

**Unterrichtsmitschrift**

# **Vernetzte IT-Systeme**

Michael Puff

2009-05-24

Oskar-von-Miller Schule Kassel  
Fachinformatiker für Anwendungsentwicklung



---

# Vorbemerkung

## Zum Inhalt

Dieses Dokument folgt dem Unterrichtsinhalt von Herrn Schäfer im Fach *Vernetzte IT-Systeme*. Die eigenen Unterrichtsmitschriften sind durch Texte und Grafiken aus den angegebenen Quellen ergänzt worden.

Diese Ausarbeitung erhebt keinen Anspruch auf Vollständigkeit.

## Kontaktmöglichkeiten

Homepage: <http://www.michael-puff.de>

E-Mail: [mail@michael-puff.de](mailto:mail@michael-puff.de)

## Copyright Hinweis

DIESES DOKUMENT STEHT UNTER DER CREATIVE COMMON LICENCE. DAS DOKUMENT DARF ZU DEN FOLGENDEN BEDINGUNGEN WEITER VERVIELFÄLTIGT UND VERBREITET WERDEN. DER NAME DES AUTORS/RECHTEHABERS (MICHAEL PUFF) IST ZU NENNEN. DIESES DOKUMENT DARF NICHT BEARBEITET ODER IN ANDERER WEISE VERÄNDERT WERDEN.



# Inhaltsverzeichnis

<b>1. Netzwerkgrundlagen</b>	<b>7</b>
1.1. Was ist Networking? . . . . .	7
1.2. Modelle, historische Entwicklung . . . . .	7
1.2.1. Centralized Computing . . . . .	7
1.2.2. Distributed Computing . . . . .	7
1.2.3. Collaborative Computing / Grid Computing . . . . .	8
1.3. Unterteilung von Netzwerken (LAN, MAN, WAN) . . . . .	8
<b>2. Netzwerkdienste</b>	<b>11</b>
<b>3. Übertragungsmedien</b>	<b>13</b>
3.1. Frequenzbereiche . . . . .	13
3.2. Einteilung von Übertragungsmedien . . . . .	14
3.2.1. Kabelmedien . . . . .	14
3.2.2. Kabellose Medien . . . . .	17
3.3. Crossover-Patchkabel . . . . .	20
3.4. Kabelabschluss . . . . .	21
3.5. Mehrfachzugriff auf Übertragungsmedien (CSMA) . . . . .	21
<b>4. Netzwerk-Koppelemente</b>	<b>23</b>
4.1. Segment-Koppelemente . . . . .	23
4.1.1. Stecker . . . . .	23
4.1.2. Netzwerkkarten . . . . .	23
4.1.3. Modems . . . . .	24
4.1.4. Repeater . . . . .	24
4.1.5. Bridge / Switch . . . . .	24
4.2. Verbundnetz-Koppelemente . . . . .	25
4.2.1. Router . . . . .	25
<b>5. Strukturierte Verkabelung</b>	<b>27</b>
5.1. Bereiche . . . . .	27
5.1.1. Der Primärbereich . . . . .	27
5.1.2. Der Sekundärbereich . . . . .	28
5.1.3. Der Tertiärbereich . . . . .	28
<b>6. Die IP-Adresse</b>	<b>29</b>
6.1. Grundlagen . . . . .	29
6.2. Aufbau . . . . .	29
6.3. Die Broadcast-Adresse . . . . .	30

6.4. Die Netzwerkmaske . . . . .	31
6.4.1. Berechnung von Netzwerk- und Hostanteil . . . . .	32
6.4.2. Subnetting . . . . .	35
6.5. Routing . . . . .	36
6.6. Netzklassen . . . . .	36
<b>7. Referenzen und Modelle</b>	<b>39</b>
7.1. Netzwerkarchitekturen – Grundlagen . . . . .	39
7.2. Das OSI-Referenzmodell . . . . .	40
7.2.1. Die einzelnen Schichten des OSI-Modells . . . . .	41
7.2.2. Datenübertragung im OSI-Modell . . . . .	46
7.3. Das TCP/IP-Referenzmodell . . . . .	46
<b>8. Routing</b>	<b>49</b>
8.1. Routing von Paketen . . . . .	49
8.2. Routing-Protokolle . . . . .	50
8.3. Das Address Resolution Protocol (ARP) . . . . .	51
8.3.1. Ablauf einer ARP-Adressauflösung . . . . .	51
8.3.2. ARP-Cache . . . . .	53
8.3.3. Probleme mit ARP . . . . .	54
8.4. Erweitertes Routing . . . . .	54
8.4.1. Network Address Translation (NAT) . . . . .	54
8.4.2. IP-Masquerading (PAT, NPAT) . . . . .	55
8.4.3. Proxy . . . . .	58
<b>A. Anhang - Zusätzliche Tabellen und Grafiken</b>	<b>59</b>
<b>Literaturverzeichnis</b>	<b>69</b>

# 1. Netzwerkgrundlagen

## 1.1. Was ist Networking?

Unter *Networking* versteht man den Austausch von Informationen und dessen gemeinsame Nutzung in einem Netzwerk.

## 1.2. Modelle, historische Entwicklung

### 1.2.1. Centralized Computing

Beim Centralized Computing steht der Hauptrechner an einem zentralen Ort an dem Terminals angeschlossen sind und über diese man die Ressourcen des zentralen Computers nutzen kann. Dies hat die Vorteile, dass die Sicherheit über das System erhöht wird, da es sich zentral an einem Ort befindet. Hinzukommt, wenn ein Terminal ausfällt, kann an einem anderem Terminal weitergearbeitet werden ohne Daten verloren zu haben. Auf der anderen Seite besteht natürlich der Nachteil, dass wenn der zentrale Computer ausfällt, das ganze System ausfällt.

Da am Anfang des Computerzeitalters Computer noch sehr teuer, groß und wartungsanfällig waren, man aber die Rechenleistung eines Computers mehreren Personen gleichzeitig zur Verfügung stellen wollte, bot sich dieses Art der Nutzung des Computers an. [1]

### 1.2.2. Distributed Computing

Verteiltes Rechnen (auch Dezentralisiertes Rechnen, Verteilte EDV; engl. Distributed Computing) ist eine Technik der Anwendungsprogrammierung, bei der die einzelnen Prozesse einer verteilten Anwendung ein gemeinsames Ergebnis berechnen. Hintergrund ist die Überlegung, dass (u. a.) die Hauptprozessoren vieler Rechner zeitweise nicht ausgelastet sind, da der Anwender meistens nur mit wenigen Programmen arbeitet, welche nur einen Teil der gesamten CPU-Leistung beanspruchen. Diese ungenutzten Ressourcen möchte man beim verteilten Rechnen nutzbar machen. Hierzu wird eine entsprechende Client-Software auf dem betroffenen Rechner installiert, die diese Aufgaben meistens weitgehend im Hintergrund übernimmt. Verteiltes Rechnen muss organisiert werden. Dazu wird eine Software zur Verfügung gestellt, die auf den Clients zur Lösung der speziellen Aufgabe laufen muss. Weiterhin müssen die Aufgaben, die abgearbeitet sind, gerade bearbeitet werden, oder noch verteilt werden müssen, verwaltet werden.

Eines der ersten Projekte, welches die Technik des verteilten Rechnens nutzte, war das SETI@home-Projekt <sup>1</sup> der University of California, Berkeley, das somit die Rechenkraft eines teuren Supercomputers erzielte. [2]

### 1.2.3. Collaborative Computing / Grid Computing

Auf der ganzen Welt existieren viele Millionen von Computern. Neben Desktoprechnern, Laptops und Supercomputern gehört aber auch ein Vielzahl von Instrumenten wie z.B. meteorologische Sensoren oder auch Satelliten dazu. Eine Menge dieser Geräte sind über das Internet miteinander zu einem großen Netzwerk verbunden. Durch das World Wide Web können diese Computer Informationen in Form von Webseiten und anderem miteinander teilen. Ein Grid geht noch einen Schritt weiter in diese Richtung. Die darin enthaltenen Computer und Instrumente teilen nicht nur Informationen miteinander, sondern auch Rechenleistung und Ressourcen wie z.B. Speicherplatz, Datenbanken oder Softwareanwendungen. [3]

**Gegenüberstellung:** Cluster - Grid

<b>Cluster</b>	<b>Grid</b>
Verbund von mehreren Rechnern	Verbund von mehreren Ressourcen
Kommunikation über LAN	Kommunikation über WAN
gemeinsamer lokaler Standort	verteilte Standorte
zentraler Admin	Jede Maschine eigener Admin
Existenz des Clusters wegen Berechnungen	Existenz des Grids aus verschiedenen Gründen
Cluster ist Hauptarbeit der Rechner	Grid ist Nebenarbeit der Ressourcen

**Tab. 1.1.:** Unterschiede zwischen einem Cluster und einem Grid

## 1.3. Unterteilung von Netzwerken (LAN, MAN, WAN)

### LAN

Local Area Network. Lokale Netze sind als feste Installation dort zu finden, wo mehrere Rechner über kleine Entfernungen an einem bestimmten Ort dauerhaft vernetzt werden sollen. Für einzelne Veranstaltungen wie LAN-Partys werden sie auch temporär aufgebaut. [4]

### MAN

Metropolitan Area Network. Ein breitbandiges, in Glasfasertechnologie realisiertes Telekommunikationsnetz, das überwiegend in ringförmiger Struktur aufgebaut ist und die wichtigsten

---

<sup>1</sup><http://setiathome.ssl.berkeley.edu/>

Bürozentren einer Großstadt miteinander verbindet. Ein MAN kann eine Ausdehnung bis zu 100 km haben. [5]

### **WAN**

Wide Area Network. Ein Weitverkehrsnetz ist ein Rechnernetz, das sich im Gegensatz zu einem LAN oder MAN über einen sehr großen geografischen Bereich erstreckt. Die Anzahl der angeschlossenen Rechner ist auf keine bestimmte Anzahl begrenzt. WANs erstrecken sich über Länder oder sogar Kontinente. WANs werden benutzt, um verschiedene LANs, aber auch einzelne Rechner miteinander zu vernetzen. Einige WANs gehören bestimmten Organisationen und werden ausschließlich von diesen genutzt. Andere WANs werden durch Internetdienstleister errichtet oder erweitert, um einen Zugang zum Internet anbieten zu können. Ein WAN arbeitet auf der Bitübertragungsschicht und der Sicherungsschicht des OSI-Referenzmodells<sup>2</sup>. [6]

---

<sup>2</sup>Als OSI-Modell (<http://de.wikipedia.org/wiki/OSI-Referenzmodell>) wird ein Schichtenmodell der Internationalen Standardisierungsorganisation (ISO) bezeichnet. Es wurde als Designgrundlage von Kommunikationsprotokollen entwickelt. Die Aufgaben der Kommunikation wurden dazu in sieben aufeinander aufbauende Schichten (layer) unterteilt. Für jede Schicht existiert eine Beschreibung, was diese zu leisten hat. Diese Anforderungen müssen von den Kommunikationsprotokollen realisiert werden. Die konkrete Umsetzung wird dabei nicht vorgegeben und kann daher sehr unterschiedlich sein.



## 2. Netzwerkdienste

Netzwerke sind Ansammlungen von Ressourcen, die gemeinsam genutzt werden. Netzwerkdienste stellen diese Ressourcen zur Verfügung.

Man unterscheidet:

**File-Services:** Dateitransfer, Datenspeicherung und -migration, Dateiabgleich, Datenarchivierung

**Print-Services:** Keine Distanz-Beschränkungen, Mehrfachzugriff, Handling gleichzeitiger Zugriffe, Netzwerk-Fax

**Message-Services:** E-Mail, Voice-Mail

**Application-Services:** Server-Spezialisierung, Skalierbarkeit

**Database-Services:** Verteilte Datenbanken, Replikation



## 3. Übertragungsmedien

### 3.1. Frequenzbereiche

Geordnet nach der Wellenlänge, befinden sich an dem einen Ende des Spektrums die Radiowellen, deren Wellenlängen von wenigen Zentimetern bis zu vielen Kilometern reichen. Am anderen Ende des Spektrums sind die sehr kurzwelligen und damit energiereichen Gammastrahlen, deren Wellenlänge bis in atomare Größenordnungen reicht. [7]

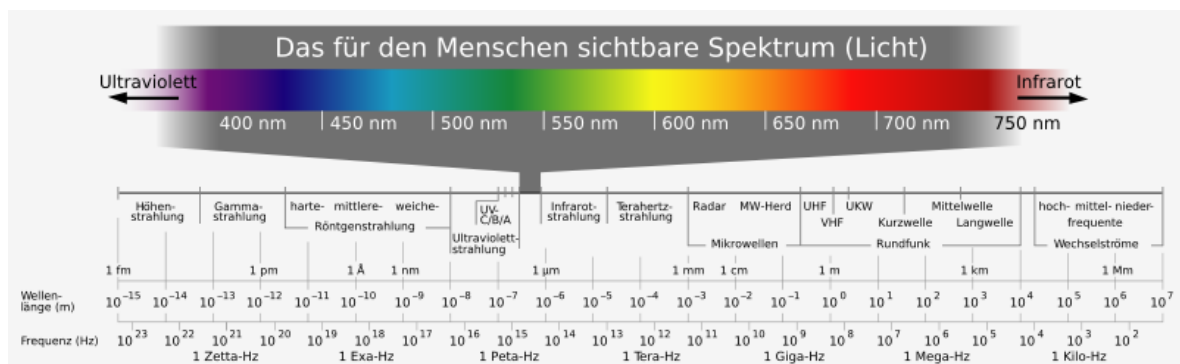


Abb. 3.1.: Das elektromagnetische Wellenspektrum

Weitere Erläuterungen dazu siehe im Anhang *Tabelle Frequenzspektrum* (Seite 60).

Die Umrechnung von der Wellenlänge in eine Frequenz erfolgt mit der einfachen Formel:

$$\text{Frequenz} = \frac{\text{Lichtgeschwindigkeit}}{\text{Wellenlänge}} \quad (3.1)$$

$$f\left[\frac{1}{s}\right] = \frac{c\left[\frac{m}{s}\right]}{\lambda[m]} \quad (3.2)$$

$$\text{Lichtgeschwindigkeit} = 3 \times 10^8 \frac{m}{s} \quad (3.3)$$

## 3.2. Einteilung von Übertragungsmedien

Für eine grafische Übersicht über die Einteilung von Übertragungsmedien siehe Grafik *Einteilung von Übertragungsmedien* (Seite 61).

### 3.2.1. Kabelmedien

#### Verdrilltes Doppelleiterkabel (Twisted Pair)



**Abb. 3.2.:** STP-Kabel im Schnitt

Als Twisted-Pair-Kabel bezeichnet man Kabeltypen, bei denen die beiden Adern eines Adernpaares miteinander verdrillt sind.

Verdrillte Adernpaare bieten Schutz gegen den störenden Einfluss von äußeren magnetischen Wechselfeldern auf die übertragenen Signale. Unterschiedliche Schlaglängen der Adernpaare reduzieren dabei ein Übersprechen zwischen benachbarten Adernpaaren im Kabel. Ein elektrisch leitender Schirm (z. B. aus Aluminiumfolie, Kupfergeflecht) bietet zusätzlich Schutz gegen störende äußere elektromagnetische Felder.

Twisted Pair Kabel gibt es in den Ausführungen nicht abgeschirmt (Unshielded Twisted Pair, UTP), abgeschirmt (Shielded Twisted Pair, STP) und teilweise abgeschirmt (S-UTP). [8]

#### UTP

Kabel mit ungeschirmten Paaren und ohne Gesamtschirm.

<b>Kenngröße</b>	<b>Bewertung</b>
Anschaffungskosten	sehr gering
Installationsaufwand	gering
Kapazität	bis 155 Mbps
Signalabschwächung	sehr hoch
Störfestigkeit	gering

**Tab. 3.1.:** UTP-Kenngrößen

#### STP-Kabel

Kabel mit geschirmten Adernpaaren.

<b>KenngroÙe</b>	<b>Bewertung</b>
Anschaffungskosten	gering
Installationsaufwand	moderat
Kapazität	bis 1000 Mbps
Signalabschwächung	hoch
Störfestigkeit	moderat

Tab. 3.2.: STP-KenngroÙen

**SUTP-Kabel**

Kabel mit ungeschirmten Adernpaaren und Gesamtschirm.

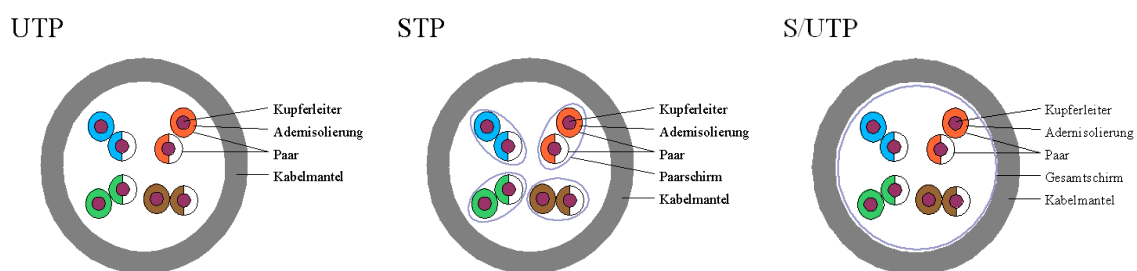


Abb. 3.3.: UTP-, STP- und SUTP-Kabel

**Koaxialkabel**

Koaxialkabel, kurz: Koaxkabel sind zweiadrige Kabel mit konzentrischem Aufbau. Sie bestehen aus einem Innenleiter, der von einem in konstantem Abstand um den Innenleiter angebrachten, hohlzylindrischen Außenleiter umgeben ist. Im Zwischenraum befindet sich ein Isolator bzw. Dielektrikum. Der Außenleiter beim Koaxialkabel ist nicht nur Schirmung, sondern einer der beiden Leiter. Hingegen ist bei einer geschirmten Leitung der Kabelschirm oft nur an einer Seite angeschlossen und hat lediglich eine abschirmende Wirkung gegenüber störenden elektrischen Feldern.

<b>KenngroÙe</b>	<b>Bewertung</b>
Anschaffungskosten	mittel
Installationsaufwand	mittel
Kapazität	bis in den Gbps Be- reich
Signalabschwächung	gering
Störfestigkeit	mittel

Tab. 3.3.: Koaxialkabel-KenngroÙen

#### Lichtwellenleiter

Lichtwellenleiter bestehen aus hochtransparenten Glasfasern, die mit einem Glas niedrigerer Brechung ummantelt sind. Die Faser besteht aus einem Kern, einem Mantel und einer Schutzbeschichtung. Der lichtführende Kern dient zum Übertragen des Signals. Der Mantel hat eine niedrigere optische Brechzahl (Dichte) als der Kern. Der Mantel bewirkt dadurch eine Totalreflexion an der Grenzschicht und somit eine Führung der Strahlung im Kern des Lichtwellenleiters. [9]



Abb. 3.4.: Funktionsweise eines Lichtwellenleiters [10]

#### Multimode

Bei Multimode (mehrere Phasen) Lichtwellenleitern wird eine Leuchtdiode als Lichtquelle für die Signale genutzt. Leuchtdioden senden aber kein streng monochromatisches<sup>1</sup> und kohärentes<sup>2</sup> Licht aus, das hat zur Folge, dass die einzelnen „Lichtstrahlen“ unterschiedlich von der Grenzschicht reflektiert werden, da die Reflexion bzw. Brechung auch abhängig von der Frequenz der Lichtwellen ist. Das Signal wird also „verwaschener“, je länger die Strecke ist, die es zurücklegt. Deswegen beträgt die maximale Übertragungreichweite bei einem Kerndurchmesser von 50  $\mu\text{m}$  ca. 550 m und bei 62,5  $\mu\text{m}$  ca. 275 m.

#### Mono- oder Singlemode

Im Gegensatz zu den Leuchtdioden bei Multimode Lichtwellenleitern, werden beim Mono- oder Singlemode Laser<sup>3</sup> als Lichtquellen für die Signale genutzt. Laserlicht ist streng monochromatisch und kohärent. Mit diese Eigenschaften lässt sich Laserlicht optimal durch Linsen bündeln bzw. reflektieren, da es eben streng monochromatisch ist. Singlemode-Fasern haben üblicherweise einen deutlich kleineren Kern als Multimode-Fasern. Die kommerziell nutzbaren, möglichen Bandbreite-Länge-Produkte betragen bei Verwendung entsprechender Zwischenverstärker heutzutage (Frühjahr 2000) größenordnungsmäßig 100 (Gbit / s)km - also beispielsweise 1 Gbit/s über 100 km. Technisch möglich sind bereits mehrere (Tbit/s)km, so dass in naher Zukunft die Einrichtung von Netzen dieser Kapazität erfolgen wird.

<sup>1</sup> monochromatisch: eine Frequenz ( einfarbig)

<sup>2</sup> kohärent: gleiche Phasenlage

<sup>3</sup> Laser steht für Light Amplification by Stimulated Emission of Radiation (Lichtverstärkung durch Induzierte Emission). [22]

<b>Kenngröße</b>	<b>Bewertung</b>
Anschaffungskosten	hoch
Installationsaufwand	hoch
Kapazität	mehrere Gbps
Signalabschwächung	sehr gering
Störfestigkeit	maximal

Tab. 3.4.: Lichtwellenleiter-Kenngrößen

	<b>UTP</b>	<b>STP</b>	<b>Koax</b>	<b>LWL</b>
<b>Anschaffungskosten</b>	sehr gering	gering	mittel	hoch
<b>Installationsaufwand</b>	gering	moderat	mittel	hoch
<b>Kapazität</b>	bis 155 Mbps	bis 1000 Mbps	wenige Gbps	mehrere Gbps
<b>Signalabschwächung</b>	sehr hoch	hoch	gering	sehr gering
<b>Störfestigkeit</b>	gering	moderat	mittel	maximal

Tab. 3.5.: Zusammenfassung: Kabelmedien

### 3.2.2. Kabellose Medien

#### Radiowellen

Radiowellen sind elektromagnetische Wellen in einem Frequenzbereich von einigen kHz (Längswellen) bis etwa 3 GHz (hier schließen sich die Mikrowellen an).

Die zu übertragende Information wird bei der Nachrichtenübertragung einer Trägerwelle durch Modulation aufgeprägt und von der Sendeantenne abgestrahlt. In der Empfangsantenne werden durch die Radiowellen gleichartige Schwingungen induziert, aus denen nach vorhergehender Verstärkung die Information wieder demoduliert wird.

<b>Kenngröße</b>	<b>Bewertung</b>
Frequenzbereich	10 kHz bis 2 GHz
Anschaffungskosten	gering bis moderat
Installationsaufwand	gering
Kapazität	bis 100 Mbps
Signalabschwächung	zwischen gering und hoch
Störfestigkeit	zwischen sehr gering und hoch

Tab. 3.6.: Radiofrequenz-Kenngrößen

Elektromagnetische Wellen können reflektiert werden. Dadurch kann es zu Interferenzen<sup>4</sup>, Auslöschungen oder Verstärkungen kommen. Metall und Wasser können die Ausbreitung behindern. So kann Putz mit einem sehr hohem Feuchtigkeitsgehalt die Ausbreitung von WLAN-Wellen behindern. Längswellen hingegen können sich auch unter Wasser ausbreiten und werden zur Kommunikation mit U-Booten genutzt.

<sup>4</sup>Interferenz: Überlagerung von zwei oder mehr Wellen

Ab dem Bereich von Mikrowellen werden Parabolantennen<sup>5</sup> anstatt Dipolantennen<sup>6</sup> (Abb. 3.5, Seite 18) zum Empfang eingesetzt (wobei die Grenze fließend ist). [11], [12], [13]



**Abb. 3.5.:** Dipolantenne

#### Berechnung der Antennenlänge

Die Länge der Antenne sollte in der Größenordnung der zu empfangenen Radiowellenlänge entsprechen. Desweiteren ist die Länge der Antenne abhängig von deren Bauweise. Üblicherweise schwingt sie mit  $\frac{\lambda}{2}$  oder  $\frac{\lambda}{4}$ . Aus der Formel 3.1 (Seite 13) für die Frequenz ergibt sich für die Wellenlänge:

$$\text{Wellenlänge} = \frac{\text{Lichtgeschwindigkeit}}{\text{Frequenz}} \quad (3.4)$$

Bei einer Frequenz von 300 Hz muss eine Antenne mit  $\frac{\lambda}{4}$

$$\frac{3 \times 10^8 \frac{m}{s}}{3 \times 10^2 \frac{1}{s}} = 1 \times 10^6 m \quad (3.5)$$

$$1.000.000m : 4 = \underline{250.000m} \quad (3.6)$$

250 km lang sein.

Entsprechend die Länge einer WLAN-Antenne ( $f = 2,4 \text{ GHz}$ ):

$$\frac{3 \times 10^8 \frac{m}{s}}{2,4 \times 10^9 \frac{1}{s}} = 1,25 \times 10^{-1} = \underline{0,125m} \quad (3.7)$$

---

<sup>5</sup>Eine Parabolantenne bündelt Mikrowellenstrahlung im Brennpunkt eines Parabolspiegels. Dort wird die Strahlung von einem Detektor erfasst und weitergeleitet.

<sup>6</sup>Eine Dipolantenne ist eine gestreckte Antenne, die aus zwei gleich langen geraden Metallstäben, -drähten oder -flächen besteht. Sie wandelt hochfrequenten Wechselstrom und elektromagnetische Wellen ineinander um.

## Mikrowellen

Der Begriff Mikrowellen fasst die Dezi-, Zenti- und Millimeterwellen zusammen. Mikrowellen sind elektromagnetische Wellen, deren Wellenlänge zwischen 1 m und 1 mm liegt, was einem Frequenzbereich von etwa 300 MHz bis etwa 300 GHz entspricht.

Aufgrund ihrer Wellenlänge sind Mikrowellen besonders zum Anregen von Dipol- und Multipolschwingungen von Molekülen geeignet. Besonders anschaulich ist dieser Effekt bei der Schwingungsanregung von Wassermolekülen im Mikrowellenherd. Die Erwärmung von Wasser beruht nicht auf einer bestimmten Resonanzfrequenz, sondern die Wassermoleküle als Dipole versuchen sich laufend nach den elektromagnetischen Wechselfeld auszurichten, wobei als dielektrischer Verlust Wärme entsteht. [14]

<b>Kenngröße</b>	<b>Bewertung</b>
Frequenzbereich	1 GHz bis etwa 25 GHz
Anschaffungskosten	mittel bis hoch
Installationsaufwand	hoch
Kapazität	bis 100 Mbps
Signalabschwächung	mittel
Störfestigkeit	sehr gering

**Tab. 3.7.:** *Mikrowellen-Kenngrößen*

**(Infrarot-)licht**

Kenngroße	Bewertung
Frequenzbereich	100 GHz bis etwa 1000 THz
Anschaffungskosten	gering
Installationsaufwand	sehr gering
Kapazität	bis 20 Mbps
Signalabschwächung	mittel
Störfestigkeit	mittel

**Tab. 3.8.:** Infrarotlicht-Kenngrößen

	Radiowellen	Mikrowellen	Infrarotlicht
<b>Anschaffungskosten</b>	gering bis moderat	mittel bis hoch	mittel
<b>Installationsaufwand</b>	gering	hoch	sehr gering
<b>Kapazität</b>	bis 100 Mbps	bis 100 Mbps	bis 20 Mbps
<b>Signalabschwächung</b>	gering bis hoch	mittel	mittel
<b>Störfestigkeit</b>	sehr gering bis hoch	sehr gering	mittel

**Tab. 3.9.:** Zusammenfassung: Kabellose Medien

**3.3. Crossover-Patchkabel**

Verbindet man zwei Netzwerkkomponenten (Computer, Router, Switch, Hub) mit einander, die zu einer Klasse gehören, so muss ein Crossover-Patchkabel verwendet werden, wenn die Komponenten (Netzwerkkarten) nicht in der Lage sind Sende- und Empfangsleitung selber auszuhandeln. Bei einem Crossover-Patchkabel handelt es sich um ein Twisted Pair Kabel mit gekreuzten Adern. Im Kabel werden also an einem Ende die Sendedaten mit den Empfangsdaten vertauscht damit bei einer 1on1 Verbindung auch der Datenaustausch erfolgt. Würde man die Sende-/ Empfangsdaten an einem Ende nicht tauschen würde keine Verbindung untereinander entstehen. [21]

Adern Belegung Crossover-Patchkabel:



**Abb. 3.6.:** Crossover-Patchkabel mit 2 ge- **Abb. 3.7.:** Crossover-Patchkabel mit 4 ge-  
nutzten Adernpaaren nutzten Adernpaaren

### 3.4. Kabelabschluss

Offene Kabelenden reflektieren das eingespeiste Signal, deswegen muss ein offenes Kabelende mit einem passenden Widerstand abgeschlossen werden (TP:  $100 \Omega$ ). In Netzwerkkarten ist standardmäßig ein solcher Widerstand eingebaut. Treffen sich reflektierte Signale, kommt es zu Kollisionen, die die übertragenen Daten unbrauchbar machen. Um auf diese Kollisionen reagieren zu können, werden entsprechende Verfahren eingesetzt. Siehe dazu Kapitel 3.5, Seite 21.

### 3.5. Mehrfachzugriff auf Übertragungsmedien (CSMA)

Damit mehrere Teilnehmer eine Busleitung benutzen können ohne sich gegenseitig zu stören, darf immer nur ein Sender senden. So bald mehr als ein Sender gleichzeitig senden, kommt es zu Kollisionen in der Busleitung und das Signal wird unbrauchbar. Um zu verhindern, dass mehrere Sender gleichzeitig senden, wird unter anderem das so genannte *Carrier Sense Multiple Access (CSMA)* (deutsch etwa: Mehrfachzugriff mit Trägerprüfung) Verfahren eingesetzt. Es handelt sich dabei um ein dezentrales Verfahren zum Erlangen des Zugriffsrechts nach dem Konkurrenzverfahren auf Busleitungen. Trägerprüfung bzw. Carrier Sense bedeutet, dass alle Teilnehmer den Status der Busleitung beobachten und ihre Nachrichten nur senden, wenn gerade kein anderer Teilnehmer sendet, der Kanal also frei ist. Ist das Medium für eine bestimmte Zeitspanne nicht belegt, wird es als frei betrachtet.

CSMA teilt sich wiederum in verschiedene Verfahren zur Behandlung oder Vermeidung einer Kollision auf dem Bus auf. Man unterscheidet drei Arten von CSMA:

- 1-Persistent: Sofort nachdem das Medium als besetzt erkannt wird, wird wieder geprüft, und wenn frei, wird gesendet (mit Wahrscheinlichkeit 1, d.h. immer).
- P-Persistent: Es wird mit der Wahrscheinlichkeit P, nachdem der Kanal als frei identifiziert wurde, angefangen zu senden.
- Non-Persistent: Nachdem das Medium als besetzt erkannt wird, wird für ein zufälliges Zeitintervall gewartet, und danach wieder geprüft; wenn frei, dann wird gesendet.

#### **Carrier Sense Multiple Access/Collision Avoidance**

CSMA/CA vermeidet Kollisionen durch eine zufällige Wartezeit nach der Kanalfrei-Erkennung. sollte jedoch nicht mit dem Multiplexverfahren CDMA, das in der Mobilfunktechnik Anwendung findet, verwechselt werden. Hauptverwendungsgebiet sind Funknetzwerke.

#### **Carrier Sense Multiple Access/Collision Detection**

CSMA/CD erkennt Kollisionen und versucht die Konkurrenzsituation durch Abbruch der aktuellen Sendung und anschließende unterschiedliche Sendeverzögerung zu vermeiden. Da die Sendeverzögerungen im Normalfall zufällig gewählt werden, handelt es sich um ein stochastisches Verfahren. CSMA/CD ist auch die Zugangstechnologie in lokalen Computernetzwerken und wird häufig mit dem Begriff Ethernet gleichgesetzt.

#### **Carrier Sense Multiple Access/Collision Resolution**

CSMA/CR erkennt Kollisionen und löst die Konkurrenzsituation durch Prioritätsanalyse beim

### *3. Übertragungsmedien*

---

gleichzeitigen Start von Übertragungen. Es handelt sich hierbei um eine nicht-deterministische Methode.

[20]

## 4. Netzwerk-Koppelemente

Mit Netzwerk-Koppelementen werden Endgeräte eines Netzwerkes miteinander an ein Übertragungsmedium angeschlossen. Man unterscheidet zwischen Segment-Koppelementen und Verbundnetz-Koppelementen.

### 4.1. Segment-Koppelemente

Segment-Koppelemente verbinden Endgeräte innerhalb eines Netzwerkes miteinander.

#### 4.1.1. Stecker

Steckertypen:

- RJ-45 (für Twisted Pair, <http://de.wikipedia.org/wiki/RJ-45>)
- BNC (für Koaxialkabel, [http://de.wikipedia.org/wiki/Koaxiale\\_Steckverbinder](http://de.wikipedia.org/wiki/Koaxiale_Steckverbinder))
- ST (für Glasfaserkabel, <http://de.wikipedia.org/wiki/ST-Stecker>)
- SC (für Glasfaserkabel, <http://de.wikipedia.org/wiki/SC-Stecker>)
- DB-15
- MIC
- DB-25

Siehe Abbildung A.2 im Anhang auf Seite 62.

#### 4.1.2. Netzwerkkarten

Eine Netzwerkkarte ist eine elektronische Schaltung zur Verbindung eines Computers mit einem lokalen Netzwerk zum Austausch von Daten. Sie ist ein Gerät der OSI-Schicht 1. Ihre primäre Aufgabe ist die Herstellung einer physikalischen Verbindung zum Netzwerk über ein geeignetes Zugriffsverfahren und die Implementierung der ersten und/oder zweiten OSI-Schicht (Siehe Fussnote Seite 9.) (meist Ethernet). [15]

### 4.1.3. Modems

Ein Modem (aus Modulator und Demodulator gebildete Abkürzung) dient dazu, digitale Daten in für eine analoge Leitung geeignete Signale umzuwandeln und auf der anderen Seite wieder in digitale Daten zurückzuwandeln. Modems gehören zu der OSI-Schicht 1. Die dafür verwendete Modulation ist auf die analoge Leitung abgestimmt. Mit einem Modem werden digitale Daten durch Modulation eines analogen Signals über analoge Kommunikationsnetze übertragen. Am anderen Endpunkt der Kommunikation werden die digitalen Daten durch Demodulation aus dem analogen Signal wieder zurückgewonnen. [16]

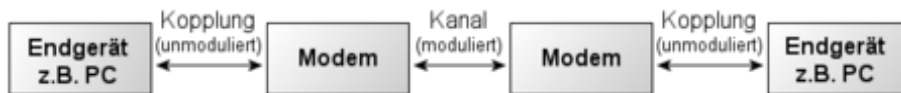


Abb. 4.1.: Prinzip eines Modems

Das hochfrequente „Zwitschern“, was man bei einem Verbindungsaufbau bei einem Modem hört, entsteht bei der Modulation des Signals. Dies kann man hören, da die Verbindung mit der geringsten Übertragungsgeschwindigkeit aufgebaut wird. Dabei wird dann die höchst mögliche Geschwindigkeit der beiden Endstellen ausgehandelt. Meist liegt diese so hoch, dass das menschliche Ohr bei der Modulation des folgenden Datenverkehrs höchsten noch ein Rauschen wahrnimmt.

### 4.1.4. Repeater

Der Repeater in der digitalen Kommunikationstechnik ist ein Signalregenerator, der in der Bitübertragungsschicht ein Signal empfängt, dieses dann neu aufbereitet und wieder aussendet. Sie sind Geräte der OSI-Schicht 1. Rauschen sowie Verzerrungen der Laufzeit (Jitter) und der Pulsform werden bei dieser Aufbereitung aus dem empfangenen Signal entfernt. In lokalen Netzen werden Repeater verwendet, um mehrere Netzsegmente miteinander zu verbinden. Der Einsatz von Repeatern bietet sich z.B. bei LANs in Bus-Topologie an, um die maximale Kabellänge von z.B. 185 m bei 10Base2<sup>1</sup> zu erweitern. Der Repeater teilt das Netz zwar in zwei physische Segmente, die logische Bus-Topologie bleibt aber erhalten. Durch diesen Effekt erhöht der Repeater die Ausfallsicherheit des Netzes, da bei Wegfall eines Teilnetzes das jeweils Andere weiter unabhängig agieren kann. Einen Multiportrepeater bezeichnet man meistens als *Hub*. Ein Hub verteilt automatisch ankommende Pakete auf alle Ausgänge. [17]

### 4.1.5. Bridge / Switch

Eine Bridge verbindet im Computernetz zwei Segmente auf der Ebene der Schicht 2 (Sicherungsschicht) des OSI-Modells. Die Pins an den Ports von Switches sind so geschaltet, dass

<sup>1</sup>10: 10 MBit/s.

**Base:** Basisband (Übertragung eines digitalen Signals mit einem Sender. Werden mehrere analoge Signale auf verschiedenen Frequenzen übertragen, spricht man von Breitband).

**2:** Entfernung in 100 Metern, hier also 200m. (Nachträglich auf 185m begrenzt.)

eine Kommunikation mit den Endgeräten über ein einfaches Patch-Kabel möglich ist. Man braucht also kein Crossover-Patchkabel (Siehe Seite 20), um Endgeräte mit einem Switch zu verbinden.

Eine Transparente Bridge lernt, welche MAC-Adressen sich in welchem Teilnetz befinden. Die Bridge lernt mögliche Empfänger, indem die Absender von Paketen in den einzelnen Teilnetzen in eine interne Weiterleitungstabelle eingetragen werden. Anhand dieser Informationen kann die Bridge den Weg zum Empfänger bestimmen. Die Absenderadressen werden laufend aktualisiert, um Änderungen sofort zu erkennen. Eine Source Routing Bridge besitzt keine Weiterleitungstabelle. Hier muss der Sender die Informationen zur Weiterleitung zum Ziel bereitstellen. Ein Paket muss nur dann an alle Teilnetze gesendet werden, wenn der Empfänger nicht in dieser Tabelle eingetragen ist und das Zielnetz somit nicht bekannt ist. Ein Broadcast wird stets in alle Teilnetze übertragen. Dies entlastet das Netz. Eine Multiport-bridge bezeichnet man auch als *Switch*. [18]

### **Uplink Port**

Manche Switches sind mit einem sogenannten *Uplink Port* ausgestattet. An diesem Port sind die Pins nicht vertauscht, so dass man über diesen Port den Switch mit einem normalen Patchkabel mit einem anderen Switch verbinden kann. Bei manchen Switches kann dieser Port auch als normaler Port verwendet werden, dann kann die Pin-Belegung entweder manuell oder automatisch entsprechend umgeschaltet werden.

## **4.2. Verbundnetz-Koppelemente**

Verbundnetz-Koppelemente verbinden Netzwerke untereinander.

### **4.2.1. Router**

Ein Router koppeln mehrere Rechnernetze. Die beim Router eintreffenden Netzwerk-Pakete eines Protokolls werden auf Basis von Layer-3-Informationen (OSI-Modell) analysiert und zum vorgesehenen Zielnetz weitergeleitet oder geroutet. Beim Eintreffen von Daten muss ein Router den richtigen Weg zum Ziel und damit die passende Schnittstelle bestimmen, über welche die Daten weiterzuleiten sind. Dazu bedient er sich einer lokal vorhandenen Routingtabelle, die angibt, über welchen Anschluss des Routers (bzw. welche Zwischenstation) welches Netz erreichbar ist. Üblicherweise ist ein Eintrag in der Routingtabelle die Default-Route (auch Standard-Gateway); diese Route wird für alle Ziele benutzt, die über keinen besser passenden Eintrag in der Routingtabelle verfügen. Professionelle Router beherrschen mittlerweile auch ein sogenanntes Policy Based Routing; dabei wird die Routingscheidung nicht nur auf Basis des gewünschten Ziel-Netzes getroffen (Layer-3), sondern auch der gewünschte Dienst berücksichtigt. Beispielsweise kann hierdurch die Default-Route für Web (HTTP) eine andere sein als die Default-Route für Mail (SMTP).

#### 4. Netzwerk-Koppelemente

---

Router arbeiten medienunabhängig<sup>2</sup>, aber protokollabhängig<sup>3</sup> - bei einer Bridge ist dies genau umgekehrt. [19]

Um zu verhindern, dass ein unzustellbares Paket unendlich lange weitergeroutet wird, gibt es im Header jedes Paketes ein Feld (Time-to-live, TTL), welches mit einem Wert initialisiert wird. bei jedem Routing-Vorgang wird dieses Feld dekrementiert. Sofern das Paket längere Zeit auf dem Router „hängt“, sollte das TTL-Feld pro Sekunde auch um eins verringert werden. So bald es den Wert null hat, wird das Paket als Irrläufer verworfen. Pakete mit speziell modifizierten TTL-Werten kommen beim so genannten Traceroute zum Einsatz.

Bei Switches hingegen wird dafür das Spanningtree Protokoll<sup>4</sup>, basierend auf dem Spanning Tree Algorithmus von Radia Perlman verwendet.

---

<sup>2</sup>Medienunabhängig bedeutet, dass die Schnittstellen eines Routers Teil unterschiedlicher Netze (wie Token Ring, Ethernet, WLAN - aber auch ISDN oder ATM) sein können.

<sup>3</sup>Die Protokollabhängigkeit eines Routers ergibt sich daraus, dass ein Router nur ihm bekannte Protokolle der Schicht 3 des OSI-Referenzmodells weiterleiten kann. Ein Router, der mehrere Protokolle weiterleiten kann (z. B. IP und IPX), wird auch Multi-Protocol-Router genannt.

<sup>4</sup>[http://de.wikipedia.org/wiki/Spanning\\_Tree\\_Protocol](http://de.wikipedia.org/wiki/Spanning_Tree_Protocol)

## 5. Strukturierte Verkabelung

Eine strukturierte Verkabelung bildet die Grundlage für eine zukunftsorientierte, anwendungsunabhängige Netzwerkinfrastruktur. Es soll teure Fehlinstallationen und Erweiterungen vermeiden und die Installation von neuen Netzwerkkomponenten erleichtern. Eine strukturierte Verkabelung basiert auf einer allgemeingültigen Verkabelungsstruktur, die auch die Anforderungen mehrerer Jahre berücksichtigt, Reserven enthält und unabhängig von der Anwendung genutzt werden kann. [40]

Die strukturierte Verkabelung ist demnach eine anwendungsneutrale, einheitlich aufgebaute Gebäudeverkabelung, in die verschiedene Dienste integriert werden können. Dabei sind Topologie, Komponenten und Übertragungstechnik fest definiert.

### 5.1. Bereiche

Man unterscheidet dabei drei Bereiche: Den Primärbereich, den Sekundärbereich und den Tertiärbereich.

#### 5.1.1. Der Primärbereich

Der Primärbereich ist die Verkabelung der Gebäude eines Standortes untereinander und wird auch als Campusverkabelung oder Geländeverkabelung bezeichnet. Der Primärbereich umfasst den Standortverteiler zur Aussenanbindung des Standortes, die Gebäudeverteiler und die Kabel zwischen den Gebäudeverteilern (Primärkabel) eines LAN. Im Primärbereich sind große Entfernungen, hohe Datenübertragungsraten sowie eine geringe Anzahl von Anschlusspunkten bestimmend. Hier ist die Glasfaser als Übertragungsmedium wegen ihrer geringen Dämpfung, großen Bandbreite (und damit Einsparung vieladrigere Kupferkabel) und der elektromagnetischen Unempfindlichkeit besonders geeignet. Zudem findet eine galvanische Trennung statt und es kann auf einen aufwendigen Potentialausgleich zwischen den Gebäuden verzichtet werden. Ebenfalls praktiziert wird eine Anbindung über die Telefonleitung mit VDSL, sofern eine entsprechende Schaltung möglich ist. Verwendete Kabelarten: Glasfaserkabel, Kupferkabel.

Maximale Längen:

- LWL : 1500 m vom Standortverteiler zum Gebäudeverteiler
- VDSL: Bis 900 m: Von 52 Mbit/s abfallend zu 26 Mbit/s; Bei 2 km ADSL Übertragungsraten

### 5.1.2. Der Sekundärbereich

Der Sekundärbereich ist die vertikale Stockwerkverkabelung; die Verkabelung der Stockwerke eines Gebäudes untereinander und wird auch als Steigbereichverkabelung bezeichnet. Der Sekundärbereich umfasst die Stockwerkverteiler oder Etagenverteiler (Switches) und die Kabel die vom Gebäudeverteiler (Serverraum) zu den einzelnen Stockwerkverteilern (Sekundärkabel) führen. Verwendete Kabelarten (nach DIN): Glasfaserkabel.

Maximale Länge: 500 m

### 5.1.3. Der Tertiärbereich

Der Tertiärbereich ist die horizontale Stockwerkverkabelung, also die Verkabelung innerhalb der Stockwerke eines Gebäudes und wird auch als Etagenverkabelung bezeichnet. Der Tertiärbereich umfasst die Kabel vom Stockwerkverteiler zu den Anschlussdosen (Tertiärkabel) und die Anschlussdosen selbst. Verwendete Kabelarten: Twisted-Pair-Kabel, bei Fiber to the Desk auch Glasfaserkabel.

Maximale Länge: 100 m, wobei 90 m feste Verkabelung (BASIC-Link, auch als Installationskabel bezeichnet) und 10 m (2 x 5 m) lose Verkabelung (CHANNEL-Link, auch als Patch- oder Rangierkabel bezeichnet) vorgesehen sind.

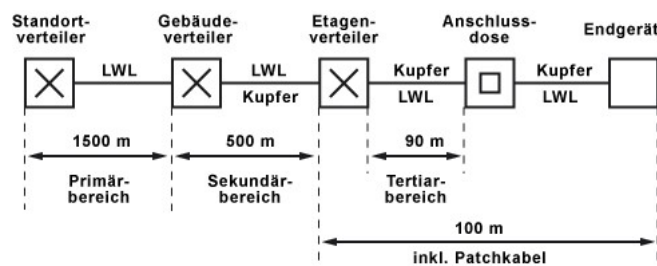


Abb. 5.1.: Übersicht der Bereiche bei der strukturierten Verkabelung

[39]

## 6. Die IP-Adresse

Eine IP-Adresse (Internet-Protocol-Adresse) dient zur eindeutigen Adressierung von Rechnern und anderen Geräten in einem IP-Netzwerk. Technisch gesehen ist die Nummer eine 32- oder 128-stellige Binärzahl. Das bekannteste Einsatzgebiet in dem IP-Adressen verwendet werden, ist das Internet. Allen am Internet teilnehmenden Rechnern wird eine IP-Adresse zugeteilt. Die IP-Adresse entspricht funktional der Telefonnummer in einem Telefonnetz.

### 6.1. Grundlagen

Um eine Kommunikation zwischen zwei technischen Geräten aufzubauen, muss jedes der Geräte in der Lage sein, dem anderen Gerät Daten zu senden. Damit diese Daten bei der richtigen Gegenstelle ankommen, muss die Gegenstelle eindeutig benannt (adressiert) werden. Dies geschieht in IP-Netzen mit einer IP-Adresse.

So wird zum Beispiel ein Webserver von einem Webbrowser direkt über seine IP-Adresse angesprochen. Der Browser fragt dazu für einen Domainnamen, zum Beispiel „www.bundestag.de“, die IP-Adresse bei einem Nameserver an und spricht deren Webserver direkt unter seiner IP-Adresse „217.79.215.140“ an.

IP-Adressen (Internet Protocol Adressen) werden in jedem IP-Paket<sup>1</sup> in die Quell- und Zieladressfelder eingetragen (Headerformat siehe IPv4-Header-Format<sup>2</sup>). Jedes IP-Paket enthält damit sowohl die Adresse des Senders als auch die des Empfängers. IP-Adressen befinden sich im OSI-Modell auf Schicht 3, der Vermittlungsschicht.

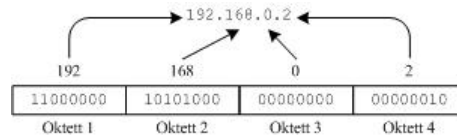
### 6.2. Aufbau

Die seit der Einführung der Version 4 des Internet Protocols überwiegend verwendeten IPv4-Adressen bestehen aus 32 Bits, also 4 Oktetts (Bytes). Damit sind  $2^{32}$ , also 4.294.967.296 Adressen darstellbar. In der dotted decimal notation werden die 4 Oktetts als vier durch Punkte voneinander getrennte ganze Zahlen in Dezimaldarstellung im Bereich von 0 bis (einschließlich) 255 geschrieben, Beispiel: 130.94.122.195. Siehe dazu Grafik 6.1 *Struktur von IPv4-Adressen* auf Seite 30.

Durch den rasch steigenden Bedarf an IP-Adressen ist absehbar, dass der nutzbare Adressraum von IPv4 früher oder später erschöpft sein wird. Vor allem aus diesem Grund wurde

<sup>1</sup>Wikipedia: <http://de.wikipedia.org/wiki/IP-Paket>

<sup>2</sup>Wikipedia: <http://de.wikipedia.org/wiki/IPv4#Header-Format>



**Abb. 6.1.:** Struktur von IPv4-Adressen

IPv6 entwickelt. Es verwendet 128 Bit zur Speicherung von Adressen, damit sind  $3,4 \times 10^{38}$  Adressen darstellbar. Diese Zahl reicht aus, um für jeden Quadratmeter der Erdoberfläche mindestens  $6,65 \times 10^{23}$  IP-Adressen bereitzustellen. Damit sollten in absehbarer Zukunft keine Adressraumprobleme bei der Verwendung von IPv6 zu befürchten sein.

Da die Dezimaldarstellung

ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd

unübersichtlich und schlecht handhabbar wäre, stellt man IPv6 Adressen hexadezimal dar. Um diese Darstellung weiter zu vereinfachen, werden jeweils zwei Oktetts der Adresse zusammengefasst und in Gruppen durch Doppelpunkt getrennt dargestellt.

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

(jeder Doppelpunkt trennt zwei Oktetts der Adresse ab).

Beispiel: 2001:0db8:85a3:08d3:1319:8a2e:0370:7344

### 6.3. Die Broadcast-Adresse

Als Broadcast bezeichnet man das Verschicken von Daten an alle im Netz erreichbaren Rechner. Es wird in einem Computernetz vorwiegend verwendet, wenn die Adresse des Empfängers der Nachricht noch unbekannt ist. Ein Beispiel dafür sind die Protokolle ARP (siehe Kapitel *Das Address Resolution Protocol*, Seite 51) und DHCP. Ebenso dient ein Broadcast der einfachen Übermittlung von Informationen an alle Teilnehmer eines Netzes, um im Gegensatz zum Unicast nicht dieselbe Information mehrfach übertragen zu müssen. Soll eine Information nur an ausgewählte Teilnehmer gesendet werden, verwendet man das Multicast-Verfahren.

Broadcasts gibt es auf verschiedenen Ebenen des OSI-Referenzmodells (siehe Kapitel *Das OSI-Referenzmodell*, Seite 40). Allen gemein ist, dass Broadcasts einer höheren Ebene auf die Ebene des verwendeten physischen Netzwerkes angepasst werden müssen. So muss z. B. ein IP-Broadcast in einem Ethernet-Netzwerk als Ethernet-Broadcast an die MAC-Adresse FF:FF:FF:FF:FF:FF versendet werden.

#### Limited Broadcast

Als Ziel wird die IP-Adresse 255.255.255.255 angegeben. Dieses Ziel liegt immer im eigenen

Netz und wird direkt in einen Ethernet-Broadcast umgesetzt. Ein limited broadcast wird von einem Router nicht weitergeleitet.

### **Directed Broadcast**

Das Ziel sind die Teilnehmer eines bestimmten Netzes. Die Adresse wird durch die Kombination aus Zielnetz und dem Setzen aller Hostbits auf 1 angegeben. Folglich lautet die Adresse für einen directed broadcast in das Netz 192.168.0.0 mit der Netzmaske 255.255.255.0 (192.168.0.0/24): 192.168.0.255. Ein directed broadcast wird von einem Router weitergeleitet, falls Quell- und Zielnetz unterschiedlich sind, und wird erst im Zielnetz in einen Broadcast umgesetzt. Falls Quell- und Zielnetz identisch sind, entspricht dies einem limited broadcast. Oft wird dieser Spezialfall auch als local broadcast bezeichnet. Ein directed broadcast kann weiter differenziert betrachtet werden. Der Broadcast kann als subnet-directed broadcast, als all-subnets-directed broadcast oder als net-directed broadcast auftreten. Ein subnet-directed broadcast hat als Ziel ein festgelegtes Subnetz eines Netzwerkes. Ein all-subnets-directed broadcast ist ein Broadcast in allen Subnetzen eines Netzwerks, und ein net-directed broadcast wird in einem klassifizierten Netzwerk, das nicht in Subnetze aufgeteilt ist, verteilt (z. B. Broadcast an die Adresse 10.255.255.255 wird in einem Klasse A IP-Netzwerk verteilt).

Aufgrund von Sicherheitsproblemen mit DoS-Angriffen wurde das voreingestellte Verhalten von Routern in RFC 2644 für directed broadcasts geändert. Router sollten directed broadcasts nicht weiterleiten.

IPv6 unterstützt keine Broadcasts mehr, es werden stattdessen Multicasts verwendet.

[35]

Um zu prüfen, ob es sich bei einer IP-Adresse um die Broadcast-Adresse handelt, verknüpft man die IP-Adresse über eine logische OR-Operation mit der Subnetzmaske. Sind alle Bits der resultierenden Adresse auf eins gesetzt, handelt es sich bei der Ausgangs IP-Adresse, um die Broadcast-Adresse.

## **6.4. Die Netzwerkmaske**

Jede IP-Adresse wird durch eine Netzmaske in einen Netzwerk- und einen Geräteteil (Hostteil) getrennt. Um die Ip-Adressen zu gruppieren wurde sie in so genannte Netzwerkklassen eingeteilt (siehe Kapitel 6.6 *Netzklassen*, Seite 36). Diese Einteilung führt allerdings schnell zu Engpässen, deshalb war eine Lösung nötig, die auch Trennstellen an anderen als an den Positionen 8, 16 oder 24 zulässt. Die Lösung war die Einführung der Subnetzmaske, die durch Kennzeichnung des Netzanteils mit dem Bit 1 und des Hostanteils mit dem Bit 0 eine Trennung an jeder Position zulässt. Die Standard Subnetzmaske für ein Klasse A Netzwerk ist also 255.0.0.0, für ein Klasse B Netzwerk 255.255.0.0 und für ein Klasse C Netzwerk 255.255.255.0. Jede Subnetzmaske beginnt mit einem gesetzten Bit (1), endet mit einer binären 0 und hat genau einen Übergang von gesetzten zu den ungesetzten Bits. Alle Bits des Netzwerkteils sind auf 1 und alle Bits des Geräteteils auf 0 gesetzt.

Da die Netzwerkmaske an gibt, an welchem Bit die IP-Adresse geteilt werden muss, ist der Netzwerkteil bei allen Hosts (Rechnern) eines Subnetzwerks identisch. Die Information, ob ein Gerät im gleichen Subnetzwerk liegt (d. h. gleicher Netzwerkteil in der IP-Adresse), wird

von einem Host benötigt, um Routing-Entscheidungen treffen zu können. Siehe Kapitel 6.5 *Routing*.

Eine Netzmaske ist genau so lang wie die IP-Adresse, auf die sie angewendet wird, also 32 Bit bei IPv4 und 128 Bit bei IPv6. Die Notation einer Netzmaske erfolgt, wie bei IP-Adressen, überwiegend nicht im Dualsystem, sondern im Dezimalsystem als dotted decimal notation oder in CIDR-Schreibweise. So lautet die IPv4-Netzmaske für einen 27-Bit-Netzwerkteil „255.255.255.224“ oder kurz „/27“. Die Zahl 255 entspricht im Dualsystemer 8 gesetzten Bit oder „11111111“. Der vordere Teil der Netzmaske 255.255.255 entspricht also  $3 \times 8$  gesetzten Bits = 24 Bits. Die letzte Zahl 224 stellt sich in Binärschreibweise als „11100000“ dar. Aus ihr ergeben sich also 3 weitere gesetzte Bits.  $3 \times 8 + 1 \times 3 = 27$ . Aus dieser Erkenntnis und aus den Regeln für Subnetzmasken ergeben sich folgende mögliche Subnetzmasken:

Binär	Dezimal
0000 0000	0
1000 0000	128
1100 0000	192
1110 0000	224
1111 0000	240
1111 1000	248
1111 1100	252
1111 1110	254
1111 1111	255

Tab. 6.1.: Mögliche Subnetzmasken

Mit dieser Kennzeichnungstechnik lassen sich jetzt auch zu einer bestehenden Adresse Unteradressen (Subnetze) definieren.

### 6.4.1. Berechnung von Netzwerk- und Hostanteil

IPv4-Adresse 192.94.122.195/27

	Dezimal	Binär	Berechnung
IP Adresse	192.094.122.195	11000000 01011110 01111010 11000011	ip-adresse
Netzmaske	255.255.255.224	11111111 11111111 11111111 11100000	AND netzmaske
Netzwerkteil	192.094.122.192	11000000 01011110 01111010 11000000	= netzwerkteil
IP Adresse	192.094.122.195	11000000 01011110 01111010 11000011	ip-adresse
Netzmaske	255.255.255.224	11111111 11111111 11111111 11100000	AND (NOT netzmaske)
Geräteteil	3	00000000 00000000 00000000 00000011	= geräteteil

Bei einer Netzmaske mit 27 gesetzten Bits verbleiben 5 Bits und damit  $2^5=32$  Adressen für den Geräteteil, wobei die größte Adresse per Definition für den Broadcast reserviert ist und die kleinste Adresse das Netzwerk selbst beschreibt. Sie zählen daher nicht zu den frei nutzbaren Adressen. Im obigen Beispiel endet die kleinste Host-Adresse mit 11000000 (dezimal: 192), die größtmögliche Host-Adresse mit dem Oktett 11011111 (dezimal: 223).

Eine an einen PC vergebene IP-Adresse muss zwei Bedingungen erfüllen. Die IP-Adresse darf weder die Netzadresse, also die niedrigste Adresse, noch die Broadcastadresse, also

die höchste Adresse, sein. Die Netzadresse bezeichnet das Netz selber und die Broadcast-adresse wird dazu verwendet, um Daten an alle Rechner im Netzwerk zu verschicken. Sie wird zum Beispiel vom *Address Resolution Protokol* (Siehe Kapitel *Routing* ab Seite 51.) verwendet, um die MAC-Adresse von Rechnern zu ermitteln.

## Übungen

Welche, der folgenden IP-Angaben für PCs, sind grundsätzlich fehlerhaft?

IP: IP-Adresse, SN: Subnetzmaske, NT: Netzwerkanteil, GT: Geräteanteil, BC: Broadcastadresse

1.)

```
IP: 10101100.10101000.01000000.10000000 (172.168.64.128)
SN: 11111111.11111111.11111111.11000000 (255.255.255.192)
-----
NT: 10101100.10101000.01000000.10000000
```

Der Netzwerkanteil entspricht der IP-Adresse. Die IP-Adresse ist somit gleichzeitig die Netzadresse und ist für PCs nicht zulässig.

2.)

```
IP: 00001010.00010100.00011110.00101000 (10.20.30.40)
SN: 11111111.11111111.00000000.00000000 (255.255.0.0)
-----
NT: 00001010.00010100.00000000.00000000
GT: 00000000.00000000.00011110.00101000
BC: 11111111.11111111.00011110.00101000
```

Die IP-Adresse ist weder die Netzadresse, noch die Broadcastadresse. Sie ist somit gültig.

3.)

```
IP: 00101000.00011110.00010100.00000000 (40.30.20.0)
SN: 11111111.00000000.00000000.00000000 (255.0.0.0)
-----
NT: 00101000.00000000.00000000.00000000
GT: 00000000.00011110.00010100.00000000
BC: 11111111.00011110.00010100.00000000
```

Die IP-Adresse ist weder die Netzadresse, noch die Broadcastadresse. Sie ist somit gültig.

4.)

```
IP: 11000000.10101000.00010001.00000100 (192.168.17.4)
SN: 11111111.11111100.10000000.00000000 (255.252.128)
```

Die Subnetzmaske fehlerhaft, da sie nicht den geforderten Aufbau hat mit nur einem Wechsel von eins nach null.

5.)

```
IP: 10101100.00010001.00000000.11111111 (172.17.0.255)
SN: 11111111.11111111.11111100.00000000 (255.255.252.0)
-----
NT: 10101100.00010001.00000000.00000000
GT: 00000000.00000000.00000011.11111111
BC: 11111111.11111111.11111100.11111111
```

Die IP-Adresse ist weder die Netzadresse, noch die Broadcastadresse. Sie ist somit gültig.

## 6.4.2. Subnetting

Die Aufteilung eines zusammenhängenden Adressraumes von IP-Adressen in mehrere kleinere Adressräume nennt man Subnetting. Ein Subnet, Subnetz bzw. Teilnetz ist ein physikalisches Segment eines Netzwerkes, in dem IP-Adressen mit der gleichen Netzwerkadresse benutzt werden. Diese Teilnetze können mit Routern miteinander verbunden werden und bilden dann ein großes zusammenhängendes Netzwerk. [27]

### Warum Subnetting?

Wird die physikalische Netzstruktur bei der IP-Adressenvergabe nicht berücksichtigt und die IP-Adressen wahllos vergeben, müssen alle Router in diesem Netzwerk wissen in welchem Teilnetz sich eine Adresse befindet. Oder sie leiten einfach alle Datenpakete weiter, in der Hoffnung, das Datenpaket kommt irgendwann am Ziel an. Höhere Übertragungsprotokolle müssen verloren geglaubte Datenpakete erneut anfordern bzw. Senden. Das erhöht die Netzlast und macht die Router praktisch überflüssig. Kommt eine neue Station hinzu, dauert es sehr lange bis alle Router davon mitbekommen. Einzelne Stationen an den Rändern eines Netzwerkes laufen Gefahr nicht mehr erreichbar zu sein, weil am anderen Ende des Netzes ihre IP-Adresse nicht bekannt ist.

Um die Netzlast sinnvoll und geordnet zu verteilen, werden Netzwerke in Abhängigkeit der örtlichen Gegebenheiten und/oder nach organisatorischen Gesichtspunkten aufgeteilt. Dabei wird auch berücksichtigt, wieviele Netzwerkstationen sich innerhalb eines Subnetzes befinden.

Die Berücksichtigung der physikalischen Netzstruktur durch die gezielte Vergabe von IP-Adressen und damit eine logische Zusammenfassung mehrerer Stationen zu einem Subnetz reduziert die Routing-Informationen auf die Angabe der Netzwerk-Adresse. Die Netzwerk-Adresse gewährleistet den Standort einer IP-Adresse in einem bestimmten Subnetz. Ein Router benötigt dann nur noch die Routing-Information zu diesem Subnetz und nicht zu allen einzelnen Stationen in diesem Subnetz. Der letzte Router, der in das Ziel-Subnetz routet ist dann für die Zustellung des IP-Datenpaketes verantwortlich. [27]

### Wie funktioniert Subnetting?

Aufgabe: Zerlegen des Netzes 192.168.1.0/24 in vier Subnetze.

Die Subnetzmaske hat 24 gesetzte Bit, bleiben 8 für den Geräteanteil übrig. Damit lassen sich  $2^8=256$  Adressen bilden. 256 geteilt durch 4 ergibt einen Bereich von 64 Adressen pro Subnetz. Daraus ergeben sich die Subnetze: 192.168.1.63, 192.168.1.127, 192.168.1.191 und 192.168.1.255. Jetzt kann auch die neue Subnetzmaske definiert werden. Wir haben 64 Adressen pro Subnetz. Somit braucht der Host-Anteil der Subnetzmaske 6 Bits ( $\ln 64 / \ln 2 = 6$ ). Das heißt, die unteren 6 Bits müssen 0 sein und der Rest 1, also: 11111111.11111111.11111111.110000 (255.255.255.192).

### Kontrolle

	Subnetz 1	Subnetz 2	Subnetz 3	Subnetz 4
Netzadresse	192.168.1.0	192.168.1.64	192.168.1.128	192.168.1.192
Broadcastadresse	192.168.1.63	192.168.1.127	192.168.1.191	192.168.1.255

**Tab. 6.2.:** Zerlegung des Netzes 192.168.1.0/24 in vier Subnetze

```
IP-Adresse PC1: 11000000.10101000.00000001.00000001 // 192.168.1.1
Subnetzmaske : 11111111.11111111.11111111.11000000 // 255.255.255.192
Netzadresse  : 11000000.10101000.00000001.00000000 // 192.168.1.0

IP-Adresse PC2: 11000000.10101000.00000001.11001000 // 192.168.1.200
Subnetzmaske : 11111111.11111111.11111111.11000000 // 255.255.255.192
Netzadresse  : 11000000.10101000.00000001.11000000 // 192.168.1.192
```

Der PC1 mit der IP-Adresse 192.168.1.1 müsste im ersten Subnetz liegen. Eine Verknüpfung mit der Subnetzmaske bestätigt dies. Es ergibt sich die Netzwerkadresse des ersten Subnetzes. Für PC2 mit der IP-Adresse 192.168.1.200 ergibt sich das Netzwerk 192.168.1.192 und somit befindet sich der PC2 im dritten Subnetz, was auch korrekt ist.

Siehe dazu auch die Webseite *Digital Ether - Arbeiten mit IP-Adressen*<sup>3</sup>.

## 6.5. Routing

Will ein Gerät ein IP-Paket versenden, werden die Netzwerkteile der Quell-IP-Adresse und Ziel-IP-Adresse verglichen. Stimmen sie überein, befindet sich der Ziel-Host im selben Netzwerk und das Paket wird direkt an den Empfänger gesendet. Im Falle von Ethernet-Netzwerken dient das ARP (Address Resolution Protocol) zum Auffinden der Hardwareadresse. Das ARP arbeitet auf der zweiten Schicht des OSI-Modells und stellt die Verbindung zur ersten Schicht her. Stimmen die Netzwerkteile dagegen nicht überein, so wird über eine Routingtabelle die IP-Adresse eines Routers (next hop) gesucht und das Paket an diesen Router gesendet. Dieser hat über eine oder mehrere Schnittstellen Kontakt zu anderen Netzwerken und routet das Paket mit demselben Verfahren weiter - er konsultiert dazu seinerseits seine eigene Routingtabelle und sendet das Paket gegebenenfalls an den nächsten Router oder an das Ziel. Bis zum Endgerät kann das Paket viele Netzwerke und Router durchlaufen. Das Durchlaufen eines Routers wird auch Hop (Sprung) genannt, das Routingverfahren Next Hop Routing. Siehe dazu auch Kapitel 8 *Routing* ab Seite 49.

Siehe dazu auch die Tabelle A.2 *Besondere IP-Adressen* auf Seite 63.

## 6.6. Netzklassen

Netzklassen waren eine von 1981 bis 1993 verwendete Unterteilung des IPv4-Adressbereiches in Teilnetze für verschiedene Nutzer. Von der Netzklasse konnte die Größe eines Netzes abgeleitet werden. Dies ist beim Routing im Internet wichtig, um zu unterscheiden, ob eine

<sup>3</sup>[http://digitaether.de/index.php?option=com\\_content&task=view&id=28&Itemid=63](http://digitaether.de/index.php?option=com_content&task=view&id=28&Itemid=63)

Ziel-IP-Adresse im eigenen oder einem fremden Netz zu finden ist. Da Netzklassen sich als zu unflexibel und wenig sparsam im Umgang mit der knappen Ressource IP-Adressen herausgestellt haben, wurden sie bereits 1993 durch die Einführung des Classless Inter-Domain Routing (kurz: CIDR<sup>4</sup>) ersetzt.

Das ursprünglich eingesetzte Konzept der IP-Adressen sah nur eine starre Aufteilung vor. Hierbei waren 8 Bit für die Adressierung des Netzes vorgesehen, die übrigen 24 Bit adressierten einen spezifischen Teilnehmer des Netzes. Bei diesem Konzept waren aber nur 256 Netze möglich. Dies wurde als zu wenig erkannt. Daher wurden im September 1981 durch RFC 791 die sogenannten Netzklassen eingeführt, die diese Aufteilung neu gestalteten.

Über die Netzklassen wurde der gesamte Adressraum in zunächst drei (später fünf) Netzklassen unterteilt. Alle Teilnetze einer Netzklasse hatten hierbei die selbe standardisierte Größe. Die Netzgrößen der Klassen unterschieden sich sehr stark, so waren in einem Netz der Klasse C nur 254 Hosts möglich, wohingegen bei einem Netz der Klasse A über 16 Millionen Hosts ermöglicht wurden. Dies sollte es ermöglichen, einzelnen Organisationen und Einrichtungen verschieden große Netzwerke je nach Bedarf zuzuweisen. Doch führten die starren Netzgrößen zu großer Verschwendung, da z.B. einem Anwender mit 100.000 Hosts ein Netz der Klasse A zugewiesen werden musste. Von diesen standen aber nur insgesamt 125 zur Verfügung und in diesem konkreten Fall wären über 16 Millionen IP-Adressen verschwendet worden. Daher wurden die IP-Klassen im Jahr 1993 per RFC 1518 und RFC 1519 durch das Classless Inter-Domain-Routing ersetzt. Bei CIDR werden innerhalb des gesamten Adressraumes Netze in flexiblen Größen vergeben, folglich ist eine Ableitung der Netzgröße aus der IP-Adresse nicht mehr möglich.

Die Netzklasse wurde durch die ersten Bits der binären IP-Adresse bestimmt. Der den Klassen D und E zugeordnete Bereich war in der ursprünglichen Spezifikation für eine erweiterte Adressierung reserviert worden. Diese wurde später in die Klassen D und E aufgeteilt wobei der Adressbereich der Klasse D auch nach Abschaffung der Netzklassen weiter für Multicast-Anwendungen herangezogen wird. Der Adressbereich der früheren Klasse E ist weiterhin reserviert.

Bis zum heutigen Tag wird das Konzept der Netzklassen vielerorts als immer noch gültig gelehrt, so beispielsweise in Vorlesungen und Praktika über Netzwerktechnik an Hochschulen[1]. Diese Lehre der Netzklassen führt oft jedoch nur zu Verwirrung, da sie mit der Einführung von CIDR überholt ist. Da das Wissen über Netzklassen nicht mehr praktisch einsetzbar ist, stellt es lediglich einen historischen Sachverhalt und keine Referenz für praktischen Einsatz dar. Es bleibt festzustellen, dass Netzklassen keinerlei praxisrelevante Bedeutung mehr haben, da die Größe eines Netzes nicht mehr nur aus der IP-Adresse abzuleiten ist, sondern zwingend die Angabe einer Netzmaske erforderlich ist.

Siehe dazu auch die Tabelle A.3 *Übersicht der Netzklassen* auf Seite 64.

[23], [24], [25], [26]

---

<sup>4</sup>Classless Inter-Domain Routing, Wikipedia: [http://de.wikipedia.org/wiki/Classless\\_Inter-Domain\\_Routing](http://de.wikipedia.org/wiki/Classless_Inter-Domain_Routing)



## 7. Referenzen und Modelle

### 7.1. Netzwerkarchitekturen – Grundlagen

Die dazu erforderliche Kommunikation ist nicht so trivial, wie es auf den ersten Blick scheint, denn es müssen eine Vielzahl von Aufgaben bewältigt und Anforderungen bezüglich Zuverlässigkeit, Sicherheit, Effizienz etc. erfüllt werden. Die Probleme, die dabei gelöst werden müssen, reichen von Fragen der elektronischen Übertragung der Signale über eine geregelte Reihenfolge in der Kommunikation bis hin zu abstrakteren Aufgaben, die sich innerhalb der kommunizierenden Anwendungen ergeben. Damit der Grad an Komplexibilität bei der Entwicklung niedrig bleibt, werden die meisten Netzwerke in einer Reihe von Schichten oder Ebenen organisiert, wobei jede Schicht auf ihrer Vorgängerschicht aufgebaut wird. Die Anzahl der Schichten und ihre Funktion sind von Netzwerk zu Netzwerk verschieden. Der Zweck jeder Schicht ist es, übergeordneten Schichten einen bestimmten Dienst zu leisten und diese Schicht von der eigentlich hinter dem Dienst steckenden Anwendungsarbeit abzuschotten.

Die Schicht  $n$  einer Maschine kommuniziert mit der Schicht  $n$  einer anderen Maschine. Die Regeln und Bestimmungen, nach denen diese Kommunikation abläuft, werden allgemein das *Protokoll* der Schicht  $n$  genannt. Die Instanzen, aus denen sich die jeweiligen Schichten auf den verschiedenen Maschinen zusammensetzen, werden Partnerprozesse genannt. Es sind also die Partnerprozesse, die über das Protokoll mit einander kommunizieren. Da aber in der Praxis keine Daten direkt von der Schicht  $n$  einer Maschine an die Schicht  $n$  der anderen Maschine übertragen werden, spricht man auch von einer virtuellen Kommunikation. Stattdessen gibt jede Schicht Daten und Steuerinformationen an die direkt unter ihr liegende Schicht weiter, bis die unterste Schicht erreicht ist. Unter der Schicht 1 befindet sich das physikalische Medium, über das die tatsächliche Kommunikation läuft.

Zwischen allen aneinander grenzenden Schichten befindet sich eine Schnittstelle. Diese Schnittstelle definiert, welche einfachen Operationen und Dienste die untere Schicht der oberen bietet. Bei der Entwicklung eines Netzwerkes muss man sich Gedanken über die Anzahl und die Funktion der einzelnen Schichten machen. Dabei ist es sehr wichtig, dass man saubere Schnittstellen zwischen den Schichten definiert. Dafür wiederum ist es erforderlich, dass jede Schicht eine bestimmte Sammlung genau definierter Funktionen ausführt. Sauber definierte Schnittstellen haben nicht den Vorteil, dass die an die nächste Schicht weitergeleiteten Informationen auf ein Minimum reduziert sind, sie machen auch das Auswechseln einzelner Schichten wesentlich leichter, weil die einzige Anforderung, der sich die neue Anwendungsschicht gegenüber sieht, die ist, dass sie ihrer übergeordneten Schicht die gleiche Sammlung an Diensten zur Verfügung stellen muss wie die alte Schicht.

Diese Sammlung von Schichten und Protokollen nennt man *Netzwerkarchitektur*. Die Spezifikation der Architektur muss dem Anwendungsentwickler die Informationen liefern, die er

braucht, damit er die für jede Schicht nötige Hard- und Software so bauen kann, dass die Schicht dem passenden Protokoll genügt.

Mit einer Analogie lässt sich solch ein mehrschichtiger Netzwerkaufbau verdeutlichen: Zwei Philosophen (Partnerprozesse in Schicht 3) wollen sich über ein Thema austauschen. Der eine wohnt in Kenia und spricht nur Kisuaheli und der andere wohnt in Indien und spricht nur indisch. Sie haben also keine gemeinsame Sprache zur Verfügung mit der sie sich austauschen könnten. Daher engagieren sie beide einen Dolmetscher (Partnerprozesse in Schicht 2), von denen sich jeder wieder an einen Techniker (Schicht 1) wendet, der die Nachricht überträgt. Will eine Philosoph nun dem anderen eine Nachricht zukommen lassen, schickt er die Nachricht über die Schnittstelle 2/3 an seinen Dolmetscher, der die Nachricht in eine Sprache übersetzt, welche das Protokoll von Schicht 2 vorschreibt. Danach übergibt der Dolmetscher die Nachricht zur Übertragung an den Techniker. Dieser übermittelt die Nachricht per Telegramm, Telefon oder über ein anderes Medium, je nachdem, was im Protokoll der Schicht 1 vereinbart wurde. Ist die Nachricht angekommen, wird sie ins indische übersetzt und über die Schnittstelle 2/3 an den Philosophen in Indien übermittelt. Wie man sieht, ist jede Schicht ist von der über- bzw. untergeordneten Schicht unabhängig. Es ist nur wichtig, dass die Schnittstellen gleich bleiben. So können zum Beispiel die Dolmetscher beliebig ausgetauscht werden. Bedingung ist nur, dass sie beide ihre Schnittstelle zu Schicht 1 und 3 beibehalten.

[30]

## 7.2. Das OSI-Referenzmodell

Das OSI-Modell stellt eine konkrete Implementierung der Schichten einer Netzwerkarchitektur dar. Das Modell basiert auf einen Vorschlag, der von der International Standards Organization (ISO) entwickelt wurde. Daher der Name ISO-OSI-(Open Systems Interconnection<sup>1</sup>)Referenzmodell und weil es sich damit beschäftigt, offene Systeme miteinander zu verbinden – das heißt, Systeme, die für die Kommunikation mit anderen Systemen offen sind.

Beim OSI-Modell sind es sieben Schichten mit festgelegten Anforderungen. Auf jeder einzelnen Schicht setzt jeweils eine Instanz die Anforderungen um. Dabei nimmt der Abstraktionsgrad von Schicht 7 bis Schicht 1 ab.

Folgende Prinzipien haben zu der Siebenschichtigkeit geführt:

1. Eine neue Schicht sollte da entstehen, wo ein neuer Abstraktionsgrad benötigt wird.
2. Jede Schicht sollte eine genau definierte Funktion erfüllen.
3. Bei der Funktionswahl sollte man die Definition internationaler genormter Protokolle im Auge behalten.
4. Die Grenze zwischen den einzelnen Schichten sollte so gewählt werden, dass der Informationsfluss über die Schnittstellen möglichst gering ist.

---

<sup>1</sup>Kommunikation offener Systeme

OSI-Schicht	Einordnung	Standard	DoD-Schicht	Einordnung	Protokollbeispiel	Einheiten	Kopplungselemente
7	Anwendung (Application)	FTAM	Anwendung	Ende zu Ende (Multihop)	HTTP FTP HTTPS SMTP LDAP NCP	Daten	Layer 4-7 Switch, Content-Switch, Gateway
6	Darstellung (Presentation)	ASN.1					
5	Sitzung (Session)	ISO 8326					
4	Transport (Transport)	ISO 8073	Transport	TCP UDP SCTP SPX	Segmente		
3	Vermittlung (Network)	CLNP	Internet	Punkt zu Punkt	ICMP IGMP IP IPX	Pakete	Router, Layer-3 Switch
2	Sicherung (Data Link)	HDLC	Netzzugang		Ethernet Token Ring FDDI ARCNET	Rahmen (Frames)	Switch, Bridge
1	Bitübertragung (Physical)	Token Bus			Bits	Hub, Repeater	

**Abb. 7.1.:** Die sieben Schichten des OSI-Modells im Überblick

5. Die Anzahl der Schichten sollte so groß sein, dass keine Notwendigkeit dafür besteht, verschiedene Funktionen auf dieselbe Schicht zu packen, und so klein, dass die gesamte Architektur nicht unhandlich wird.

Man beachte, dass das OSI-Modell keine Netzwerkarchitektur ist, da die genauen Dienste und Protokolle, die in jeder Schicht verwendet werden sollen, nicht festgelegt werden. Das OSI-Modell sagt lediglich aus, was die jeweilige Schicht können soll.

[30], [28]

### 7.2.1. Die einzelnen Schichten des OSI-Modells

Um sich die einzelnen Schichten und deren Position im OSI-Modell merken zu können, gibt es diverse Merksprüche, wobei die Anfangsbuchstaben der Wörter den Anfangsbuchstaben der englischen Bezeichnungen der Layer entsprechen.

Von Schicht 7 nach Schicht 1:

- Alle Priester saufen Tequilla nach der Predigt.
- A Pussy So Tight No Dick Penetrates.
- All People Send Their Network Data Physically.
- All People Seem To Need Data Processing.
- All People Standing Totally Nude Don't Perspire.
- Alle Personen Senden Tolle NetzwerkDaten Physisch.
- Alle Prüfer saufen Tequila nach der Prüfung.
- Affen pinkeln stets total neben den Pott.
- Alle Professoren scheißen täglich neben den Pott.
- Alte Penner sitzen traurig neben der Parkbank.

- Auf Party saufen treibt natürlich die Pisse.
- Alle deutschen Schüler trinken verschiedene Sorten Bier. (deutsche Version)

Von Schicht 1 nach Schicht 7:

- Please Do Not Throw Salami Pizza Away.
- Princess Di Never Tried Screwing Prince Andrew.
- Petrus Darf Nicht Traurig Sein Per Anweisung.
- People Don't Need To See Pamela Anderson.
- Paul Darf Nicht Träumen Sonst Pennen Alle.
- Physische Daten verNetzen Transportable Sitzende und Präsentierende Anwendungen.
- Bin Sehr Voll, Tolle Sache Der Asbach. (Deutsches Modell)

### **Physical layer – Bitübertragungsschicht**

Die Bitübertragungsschicht (engl. physical layer) ist die unterste Schicht. Diese Schicht stellt mechanische, elektrische und weitere funktionale Hilfsmittel zur Verfügung, um physikalische Verbindungen zu aktivieren bzw. deaktivieren, sie aufrechtzuerhalten und Bits darüber zu übertragen. Auf der Bitübertragungsschicht wird die digitale Bitübertragung auf einer leitungsgebundenen oder leitungslosen Übertragungsstrecke bewerkstelligt. Die Adressierung erfolgt über die MAC-Adresse. Auf dieser Ebene muss sichergestellt werden, dass ein mit der Wertigkeit 1 gesendetes Bit auch als Bit mit der Wertigkeit 1 vom Empfänger erkannt wird. Typische Fragen die an dieser Stelle geklärt werden sind:

1. Wieviel Volt sollen eine logischen 1 entsprechen und wieviel einer logischen 0?
2. Wie lange soll ein Bit dauern?
3. Soll die Übertragung in beide Richtungen gleichzeitig erfolgen?
4. Wie kommt die erste Verbindung zustande?
5. Wieviele Pins hat die Endsystemverbindung und wie werden sie genutzt?

Die Funktionen im Überblick:

- Verbindungsarten
- Physikalische Topologie
- Signalkodierungsverfahren
- Bitsynchronisation
- Bandbreitennutzung
- Multiplexing

Hardware auf dieser Schicht: Hub, Repeater

Protokolle und Normen: X.25, ISO 8208, ISO 8473 (CLNP), ISO 9542 (ESIS), IP, IPsec, ICMP

## Data link layer – Sicherungsschicht

Aufgabe der Sicherungsschicht ist es, eine zuverlässige, das heißt weitgehend fehlerfreie Übertragung zu gewährleisten und den Zugriff auf das Übertragungsmedium zu regeln. Dazu dient das Aufteilen des Bitdatenstromes in Blöcke und das Hinzufügen von Folgenummern und Prüfsummen. Fehlerhafte, verfälschte oder verloren gegangene Blöcke können vom Empfänger durch Quittungs- und Wiederholungsmechanismen erneut angefordert werden. Die Blöcke werden auch als Frames oder Rahmen bezeichnet. Da die Bitübertragungsschicht einfach nur einen Strom von Bits annimmt, ist es Sache der Sicherungsschicht, Rahmengrenzen einzufügen und zu erkennen.

Nach IEEE ist Layer 2 in zwei Sub-Layers unterteilt: LLC (Logical Link Control) und MAC (Media Access Control).

Die Funktionen im Überblick:

- Logische Topologie
- Medienzugriff
- Hardware-Adressierung
- Übertragungssynchronisation
- Übertragungssicherung

Hardware auf dieser Schicht: Bridge, Switch (Multiport-Bridge)

Protokolle und Normen: HDLC, SDLC, DDCMP, IEEE 802.2 (LLC), IEEE 802.3 (CSMA/CD), IEEE 802.11 (WLAN), IEEE 802.4 (Token Bus), IEEE 802.5 (Token Ring), ARP

## Network layer – Vermittlungsschicht

Die Vermittlungsschicht sorgt bei leitungsorientierten Diensten für das Schalten von Verbindungen und bei paketorientierten Diensten für die Weitervermittlung von Datenpaketen. Die Datenübertragung geht in beiden Fällen jeweils über das gesamte Kommunikationsnetz hinweg und schließt die Wegesuche (Routing) zwischen den Netzknoten mit ein. Da nicht immer eine direkte Kommunikation zwischen Absender und Ziel möglich ist, müssen Pakete von Knoten, die auf dem Weg liegen, weitergeleitet werden. Weitervermittelte Pakete gelangen nicht in die höheren Schichten, sondern werden mit einem neuen Zwischenziel versehen und an den nächsten Knoten gesendet.

In dieser Schicht sind auch die Routing Protokolle angesiedelt. Man unterscheidet zwischen statischen und dynamischen Routing. Beim dynamischen Routing trifft der Router die Entscheidung an welchen Router er die Datenpakete weiterleitet. Im Gegensatz dazu bestimmt ein Administrator über eine manuell konfigurierte Routingtabelle an welchen Router bestimmte Pakete weitergeleitet werden. Siehe dazu auch Kapitel 8 *Routing* ab Seite 49. Die Adressierung erfolgt in dieser Schicht über die IOP-Adresse.

Zu den wichtigsten Aufgaben der Vermittlungsschicht zählen der Aufbau und die Aktualisierung von Routingtabellen sowie die Flusskontrolle. Auch die Netzadressen gehören zu dieser

Schicht. Da ein Kommunikationsnetz aus mehreren Teilnetzen unterschiedlicher Technologien bestehen kann, sind in dieser Schicht auch die Umsetzungsfunktionen angesiedelt, die für eine Weiterleitung zwischen den Teilnetzen notwendig sind.

Die Funktionen im Überblick:

- Adressierung
- Vermittlung
- Wegewahl, Wegfindung
- Übertragungssicherung

Hardware auf dieser Schicht: Router, Layer-3-Switch (BRouter)

Protokolle und Normen: X.25, ISO 8208, ISO 8473 (CLNP), ISO 9542 (ESIS), IP, IPsec, ICMP

### **Transport layer – Transportschicht**

Die Transportschicht, ist die letzter der Schichten, die für den Transport der Daten verantwortlich ist. Deswegen werden auch die ersten vier Schichten, als die transportorientierten Schichten bezeichnet. Desweiteren ist sie die unterste Schicht, die eine vollständige Ende-zu-Ende Kommunikation zwischen Sender und Empfänger zur Verfügung stellt. Sie bietet den anwendungsorientierten Schichten 5-7 einen einheitlichen Zugriff, sodass diese die Eigenschaften des Kommunikationsnetzes nicht zu berücksichtigen brauchen.

In der Transportschicht findet die Adress-/Namensabbildung statt. Hier werden die URLs in IP-Adressen umgesetzt. Desweiteren werden an dieser Stelle auch die lokalen Ports verwaltet und zugewiesen. Zu den Aufgaben der Transportschicht zählt auch die Segmentierung, von Datenpaketen, also die Aufteilung der Daten in Pakete. Letzte Aufgabe der Transportschicht ist die Übertragungssicherung, darunter versteht man die Fehlererkennung und die Datenflusssteuerung (Reihenfolge der Pakete).

Die Funktionen im Überblick:

- Adress-/Namensabbildung
- Transaktionsadressierung
- Segmentierung
- Übertragungssicherung

Protokolle und Normen: ISO 8073/X.224, ISO 8602, TCP, UDP, SCTP

### **Session layer – Sitzungsschicht**

Die Schicht 5 sorgt für die Prozesskommunikation zwischen zwei Systemen. Hier wird entschieden wie die Kommunikation erfolgen soll, ob im Simplex-, Halbduplex- oder Vollduplexverfahren.

Die Sitzungsschicht, ist wie ihr Name schon sagt auch für die Verwaltung der Sitzungen verantwortlich. Hier werden Sitzungen aufgebaut, Passwörter ausgehandelt und auch die

Sitzung wieder abgebaut. Um Zusammenbrüche der Sitzung und ähnliche Probleme zu beheben, stellt die Sitzungsschicht Dienste für einen organisierten und synchronisierten Datenaustausch zur Verfügung. Zu diesem Zweck werden Wiederaufsetzpunkte, so genannte Fixpunkte (Check Points) eingeführt, an denen die Sitzung nach einem Ausfall einer Transportverbindung wieder synchronisiert werden kann, ohne dass die Übertragung wieder von vorne beginnen muss. Dabei erfolgt auch eine Überwachung der Daten.

Die Funktionen im Überblick:

- Kommunikationssteuerung
- Sitzungsverwaltung

Protokolle und Normen: ISO 8306 / X.215 (Session Service), ISO 8327 / X.225 (Connection-Oriented Session Protocol), ISO 9548 (Connectionless Session Protocol)

### **Presentation layer – Darstellungsschicht**

Die Darstellungsschicht setzt die systemabhängige Darstellung der Daten (Bit- und Byte-reihenfolge, Zeichensatz, Dateisystem) in eine unabhängige Form um und ermöglicht somit den syntaktisch korrekten Datenaustausch zwischen unterschiedlichen Systemen. Auch Aufgaben wie die Datenkompression und die Verschlüsselung gehören zur Schicht 6. Die Darstellungsschicht gewährleistet, dass Daten, die von der Anwendungsschicht eines Systems gesendet werden, von der Anwendungsschicht eines anderen Systems gelesen werden können. Falls erforderlich, agiert die Darstellungsschicht als Übersetzer zwischen verschiedenen Datenformaten, indem sie ein für beide Systeme verständliches Datenformat, die ASN.1 (Abstract Syntax Notation One), verwendet.

Die Funktionen im Überblick:

- Übersetzung
- Verschlüsselung
- Kompression

Protokolle und Normen: ISO 8822 / X.216 (Presentation Service), ISO 8823 / X.226 (Connection-Oriented Presentation Protocol), ISO 9576 (Connectionless Presentation Protocol)

### **Application layer – Anwendungsschicht**

Die Verarbeitungsschicht ist die oberste der sieben hierarchischen Schichten. Sie stellt den Anwendungen eine Vielzahl an Funktionalitäten zur Verfügung (zum Beispiel Datenübertragung, E-Mail, Virtual Terminal, Remote login etc.). Der eigentliche Anwendungsprozess liegt oberhalb der Schicht und wird nicht vom OSI-Modell erfasst.

Die Funktionen im Überblick:

- Bereitstellung der Netzwerkdienste
- Bekanntmachung der Dienste

Hardware auf dieser Schicht: Gateway

Protokolle und Normen: X.400, X.500, ISO 8571 (FTAM), ISO 9040/9041 (VT), ISO 9506 (MMS), MHS, VTP, FTP, NFS, Telnet, SMTP, HTTP, LDAP

[30], [28]

### 7.2.2. Datenübertragung im OSI-Modell

Will nun eine Sender einem Empfänger Daten zukommen lassen, gibt er die Daten an die Anwendungsschicht weiter. Dieser setzt, bei Bedarf, vor die Nachricht den Anwendungsnachrichtenkopf mit für die Schicht relevanten Informationen. Diese Daten werden dann an die Darstellungsschicht weitergegeben. Die Darstellungsschicht wandelt diese Einheit möglicherweise ein paar mal um, setzt vielleicht einen weiteren Nachrichtenkopf vorne dran und gibt das Ergebnis an die Sitzungsschicht weiter. Die Darstellungsschicht hat dabei kein Wissen darüber, welcher Teil der Daten die ursprünglich gesendeten Daten sind und welche eventuell zum Anwendungsnachrichtenkopf gehören. Dies braucht sie auch gar nicht wissen. Der Vorgang des Weiterreichens wiederholt sich so lange, bis die Daten die Bitübertragungsschicht erreichen, von wo sie dann auf die Empfängermaschine übertragen werden. Auf der Empfängermaschine werden die verschiedenen Nachrichtenköpfe durch die verschiedenen Schichten wieder entfernt, während sich die Daten in den Schichten nach oben bewegen.

Dabei ist jede Schicht so programmiert, dass die Datenübertragung vertikal ist, aber der Anschein erweckt wird, als sei die Datenübertragung horizontal. Wenn zum Beispiel die Transportschicht des Senders eine Nachricht von der Sitzungsschicht erhält, fügt dieser einen Transportnachrichtenkopf an und schickt sie an die Transportschicht des Empfängers. Aus ihrer Sicht ist die Tatsache, dass sie die Nachricht tatsächlich an die Vermittlungsschicht ihrer eigenen Maschine weiterleiten muss, unwichtiges Drumherum. Analog dazu wendet sich ein spanisch sprechender Diplomat von den Vereinten Nationen auch direkt an die anderen Diplomaten. Dass er dabei eigentlich mit seinen Dolmetscher spricht, wird nur als technisches Detail gesehen.

### 7.3. Das TCP/IP-Referenzmodell

Im Gegensatz zum OSI-Referenzmodell gibt es noch das TCP/IP-Referenzmodell. Es gehört zu Internetprotokollfamilie und ist eins von rund 500 anderen Netzwerkprotokollen.

Zur Gliederung der Kommunikationsaufgaben werden in Netzwerken funktionale Ebenen, so genannte Schichten (layer), unterschieden. Für die Internetprotokollfamilie ist dabei das TCP/IP-Referenzmodell maßgebend. Es beschreibt den Aufbau und das Zusammenwirken der Netzwerkprotokolle aus der Internet-Protokoll-Familie und gliedert sie in vier aufeinander aufbauende Schichten. TCP/IP steht für Transmission Control Protocol/Internet Protocol. Das TCP/IP-Referenzmodell ist auf die Internet-Protokolle zugeschnitten, die den Datenaustausch über die Grenzen lokaler Netzwerke hinaus ermöglichen. Es wird weder der Zugriff auf ein Übertragungsmedium noch die Datenübertragungstechnik definiert. Vielmehr

sind die Internet-Protokolle dafür zuständig, Datenpakete über mehrere Punkt-zu-Punkt-Verbindungen (Hops) weiterzuvermitteln und auf dieser Basis Verbindungen zwischen Netzwerkteilnehmern über mehrere Hops herzustellen.

TCP/IP-Schicht	≈ OSI-Schicht	Beispiel
Anwendungsschicht	5-7	HTTP, FTP, SMTP
Transportschicht	4	TCP, UDP
Vermittlungsschicht	3	IPv4, IPv6
Netzzugangsschicht	1-2	Ethernet, Token Ring, FDDI

**Abb. 7.2.:** Gegenüberstellung OSI Modell – TCP/IP-Modell

Die einzelnen Schichten erfüllen folgende Funktionen:

- *Anwendungsschicht* (application layer): Die Anwendungsschicht umfasst alle Protokolle, die mit Anwendungsprogrammen zusammenarbeiten und die Netzwerkinfrastruktur für den Austausch anwendungsspezifischer Daten nutzen.
- *Transportschicht* (transport layer): Die Transportschicht stellt eine Ende-zu-Ende-Verbindung her. Das wichtigste Protokoll dieser Schicht ist das Transmission Control Protocol (TCP), das Verbindungen zwischen jeweils zwei Netzwerkteilnehmern zum zuverlässigen (nicht „sicheren“, da das Wort „sicher“ im Sinne von fälschungssicher/abhörsicher gebraucht wird) Versenden von Datenströmen herstellt. Es gehören aber auch Datagramm-Protokolle – zum Beispiel das User Datagram Protocol (UDP) – in diese Schicht, bei denen nur die Zustellung an den richtigen Dienst zuverlässig gemacht und keine Verbindung aufgebaut wird.
- *Vermittlungsschicht* (internet layer): Die Vermittlungsschicht ist für die Weitervermittlung von Paketen und die Wegewahl (Routing) zuständig. Auf dieser Schicht und den darunterliegenden Schichten werden Punkt-zu-Punkt-Verbindungen betrachtet. Die Aufgabe dieser Schicht ist es, zu einem empfangenen Paket das nächste Zwischenziel zu ermitteln und das Paket dorthin weiterzuleiten. Kern dieser Schicht ist das Internet Protocol (IP), das einen Paketauslieferungsdienst bereitstellt. Die Vermittlungsschicht entspricht im ISO-OSI-Referenzmodell der Vermittlungsschicht.
- *Netzzugangsschicht* (auch: host-to-network layer): Die Netzwerkschicht ist im TCP/IP-Referenzmodell spezifiziert, enthält jedoch keine Protokolle der TCP/IP-Familie. Sie ist vielmehr als Platzhalter für verschiedene Techniken zur Datenübertragung von Punkt zu Punkt zu verstehen. Die Internet-Protokolle wurden mit dem Ziel entwickelt, verschiedene Subnetze zusammenzuschließen. Daher kann die Host-an-Netz-Schicht durch Protokolle wie Ethernet, FDDI, PPP (Punkt-zu-Punkt-Verbindung) oder 802.11 (WLAN) ausgefüllt werden. Die Netzzugangsschicht entspricht im ISO/OSI-Referenzmodell der Sicherungs- und Bitübertragungsschicht.

Es gibt aber wesentliche konzeptionelle Unterschiede zum OSI-Modell. OSI legt die Dienste genau fest, die jede Schicht für die nächsthöhere zu erbringen hat. TCP/IP hat kein derartig strenges Schichtenkonzept wie OSI. Weder sind die Funktionen der Schichten genau festgelegt, noch die Dienste. Es ist erlaubt, dass eine untere Schicht unter Umgehung zwischenliegender Schichten direkt von einer höheren Schicht benutzt wird. TCP/IP ist damit erheblich effizienter als die OSI-Protokolle. Nachteil bei TCP/IP ist, dass es für viele kleine und kleinste Dienste jeweils ein eigenes Netzprotokoll gibt. OSI hat dagegen für seine Protokolle jeweils einen großen Leistungsumfang festgelegt, der sehr viele Optionen hat.

[29]

## 8. Routing

Allgemein versteht man unter Routing in der Telekommunikation das Festlegen von Wegen für Nachrichtenströme bei der Nachrichtenübermittlung über vermaschte Nachrichtennetze bzw. Rechnernetze. Insbesondere in paketvermittelten Datennetzen ist hierbei strenggenommen zwischen den beiden verschiedenen Prozessen Routing und Forwarding zu unterscheiden: Das Routing bestimmt den gesamten Weg eines Nachrichtenstroms durch das Netzwerk; das Forwarding beschreibt hingegen den Entscheidungsprozess eines einzelnen Netzknotens, über welchen seiner Nachbarn er eine vorliegende Nachricht weiterleiten soll. Häufig werden jedoch Routing und Forwarding unter dem Begriff *Routing* miteinander vermischt; in diesem Fall bezeichnet Routing ganz allgemein die Übermittlung von Nachrichten über vermaschte Nachrichtennetze. Handelt es sich um eine leitungsvermittelte Verbindung, wird ein Übertragungskanal für die gesamte Zeit der Verbindung ausgewählt, und alle Nachrichten werden über denselben Weg geleitet. Handelt es sich dagegen um eine paketvermittelte Datenübertragung, wird der Weg für jedes Paket von jedem Netzknoten neu bestimmt. Im Internet findet die paktevermittelte Datenübertragung Anwendung.

[31]

### 8.1. Routing von Paketen

Beim paketvermittelten Routing, wie es z. B. im Internet stattfindet, wird dafür gesorgt, dass logisch adressierte Pakete aus dem Ursprungs-Netz herauskommen und in Richtung ihres Ziel-Netzes weitergeleitet werden. Routing ist die Basis des Internet – ohne Routing würde das Internet nicht existieren, und alle Netze wären autonom. Die Datenpakete können dabei viele verschiedene Zwischen-Netze auf dem Weg zu ihrem Ziel passieren. Im Internet wird das Routing (üblicherweise) auf der IP-Schicht durchgeführt. Im ISO/OSI-Modell ist Routing eine der wesentlichen Aufgaben der dritten Schicht.

Um zu wissen, wohin Pakete gesendet werden sollen, muss man die Struktur des Netzes kennen. In kleinen Netzen kann das Routing sehr einfach sein und wird oft per Hand konfiguriert. Man spricht dann auch von *statischem Routing*. Große Netze können eine komplexe Topologie haben, die sich möglicherweise häufig ändert, was unter anderem das Routing zu einer komplexen Angelegenheit macht. Hier wird in der Regel ein *dynamisches Routing* angewandt.

Typische dynamische Routingverfahren zur Wegfindung sind das *Entfernungsvektorverfahren* (Distance vector) oder das *Link state* Verfahren. Bei Entfernungsvektorverfahren wird

der Weg mit den wenigsten Zwischenstationen (Hops) gewählt. Die Leitungsqualität, Auslastung und/oder Geschwindigkeit wird dabei nicht berücksichtigt. Diese Kriterien finden hingegen beim Link state Verfahren Verwendung. Die Wegfindung kann zum Beispiel mit dem Algorithmus von Dijkstra<sup>1</sup> erfolgen.

Basierend auf den Einträgen in der oder den Routingtabelle(n) berechnet ein Router eine sogenannte Forwarding-Tabelle; sie enthält einfach Einträge der Form Zieladressenmuster?Ausgabeschnittstelle. In seiner Forwardingtabelle schlägt ein Router dann für jedes neu eingetroffene Paket nach, über welche Schnittstelle er das Paket weiterleiten muss.

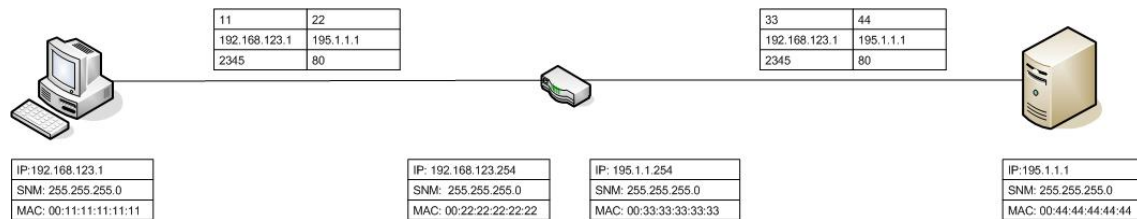


Abb. 8.1.: Paket-Adressierung beim Routing

[31]

## 8.2. Routing-Protokolle

Routing-Protokolle sorgen für den Austausch von Routing-Informationen zwischen den Netzen und erlauben es den Routern, ihre Routing-Tabellen dynamisch aufzubauen. Traditionelles IP-Routing bleibt einfach, da Next-Hop-Routing benutzt wird: Der Router sendet das Paket an denjenigen Nachbar-Router, von dem er glaubt, dass er am günstigsten zum Zielnetz liegt. Um den weiteren Weg des Pakets braucht sich der Router nicht zu kümmern. Selbst wenn er falsch lag und das Paket nicht an den „optimalen“ Nachbarn gesendet hat, sollte das Paket trotzdem früher oder später am Ziel ankommen.

Obwohl dynamisches Routing sehr komplex werden kann, macht es das Internet sehr flexibel und erlaubte das exponentielle Wachstum des Internets seit der Einführung von IP im Jahre 1983. Wenn Teile der Backbones ausfallen (so geschehen z. B. im Sommer 2002, als der Carrier KPNQwest sein europaweites Glasfasernetz wegen Insolvenz abschalten musste), können innerhalb von Sekunden Alternativrouten propagiert werden und die betroffenen Netzbereiche weiträumig umgangen werden.

Dem Ausfall des sogenannten Standardgateways - das ist meist der erste Router vom Sender aus gesehen - wirkt dynamisches Routing jedoch nicht entgegen. Da ein Host im Normalfall keine Alternative zum Standardgateway hat, ist dies der wichtigste Router der Route.

[31]

<sup>1</sup> Der Algorithmus von Dijkstra (nach seinem Erfinder Edsger W. Dijkstra) dient der Berechnung eines kürzesten Pfades zwischen einem Startknoten und einem beliebigen Knoten in einem kantengewichteten Graphen.

Man unterscheidet zwischen internen Routing-Protokollen (Interior Gateway Protocol, IGP), die nur im internen Netzwerk Verwendung finden und den externen Routing-Protokolle (Exterior Gateway Protocol, EGP). Diese Protokolle beinhalten Routing-Informationen für Netzwerke außerhalb Ihres eigenen Netzwerkes. EGPs sind nicht in der Lage, Daten innerhalb Ihres Netzwerkes zu transportieren, sondern können dies lediglich außerhalb. Derzeit sind verschiedene IGPs in Gebrauch, aber nur ein einziges EGP, nämlich das Border Gateway Protocol (BGP). Das ist auch das Routing-Protokoll des Internets.

[34]

Siehe dazu die Tabellen im Anhang ab Seite 65 mit einer Übersicht über die gebräuchlichsten Routing Protokolle.

### 8.3. Das Address Resolution Protocol (ARP)

Das Address Resolution Protocol (ARP) arbeitet auf der Schicht 2, der Sicherungsschicht, des OSI-Schichtenmodells und setzt IP-Adressen in Hardware- und MAC-Adressen um. Damit nun ein IP-Paket an sein Ziel findet, muss die Hardware-Adresse des Ziels bekannt sein.

[32]

#### 8.3.1. Ablauf einer ARP-Adressauflösung

Eine ARP-Auflösung unterscheidet zwischen lokalen IP-Adressen und IP-Adressen in einem anderen Subnetz.

**Fall 1:** Ziel IP-Adresse befindet sich im gleichen Subnetz.

1. Der ARP-Cache wird überprüft, ob bereits eine MAC-Adresse für die IP-Adresse hinterlegt ist. Wenn ja, dann wird die MAC-Adresse zur Adressierung verwendet.
2. Wenn nicht, setzt ARP eine Anfrage mit der IP-Adresse nach der Hardware-Adresse in das Netzwerk. Dazu wird die MAC-Broadcast Adresse `ff-ff-ff-ff-ff-ff` verwendet. Diese Anfrage wird von allen Stationen im selben Subnetz entgegengenommen und ausgewertet.
3. Die Stationen vergleichen die gesendete IP-Adresse mit ihrer eigenen. Wenn sie nicht übereinstimmt, wird die Anfrage verworfen.
4. Wenn die IP-Adresse übereinstimmt schickt die betreffende Station eine ARP-Antwort direkt an den Sender der ARP-Anfrage.
5. Dieser Speichert die Hardware-Adresse in seinem Cache.
6. Da bei beiden Stationen die Hardware-Adresse bekannt sind, können sie nun miteinander Daten austauschen.

**Fall 2:** Ziel IP-Adresse befindet sich *nicht* im gleichen Subnetz.

1. Eine ARP-Anfrage wird an das Standard-Gateway geschickt.
2. Findet ARP die Hardware-Adresse des Standard-Gateways im Cache nicht, wird eine lokale ARP-Adressauflösung ausgelöst.

3. Ist die Hardware-Adresse des Standard-Gateways bekannt, schickt der Sender bereits sein erstes Datenpaket an die Ziel-Station.
4. Der Router (Standard-Gateway) nimmt das Datenpaket in Empfang und untersucht den IP-Header.
5. Der Router überprüft, ob sich die Ziel-IP-Adresse in einem angeschlossenen Subnetz befindet. Wenn ja, ermittelt er anhand der lokalen ARP-Adressauflösung die MAC-Adresse der Ziel-Station.
6. Anschließend leitet er das Datenpaket weiter.
7. Ist das Ziel in einem entfernten Subnetz, überprüft der Router seine Routing-Tabelle, ob ein Weg zum Ziel bekannt ist. Ist das nicht der Fall steht dem Router auch ein Standard-Gateway zu Verfügung.
8. Der Router führt für sein Standard-Gateway eine ARP-Adressauflösung durch und leitet das Datenpaket an dieses weiter.

Die vorangegangenen Schritte wiederholen sich dann so oft, bis das Datenpaket sein Ziel erreicht oder das IP-Header-Feld TTL auf den Wert 0 springt. Dann wird das Datenpaket vom Netz genommen. Erreicht dann irgendwann das Datenpaket doch sein Ziel, schreibt die betreffende Station seine Rückantwort in ein ICMP-Paket an den Sender. In dieser Antwort wird falls möglich ein Gateway vermerkt, über das die beiden Stationen miteinander kommunizieren. So werden weitere ARP-Adressauflösungen und dadurch Broadcasts vermieden.

[32]

Diese Adressauflösung könnte man noch in viele weitere Schritte zerlegen:

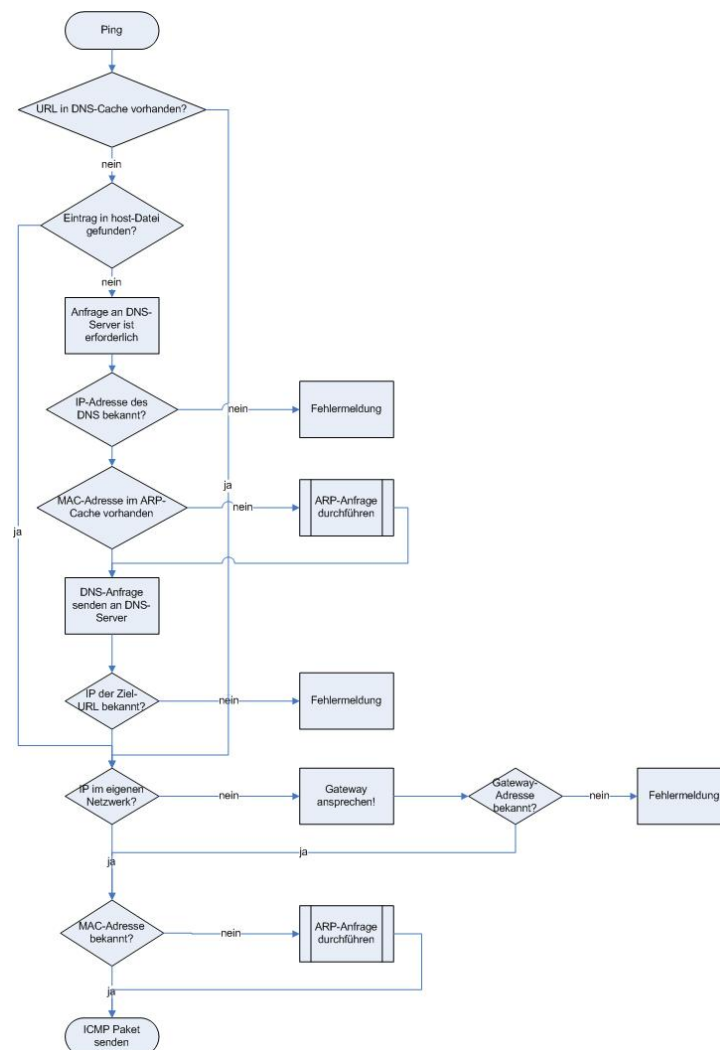


Abb. 8.2.: Beispiel einer Adressauflösung an Hand eines Pings

### 8.3.2. ARP-Cache

Durch den ARP-Cache wird vermieden, dass bei jedem Datenpaket an das selbe Ziel wieder und immer wieder ein ARP-Broadcast ausgelöst wird. Häufig benutzte Hardware-Adressen sind im ARP-Cache gespeichert. Die Einträge im ARP-Cache können statisch oder dynamisch sein. Statische Einträge können manuell hinzugefügt und gelöscht werden. Dynamische Einträge werden durch die ARP-Adressauflösung erzeugt.

### 8.3.3. Probleme mit ARP

ARP ist für den Benutzer unsichtbar, so dass das Vorhandensein dieses Protokolls meist nur bemerkt wird, wenn seltene Fehler auftreten.

Die Länge der Gültigkeit eines ARP-Eintrags (normalerweise wenige Minuten) kann ein Problem darstellen, wenn falsche Einträge vorhanden sind. Solange ein fehlerhafter Eintrag existiert, kann mit dem betreffenden Host nicht kommuniziert werden. Die Fehlfunktion wird häufig nicht dem ARP-Protokoll zugeschrieben, sondern dem Netz oder einem Fehler in der Netzwerkimplementierung. Darüber hinaus ermöglicht nicht jedes Betriebssystem das Erzeugen eines korrigierten Eintrags oder einer Anforderung.

Gravierender ist das Eintragen von Daten in den ARP-Cache aus Paketen, für die keine Anforderung erzeugt wurde (blinder Glaube). Ein überlasteter Host, der eine alte IP-Adresse führt, antwortet mit großer Wahrscheinlichkeit als letzter auf eine ARP-Anforderung mit einer Antwort, die die falsche Adresse enthält. Dieses letzte Paket überschreibt die ARP-Tabelle aller Geräte im Netz, ein fehlerhafter Eintrag bleibt übrig.

Mit ARP-Spoofing<sup>2</sup> ist es auch möglich, absichtlich eine falsche Hardwareadresse in einem Netz zu verteilen, teilweise sogar von außen über einen Remote-Broadcast. Dadurch kann der Datenverkehr für einen Rechner auf einen anderen umgelenkt und eventuell von diesem sogar gefiltert werden (Man-In-The-Middle-Angriff). Dies stellt ein Sicherheitsproblem dar.

Moderne Implementierungen ändern die ARP-Tabelle nur für ARP-Antworten, für die vorher von dem betreffenden Host eine -Anforderung generiert wurde.

[33]

## 8.4. Erweitertes Routing

### 8.4.1. Network Address Translation (NAT)

Network Address Translation (NAT) ist in Rechnernetzen der Sammelbegriff für Verfahren, um automatisiert und transparent Adressinformationen in Datenpaketen durch andere zu ersetzen. Diese kommen typischerweise auf Routern und Firewalls zum Einsatz.

Beim NAT werden die Adressen eines privaten Netzes über Tabellen öffentlich registrierten IP-Adressen zugeordnet. Dieses hat den Vorteil, dass Rechner, die innerhalb eines privaten Netzes miteinander kommunizieren müssen keine öffentlichen IP-Adressen benötigen. IP-Adressen interner Rechner, die eine Kommunikation mit Zielen im Internet aufbauen müssen erhalten in dem Router, der zwischen dem Internet Service Provider (ISP) und dem privaten Netzwerk steht, einen Tabelleneintrag. Durch diese Eins-zu-Eins-Zuordnung, sind diese Rechner nicht nur in der Lage, eine Verbindung zu Zielen im Internet aufzubauen, sondern sie sind auch aus dem Internet erreichbar. Die interne Struktur des Firmennetzwerkes bleibt jedoch nach außen verborgen.

---

<sup>2</sup>Siehe dazu auch den heise.de Artikel *Angriff von innen - Technik und Abwehr von ARP-Spoofing-Angriffen* (<http://www.heise.de/security/Angriff-von-innen--/artikel/55269>)

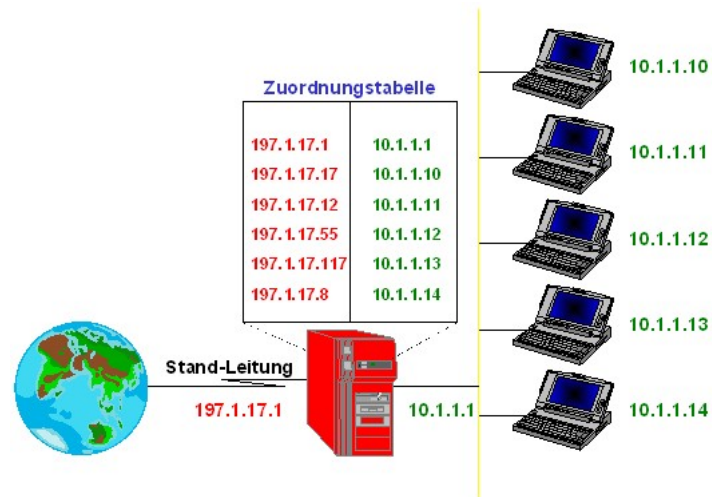


Abb. 8.3.: Funktionsweise NAT

Der Nachteil besteht allerdings darin, dass nur so viele Rechner sich mit dem Internet gleichzeitig verbinden können, wie externe IP-Adressen vorhanden sind. Da feste, externe IP-Adressen mitunter teuer sein können, ist dieses Verfahren recht unwirtschaftlich und wird nur noch selten verwendet. Hinzukommt, dass ein solches Netzwerk, kaum bis gar nicht skalierbar ist. NAT bietet auf diese Art und Weise auch keinen Schutz vor Angriffen von außen. Die Pakete gehen zwar durch den NAT Router, werden aber direkt an die internen Clients weitergereicht durch die direkte IP-Adressen Umsetzung.

### Paket-Adressierung

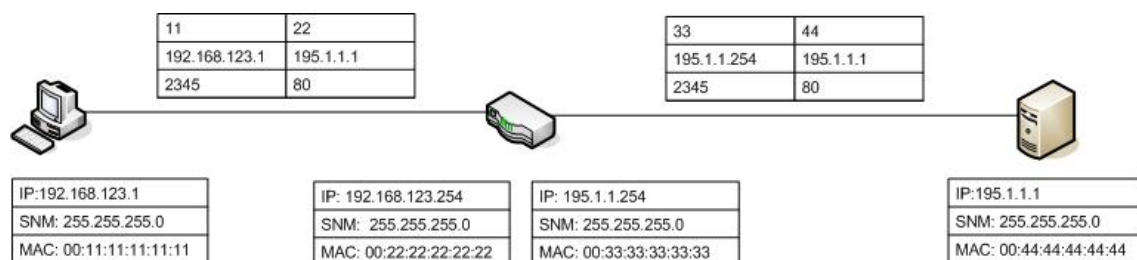


Abb. 8.4.: Paket-Adressierung NAT Routing

### 8.4.2. IP-Masquerading (PAT, NPT)

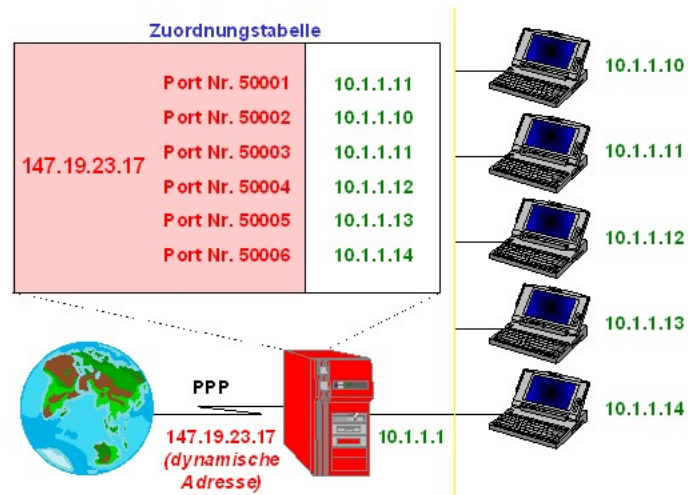
Das PAT-Konzept erweitert das NAT-Konzept um eine dynamische Portumsetzung, mit dem Ziel, über ein einziges PAT-Gerät mehreren Rechnern des internen (privaten) Netzwerks gleichzeitig den Zugang zum Internet zu ermöglichen.

Beim IP Masquerading, manchmal auch als PAT (Port and Address Translation), NPAT (Network and Port Address Translation) bezeichnet, bildet alle Adressen eines privaten Netzwerkes auf eine einzelne öffentliche (dynamische) IP-Adresse ab. Um nun mehrere Rechner über ein einziges PAT-Gerät mit dem Internet zu verbinden, müssen die am Gerät eingehenden Pakete den jeweiligen Internetsitzungen zugeordnet werden können. Aus dem internen Netz heraus stellt dies kein Problem dar, da alle Netzwerkpakete eine eindeutige Absenderadresse aufweisen. Verwenden aber zwei interne Rechner denselben Rückgabeport und haben denselben Internetserver als Ziel, so ist eine eindeutige Zuordnung der Sitzung nicht mehr möglich, wenn die Pakete aus dem Internet heraus das Gerät erreichen (die Pakete sind an denselben Port des Gerätes adressiert und weisen dieselbe Absenderadresse – den Internetserver – auf, weshalb sie nicht mehr auseinander gehalten werden können). Dieses Problem wird gelöst, indem allen aus dem internen Netz angeforderten Internetsitzungen dynamisch ein anderer Port des PAT-Gerätes zugewiesen wird. PAT übersetzt im Unterschied zu NAT also nicht nur die IP-Adresse des Absenders, sondern auch den Port, ehe die Pakete in das Internet geleitet werden. Dies geschieht dadurch, dass bei einer existierenden Verbindung zusätzlich zu den Adressen auch die Portnummern verwendet wird, um eingehende Pakete wieder den internen Rechnern zuzuordnen. Kommt ein Paket aus dem internen Netz, vergibt der NAT Router dem Absender eine mehr oder weniger zufällige Portnummer, welche er sich in einer Tabelle merkt. Kommt die Antwort vom Server, guckt er in der Tabelle nach zu welchem Client, die Portnummer gehört und leitet das Paket an den zugehörigen Rechner weiter. Auf diese Weise benötigt ein gesamtes privates Netz nur eine einzige registrierte öffentliche IP-Adresse.

Befinden sich hinter dem NAT-Router Stationen mit Server-Diensten kann in der Router-Konfiguration eine Station einem TCP-Port zugewiesen werden. Daraufhin leitet der Router alle auf diesem Port eingehenden Datenpakete an diese Station weiter. Diesen Vorgang nennt man Port-Forwarding. Das Verfahren selber Destination NAT (DNAT). Dabei werden für einen bestimmten Port eintreffende Datenpakete an eine bestimmte Netzwerk-Station weitergeleitet.

Nachteil dieser Lösung: Die Rechner im privaten Netzwerk können nicht aus dem Internet angewählt werden. IP Masquerading ist das NAT Verfahren, was auch in den meisten DSL-WLAN Routern zum Einsatz kommt und wird dort meist nur (fälschlicherweise) als NAT bezeichnet.

Allerdings können beim IP Masquerading Rechner im internen Netz von aussen nicht erreicht werden. Da durch PAT lediglich einzelne Ports bei einer internen Verbindungsanforderung dynamisch mit einem internen Rechner verbunden werden, wird hier eine Filterung der Pakete realisiert. Eine Anfrage aus dem Internet an einen Client blockiert das PAT-Gerät, solange keine Port-Forwarding-Regel darauf existiert. Denn je nach Implementierung sind selbst die dynamisch geöffneten Ports nur von der Adresse aus ansprechbar, an die die Verbindung gerichtet ist, wobei alle anderen Ports gesperrt bleiben (wo sollten sie auch hinzeigen?). Desweiteren ist IP Masquerading bisher nur unter Linux nutzbar und für spezielle Protokolle müssen entsprechende Module geladen werden. Dafür erfordert es aber nur eine externe Adresse und bei den Clientrechnern ist keine großartige Konfiguration, wie beim Proxy, nötig, da einfach der NPAT-Server als Standardgateway eingetragen wird.

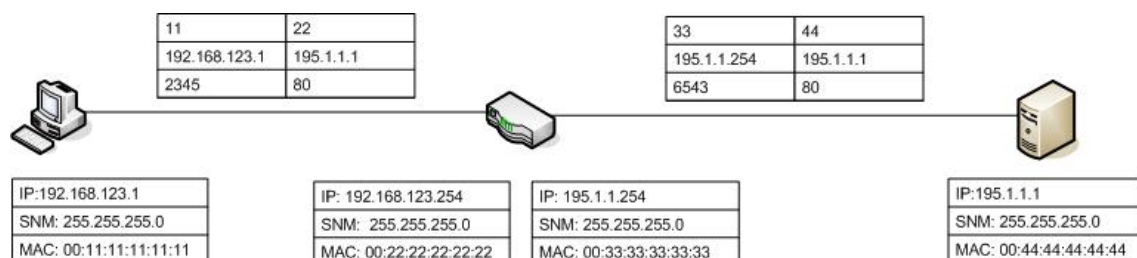


**Abb. 8.5.:** Funktionsweise IP Masquerading

### NAT-Router als Firewall

Die Default-Arbeitsweise eines NAT-Routers ist das Weiterleiten von Datenpaketen von speziell konfigurierten TCP-Ports und vom Datenstrom, der aus dem lokalen Netz initiiert wurde. Alle anderen eingehenden Pakete werden verworfen und bekommen so keinen Zugang zum lokalen Netz. Hacker, die zyklisch alle TCP-Ports einer IP-Adresse nach offenen Ports absuchen (Port-Scan) bekommen keine Antwort vom Router. Wichtig: Ein Router mit NAT ersetzt keine richtige Firewall. Er verhindert nur Datenverbindungen, die nicht vom lokalen Netz aus initiiert wurden oder für die vorher kein Datenverkehr registriert wurde. Vorsicht auch beim Freischalten von TCP-Ports (Port-Forwarding). Wer keine Server-Dienste für Stationen aus dem Internet zu Verfügung stellt, sollte alle TCP-Ports des Routers (unter 1024) sperren. Wer darauf nicht verzichten kann, sollte aus Sicherheitsgründen eine Demilitarisierte Zone (DMZ) einrichten und so den Datenverkehr aus dem Internet aus dem lokalen Netzwerk heraus halten.

### Paket-Adressierung



**Abb. 8.6.:** Paket-Adressierung PNAT Routing

### 8.4.3. Proxy

Proxies setzen ebenfalls Adressen um, während das Netzwerkpaket den Proxy passiert. Jedoch verwenden die meisten dafür kein NAT. Vielmehr nimmt der Proxy die Anfrage der einen Seite als Kommunikationspartner entgegen und baut eine eigene Verbindung zur anderen Seite auf. Als aktive Kommunikationspartner operieren diese Proxies auf der OSI-Schicht 7 und sind in der Lage, eine weit reichende Analyse und Anpassungen der Paketinhalte vorzunehmen, ehe sie die Daten an die andere Seite übermitteln. Ein solcher Proxy terminiert somit die Verbindungen auf beiden Seiten (es handelt sich also um zwei eigenständige Verbindungen), statt die Pakete einfach wie ein NAT-Gerät weiterzuleiten.

Dagegen gibt es bei generischen Proxies durchaus Überschneidungen zu NAT: Der *circuit level Proxy*, die erste Form eines Proxys überhaupt, realisiert die Adressumsetzung als NAT-Gerät auf der OSI-Schicht 3. Parallel dazu bietet er eine Adressfilterung an, die ebenfalls auf der dritten OSI-Schicht angesiedelt ist, wobei er für die Filterung von Ports zudem auf der OSI-Schicht 4 operiert. Solche (Layer 3 + 4) Proxies reichen die Pakete schlicht durch, ohne die Verbindungen selbst zu terminieren. Von diesem Sonderfall einmal abgesehen, nimmt NAT jedoch eine zu vernachlässigende und daher kaum beachtete Rolle unter den Proxies ein.

#### Paket-Adressierung

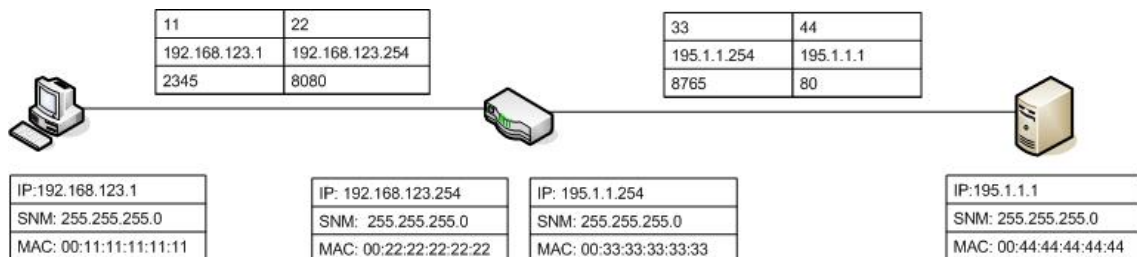


Abb. 8.7.: Paket-Adressierung Proxy Routing

[36], [37], [38]

## **A. Anhang - Zusätzliche Tabellen und Grafiken**

Hier befinden sich Tabellen und Grafiken, die für den Text zu groß geworden wären bzw. zu stark verkleinert hätten werden müssen.

Bezeichnung	Wellenlänge	Frequenz	Technischer Einsatz
Niederfrequenz Längstwellen	> 10 km	< 30 KHz	U-Boot-Kommunikation (DHO38, ZEVS, Sanguine, SAQ), Funknavigation
Radiowellen	< 10 km	> 30 KHz	Langwellenrundfunk
Langwelle (LW)	< 10 km	> 30 KHz	
Mittelwelle (MW)	< 650 m	> 650 KHz	
Kurzwelle (KW)	< 180 m	> 1,7 MHz	
Ultrakurzwelle (UKW)	< 10 m	> 30 MHz	
Mikrowellen	1 mm - 1 m	300 MHz - 300 GHz	Magnetresonanztomografie, Mobilfunk, Fernsehen, Mikro- wellenherd, WLAN, Bluetooth, GPS
Dezimeterwellen	10 cm - 1 m	300 MHz - 3 GHz	
Zentimeterwellen	1 cm - 10 cm	3 - 30 GHz	Radioastronomie, Richtfunk, Satellitenfernsehen, WLAN
Millimeterwellen	1 mm - 1 cm	30 - 300 GHz	
Terahertzstrahlung	30 $\mu$ m - 3 mm	0,1 THz - 10 THz	
Infrarotstrahlung (Wärmestrahlung)	780 nm - 1,0 mm	> 300 GHz	Radioastronomie, Spektroskopie, Abbildungsverfahren IR-Spektrometer, Infrarotastronomie
Fernes Infrarot	50 $\mu$ m - 1,0 mm	> 300 GHz	
Mittleres Infrarot	2,5 $\mu$ m - 50 $\mu$ m	> 6,00 THz	Fernbedienung, Datenkommunikation (FRDA), CD Beleuchtung, Colorimetrie, Fotometrie DVD, Laserpointer, Lichtzeichenanlage
Nahes Infrarot	780 nm - 2,5 $\mu$ m	> 120 THz	
Licht	380 nm - 780 nm	> 384 THz	
Rot	640 nm - 780 nm	384 - 468 THz	Lichtzeichenanlage
Orange	600 nm - 640 nm	468 - 500 THz	
Gelb	570 nm - 600 nm	500 - 526 THz	
Grün	490 nm - 570 nm	526 - 612 THz	
Blau	430 nm - 490 nm	612 - 697 THz	Blu-ray Disc Desinfektion, UV-Licht, Spektroskopie
Violett	380 nm - 430 nm	697 - 789 THz	
UV-Strahlen	1 nm - 380 nm	> 789 THz	Schwarzlicht Fluoreszenz, Phosphoreszenz, Banknotenprü- fung, Fotolithografie
schwache UV-Strahlen	200 nm - 380 nm	> 789 THz	
Starke UV-Strahlen	50 nm - 200 nm	> 1,5 PHz	EUV-Lithografie, Röntgenmikroskopie, Nanoskopie medizinische Diagnostik, Sicherheitstechnik, Röntgen- Strukturanalyse, Röntgen-Beugung, Spektroskopie
XUV	1 - 50 nm	6 PHz - 300 PHz	
Röntgenstrahlen	10 pm - 1 nm	> 300 PHz	
Gammastrahlen	< 10 pm	> 30 EHz	

Tab. A.1.: Frequenzspektrum

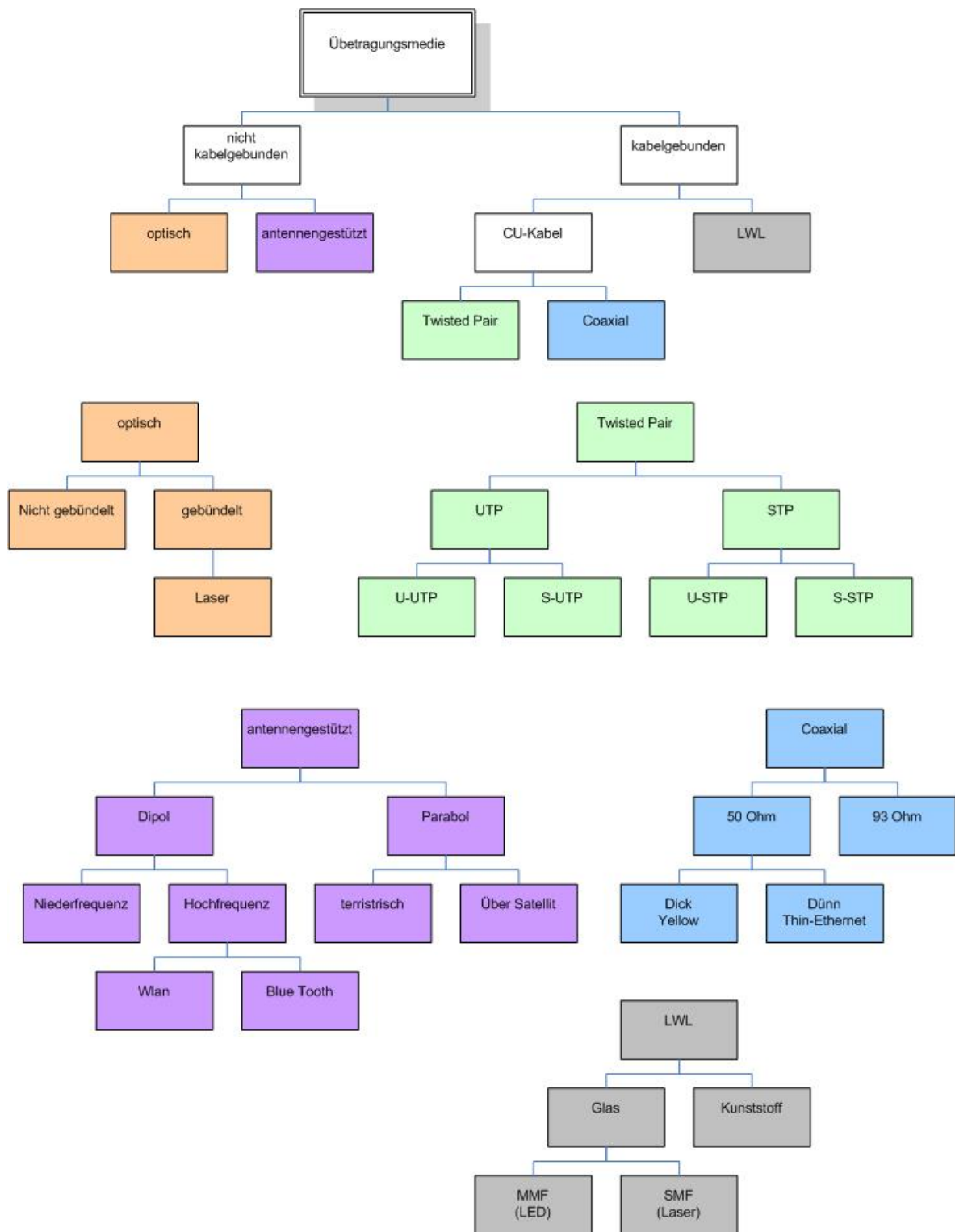
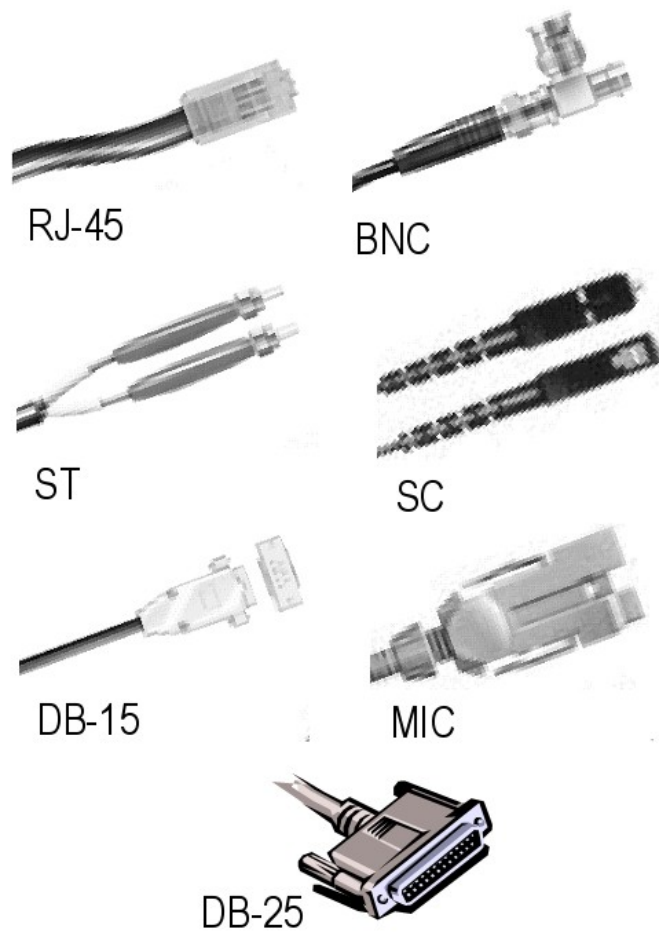


Abb. A.1.: Einteilung von Übertragungsmedien



**Abb. A.2.:** Steckertypen

<b>CIDR<sup>a</sup></b>	<b>Beschreibung</b>	<b>RFC<sup>b</sup></b>
0.0.0.0/8	Aktuelles Netzwerk (nur als Quelladresse gültig)	RFC 3232 (ersetzt RFC 1700)
10.0.0.0/8	Privates Netzwerk	RFC 1918
14.0.0.0/8	Öffentliches Datennetzwerk	RFC 3232 (ersetzt RFC 1700)
39.0.0.0/8	Reserviert	RFC 1797
127.0.0.0/81)	Localhost	RFC 3330
128.0.0.0/16	Reserviert	
169.254.0.0/16	Zeroconf	RFC 3927
172.16.0.0/12	Privates Netzwerk	RFC 1918
191.255.0.0/16	durch IANA <sup>c</sup>	reserviert
192.0.0.0/24	durch IANA	reserviert
192.0.2.0/24	Dokumentation und Beispielcode (TEST-NET)	RFC 3330
192.88.99.0/24	6to4-Anycast-Weiterleitungspräfix	RFC 3068
192.168.0.0/16	Privates Netzwerk	RFC 1918
198.18.0.0/15	Netzwerk-Benchmark-Tests	RFC 2544
223.255.255.0/24	Reserviert	RFC 3330
224.0.0.0/4	Multicasts (früheres Klasse-D-Netzwerk)	RFC 3171
240.0.0.0/4	Reserviert (früheres Klasse-E-Netzwerk)	RFC 3232 (ersetzt RFC 1700)
255.255.255.255/24	Broadcast	

**Tab. A.2.: Besondere IP-Adressen nach RFC 3330**

<sup>a</sup>Classless Inter-Domain Routing

<sup>b</sup>Request for Comments

<sup>c</sup>Internet Assigned Numbers Authority

Netzklasse	Präfix	Adressbereich	Netzmaske	Netzlänge (mit Präfix)	Netzlänge(ohne Präfix)	Hostlänge	Netze	Hosts pro Netz
Klasse A	0...	0.0.0.0 - 127.255.255.255	255.0.0.0	8 Bit	7 Bit	24 Bit	128	16.777.214
Klasse B	10...	128.0.0.0 - 191.255.255.255	255.255.0.0	16 Bit	14 Bit	16 Bit	16.384	65.534
Klasse C	110...	192.0.0.0 - 223.255.255.255	255.255.255.0	24 Bit	21 Bit	8 Bit	2.097.152	254
Klasse D <sup>a</sup>	1110...	224.0.0.0 - 239.255.255.255	-	-	-	-	2.097.152	254
Klasse E	1111...	240.0.0.0 - 255.255.255.255	-	-	-	-	2.097.152	254

**Tab. A.3.: Netzklassen**

<sup>a</sup>Die Klasse D wird für Verwendung für Multicast-Anwendungen verwendet und die Klasse E ist reserviert.

<b>Name</b>	<b>RIP V1-Routing Information Protocol</b>
Ursprung	Beruhrt auf RFC 1058.
Protokolltyp	Entfernungsvektor auf der Grundlage des Entfernungsvektoralgorithmus von Bellman-Ford.
Metrik	Hop-Count.
Methodik	Wählt die Router mit dem niedrigsten Hop-Count aus und aktualisiert die anderen Router durch Versendung der vollständigen Routing-Tabelle an sämtliche Router im Abstand von 30 Sekunden.
Ideale Topologie	Kleinere Netzwerke von geringer Dynamik mit weniger als 15 Hops und ohne Subnetze mit klassifizierten Grenzen.
Stärken	Einfach zu konfigurieren und zu benutzen. Gut bekannt und weit verbreitet, da schon seit langem im Einsatz.
Schwächen	Auf einen Hop-Count von 15 begrenzt. Unterstützt keine Subnet-Masken mit variabler Länge. Funktioniert nicht in Netzwerken mit Teilnetzen, deren Parameter von den normalen /8, /16, /24 (255.0.0.0, 255.255.0.0, 255.255.255.0) abweichen oder nicht den Netzwerk-grenzen der Klassen A, B und C angehören. Konvergiert langsam, insbesondere in großen Netzwerken. Kennt die Bandbreite einer Verbindung nicht. Unterstützt nicht mehrere Pfade für dieselbe Route. Verschicken der vollständigen Routing-Tabelle beansprucht Bandbreite. Neigt zu Routing-Schleifen.

---

**Tab. A.4.:** *RIP V1*

<b>Name</b>	<b>RIP V2-Routing Information Protocol</b>
Ursprung	Beruhrt auf RFC 1388.
Protokolltyp	Entfernungsvektor auf der Grundlage des Entfernungsvektoralgorithmus von Bellman-Ford.
Metrik	Hop-Count.
Methodik	Wählt die Router mit dem niedrigsten Hop-Count aus und aktualisiert die anderen Router durch Versendung der vollständigen Routing-Tabelle an sämtliche Router im Abstand von 30 Sekunden.
Ideale Topologie	Kleinere Netzwerke von geringer Dynamik mit weniger als 15 Hops und ohne Subnetze mit klassifizierten Grenzen.
Stärken	Einfach zu konfigurieren und zu benutzen. Gut bekannt und weit verbreitet, da schon seit langem im Einsatz. Version 2 unterstützt auch VSLM und Classless Internet Domain Routing (CIDR), MD5 Authentication und Routen-Summierung.
Schwächen	Auf einen Hop-Count von 15 begrenzt. Konvergiert langsam, insbesondere in großen Netzwerken. Kennt die Bandbreite einer Verbindung nicht. Unterstützt nicht mehrere Pfade für dieselbe Route. Verschicken der vollständigen Routing-Tabelle beansprucht Bandbreite. Neigt zu Routing-Schleifen.

---

**Tab. A.5.:** *RIP V2*

<b>Name</b>	<b>IGRP-Interior Gateway Routing Protocol</b>
Ursprung	Beruhrt auf der Implementierung von Cisco und nicht auf einem Internet RFC.
Protokolltyp	Entfernungsvektor auf der Grundlage des Entfernungsvektoralgorithmus von Bellman-Ford.
Metrik	Verzögerung, Bandbreite, Verfügbarkeit und Last.
Methodik	Verschickt alle 5 Sekunden Hello-Pakete an seine Nachbarn, um festzustellen, ob diese noch verfügbar sind; aktualisiert andere Router nur nach Routenwechsel.
Ideale Topologie	Alle Netzwerke von klein bis sehr groß; alle Router müssen von Cisco sein. Kann Netzwerke nicht in Teilnetze über die klassifizierten Grenzen hinaus aufteilen.
Stärken	Einfach zu konfigurieren und zu benutzen. Nutzt Verzögerungen, Bandbreite, Verfügbarkeit und Last von Verbindungen als Metrik. Ist daher sehr exakt bei der Auswahl der geeigneten Route.
Schwächen	Kein Internet-Standard; alle Router müssen von Cisco Systems sein. Konvergiert langsam; langsamer als RIP. Unterstützt VLSM nicht. Neigt zu Routing-Schleifen.

**Tab. A.6.: IGRP**

<b>Name</b>	<b>EIGRP-Enhanced Interior Gateway Routing Protocol</b>
Ursprung	Beruhrt auf der Implementierung von Cisco und nicht auf einem Internet RFC.
Protokolltyp	Hybrider Entfernungsvektor.
Metrik	Verzögerung, Bandbreite, Verfügbarkeit und Last, nutzt den Diffusing Update Algorithm (DUAL).
Methodik	Verschickt alle 5 Sekunden Hello-Pakete an seine Nachbarn, um festzustellen, ob diese noch verfügbar sind; aktualisiert andere Router nur nach Routenwechsel.
Ideale Topologie	Alle Netzwerke von klein bis sehr groß; alle Router müssen von Cisco sein.
Stärken	Nutzt DUAL und bietet damit eine sehr schnelle Konvergenz und ein schleifenfreies Netzwerk. Unterstützt IP und IPX. Beansprucht CPU weniger als OSPF (siehe nächsten Abschnitt) Beansprucht wenig Bandbreite für die Routing-Updates. Unterstützt VLSM oder CIDR. Nutzt Verzögerungen, Bandbreite, Verfügbarkeit und Last von Verbindungen als Metrik und ist daher sehr exakt bei der Auswahl der geeigneten Route. Bietet Abwärtskompatibilität mit IGRP.
Schwächen	Kein Internet-Standard; alle Router müssen von Cisco Systems sein.

**Tab. A.7.: IGRP**

<b>Name</b>	<b>OSPF V2-Open Shortest Path First</b>
Ursprung	Beruhet auf RFC 2328. Version 1 wurde nie implementiert.
Protokolltyp	Link-Status, benutzt den Dijkstra-Algorithmus zur Berechnung des Baumes mit dem kürzesten Pfad (SPF = Shortest Path First).
Metrik	Berechnet den Aufwand für die Durchquerung der Router-Links bis zum Erreichen des Ziels, berücksichtigt dabei die Bandbreite der Verbindungen.
Methodik	Baut eine Umgebung mit seinen Nachbarn auf, versendet periodisch Hello-Pakete an die Nachbarn, gibt Veränderungen an die Nachbarn weiter, wenn sich der Link-Status verändert und sendet alle 30 Minuten „Paranoia-Updates“ über alle neuen Veränderungen des Link-Status an seine Nachbarn.
Ideale Topologie	Sämtliche Netzwerke von klein bis sehr groß.
Stärken	Konvergiert schnell im Vergleich zum Entfernungsvektorprotokoll. Update-Pakete für das Routing sind klein, denn es wird nicht die vollständige Routing-Tabelle verschickt. Neigt nicht zu Routing-Schleifen. Passt sich großen Netzwerken sehr gut an. Erkennt die Bandbreite einer Verbindung, berücksichtigt diese bei der Auswahl der Verbindung. Unterstützt VLSM oder CIDR. Unterstützt eine Vielzahl von optionalen Features, die andere Protokolle nicht unterstützen.
Schwächen	Komplexere Konfiguration und schwieriger zu verstehen als das Entfernungsvektorprotokoll.

**Tab. A.8.:** *OSPF*



---

# Literaturverzeichnis

- [1] Wikipedia: *Centralized computing*.  
[http://en.wikipedia.org/wiki/Centralized\\_computing](http://en.wikipedia.org/wiki/Centralized_computing), Stand: 2008-01-08
- [2] Wikipedia: *Verteiltes Rechnen*.  
[http://de.wikipedia.org/wiki/Verteiltes\\_Rechnen](http://de.wikipedia.org/wiki/Verteiltes_Rechnen), Stand: 2008-01-08
- [3] Marko Heinrich: *Seminararbeit zum Seminar Semantic Grid*. Universität Koblenz-Landau  
[https://www.uni-koblenz.de/FB4/Institutes/IFI/AGStaab/Teaching/WS0405/seminar\\_semGrid/docs/I.1-GridEinfuehrung\\_Ausarbeitung.pdf](https://www.uni-koblenz.de/FB4/Institutes/IFI/AGStaab/Teaching/WS0405/seminar_semGrid/docs/I.1-GridEinfuehrung_Ausarbeitung.pdf), Stand: 2008-01-08
- [4] Wikipedia: *Local Area Network*.  
[http://de.wikipedia.org/wiki/Local\\_Area\\_Network](http://de.wikipedia.org/wiki/Local_Area_Network), Stand: 2008-01-08
- [5] Wikipedia: *Metropolitan Area Network*.  
[http://de.wikipedia.org/wiki/Metropolitan\\_Area\\_Network](http://de.wikipedia.org/wiki/Metropolitan_Area_Network), Stand: 2008-01-08
- [6] Wikipedia: *Wide Area Network*.  
[http://de.wikipedia.org/wiki/Wide\\_Area\\_Network](http://de.wikipedia.org/wiki/Wide_Area_Network), Stand: 2008-01-08
- [7] Wikipedia: *Elektromagnetisches Spektrum*.  
[http://de.wikipedia.org/wiki/Elektromagnetisches\\_Spektrum](http://de.wikipedia.org/wiki/Elektromagnetisches_Spektrum), Stand: 2008-01-08
- [8] Wikipedia: *Twisted-Pair-Kabel*.  
<http://de.wikipedia.org/wiki/Twisted-Pair-Kabel>, Stand: 2008-01-08
- [9] Wikipedia: *Lichtwellenleiter*.  
<http://de.wikipedia.org/wiki/Lichtwellenleiter>, Stand: 2008-01-08
- [10] Wikipedia: *MultiMediaModul Lichtwellenleiter*.  
<http://it.tud.uni-essen.de/lwltypen.htm>, Stand: 2008-01-09
- [11] Wikipedia: *Radiowelle*.  
<http://de.wikipedia.org/wiki/Radiowelle>, Stand: 2008-01-09
- [12] Wikipedia: *Dipolantenne*.  
<http://de.wikipedia.org/wiki/Dipolantenne>, Stand: 2008-01-09
- [13] Wikipedia: *Parabolantenne*.  
<http://de.wikipedia.org/wiki/Parabolantenne>, Stand: 2008-01-09
- [14] Wikipedia: *Mikrowellen*.  
<http://de.wikipedia.org/wiki/Mikrowellen>, Stand: 2008-01-09
- [15] Wikipedia: *Netzwerkkarte*.  
<http://de.wikipedia.org/wiki/Netzwerkkarte>, Stand: 2008-01-09

- [16] Wikipedia: *Modem*.  
<http://de.wikipedia.org/wiki/Modem>, Stand: 2008-01-09
- [17] Wikipedia: *Repeater*.  
<http://de.wikipedia.org/wiki/Repeater>, Stand: 2008-01-09
- [18] Wikipedia: *Bridge*.  
[http://de.wikipedia.org/wiki/Bridge\\_%28Netzwerk%29](http://de.wikipedia.org/wiki/Bridge_%28Netzwerk%29), Stand: 2008-01-09
- [19] Wikipedia: *Router*.  
<http://de.wikipedia.org/wiki/Router>, Stand: 2008-01-09
- [20] Wikipedia: *Carrier Sense Multiple Access*.  
[http://de.wikipedia.org/wiki/Carrier\\_Sense\\_Multiple\\_Access](http://de.wikipedia.org/wiki/Carrier_Sense_Multiple_Access), Stand: 2008-01-16
- [21] Wikipedia: *Crosskabel*.  
<http://de.wikipedia.org/wiki/Crosskabel>, Stand: 2008-01-16
- [22] Wikipedia: *Laser*.  
<http://de.wikipedia.org/wiki/Laser>, Stand: 2008-01-29
- [23] Wikipedia: *IP-Adresse*.  
<http://de.wikipedia.org/wiki/IP-Adresse>, Stand: 2008-03-07
- [24] Wikipedia: *Netzmaske*.  
<http://de.wikipedia.org/wiki/Netzmaske>, Stand: 2008-03-07
- [25] Digital Ether: *Arbeiten mit IP-Adressen*.  
[http://digitaletter.de/index.php?option=com\\_content&task=view&id=28&Itemid=43](http://digitaletter.de/index.php?option=com_content&task=view&id=28&Itemid=43),  
Stand: 2008-03-07
- [26] Wikipedia: *Netzklasse*.  
<http://de.wikipedia.org/wiki/Netzklasse>, Stand: 2008-03-07
- [27] Das elektronik Kompendium [ELKO]: *Subnetting*.  
<http://www.elektronik-kompendium.de/sites/net/0907201.htm>, Stand: 2008-04-27
- [28] Wikipedia: *OSI-Modell*.  
<http://de.wikipedia.org/wiki/OSI-Modell>, Stand: 2008-04-14
- [29] Wikipedia: *Internetprotokollfamilie*.  
<http://de.wikipedia.org/wiki/TCP/IP-Referenzmodell#TCP.2FIP-Referenzmodell>,  
Stand: 2008-04-14
- [30] Andrew S. Tanenbaum: *Computer-Netzwerke*. Wolfram's Verlag, 2. Auflage 1992 -  
Attenkirchen, ISBN 3-925328-79-3
- [31] Wikipedia: *Routing*.  
<http://de.wikipedia.org/wiki/Routing>, Stand: 2008-06-13
- [32] Das Elektronik Kompendium: *ARP - Address Resolution Protocol*.  
<http://www.elektronik-kompendium.de/sites/net/0901061.htm>, Stand: 2008-06-17
- [33] Wikipedia: *Address Resolution Protocol*.  
[http://de.wikipedia.org/wiki/Address\\_Resolution\\_Protocol](http://de.wikipedia.org/wiki/Address_Resolution_Protocol), Stand: 2008-06-17

- [34] David Davis : Artikel *Das beste Routing-Protokoll fuer Ihr Netzwerk*. 2002-02-18.
  
- [35] Wikipedia: *Broadcast*.  
<http://de.wikipedia.org/wiki/Broadcast>, Stand: 2008-06-25
  
- [36] tcp-ip-info.de: *Network Address Translation (NAT/ PAT/ IP Masquerading)*.  
[http://www.tcp-ip-info.de/tcp\\_ip\\_und\\_internet/ip\\_masquerading.htm](http://www.tcp-ip-info.de/tcp_ip_und_internet/ip_masquerading.htm), Stand: 2008-09-17
  
- [37] Hacker Board Wiki: *NAT, NAT-Router und PAT*.  
[http://wiki.hackerboard.de/index.php/NAT,\\_NAT-Router\\_und\\_PAT](http://wiki.hackerboard.de/index.php/NAT,_NAT-Router_und_PAT), Stand: 2008-09-17
  
- [38] Das Elektronik Kompendium: *NAT - Network Address Translation*.  
<http://www.elektronik-kompendium.de/sites/net/0812111.htm>, Stand: 2008-09-17
  
- [39] Wikipedia: *Strukturierte Verkabelung*.  
[http://de.wikipedia.org/wiki/Strukturierte\\_Verkabelung](http://de.wikipedia.org/wiki/Strukturierte_Verkabelung), Stand: 2008-11-18
  
- [40] Das Elektronik Kompendium: *Strukturierte Verkabelung*.  
<http://www.elektronik-kompendium.de/sites/net/0908031.htm>, Stand: 2008-11-18