adresse Zugriff auf den Webserver hat und welche nicht, was aber eher umständlich wäre.

- Auf der Firewall läuft ein Stellvertreterprogramm (z.B. HTTP-Proxy)
- Firewall erkennt und kontrolliert die ganze Verbindung und nicht nur einzelne Pakete
- Wird im allgemeinen nur für TCP-Dienste eingesetzt
- Eine Authentifikation ist denkbar, welche nicht pro Paket sondern pro Verbindung Gültigkeit hat
- Nicht nur Sicherheitsfunktionen anwendbar sondern z.B. ebenso für WWW-Proxies als Cache-Server

20.2. VPN & IpSec

Um eine sichere Verbindung aufzubauen, stellt das VPN dem Benutzer beispielsweise eine virtuelle IP-Verbindung zur Verfügung.

Die über diese Verbindung übertragenen Datenpakete verschlüsselt der Client und packt sie in ein Datenpaket ein, das er über das öffentliche Netz an den VPN-Server verschickt. Im Fall des Internets also wiederum ein IP-Paket.

Der VPN-Server entschlüsselt wieder das Originalpaket und verarbeitet es weiter.

Bei VPNs unterscheidet man generell drei Architekturvarianten:

- Ein Remote-Access-VPN stellt die sichere Verbindung von Home- und Mobile-Workern mit einer Firmenzentrale her. Es ersetzt also die klassische Dial-in-Anbindung über analoge oder ISDN Wählleitungen. Dabei steigert das VPN die Verfügbarkeit des Zugangs, während sich die Einwahlkosten in der Regel reduzieren.
- Ein Site-to-Site-VPN verbindet verteilte Firmenstandorte über das Internet. Es übernimmt dabei die Rolle, die im klassischen Aufbau Standleitungen beziehungsweise Frame-Relay- oder ATM-Kanäle spielen. Dabei steigt meist die verfügbare Bandbreite, während die Kosten wiederum sinken.
- Ein Extranet-VPN bindet externe Geschäftspartner an. Das vereinfacht und verbilligt die Nutzung von Diensten wie Fax, Mail oder EDI (Electronic Data Interchange).

Für die eigentliche Implementation eines VPNs gibt es verschiedene Verfahren. Die verbreitetsten sind:

- Das Point-to-Point Tunneling Protocol (PPTP) eignet sich für den Transfer von IP, IPX oder NetBEUI über ein IP-Netzwerk.
- Das Layer 2 Tunneling Protocol (L2TP) eignet sich für den Transfer von IP, IPX oder NetBEUI über ein beliebiges Medium, das die Übertragung von Punkt-zu-Punkt-Datagrammen erlaubt. Etwa IP, X.25, Frame Relay oder ATM.
- Das IP Security Protocol (IPSec) eignet sich für den Transfer von IP -Daten über ein darüber gelagertes IP - Netzwerk.

Das Tunneling kann auf zwei verschiedenen Ebenen des OSI-Schichtenmodells erfolgen. PPTP und L2TP verwenden die Datenverbindungsschicht (Ebene 2) und packen die Datenpakete in Frames des Punkt-zu-Punkt-Protokolls (PPP) ein. Dabei können sie auf Features des PPP zurückgreifen, wie Benutzer-Authentifizierung (über CHAP), dynamische Adressvergabe (etwa DHCP), Datenkompression oder Datenverschlüsselung.

PPTP verpackt die PPP-Rahmen vor der Übermittlung in IP-Pakete und übermittelt sie über ein IP-Netzwerk zum Zielknoten.

IPSec arbeitet im Gegensatz zu PPTP und L2TP auf der Netzwerkschicht (Ebene 3). Es verschlüsselt die zu sendenden Datenpakete inklusive aller Informationen wie Empfänger und Statusmeldungen und fügt einen normalen IP-Header hinzu, der an das andere Ende des Tunnels geschickt wird. Der Rechner dort entfernt den

zusätzlichen IP-Header, entschlüsselt das Originalpaket und leitet es an die eigentliche Zielstation weiter.

IPSec hat gegenüber den anderen Verfahren einen weiteren Vorteil: Es kann auch als "normales" Transportprotokoll verwendet werden. Dabei wird nicht wie beim Tunnel-Modus das gesamte IP - Paket verschlüsselt und in ein neues eingepackt. Stattdessen wird nur die reine Nutzlast verschlüsselt. Der Original-Header mit Absender- und Zielangaben bleibt erhalten. Dadurch müssen weniger zusätzliche Daten (Overhead) übermittelt werden.

20.3. SSL

SSL ist ein Sicherheitsprotokoll, das die Datensicherheit auf einer Schicht zwischen seiner Anwendungsschicht und TCP/IP gewährleistet. Es ermöglicht verschlüsselte Verbindungen, Echtheitsbestätigungen mit Zertifikaten sowie die Sicherstellung der Datenintegrität.

Vor dem Beginn der Datenübertragung arbeiten Client und Server ein Handshake Protokoll ab, in dem sie sich auf eine gemeinsame Sicherheitsstufe einigen , die notwendigen Authenzitätsprüfungen vorgenommen werden und ein Session Key für die spätere Verschlüsselung festgelegt wird.

Vorgehensweise bei Client und Server:

- Der Client sendet eine Verbindungsanfrage an den Server.
- Der Server antwortet mit derselben Nachricht und sendet eventuell ein Zertifikat.
- Der Client versucht, das Zertifikat zu authentifizieren (bei Misserfolg wird die Verbindung abgebrochen). Dieses Zertifikat enthält den öffentlichen Schlüssel des Servers.

- Nach erfolgter Authentifizierung erstellt der Client das pre-master secret, verschlüsselt dieses mit dem öffentlichen Schlüssel des Servers und sendet es an den Server. Ebenfalls erzeugt der Client daraus das master secret.
- Der Server entschlüsselt das pre-master secret mit seinem privaten Schlüssel, der komplementär zu seinem öffentlichen Schlüssel ist und erstellt das master secret.
- Client und Server erstellen aus dem master secret den session key. Das ist ein einmalig benutzter symmetrischer Schlüssel, der während der Verbindung zum Ver- und Entschlüsseln der Daten genutzt wird. SSL unterstützt für die symmetrische Verschlüsselung mit diesem session-key u.a. DES und Triple DES.
- Client und Server tauschen mit diesem session key verschlüsselte Nachrichten aus und signalisieren damit ihre Kommunikationsbereitschaft.
- Die SSL-Verbindung ist aufgebaut.

Der Vorteil des SSL-Protokolls ist die Möglichkeit, jedes höhere Protokoll auf Basis des SSL Protokolls zu implementieren. Damit ist eine Unabhängigkeit von Applikationen und Systemen gewährleistet.

21. Abbildungsverzeichnis

Abbildung 1 Schichtenmodelle 6
Abbildung 2 Encapsulation 7
Abbildung 3 IPv4 Header 9
Abbildung 4 IP TOS Feld 9
Abbildung 5 IP Optionen 10
Abbildung 6 IP-Klassen 11
Abbildung 7 IP Header mit ICMP Daten 13
Abbildung 8 ICMP Destination Unreachable 13
Abbildung 9 ICMP Redirect 13
Abbildung 10 ICMP Codes 14
Abbildung 11 TCP 3-way Handshake 15
Abbildung 12 TCP Verbindungsabbau 16
Abbildung 13 TCP-Header 16
Abbildung 14 UDP-Header 18
Abbildung 15 CIDR Routing (Supernetting) 20
Abbildung 16 IPv6 Adress-Typen 21
Abbildung 17 IP Routing Algorithmus 23
Abbildung 18 Ethernet Version 2.0 Frame 28
Abbildung 19 Ethernet Version 2.0 Tagged-Frame 29
Abbildung 20 ATM Switching 37
Abbildung 21 VoIP-Gateway/Gatekeeper mit H.323 40
Abbildung 22 SNMP Manager und Agent 42

22. Tabellenverzeichnis

Tabelle 1 OSI-Schichten 6
Tabelle 2 TCP/IP Schichten 6
Tabelle 3 PAT/NAPT/Masquerading Tabelle 18
Tabelle 4 DSL-Technologien 35

23. Index

802.11 ... **32**
802.11a ... **32**
802.11b ... **32**
802.11g ... **32**
802.1q ... **32**
ASN.1 ... **43**
ATM ... **36**
BGP ... **26**
CGMP ... **27**
CIDR ... **20**
CSMA/CA ... **33**
CSMA/CD ... **28**
CTI ... **39**
DHCP ... **19**
DiffServ ... **41**
Distanz Vektor Routing . **25**
DSL ... **35**
Encapsulation ... **7**
Ethernet ... **28**
Frame ... 28
Firewalls ... **44**
Hubs ... **29**
ICMP ... **13**
IGMP ... **27**
IGRP ... **25**
IpSec ... **44**
IPv4 Header ... **9**
IPv4-Adressierung ... **11**
IPv6 ... **21**
Adressierung ... 21
Header ... 22
ISDN ... **35**
Link State Routing ... **25**
MIB ... **42**
Modem ... **35**
MPLS ... **24**
Multicasting ... **27**
NAT ... **18**
Netzwerkmanagement .. **42**
OSI Modell ... **6**
Application ... 8
Data Link ... 7
Network ... 7
Physical ... 7
Presentation ... 8
Session ... 8
Transport ... 8
OSPF ... **25**
PAT ... **18**
PPP ... **38**
Protokollfamilien ... **8**
RIP ... **25**
RMON ... **43**
Routing ... **23**
Routingprotokolle ... **23**
RSVP ... **41**
Schichtenmodelle ... **6**
Sicherheit ... **44**
SNMP ... **42**
SSID ... **33**
SSL ... **45**
Switches ... **29**
Cat-Through ... 29
Spanning-Tree ... 30
Store-And-Forward ... 29
TCP ... **15**
TCP/IP ... **9**
TCP/IP Modell ... **6**
UDP ... **18**
VLAN ... **32**
VoIP ... **39**
VPN ... **44**
WAN ... **35**
WEP ... **33**
WLAN ... **32**
WPA ... **34**