Vorwort

Präambel

Das vorliegende Manuskript ist das Ergebnis des am Lehrstuhl für Rechnerkommunikation durchgeführten Hauptseminars "Netzwerktechniken der nächsten Generation".

Die einzelnen Beiträge wurden von dem jeweiligen Referenten nach seinem Vortrag ausgearbeitet und von uns in diesem Dokument zusammengestellt. In den einzelnen Kapiteln sind deshalb Sachverhalte mehrfach aufgeführt, bzw. werden von verschiedenen Sichtweisen aus dargestellt. Aber gerade die Vermittlung und Vertiefung dieser wichtigen Sachverhalte, war ein wesentliches Ziel dieser Vortragsreihe. Nachdem diese einzelnen Beiträge aus den Federn vieler Autoren stammen konnte natürlich kein homogenes Dokument entstehen.

Wir hoffen, dass dieses Skript eine wertvolle Einführung in die wichtigsten Netzwerktechniken der nächsten Generation darstellt, auch deshalb, weil auf die sonst übliche Strenge und Abstraktion in der Darstellung der Sachverhalte verzichtet wurde.

Wir bitten alle Leser die vielen kleinen und großen Fehler, welche sich noch im Dokument befinden, zu entschuldigen und uns falls möglich Korrekturvorschläge zukommen zu lassen[1].

München im März 2000

Volker Gerd Fischer und Hans-Peter Schwefel.

Ankündigung des Hauptseminars

Einführung

Internet, WWW, ATM, Gigabit-Ethernet. Das sind nur einige Schlagworte, die zur Zeit aus dem Bereich der Telekommunikations- und Datennetze sogar in nicht Fachkreisen breite Aufmerksamkeit finden. Hinter diesen Konzepten verbergen sich jedoch die Ergebnisse von mehr als 20 Jahren Entwicklungsarbeit und wissenschaftlicher Forschung. Der zunehmende Bedarf an Kommunikation, sowohl mobil als auch stationär, bei erhöhten Anforderungen an Bandbreite und Quality of Service wird die Entwicklung in der nächsten Zeit wohl noch beschleunigen. Spezialisten im Bereich Rechnernetze müssen diese Entwicklungen verstehen um auch in Zukunft die richtigen Entscheidungen "Welche Technik für welchen Zweck" treffen zu können.

Ziel dieses Hauptseminars ist es, tiefere Einblicke in den aktuellen Stand der Evolution von Rechnernetzen zu erlangen und die zugrunde liegenden Konzepte und Entwicklungen zu verstehen. Dazu sollen in den einzelnen Vorträgen die theoretischen Grundlagen mit der Lösung realer Probleme verbunden werden (Bottom-Up-Approach).

[1] email: `fischerv@in.tum.de` und `schwefel@in.tum.de`

Themen

1. SDH & WDM - Gigabit Wide Area Networks
2. ATM - Die Technik des B-ISDN
3. IEEE 802.x - LAN Technologien
4. IPv6 & MPLS - Internetprotokolle
5. RSVP & IP over ATM
6. xDSL & Powerline & Cable - Schnelle Zugangstechniken
7. VLANs & IPsec - Virtuelle Private Netze
8. OSPF & PNNI - Routingtechnologien und Topologieplanung
9. GSM & DECT & UMTS & IMT-2000 - Mobilkommunikation

Organisatorisches

Das Seminar richtete sich vorwiegend an die Studenten im Hauptstudium des Diplomstudiengangs Informatik an der TU und der LMU München. Nach erfolgreicher Teilnahme wurde ein Schein ausgestellt, der an beiden Universitäten als Hauptseminarschein anerkannt wird.

Teilnehmer

Vortrag	Vortragender	Vortragsdatum	Betreuer
1	Daniel Höllisch	11.11.99	Volker Fischer
2	Marcus Adlwart	18.11.99	Volker Fischer
3	Bernhard Wodok	25.11.99	Volker Fischer
4	Dimitri Dering	02.12.99	Volker Fischer
5	Raimund Brandt	09.12.99	Hans-Peter Schwefel
6	Martin Bitzinger	16.12.99	Volker Fischer
7	Hans-Peter Hagg	13.01.00	Volker Fischer
8	Tobias Weishäupl	20.01.00	Volker Fischer
9	Marco Hoffmann	27.1.00	Volker Fischer

Inhaltsverzeichnis

1 SDH & WDM - Gigabit Wide Area Networks

1.1 Einführung

Der Bedarf an Übertragungskapazität steigt stetig an. Dies gilt nicht erst seit dem Zeitalter des Internet. Schon damals, als die einzigen Netzbetreiber die Telefongesellschaften waren, stand man vor dem gleichen Problem. Die ständig ansteigende Zahl von Telefonteilnehmern und somit des Telefonverkehrs, führte zur Entwicklung von FDM-Systemen (Frequency Division Multiplex), um mehrere Verbindungen gleichzeitig über ein Kabel zu übertragen. Dazu modulierte man die Telefonkanäle mit verschiedenen Trägerfrequenzen, um diese Kanäle in andere Frequenzbereiche zu verschieben. In den 60'er Jahren schließlich kam die PCM (Pulse Code Modulation) auf

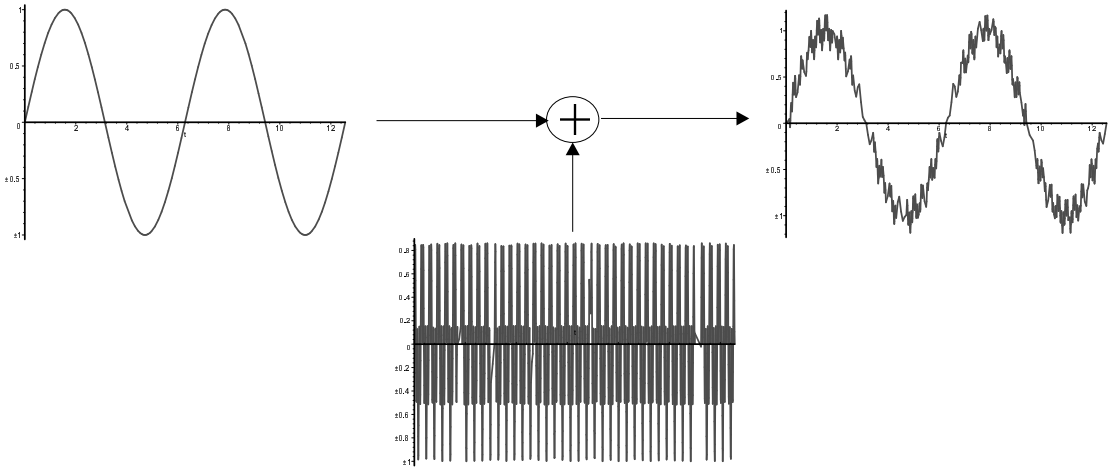


Abbildung 1: Modulation auf Trägerwelle

den Markt. Dies machte erstmals die Mehrfachausnutzung einer Leitung durch digitales Zeitmultiplexing möglich. Das analoge Telefonsignal wird hierzu mit einer Bandbreite von 3.1 kHz abgetastet, quantisiert und mit einer Bitrate von 64 kbit/s übertragen. In den 70'er Jahren

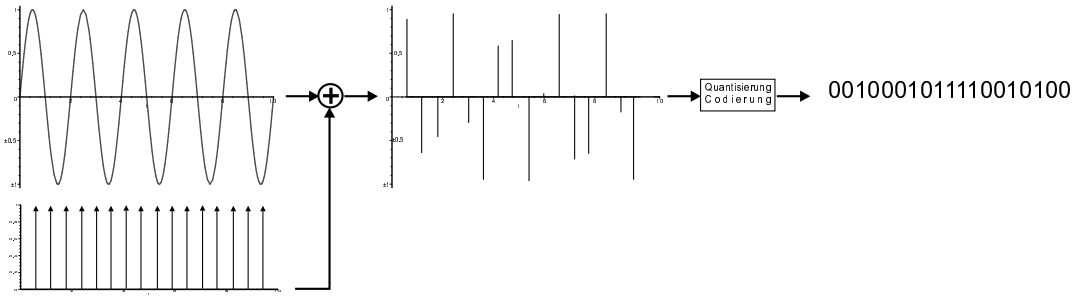


Abbildung 2: Pulse Code Modulation

wurde PDH (Plesiochronous Digital Hierarchy) entwickelt und durch die ITU-T Empfehlung *G.702* standardisiert. Hierarchie bedeutet, dass die verschiedenen Übertragungsraten von PDH jeweils ein Vielfaches der Basisübertragungsrate von 2048 kbit/s sind. Diese Rate ergibt sich aus 30 der oben beschriebenen 64 kbit/s Kanälen, plus Signalisierungsinformationen, welche zum Basisrahmen für PDH zusammengefaßt werden. Die Basisübertragungsrate ist somit das erste

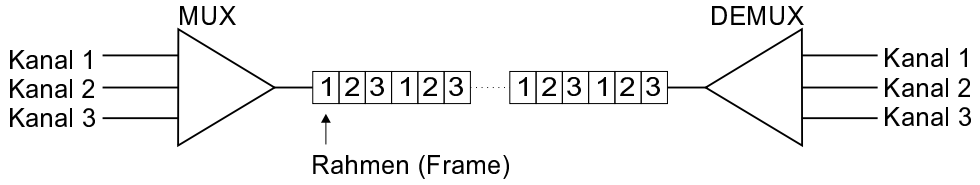


Abbildung 3: Time Division Multiplex

Niveau der Hierarchie und wird mit *E1* bezeichnet.
Diese Aussagen beziehen sich nicht auf die USA, Kanada und Japan, welche eine Basisübertragungsrate von 1544 kbit/s verwenden, dies entspricht 24 zusammengefaßten Kanälen.
Die Bezeichnung *Plesiochron*, also fast synchron, bezieht sich auf die Arbeitsweise der Multiplexer. Diese können mehrere Kanäle eines Hierarchieniveaus zu einem Kanal höheren Niveaus multiplexen. Die Bitraten der Eingangskanäle können jedoch leicht unterhalb der nominalen Übertragungsrate des Niveaus schwanken, die Differenz wird mit Füllbytes kompensiert. Die Multiplexer arbeiten darum nicht ganz synchron. Synchrones Takten war aufgrund der damaligen Technologie nicht möglich. Dieses sogenannte Stopf-Multiplexen hat den großen Nachteil, dass um einen einzigen Kanal abzuzweigen, z.B. in einem Router, wegen den leichten zeitlichen Schwankungen, der gesamte Datenstrom auseinandergenommen und wieder neu zusammengesetzt werden muss. Dies ist auch der Fall, wenn ein weiterer Kanal hinzugefügt werden soll. Diese Stopf-Multiplexer nennt man auch Add/Drop-Multiplexer.
Ein weiteres Problem von PDH ist, dass zur Leistungsmessung, dem Umleiten von Signalen bei Netzfehlern und dem Management entfernter Netzstationen, die hierzu notwendigen Informationen nicht vorhanden sind. Dies macht das Management von PDH-Netzen sehr schwierig.

Europa			**Nordamerika**		
Niveau	Faktor	Bitrate (Mbit/s)	Niveau	Faktor	Bitrate (Mbit/s)
E1	1	1,048	DS1	1	1,544
E2	4	8,448	DS2	4	6,312
E3	16	34,368	DS3	28	44,736
E4	64	139,264	-	-	-

Tabelle 1: PDH-Hierarchie in Europa und Nordamerika

1.2 Warum SDH?

In den 80'er Jahren schließlich überlegte man sich, wie man von diesem umständlichen Stopf-Multiplexen wegkommen könnte. Die Lösung hierzu wäre ein synchron getaktetes Netzwerk; somit könnte ein Multiplexer jederzeit einen Datenrahmen identifizieren, ihn gegebenenfalls umleiten, entfernen, oder einen Rahmen hinzufügen. Alles ohne den Datenstrom neu erzeugen zu müssen. Diese Überlegungen führten in Nordamerika zur Entwicklung von SONET (Synchronous Optical NETwork), ein Konzept von Bellcore, welches von ANSI standardisiert wurde. In Europa wurde daraus SDH (Synchronous Digital Hierarchy) abgeleitet und von der ITU-T als internationaler Standard definiert. SDH ist in den Empfehlungen *G.707, G.708* und *G.709*

definiert und enthält nur eine Teilmenge von SONET. Im weiteren wird nur noch auf SDH eingegangen.
Die Verwendung von SDH hat gegenüber PDH folgende Vorteile:[120]

1. Hohe Übertragungsraten
   Bald nach dem Jahr 2000 werden Übertragungsraten von über 40 Gbit/s erwartet. Bis 155 Mbit/s ist SDH sogar für Kupferleitungen definiert. SDH stellt also die ideale Technologie für Backbones dar.

2. Einfaches Add/Drop-Multiplexen
   Wie schon erwähnt, können Rahmen leicht aus dem Datenstrom entnommen und umgeleitet werden. Im Gegensatz zu PDH.

3. Hohe Verfügbarkeit und Kapazitätsauslastung
   Das Management wird wesentlich vereinfacht, da über ein Managementsystem (TMN - Telecommunication Network Management) auf einfache Weise, standardisierte Netzwerkkomponenten gesteuert werden. Somit ist es möglich, Mietleitungen innerhalb von Minuten(!) einzurichten. Bei PDH undenkbar!

4. Sicherheit
   SDH beinhaltet verschiedene automatische Sicherungs- und Reperaturmechanismen (Automated Protection Switching, APS). Der Ausfall einer Verbindung kann durch eine automatisch geschaltete Ersatzleitung kompensiert werden. Dies ist durch das TMN möglich.

5. Erweiterbarkeit
   SDH ist sowohl für heutige Dienste, wie z.B.: ISDN, Mobilfunk etc., als auch für die in der Zukunft kommenden Dienste, wie z.B.: Video-on-Demand oder Digital Broadcasting über ATM geeignet.

6. Interconnection
   Die standardisierten SDH-Schnittstellen erlauben, verschiedene Netze auf einfache Weise miteinander (über Gateways) zu verbinden. Sogar Verbindungen zu SONET-Netzen sind bedingt möglich. Durch die Standardisierung ist es auch möglich, ein Netz mit Komponenten verschiedener Anbieter aufzubauen. Dadurch sinken die Netzkosten, verglichen mit PDH.

1.3 SDH Pfadtopologie

Wie oben schon erwähnt, ist SDH bis zu einer Übertragungsrate von 155 Mbit/s sogar für Kupferleitungen definiert. Im Allgemeinen wird man SDH jedoch in optischen Netzwerken verwenden. Die Topologie einer SDH Verbindung zwischen zwei Terminal-Multiplexern[2] sieht folgendermaßen aus: Die Verbindung zwischen zwei Terminal-Multiplexern heißt *Pfad* (Path), dies ist also die Verbindung zu Quelle und Ziel. Die Verbindung zwischen weiteren Add/Drop-Multiplexern im Pfad, heißen *Leitungen* (Lines), eine Teilstrecke einer Leitung kann einen, oder mehrere Regeneratoren[3] (Repeater) enthalten, diese Teilstrecken nennt man *Abschnitte* (Sections). Ein Abschnitt ist also ein ununterbrochenes Stück Glasfaserkabel.

[2] Multiplexer mit Verbindung zu den Endstellen.
[3] Falls die zu überbrückende Distanz zu groß ist.

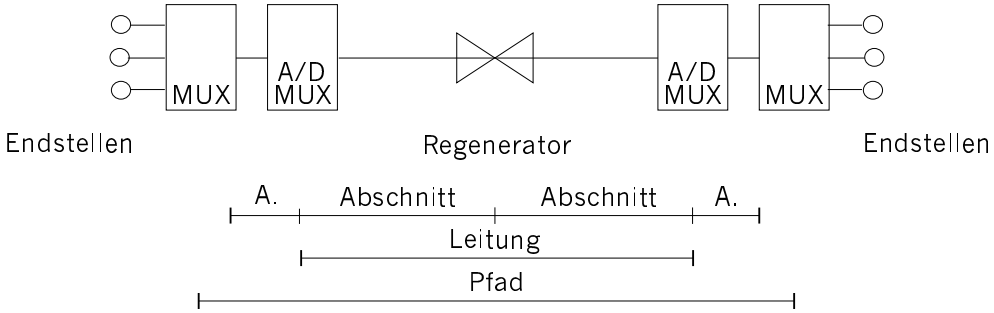


Abbildung 4: SDH Teilstreckenbezeichnungen

1.4 SDH-Aufbau

Der Basisrahmen von SDH, genannt STM-1 (Synchronous Transport Module), ist 2430 Bytes groß und in 9 Zeilen und 270 Spalten angeordnet. Die Rahmendauer beträgt 125 μs, das sind 8000 Rahmen pro Sekunde. Jedes Feld im Rahmen entspricht einem Byte und mit jedem Byte wird eine Kapazität von 64 kbit/s übertragen.
Um ein besseres Verständnis zu bekommen, wie SDH funktioniert, bietet sich das aus anderen Telekommunikationstechnologien bekannte Schichtenmodell an. Die unterste Schicht ist, wie üblich, die Physikalische: Also Kupferleitungen, Richtfunk- oder Satellitenstrecken, in der Regel aber Glasfaserverbindungen. Die nächste Schicht betrifft die Abschnitte zwischen den Regeneratoren, in Abbildung 4 sind das die *Abschnitte* (Sections). Ein Teil des SOH, der RSOH (Regenerator Section Overhead), steht für die Signalisierung in dieser Schicht zur Verfügung. Der Rest des SOH besteht aus dem MSOH (Multiplex Section Overhead), welcher für die SDH-Verbindungen zwischen den Multiplexern zur Verfügung steht. Auf diese drei Schichten bauen die beiden Schichten der Payload auf, die sog. Virtuellen Container (Virtual Container, VC). VC-4 welcher z.B. ATM, oder IP transportiert und VC-12, welcher auf VC-4 aufsetzt und z.B. ISDN transportiert. Das Transportieren der Payload in den VC's heißt Mapping, wie das funktioniert, erklären die folgenden Abschnitte. Nun aber genauer zum Basisrahmen STM-1:

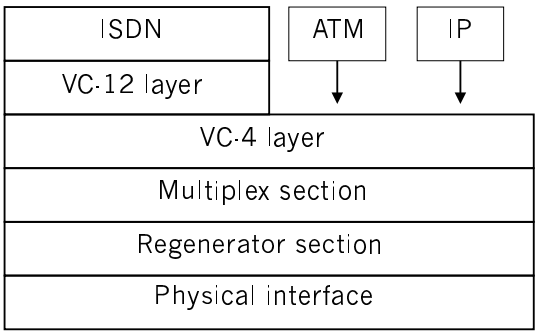


Abbildung 5: Das SDH Schichtmodell

Wie man aus Abbildung 6 ersieht, besteht der SOH aus drei Zeilen RSOH, einem Pointer, auf dessen Funktion später eingegangen wird und vier Zeilen MSOH. Der VC im Payloadbereich enthält noch den Pfad Overhead (Path Overhead, POH), auch dazu später mehr.

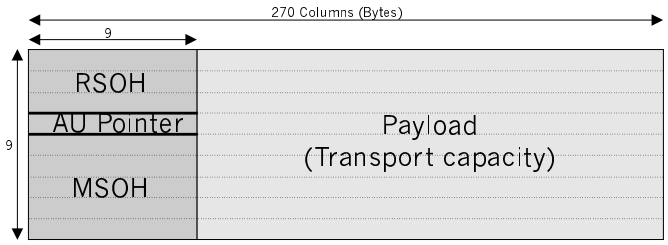


Abbildung 6: Synchronous Transport Module - 1

A1	A1	A1	A2	A2	A2	J0	Z	Z
B1	*	*	E1	*	X	F1	Z	Z
D1	*	*	D2	*	X	D3	X	X
AU Pointer								
B2	B2	B2	K1	X	X	K2	X	X
D4	X	X	D5	X	X	D6	X	X
D7	X	X	D8	X	X	D9	X	X
D10	X	X	D11	X	X	D12	X	X
S1	X	X	X	X	M1	E2	X	X

Tabelle 2: Section Overhead

Die einzelnen Felder in den Overheads sind alle, wie erwähnt, ein Byte groß. Die Bezeichnungen dieser stehen für folgende Funktionalitäten:

- **A** Rahmensynchronisation
- **B** Qualitätsüberwachung, Paritäts Bytes
- **C** Identifikation
- **D** Netzmanagement, data-communication channel
- **E** Sprachverbindung
- **K** Steuerung automatischer Ersatzschaltungen (APS)
- **Z** national use
- ***** Medienabhängig, z.B. Funk-, Satellitenstrecke
- **X** nicht definiert

Tabelle 3: Bedeutung der Bytes der Overheads

Sie dienen zur Synchronisation, Bitfehlerüberwachung, Signalkennzeichnung, Ersatzschaltungsverständigung, sowie der allgemeinen Systemsteuerung.[62]
Jedes der B - Bytes bietet also dem Betreiber einen standard Telefonkanal, mit 64 kbit/s. Mittels der D - Bytes werden Konfigurationsdaten zwischen den einzelnen Netzwerkknoten übertragen. Das macht das Management des Netzwerkes von einem zentralen Managementsystem aus möglich.

1.5 Datenübertragung mit SDH

Als Backbonetechnologie muss SDH natürlich in der Lage sein, den Datenverkehr anderer Netzwerktechnologien, wie z.B. ATM, PDH, oder IP zu transportieren. Hierzu wird das zu übertragende Signal zerteilt, und in einen sog. Container verpackt. Dazu kommt noch der POH, zur Wegesteuerung des Fragments im SDH-Netzwerk. Beides zusammen bildet den VC (Virtual Container). Da die ankommenden Signale natürlich nicht synchron zum SDH-Netz laufen, kann es sein, dass der Beginn des VC's innerhalb des Payload Bereiches, Administrative Unit (AU) genannt, schwankt. Zur Lokalisierung des VC's dient der schon erwähnte AU-Pointer im SOH. Es existieren verschieden große Container, um unterschiedliche Datenraten nach SDH mappen[4] zu können.
Der VC-4 ist der größte virtuelle Container. Benötigt man z.B. VC-3's zum Verpacken des Signals, werden drei dieser in einen VC-4 gemultiplext und in die Payload des STM gesteckt. Die Grafik unten, gibt die SDH-Multiplexingstruktur wieder. Wie man sieht, werden VC's zu

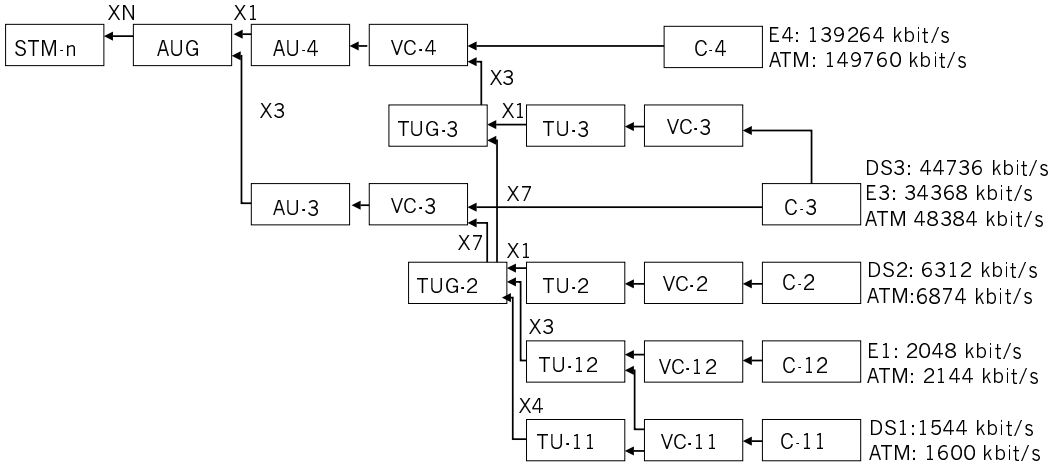


Abbildung 7: SDH Multiplex Struktur

Tributary[5] Units (TU) und diese wiederum zu Gruppen zusammengefaßt (TUG) . Die TUG's werden wieder in VC's höherer Ordnung verpackt, diese bilden zusammen mit ihren Pointern die AU's, diese bilden wieder Gruppen, schließlich werden die AUG's zur Payload der STM-N. Was es mit dem Faktor N auf sich hat, wird weiter unten erklärt.

Zusammen mit dem Path Overhead, bildet ein Container also einen Virtual Container. Der POH dient hierbei, neben der schon erwähnten Wegesteuerung, zur Qualitätsüberwachung und zur Kennzeichnung. Es gibt zwei verschiedene POH, einen für den VC-3 und VC-4, und einen für den VC-11 und VC-12.

1.6 Pointerarithmetik

Sehen wir uns einmal die Pointertechnik anhand einiger Beispiele etwas genauer an. Nehmen wir an, das Zubringersignal ist ein PDH Datenstrom, der Primärmultiplexrahmen hat eine Datenrate von 1,048 Mbit/s (vgl. Tabelle 1), mit 30 Telefonkanälen und zwei Synchron- und Kennzeichenkanälen. Die Rahmendauer dieses *E1*-Rahmens beträgt 125μs, wie wir aus 1.4 wissen, ist das

[4] Das Abbilden des Signals auf SDH
[5] eng. Tributary: Versorgung, Zubringer

J1	Pfadkennung
B3	Qualitätsüberwachung
C2	Zusammensetzung des Containers
G1	Rückmeldung Übertragungsfehler
F2	Wartung
H4	Kennzeichnung Überrahmen
F3	Wartung
K3	Automatische Ersatzschaltung
N1	Tandem Connection Monitoring

Tabelle 4: VC-3/4 Path Overhead

V5	Kennzeichnung und Fehlerüberwachung
J2	Pfadkennung
N2	Tandem Connection Monitoring
K4	Automatische Ersatzschaltung

Tabelle 5: VC-11/12 Path Overhead

auch die Rahmendauer des *STM-1*, also durchaus sinnvoll gewählt.
Das ankommende Signal wird nun fragmentiert und in einen VC gesteckt. Da das Zubringersignal jedoch nicht synchron zum SDH-Netz getaktet ist, "schwimmt" der VC quasi innerhalb der AU. Um den Anfang des VC lokalisieren zu können, zeigt der AU-Pointer auf dessen Anfang. Das ist das J1-Byte des POH. Um das System störfester gegen Übertragungsfehler zu machen, werden Veränderungen des Pointers mehrfach zuvor angekündigt. Der Pointer kann bei einem AU-4 pro Änderung nur um drei Bytes erhöht, oder erniedrigt werden. Das Schwimmen des VC in der AU hat zwei Ursachen:

1. Das Zubringersignal ist schneller als das Multiplexsystem. Um die zu große Datenmenge aufnehmen zu können, werden die H3-Bytes aus dem Pointerbereich benutzt. Dies wird als *negatives Stopfen* bezeichnet.

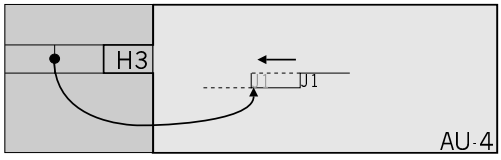


Abbildung 8: Negatives Stopfen

2. Das Zubringersignal ist langsamer als das Multiplexsystem. Der Pointer wird auf die neue Anfangsposition des VC verändert, dadurch bleiben Bytes aus dem Payload-Bereich ungenutzt. Dies wird als positives Stopfen bezeichnet.

Nehmen wir nun an, das Eingangssignal ist ein 48384 kbit/s ATM Datenstrom. Hier werden die Fragmente in VC-3's verpackt, je drei der VC's kommen als Payload in einen VC-4. Wie gehabt,

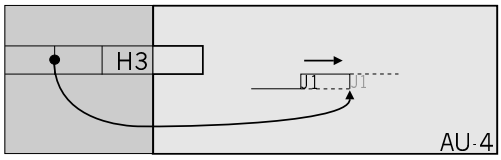


Abbildung 9: Positives Stopfen

zeigt der AU-Pointer auf den Beginn des VC-4. Innerhalb des VC-4 stehen, an festem Platz, drei weitere Pointer, welche auf die Startpositionen der VC-3's zeigen. Welche Kombinationen an VC-Verschachtelungen es gibt, ist aus der Multiplexhierarchie in Abbildung 7 ersichtlich. Durch das schwimmen der VC's innerhalb des Payload-Bereiches und die dadurch resultierenden Pointeraktionen, entsteht ein sog. *Jitter*, also ein Schwanken der Phasenlage des Datenstroms. Um diesen Jitter zu begrenzen, ist das Unterbringen dreier VC-3's in einem VC-4 das maximal erlaubte Maß an Pointerverschachtelung. Falls alle vier Pointer gleichzeitig schwanken, ergibt dies den maximal möglichen Jitter.

1.7 Multiframing

Nehmen wir nun an, der VC-4 ist zu klein um seine Payload aufnehmen zu können. In diesem Fall gibt es die Möglichkeit, mehrere VC-4's zusammen zu hängen. Der AU-4-4c ist z.B. für den Transport von B-ISDN-Bitraten vorgesehen [120]. Daraus ergibt sich der Vorteil, dass die Payload nicht fragmentiert werden muss. Alle Pointer der einzelnen VC-4 werden hierzu auf *Concatenation Indication* (CI) gesetzt. Sollten Pointeraktionen nötig sein, geschieht dies mittels des AU-4 Pointers innerhalb des SOH. Die entstehende Frame heißt dann STM-4. In manchen

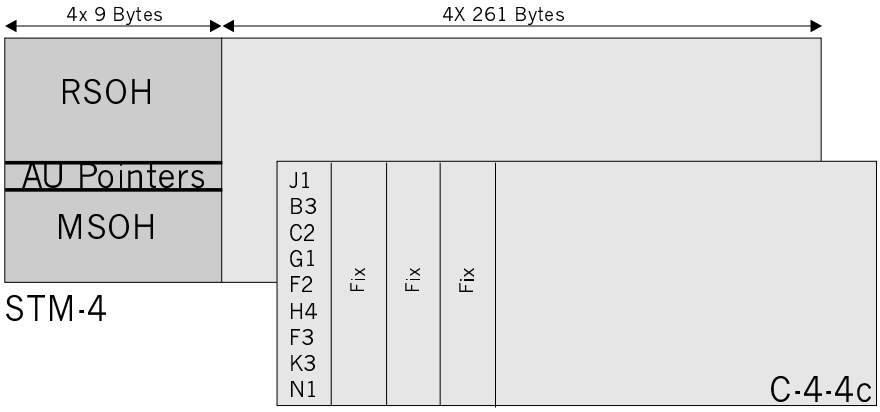


Abbildung 10: AU-4 Virtual Concatenation

Fällen, ist es den SDH-Cross-Connectoren (mehr dazu später) nicht möglich, die AU-4-4c als ganzes zu übertragen, dann wird diese in ihre einzelnen AU-4's zerlegt, übertragen, und am Ende wieder zum AU-4-4c zusammengefügt.

Tabelle 6 zeigt die für Multiframe-Bitraten definierten SDH-Hierarchiestufen. Es existiert noch eine zusätzliche Hierarchiestufe, nämlich *STM-0*, diese wird für Gateways zu SONET-Netzen, oder Richtfunk- und Satellitenverbindungen eingesetzt. Die STM-0 Bitrate beträgt 51,84

STM	1	155,52	Mbit/s
STM	4	622,08	Mbit/s
STM	16	2488,32	Mbit/s
STM	64	9953,28	Mbit/s

Tabelle 6: SDH-Hierarchiestufen für Multiframe-Bitraten

Mbit/s[120]. Die STM-0 Bitrate entspricht somit dem ersten Niveau, der SONET-Hierarchie, nämlich STS-1 OC-1.

1.8 Netzwerkkomponenten

Nun kommen wir zu den Komponenten aus denen ein SDH-Netzwerk aufgebaut ist.
Die Funktionen von Multiplexer und Regenerator sind uns schon aus 1.3 bekannt, hier eine Zusammenfassung:

- **Multiplexer**
  Terminal Multiplexer dienen zur Zusammenfassung plesio- und synchroner Eingangssignale.

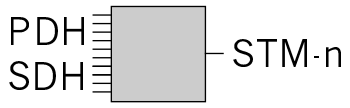


Abbildung 11: Terminal Multiplexer

  Add Drop Multiplexer dienen dazu, aus dem SDH - Bitstrom einzelne SDH, oder PDH - Signale auszulösen, oder einzufügen.

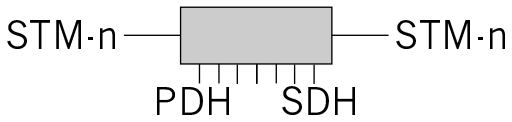


Abbildung 12: Add Drop Multiplexer

- **Regenerator**
  Dieser dient dazu, Signale zu verstärken, um die Übertragungsdistanz zu erhöhen.
- **Cross Connect**
  Eine weitere Komponente ist der *Cross Connect*, welcher in Abschnitt 1.7 zwar schon erwähnt, aber noch nicht erklärt wurde.
  Dieser dient sowohl dazu, PDH-Signale in VC's zu mappen, als auch VC-n's zu vermitteln.
  Ein Cross Connector heißt darum auch *Circuit* ***Switch***.

Um ein Netzwerk aufzubauen, gibt es drei grundsätzliche Topologien. Jede hat dabei ihre Vor- und Nachteile.

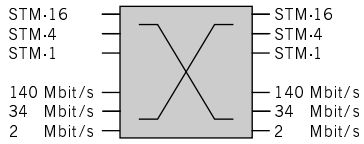


Abbildung 13: Cross Connector

1. **Bustopologie**
   Dies ist die preiswerteste Variante, da hier am wenigsten Kabel verbraucht wird. Im Falle eines Leitungsdefekts liegt fast das gesamte Netz lahm. Eine Ersatzschaltung kann

Abbildung 14: Bus Topologie

   hier nur durch eine sog. *Linear Protection* realisiert werden. Dazu muss zusätzlich zur sog. *Working Line* jeweils eine *Protection Line* vorhanden sein. Falls jede Working Line ihre eigene Protection Line hat, also zu 100% redundant ist, spricht man von einer 1+1 Architektur, falls sich mehrere Working Lines eine Protection Line teilen von einer 1:N Architektur.

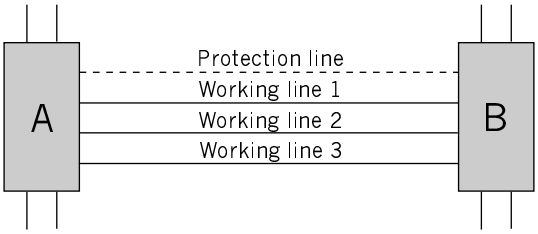


Abbildung 15: Linear Protection

2. **Sterntopologie**
   Hier laufen alle Verbindungen über eine zentrale Vermittlungsstelle. Dies hat zwar den Vorteil, dass bei Ausfall einer Leitung nur die damit verbundene Komponente ausfällt. Um dies zu kompensieren, ist es natürlich nötig jeden Zweig 1:N abzusichern.

3. **Ringtopologie**
   Diese hat oft das beste Preis- Leistungsverhältnis. Zum Einen wird im Vergleich zur Sterntopologie relativ wenig Kabel benötigt, zum Anderen bringt diese Topologie schon von Hause aus Sicherungsmöglichkeiten mit sich.

   - **Unidirektionale Ringe**
     Angenommen, es existiert ein Pfad von x1 nach x2 über A, B und C; dito einen Pfad von y1 nach y2 (siehe Abbildung). Fällt nun die Verbindung zwischen A und B aus, so wird automatisch vom SDH-System eine Ersatzschaltung über A, D und C eingerichtet. Somit bleiben die Datenpfade funktionsfähig.

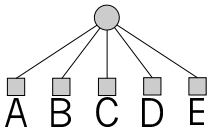


Abbildung 16: Stern Topologie

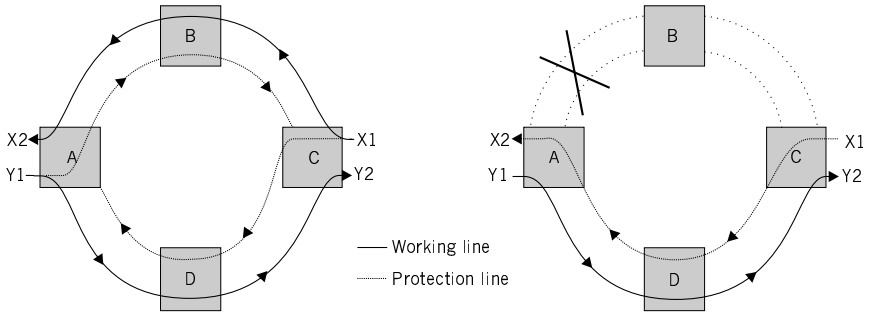


Abbildung 17: Unidirektionale Ring Topologie

- **Bidirektionale Ringe**
  Der Unterschied zum unidirektionalen Ring ist, dass hier eine Verbindung mit Hin- und Rückkanal auf einem einzigen Pfad geschaltet wird. Im Gegensatz dazu benötigt man beim unidirektionalen Ring immer einen kompletten virtuellen Ring. Bricht hier nur z.B. die Verbindung zwischen B und A ab, so kann das Netzelement in B einfach den Datenverkehr auf anderem Wege im Ring umleiten.

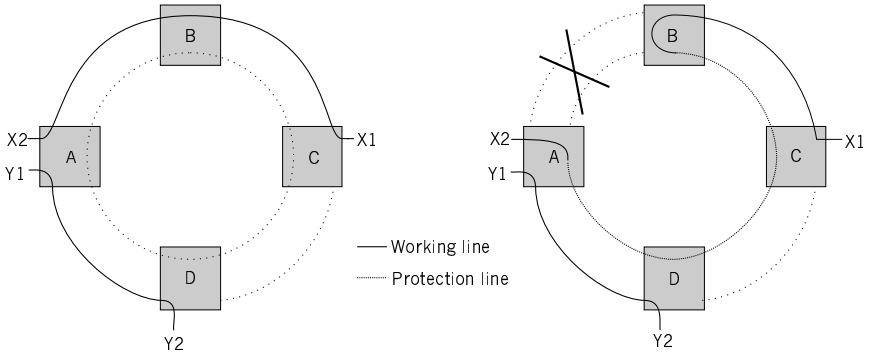


Abbildung 18: Bidirektionale Ring Topologie

Die Konfiguration der Netzelemente bei der automatischen Ersatzschaltung wird mittels der K1- und K2-Bytes des SOH gesteuert. Natürlich können die einzelnen Verbindungen im Ring wiederum mittels Linear Protection abgesichert werden.

In der Praxis existieren auch Kombinationen aus Ring und Stern Topologien, man spricht hier von einer sog. Maschen Topologie (engl: Mesh).

1.9 Lichtwellenleiter - physikalische Grundlagen

In der Regel wird man beim Aufbau eines SDH-Netzes Lichtwellenleiter (LWL) verwenden. Diese bieten die Möglichkeit, sehr weite Distanzen zu überwinden, und sind außerdem störungsunempfindlich gegen elektromagnetische Felder und abhörsicher.
Wie funktioniert aber so ein Lichtwellenleiter? Zunächst braucht man natürlich ein Medium, durch das man das Licht schicken will. Hier gibt es zwei Möglichkeiten: erstens Polymer, welches im WAN (Wide Area Network) / MAN (Metropolitan Area Network) - Bereich keine Rolle spielt; zweitens Glas, welches natürlich extrem rein sein muss. Um nun den Lichtstrahl innerhalb des Leiters halten zu können, muss man es irgendwie schaffen, dass er an der Leiteroberfläche reflektiert wird. Man macht sich hier einen physikalischen Effekt, die Totalreflexion, zu Nutze. Dieser tritt auf, wenn ein Lichtstrahl ab einem bestimmten Winkel auf eine Grenzfläche zweier Medien mit unterschiedlichen Brechungsindizes auftrifft. Sei n_1, der Brechungsindex des ersten Mediums und n_2 der des zweiten. So gibt die Formel $\sin\beta = \frac{n_1}{n_2}$ den Grenzwinkel der Totalreflexion an.
Bei LWL'n erzielt man diesen Effekt, indem man eine dünne Faser optisch "dicken" Substrats mit einem Mantel optisch "dünneren" Substrats umgibt. Es gibt dabei drei Typen von Lichtwellenleitern:

1. **Multimodefaser mit Stufenprofil**
   Als *Moden* (engl. modes) bezeichnet man die einzelnen Wellen, aus denen ein Lichtstrahl besteht. Multimode Fasern haben den oben beschriebenen Aufbau. Man nennt dies ein Stufenprofil des Brechungsindex innerhalb der Faser. Wie man im Bild sieht, legen die einzelnen Moden eines Lichtimpulses verschieden lange Strecken auf dem Weg durch die Faser zurück, je nachdem ob sie häufiger oder seltener reflektiert werden. Dadurch "verschmiert" der Rechteckimpuls etwas, das heißt, manche Moden kommen früher, manche später am Ende an. Dies ergibt das Glockenkurven-ähnliche Ausgangssignal[6]. Außerdem nimmt die Amplitude des Signals etwas ab, dazu aber später mehr.

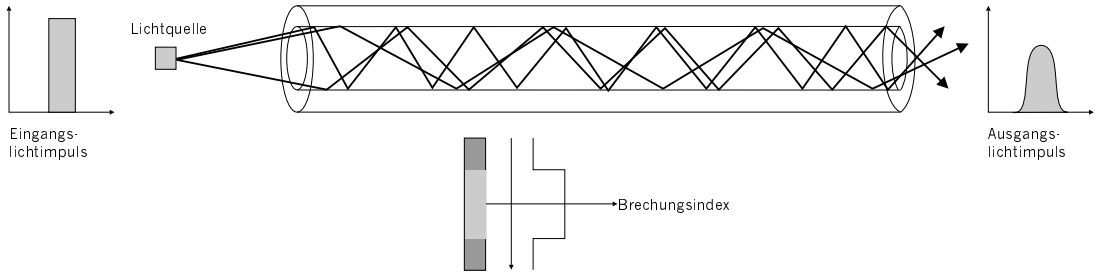


Abbildung 19: Multimodefaser mit Stufenprofil

2. **Multimodefaser mit Gradientprofil**
   Bei dieser Art von Glasfaser ändert sich der Brechungsindex innerhalb der Faser nach einer Parabolfunktion. Dies hat den Vorteil, dass die Spreizung des Eingangssignals, welche als Modendispersion bezeichnet wird, sehr effektiv unterdrückt wird. Dies funktioniert folgendermaßen: Im Kern der Faser, indem der optische Leiter dichter ist, bewegt sich die Mode etwas langsamer als jene Moden in den äußeren Bereichen der Faser. Dies hat

[6]Eigentlich müßten die Moden tatsächlich normalverteilt am Ausgang ankommen (Siehe Wahrscheinlichkeitstheorie). Hinweise dazu gab es jedoch in der mir zur Verfügung stehenden Literatur nicht.

zur Folge, dass sich häufig reflektierte Moden durchschnittlich schneller bewegen als die geradlinigeren Moden. Da die äußeren Moden jedoch auch längere Strecken zurücklegen, kompensiert dies die Modendispersion nahezu.

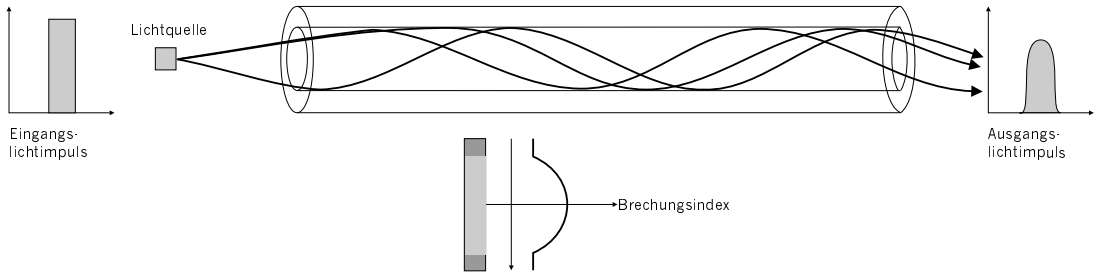


Abbildung 20: Multimodefaser mit Gradientprofil

3. **Monomodefaser**
Eine effektive Methode, die Modendispersion zu eliminieren, ist den Faserkern so weit zu verengen, dass nur noch eine Mode, nämlich jene auf der Mittelachse, durch die Faser paßt. Theoretisch kommt es hier nicht einmal mehr zu Reflexionen in der Faser. Tatsächlich ist bei Monomodefasern die Modendispersion zu vernachlässigen.

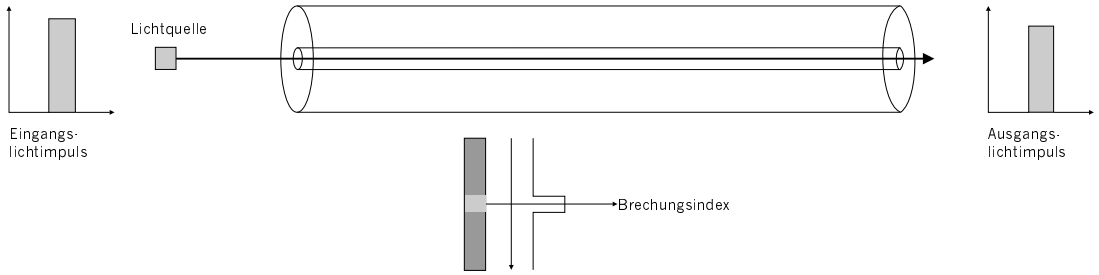


Abbildung 21: Monomodefaser mit Stufenprofil

Neben der Modendispersion gibt es noch die chromatische Dispersion, welche daher rührt, dass sich Lichtwellen unterschiedlicher Wellenlängen[7] auch mit unterschiedlichen Geschwindigkeiten durch das zu durchquerende Medium bewegen. Um die chromatische Dispersion zu eliminieren, verwendet man kohärentes Licht, also Licht von nur einer Wellenlänge. Dieses läßt sich mit Laserdioden erzeugen.
Wie wir gesehen haben, nimmt die Amplitude des Signals ab, wenn es den Leiter durchquert. Dies geht auf die sog. Dämpfung des LWL's zurück, welche sich je nach Wellenlänge ändert. Das Bild unten zeigt die Dämpfung einer Glasfaser in Abhängigkeit zur Wellenlänge des verwendeten Lichts. Wie man sieht, wird bei etwa 1400 nm (nanometer) sehr viel Licht absorbiert. Das liegt an den im Glas eingeschlossenen HO-Ionen, welche auf eben diese Wellenlänge ansprechen. Zum anderen werden Moden, die in einem ungünstigen Winkel auf die Grenzfläche der Substrate auftreffen, nicht total reflektiert. Ein Teil des Lichts kann so in den Mantel entweichen. Ein anderes Problem stellen die Verbindungs- und Anschlusstücke der Faser dar. Hier kann es an den Grenzflächen der Koppelungen ebenfalls zu Reflexionen kommen, welche dann in Gegenrichtung

[7] Also Licht unterschiedlicher Farbe.

in der Faser laufen. Das Bild unten zeigt die drei Wellenlängen, innerhalb welcher Glasfasern genutzt werden. Während die Dämpfung nur die Amplitude eines Signals schwächt, begrenzt die Modendispersion außerdem noch die mögliche Bandbreite des LWL. Wenn die Impulse zu eng hintereinander gesendet werden, kann es dazu kommen, dass eine Gruppe von Impulsen zu einem einzigen unförmigen Impuls "verschmiert".

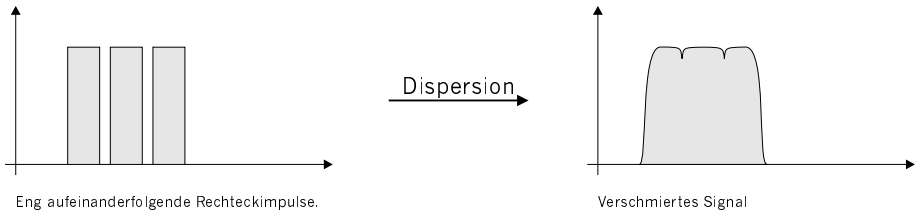


Abbildung 22: Verschmieren eines Signals, aufgrund Dispersion.

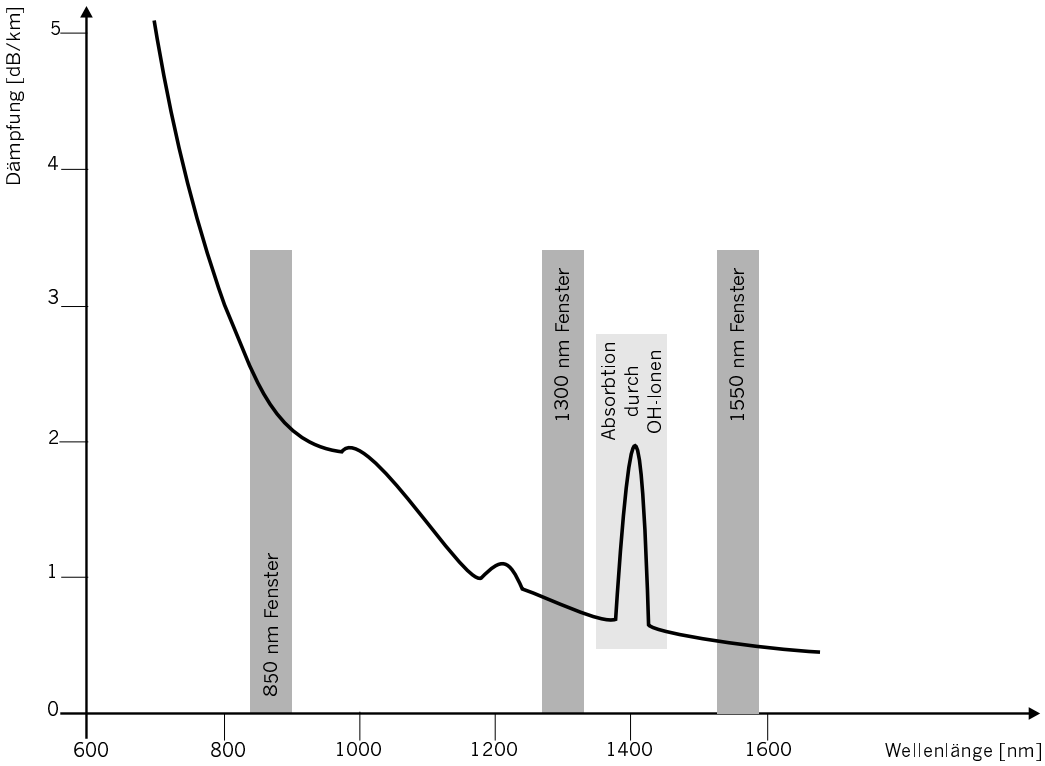


Abbildung 23: Dämpfung in Abhängigkeit zur Wellenlänge
[12]

1.10 Wavelength Division Multiplexing

Zusätzlich zu den Vorteilen der Glasfaser gegenüber Kupferkabeln, dass die Reichweite höher ist, sie störunempfindlich sind und sie keine zum Ausspähen von Daten nötige Emissionen abgeben, gibt es einen weiteren Vorteil. Ähnlich wie beim Frequenz-Multiplexen (FDM) auf Kupferkabeln ist es möglich, mehrere Signale gleichzeitig durch die Faser zu übertragen. Diese Technik trägt

den Namen *Wavelength Division Multiplexing* (WDM), zu deutsch. Im Gegensatz zum FDM wird hierzu jedoch keine Trägerwelle benötigt, sondern die Signale werden direkt nebeneinander durch die Faser geschickt. Dies funktioniert, da die Signale mit unterschiedlichen Wellenlängen innerhalb eines Übertragungsfensters (vgl. Abb. 23) übertragen werden. Die Wellenlängen haben dabei im Frequenzbereich soviel Abstand zueinander, dass sie nicht miteinander interferieren. Ein einziger LWL wird somit zu n virtuellen LWL'n. Die bei einer einfachen Verbindung benötigten Komponenten sind elektro-optische Transmitter, welche das ankommende elektrische Signal in ein optisches umwandeln. Ausserdem werden optische Multiplexer benötigt, welche die verschiedenen eingehenden Lichtsignale zu einem einzigen zusammenfassen und in die Faser einspeisen. Gegebenenfalls benötigt man einen optischen Verstärker, um die mögliche Übertragungsdistanz zu erhöhen, dann einen optischen Demultiplexer, und Empfängern, welche die optischen Signale wieder in elektrische umsetzt. Diese einfache Konfiguration stellt folgende Abbildung dar.

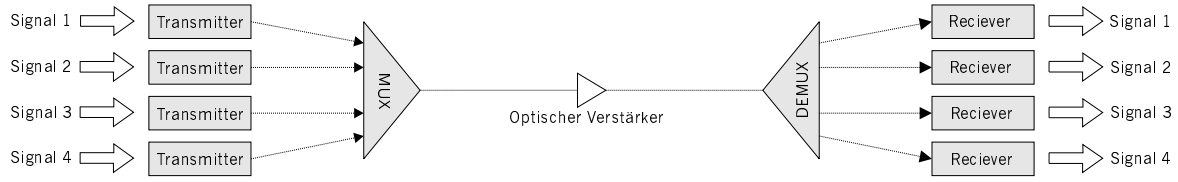


Abbildung 24: Komponenten einer einfachen WDM Konfiguration

Zur Zeit auf dem Markt erhältliche optische Multiplexer stellen bereits 80 Kanäle zur Verfügung (Wavestar von Lucent). Man spricht dabei von *Dense Wavelength Division Multiplexing*. Im Labor wurde bereits das Multiplexen von 400 Kanälen erreicht (Lucent). Man geht davon aus, dass 1000 Kanäle technisch machbar sind. Das heißt, die Bandbreite des LWL im Labor, mit standardmäßig 2,5 Gbit/s Übertragungskapazität vervielfacht seine mögliche Bandbreite somit auf 1000 Gbit/s. Es sind jedoch auch komplexere Netzwerkstrukturen als die eines einfachen Pfades möglich. So gibt es z.B. neben optischen Add/Drop Multiplexern sogar optische Switches, welche ähnlich ihrer elektronischen Vorbilder verschiedene Wellenlängen an verschiedene Ports umleiten können. Da all die optischen Komponenten wirklich nur optisch funktionieren, völlig ohne elektrische Energie, tun sie dies gleichermaßen in Hin- und Rückrichtung. D.h. z.B. ein Multiplexer ist zugleich auch ein Demultiplexer. Ebenso funktioniert ein optischer Verstärker, der in der Regel aus mit Erbium dotiertem Glas besteht (Erbium Doped Fiber Amplifier - EDFA), ebenfalls bidirektional. Dies ermöglicht sogar, Daten im Vollduplex, d.h. in beide Richtungen gleichzeitig, zu übertragen. Zu den Verstärkern ist noch zu sagen, dass sie das ankommende Signal natürlich nur in der Amplitude verändern. D.h. ein durch Dispersion verschmiertes Signal ist nach der Verstärkung immer noch verschmiert. Ab einer gewissen Distanz hilft nur noch das Zurückwandeln in ein elektrisches Signal, dies zu restaurieren und es verstärkt wieder optisch weiter zu schicken. Es gibt sogar optische Cross - Konnektoren (OXC, Optical Cross Connect), welche das Signal im Frequenzbereich verschieben.[8] Dies kann z.B. für das Routing eines Signals eingesetzt werden.
Mit Hilfe der genannten Komponenten sind grundsätzlich zwei Netzwerktypen möglich: Fixe und dynamische Topologien. Bei der fixen Topologie ist das Netzwerk so aufgebaut, dass sog. Lichtpfade fest im Netzwerk eingerichtet werden. Um eine Verbindung zur gewünschten Endstelle aufzubauen, muss man hier die richtige Wellenlänge für das Signal wählen.

Die dynamischen Variante des Netzwerkes unterscheidet sich im Wesentlichen kaum von der statischen. Der Unterschied ist, dass einige Komponenten "ferngesteuert" werden können. D.h.

[8] Also in eine andere Farbe umwandeln.

sie können von einer zentralen Stelle aus gesteuert werden. Es können einerseits die Add/Drop-Multiplexer so angesteuert werden, dass sie die eingehenden Wellenlängen an andere Ports ausgeben. Andererseits können die Cross-Connectoren die Wellenlängen in die gewünschte Wellenlänge umwandeln, damit dieses Signal am nächsten Add/Drop-Multiplexer an den korrekten Port weitergeleitet wird. Das Verändern des Ausgabeports kann z.B. durch eine Winkeländerung an einem Spiegel geschehen.
Das Finden der besten Route durch das Netzwerk ist NP-vollständig. Dies entspricht dem färben eines Graphen (graph coloring problem, vgl. Vorlesung Diskrete Strukturen 1).
Abschließend sei noch erwähnt, dass WDM es natürlich erlaubt, verschiedene Übertragungsprotokolle gleichzeitig zu übertragen, da das ganze System nur auf der optischen Ebene (Photonic Layer) arbeitet.

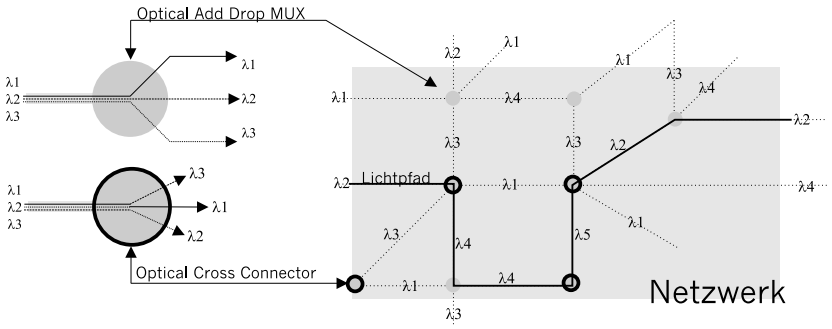


Abbildung 25: Statische/Dynamische Netzwerktopologie

2 ATM - Die Technik des B-ISDN

2.1 Einführung

Innerhalb weniger Jahre hat sich die Computertechnik rasant entwickelt. Während bis vor wenigen Jahren der einzelne Personal Computer im Vordergrund stand und Netzwerke vorwiegend von großen Firmen im LAN-Bereich genutzt wurden, steht heutzutage die globale Kommunikation im Vordergrund. Immer neue Anforderungen an die Daten- und Telekommunikation ließen alsbald auch die klassischen Netzwerk-Techniken an ihre Grenzen stoßen. Als ideale Technik zur Bewältigung heutiger Kommunikationsprobleme wurde in einer Kooperation zwischen Forschung und Telekommunikationsindustrie der **Asynchrone Transfer-Modus** (ATM) entwickelt. Im folgenden soll ein Überblick über die Eigenschaften und Anwendungsgebiete dieser Technik gegeben werden.

2.2 Eigenschaften von ATM

2.2.1 Übertragungsprinzip

ATM gehört zur Klasse der verbindungsorientierten Übertragungsverfahren, was bedeutet, daß vor jeder Übertragung eine Verbindung aufgebaut und gesichert sein muß. Die eigentliche Übertragung basiert darauf, daß verschiedenste ankommende Datenströme in Übertragungspaketen zu je 53 Byte (5 Byte ATM-Header und 48 Byte Nutzdaten), sogenannten ATM-Zellen transformiert werden. Das Vereinigen der verschiedenen Zellströme zu einem Gesamtstrom nennt man asynchrones Zeit-Multiplexing.

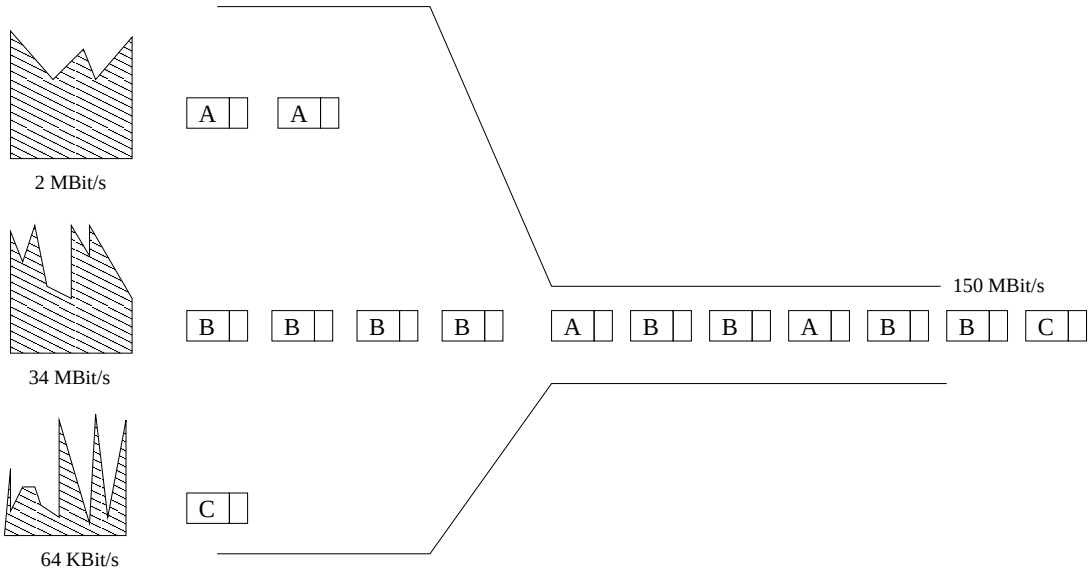


Abbildung 26: ATM-Prinzip des asynchronen Zeit-Multiplexings

Die Zellgröße von 53 Byte ist ein Kompromiß zwischen Europa und den USA. Die Vereinigten Staaten wollten eine Länge von 64 Byte durchsetzen, da aufgrund des geringen Headers große Datenmengen ökonomisch übertragen werden konnten. Da der reine Datenverkehr in Europa jedoch noch nicht die Bedeutung wie in Amerika hatte, legten die Europäer mehr Wert auf kürzere Zellen für die Übertragung analoger Sprachsignale und schlugen 32 Byte vor. Daher

einigte man sich auf 53 Byte, das einerseits kurz genug ist, um analoge Sprachsignale bei hohen Übertragungsraten zu übermitteln, und andererseits aufgrund des nur 5 Byte großen Headers die effiziente Übertragung reiner Datenströme ermöglicht. Die ATM-Zellen werden dann mittels sogenannter ATM-Switches und Crossconnects weitergeleitet. ATM-Zellen werden in sogenannten virtuellen Kanälen übertragen. Das bedeutet, aus Sicht des Senders besteht die Verbindung aus **einer** logischen Verbindung, während sie physikalisch über mehrere Knotenpunkte läuft. Virtuelle Kanäle sind prinzipiell unidirektional, deshalb werden für eine Verbindung jeweils virtuelle Kanalpaare geöffnet. Laufen mehrere virtuelle Kanäle für einen gemeinsamen Übertragungsabschnitt über dieselbe Leitung, so werden sie für diese Abschnitte zu virtuellen Kanalbündeln, sogenannten virtuellen Pfaden gebündelt.

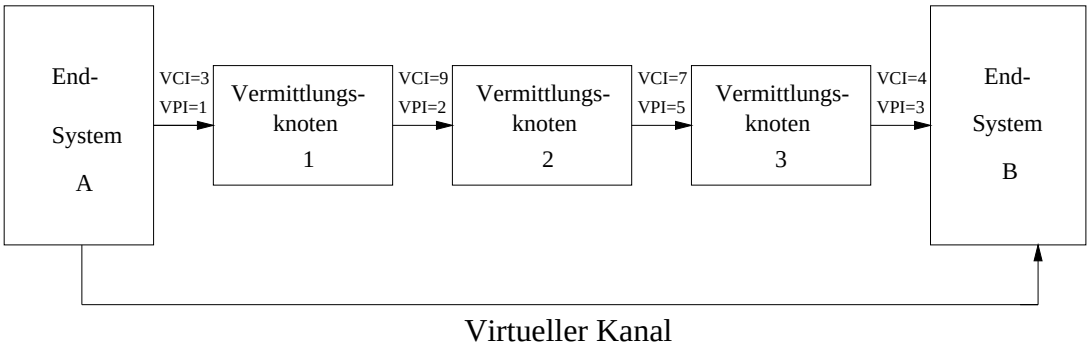


Abbildung 27: Prinzip des virtuellen Kanals

Der Header jeder ATM-Zelle enthält Kanalinformationen (VCI - Virtual Channel Identifier) und Pfadinformationen (VPI - Virtual Path Identifier), die die jeweiligen Switches und Crossconnects auswerten. Virtuelle Kanäle, die innerhalb eines Übertragungsabschnittes zu einem virtuellen Pfad gebündelt werden, haben für diesen Zeitraum dieselbe VPI-Nummer . Da alle Zellen einer ATM-Verbindung die gleiche VCI/VPI-Nummer haben, kann jede Zelle durch dieses Zahlenpaar eindeutig einer Verbindung zugeordnet werden. In einem Crossconnect werden alle ankommenden virtuellen Pfade umgeleitet, während die virtuellen Kanalnummern unverändert bleiben. In einem Switch werden sowohl die virtuellen Pfadnummern als auch die virtuellen Kanalnummern verändert. Abbildung 28 zeigt ein Weiterleiten durch Switches und Crossconnects.

2.3 Multiplexen mit SONET/SDH

SONET (Synchronous Optical NETwork) ist ein optisches Übertragungsystem, das seit 1989 durch die CCITT (heutige ITU) standardisiert ist. Neben diesem Standard existieren eine Reihe von Empfehlungen der CCITT, die als SDH (Synchronous Digital Hierarchy) bezeichnet werden. SDH und SONET sind in weiten Teilen ähnlich, so daß auch immer SDH gemeint ist, wenn im folgenden vom SONET die Rede ist. Aufgabe von SONET ist das Multiplexen von Datenströmen, hier Teilbitströme genannt. SONET ordnet der Bandbreite eines Glasfaserkabels einem Kanal mittels Zeitschlitzen Unterkanälen zu. Anschließend werden die Bits synchron in exakten Intervallen von einem Mastertakt ($\sim$ 1GHz) gesteuert, übertragen. Das SONET-System, bestehend aus über Glasfaser verbundenen Vermittlern, Multiplexern und Repeatern, könnte nun folgendermaßen arbeiten: Zunächst werden die ankommenden Teilbitströme (T1, T3) auf die SONET-Grundrate von 51.85 Mbps umgewandelt. Eine solche SONET-Grundrate wird STS-1 genannt (Synchronous Transport Signal-1). Anschließend werden immer drei STS-1-Ströme in einem Multiplexer zu einem STS-3 Teilbitstrom mit 155.52 Mbps gemultiplext. Danach werden

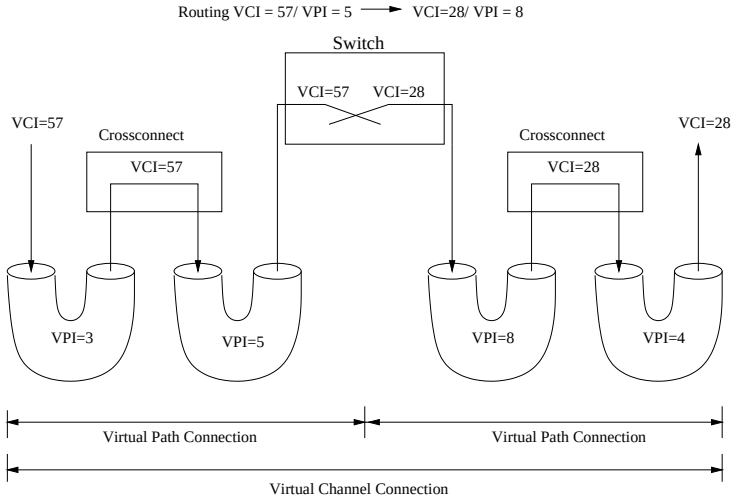


Abbildung 28: Weiterleitung in einer ATM-Verbindung

wieder mehrere solcher STS-3-Teilbitströme gemultiplext. Durch weiteres Multiplexing entsteht dann der endgültige Datenstrom STS-n. Das Signal wird nun durch eine feste mathematische Funktion durcheinander gewürfelt (Scrambling), um eine Störung im Takt durch lange Null- oder Einserreihen zu vermeiden. Der Elektrooptische Konverter wandelt schließlich das elektrische Signal in ein optisches Signal um. Der optische Träger des Signals wird OC-n (Optical Carrier) genannt. Er entspricht, abgesehen von den Scrambling-Bits, STS-n. Abbildung 29 zeigt schematisch einen SONET-Multiplexvorgang mit STS-12.

SONET basiert auf byte-weisem Multiplexing. Das bedeutet, der Multiplexer liest zunächst der Reihe nach ein Byte von jedem Teilbitstrom, multiplext und beginnt dann wieder von vorne. Es sind mittlerweile Datenraten von STS-1 (51.85 Mbps) bis zu STS-192 ($\sim 10 Gbps$) definiert. Hier unterscheiden sich die SDH-Bezeichnungen von den SONET-Raten, da SDH-Raten erst mit STS-3 beginnen. Somit liegt die maximale Rate bei STM-48. Die Einteilung der verschiedenen SONET/SDH-Datenraten nennt man Hierarchien. Durch das Multiplexen können mehr Daten übertragen werden, als die Summe der Spitzenframes der einzelnen Verbindungen erlaubt [59].

2.3.1 Verbindungsaufbau

Wie bereits oben erwähnt, muß beim Asynchronen Transfermodus die Verbindung vor der Übertragung gesichert sein. Dazu wird zu Beginn jeder einzelnen ATM-Verbindung ein virtueller Kanal aufgebaut. Dazu übermittelt der Sender über den well-known Kanal VCI=5/VPI=0 eine Anfrage (**SETUP**) an das ATM-Netz. Das Netz antwortet daraufhin mit einer Bestätigung der Anfrage (**CALL PROCEEDING**). Im Erfolgsfall meldet das Netz daraufhin die Akzeptanz der Anfrage (**CONNECT**), die der Sender mit einem **CONNECT ACK** beantwortet. Die einzelnen ATM-Schaltelemente verwenden dieselbe Prozedur bis hin zum Empfänger. Wurde überall das **CONNECT ACK** gesendet, so steht die Verbindung. Soll eine Verbindung abgebrochen werden, so wird dasselbe Procedere mit den Signalen **RELEASE** und **RELEASE COMPLETE** verwendet. Abbildung 30 zeigt schematisch einen Verbindungsauf- und abbau .

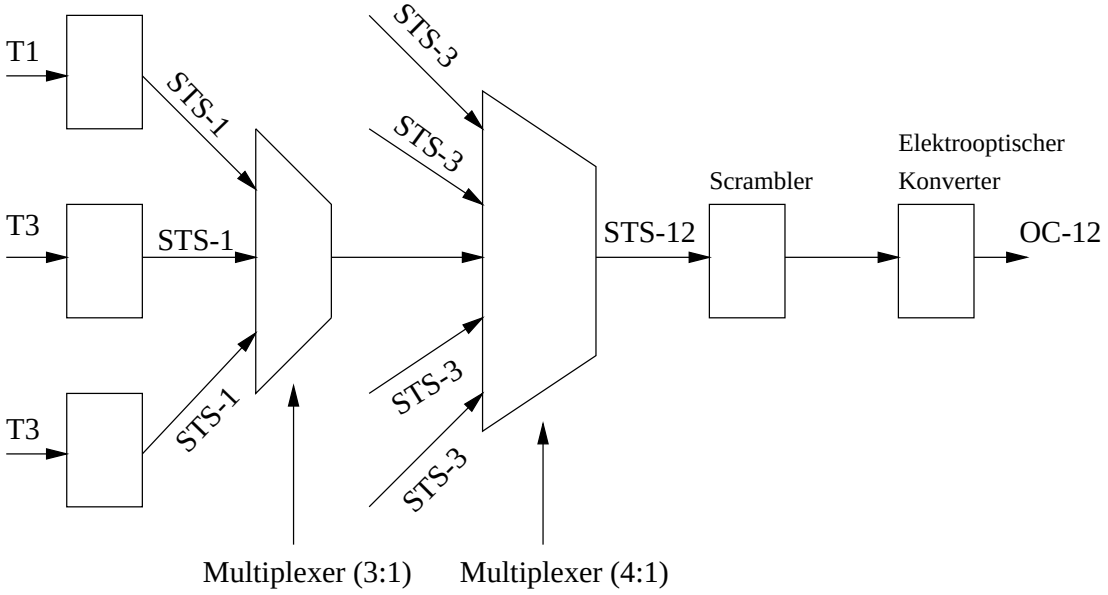


Abbildung 29: Multiplexvorgang mit SONET

2.3.2 Verkehrskontrakt

Bei jedem Verbindungsaufbau wird ein sogenannter Verkehrskontrakt zwischen beiden Partnern vereinbart, der nach [135] aus drei Teilen besteht:

- Art des angebotenen Verkehrs
- Dienstvereinbarungen
- Erfüllung der Anforderungen

Als Kompromiß zwischen den Anforderungen des Senders und den zur Verfügung stehenden Ressourcen des Netzes wird dabei die Dienstgüte (Quality of Service - QoS) der Verbindung durch Verkehrsparameter ausgehandelt. Tabelle 7 zeigt die einzelnen Parameter und ihre Bedeutung [135].

Es ist dabei wichtig zu erwähnen, daß sobald ein geforderter Parameter vom Netz nicht erfüllt werden kann, die Verbindung nicht mit niedrigeren QoS-Parametern aufgebaut, sondern verweigert wird.

2.3.3 Dienstklassen

Um die Übertragung verschiedenster Arten von Datenströmen zu gewährleisten, wurden vom ATM-Forum (siehe Kapitel 2.7) fünf Dienstklassen definiert, die auf die einzelnen Datenströme zugeschnitten sind [80]:

- Constant Bit Rate - CBR

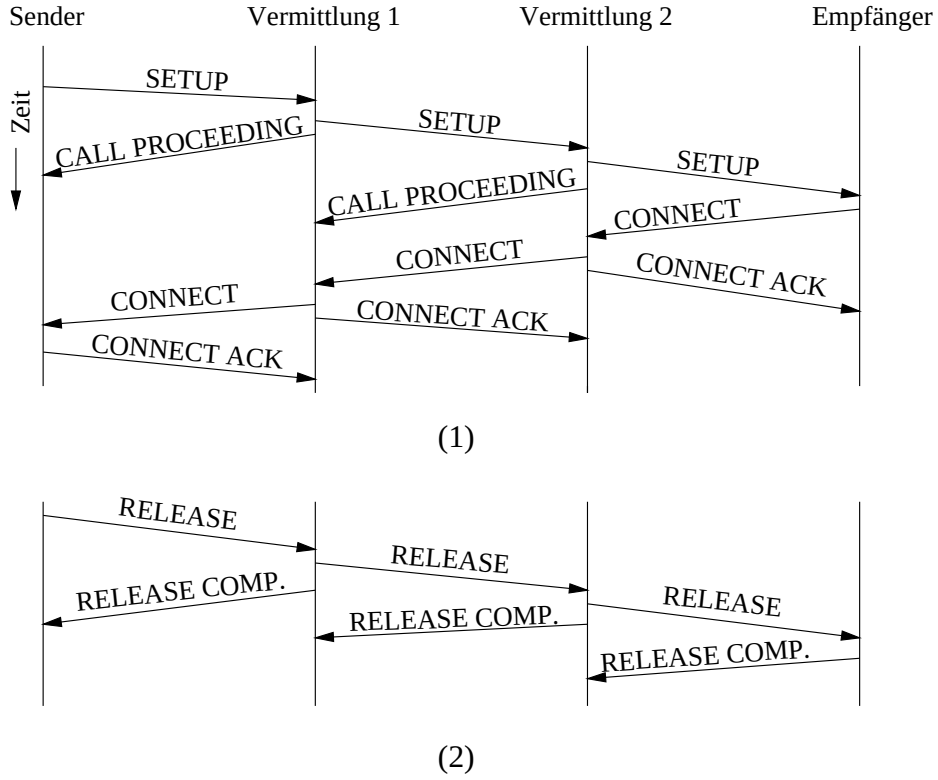


Abbildung 30: Verbindungsaufbau (1) und Verbindungsabbau (2) in ATM-Netzen

- Real-Time Variable Bit Rate - rt-VBR
- Non-Real-Time Variable Bit Rate - nrt-VBR
- Unspecified Bit Rate - UBR
- Available Bit Rate - ABR

CBR-Klasse

Diese Dienstklasse ist für die Übertragung von Datenströmen mit konstanter Bitrate konzipiert, die eine feste Bandbreite benötigen. Die charakteristischen Verkehrsparameter sind hierbei PCR (gibt die Höhe der konstanten Datenrate an), sowie CDV und CTD. Mit Hilfe der CBR-Klasse werden Real-Time-Applikationen sowie unkomprimierte Video- und Audiotransfers übertragen.

rt-VBR-Klasse

Die rt-VBR-Klasse wird für Übertragungen von Real-Time Applikationen genutzt, die mit variabler Zellrate senden. Dies ist zum Beispiel der Fall bei komprimierten Video- bzw. Audioübertragungen (MPEG). Derartige Datenströme werden durch die durchschnittliche und die maximale Zellrate (SCR und PCR) sowie durch MBR (Maximum Burst Ratio), das heißt die Anzahl von Zellen, die mit PCR übertragen werden kann, charakterisiert.

nrt-VBR-Klasse

Parameter	**Akronym**	**Bedeutung**
Peak Cell Rate	PCR	Maximale Zellrate
Sustainable Cell Rate	SCR	Langfristiger Durchschnitt der Zellrate
Minimum Cell Rate	MCR	Die als Minimum akzeptierte Zellrate
Cell Delay Variation Tolerance	CDVT	Toleranz für die Zellverzögerungsschwankungen
Cell Loss Ratio	CLR	Zellverlustrate
Cell Transfer Delay	CTD	Dauer der Verzögerung (Mittel und Maximum)
Cell Delay Variation	CDV	Abweichung in den Zustellzeiten von Zellen
Cell Error Rate	CER	Fehlerfrei zugestellter Bruchteil von Zellen
Cell Misinsertion Rate	CMR	Der falsche zugestellte Bruchteil von Zellen

Tabelle 7: Quality of Service Verkehrsparameter

Diese Dienstkategorie wird für Datenströme mit variabler Zellrate benötigt, für die eine zeitgerechte Zustellung zwar wichtig ist, aber eine bestimmte Abweichung von der Anwendung toleriert wird (keine Echtzeit-Anforderungen). nrt-VBR ist wie rt-VBR charakterisiert durch PCR, SCR und MBR. Bei der Übertragung durch diese Klasse wird eine geringe Zellverlustrate (CLR), aber keinerlei maximale Verzögerungszeiten (maxCTD) vereinbart. Beispiel für eine Anwendung wäre multimediales Email, das vor dem Anzeigen zunächst auf die Festplatte des Benutzers gespeichert wird, um eventuelle Verzögerungen in den Zellzustellzeiten zu verhindern.

UBR-Klasse

Diese Service-Klasse ist für den klassischen Datenverkehr ohne Echtzeit-Anforderungen konzipiert. Es werden keine QoS-Parameter außer einer PCR vereinbart, so daß die Übertragungskontrolle in höheren Schichten erfolgen muß. UBR gibt auch keine Bestätigung im Falle von Überlastung. Tritt Überlastung im Netz auf, so werden die UBR-Zellen ohne Warnung an den Sender verworfen. Die Übertragungskontrolle muß deshalb bei UBR in den höheren Schichten realisiert werden. Typische Anwendungen von UBR sind Email und Dateitransfer.

ABR-Klasse

Die ABR-Klasse überträgt ebenfalls Datenströme ohne Echtzeit-Anforderungen. Im Gegensatz zu allen anderen Klassen erhält jedoch der Sender vom Netz laufend Informationen über die aktuelle Netzlastsituation, sowie die Aufforderung, bei Überlast seine Senderate zu verlangsamen. Dadurch ist die Zellverlustrate bei dieser Art der Übertragung gering. Diese Klasse ist charakterisiert durch die PCR, sowie eine minimale Zellrate (MCR), die das Netz ständig gewährleisten muß. Werden also in einer Verbindung 3 Mbps als MCR und 8 Mbps als PCR vereinbart, so **muß** das Netz ständig 3 Mbps gewährleisten, während die 8 Mbps ohne Garantie nach Möglichkeit bereitgestellt werden. Anwendungen für ABR sind Surfen im Web oder Datenaustausch zwischen lokalen Netzwerken.

Tabelle 8 zeigt nochmal einen Überblick:

Leistungsmerkmal	CBR	rt-VBR	nrt-VBR	ABR	UBR
Garantierte Bandbreite	Ja	Ja	Ja	Optional	Nein
Geeignet für Echtzeitverkehr	Ja	Ja	Nein	Nein	Nein
Geeignet für Umgebungen mit CDV	Nein	Nein	Ja	Ja	Ja
Bestätigung im Fall von Überlastung	Nein	Nein	Nein	Ja	Nein

Tabelle 8: Merkmale der ATM-Dienstklassen

2.4 Das ATM-Referenzmodell

1987 wählte die CCITT (Comitté Consultatif International Télégraphique et Téléphonique) (vgl. Kapitel 2.7), die heutige ITU-T (International Telecommunication Union - Telecommunication Standardization Sector) den Asynchronen Tansfermodus als die Technik zur Realisierung des Breitband-ISDN. Dazu wurde ein Referenzmodell ausgearbeitet, daß sich vom ISO/OSI-Referenzmodell unterscheidet. Abbildung 31 zeigt das Referenzmodell:

Das Schichtenmodell ist im Gegensatz zu früheren Modellen nicht mehr zweidimensional, sondern dreidimensional. Es ist unterteilt in Benutzer- und Steuerebene (User Plane, Control Plane), Schichtenmanagement (Layer Management) und Ebenenmanagement (Plane Management). Das Modell läßt sich mit dem ISO/OSI-Modell nur schwer in Einklang bringen, da beispielsweise keine direkte Zuordnung zur Vermittlungs- oder Transportschicht möglich ist, bzw. zum Teil die gleichen Funktionen in den verschiedenen Modellen von unterschiedlichen Schichten erledigt werden.

Das Referenzmodell besteht aus drei Schichten - den oberen Benutzer-Schichten, der ATM- und ATM-Anpassungschicht (ATM - Adaption Layer - AAL) und der physikalischen Schicht.

Die ATM-Schicht definiert das Zellenlayout, die Bedeutung der Felder im Zellheader, das Einrichten und Abbrechen virtueller Verbindungen, sowie die Überlaststeuerung.

Die ATM-Adaptionsschicht ist dagegen dafür zuständig, die zu versendenden Pakete in ATM-Zellen zu zerlegen, respektive ankommende Zellen wieder zu den ursprünglichen Paketen zusammenzusetzen. Sie ist unterteilt in die Konvergenzteilschicht (Convergence Sublayer), die die Standardschnittstelle bildet, und die Segmentierungs- und Zusammensetzungsschicht (Segmentation- and Reassembly Sublayer), die dann die tatsächliche Zerlegung bzw. die erneute Zusammensetzung realisiert.

Die physikalische Schicht hat die Aufgabe der tatsächlichen Übertragung auf physikalischer Ebene. Wichtig ist dabei, daß ATM über die verschiedensten Medien übertragen werden kann (Kupferkabel, Glasfaser), also medienunabhängig ausgelegt ist [135]. Wie bereits erwähnt, läßt sich das ATM-Referenzmodell nicht mit dem ISO/OSI-Referenzmodell in Einklang bringen. Die folgende Tabelle ist daher nur der Versuch, die einzelnen Schichten zur Orientierung ungefähr in das bekannte Modell einzuordnen:

2.4.1 Managementebenen

Die Benutzerebene (User Plane) übernimmt die Benutzerfunktion. Dazu gehören unter anderem der Datentransport, die Steuerung des Datenflußes, und die Fehlerkorrektur. Die Steuerebene

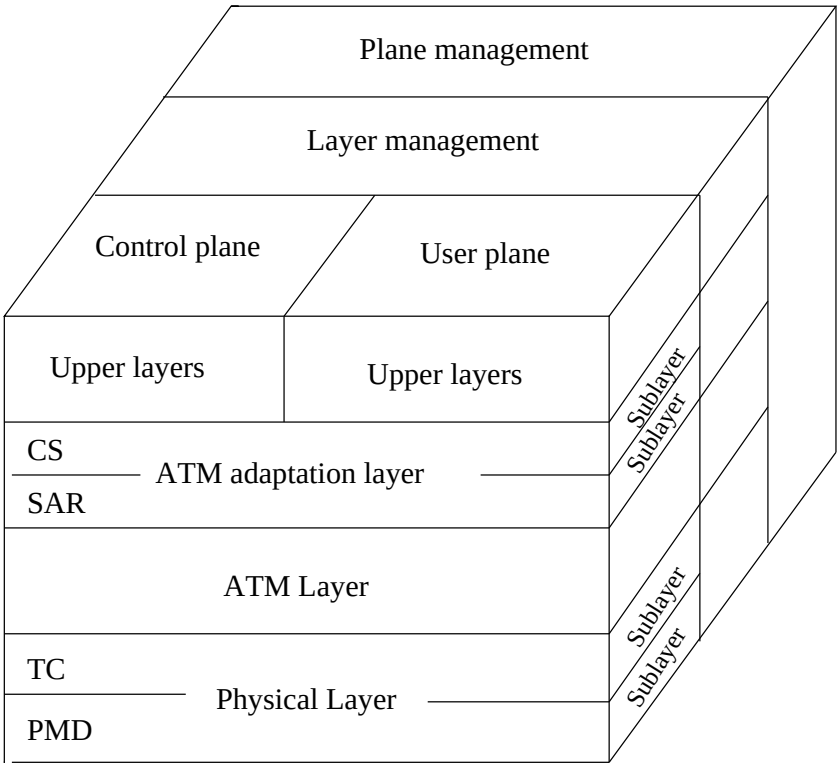


Abbildung 31: ATM-Referenzmodell

(Control Plane) betrifft Verbindungsmanagement, die Signalisierung und verschiedene Kontrollfunktionen. Das Ebenenmanagement (Plane Management) regelt die Koordination zwischen den einzelnen Schichten und Ebenen. Diese Ebene ist selbst **nicht** unterteilt. Das Schichtenmanagement (Layer Management) ist selbst in Schichten unterteilt und bewältigt das Management der jeweiligen Protokolle auf den einzelnen Schichten.

2.4.2 Die ATM-Adaptionsschicht

Die ATM-Adaptionsschicht (ATM Adaption Layer - AAL), die unterhalb der höheren Schichten liegt, hat einerseits zum Ziel, "Dienste für Anwendungsprogramme bereitzustellen und andererseits sie vor der Aufteilung von Daten in Zellen an der Quelle und das erneute Ziel abzuschirmen." [135]. Dabei muß die AAL-Schicht die verschiedenen Arten von Datenströmen berücksichtigen. Deshalb wurde die AAL-Schicht von der ITU zunächst in drei Dienst-Achsen eingeteilt:

1. Echtzeitdienste und Dienste ohne Echtzeit
2. Dienste mit konstanter und variabler Bitrate

OSI-Schicht	ATM-Schicht	ATM-Teilschicht	Funktionalität
3 und 4	AAL	CS	Bereitstellung der Standardschnittstelle
		SAR	Segmentierung und erneute Zusammensetzung
2 und 3	ATM		Flußsteuerung Erzeugung/Extraktion des Zellenheaders Management des virt. Pfades/der Verbindung Multiplexen/Demultiplexen der Zellen
2		TC	Entkoppeln der Zellenrate Erzeugung/Verifikation der Header-Prüfsumme Erzeugung der Zellen Ein-/Auspacken der Zellen in/aus dem Umschlag Erzeugung von Frames
	Physisch		
1		PMD	Bitzeitgabe Physischer Netzzugriff

Tabelle 9: Funktionen der ATM-Schichten

3. verbindungsorientierte und verbindungslose Dienste

Dieses Konzept ist jedoch seit der Standardisierung von UNI 4.0 überholt. Heute wird zwischen den in Kapitel 2.3.3 vorgestellten Typen unterschieden.

Die ITU unterteilte die AAL-Schichten in vier Unterklassen. Da sich AAL-Typ 3 und AAL-Typ 4 sehr ähneln, wurden sie zu einem Typ zusammengefaßt. Da einige der vier Typen einen gewaltigen Protokoll-Overhead hatten, lehnte die Industrie die Definitionen der ITU ab und entwickelte mit dem SEAL-Protokoll (Simple Efficient Adaption Layer) den AAL-Typ 5.

2.4.3 die AAL-Teilschichten

Generell ist die AAL-Schicht in zwei Teile strukturiert. Den einen Teil bildet die Konvergenzteilschicht (CS), die ihrerseits in einen dienstspezifischen Teil (Specific Service Convergence Sublayer - SSCS) und einen allgemeinen Teil (Common Part Convergence Sublayer - CPCS) gegliedert ist, den zweiten Teil die Segmentierungs- und Zusammensetzungsschicht (SAR).

Ein Datenblock, den eine Teilschicht von einer übergeordneten Schicht erhält, nennt man Service Data Unit (SDU). Versieht nun die Teilschicht den Block mit einem Header und einem Trailer, so nennt man diesen Block anschließend Protocol Data Unit (PDU). Generell erkennt die Konvergenzteilschicht verlorene und falsch eingefügte Zellen. Außerdem teilt die CS die Eingangsdaten in Teile zu 46 oder 47 Byte auf und reicht sie an die SAR weiter bzw. setzt auf der anderen Seite die von der SAR kommenden Teile wieder zusammen. Die SAR-Schicht versieht die von der Konvergenzteilschicht kommenden Einheiten mit einem ein Byte großen SAR-PDU-Header und reicht sie an die ATM-Schicht weiter. Analog dazu entfernt sie die ein Byte großen Header von ankommenden Zellen und gibt die Zellen an die CS weiter.

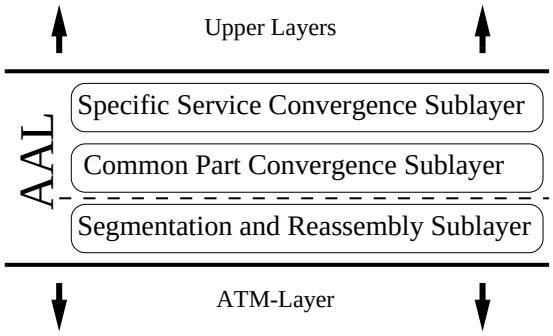


Abbildung 32: Struktur der AAL-Schicht

2.4.4 Unterschiede zwischen den AAL-Typen

AAL-Typ 1 wurde konzipiert zur Übertragung von verbindungsoriertiertem Echtzeitdatenverkehr mit fester Bitrate. Typische Anwendungen sind beispielsweise unkomprimierte Audio- und Videoübertragung. AAL 1 unterstützt Zellpufferung und Zeit-Synchronisation, so daß sichergestellt ist, daß die Zellen mit derselben Frequenz gesendet und empfangen werden. AAL 1 unterstützt bit-orientierten "Unstructured Data Transfer-Mode" (UDT) und den byte-orientierten "Structured Data Transfer-Mode" (SDT), der z.B. für das Übertragen von 8-bit Samples verwendet wird.

AAL-Typ 2 ist ausgelegt auf verbindungsorientierten Echtzeitdatenverkehr mit variabler Bitrate, wie er z.B. bei komprimiertem Audio und Video auftritt. Da die Länge der einzelnen Rahmen sehr unterschiedlich sein kann, hat AAL 2 im Header ein sogenanntes IT-Feld, das kennzeichnet, ob eine Zelle nun der Anfang, das Ende oder in der Mitte eines Rahmens ist. Ist innerhalb eines Frames eine Zelle verlorengegangen, muß der gesamte Frame neu übertragen werden. Die Markierung dient daher der gezielten Strukturierung der Zellverwerfung im Falle einer Netzüberlastung. Da AAL 2 zusätzlich zum Zellheader noch einen 2 Byte großen Trailer anlegt, ist der Nutzdatenanteil pro Zelle maximal 45 Bytes.

AAL-Typ 3/4 wird für zeitunabhängige Datenpakete variabler Länge verwendet (verbindungsorientiert und verbindungslos). Dabei gibt es verschiedene Modi:

- **Streaming-Modus**:

  Im Streaming-Modus werden Datengrenzen nicht eingehalten und Datenpakete weitergegeben, obwohl eine Nachricht noch nicht vollständig ist.

- **Message-Modus**:

  Dieser Modus hält die Datengrenzen ein. Die Nachricht wird erst weitergegeben, wenn die vollständige AAL-SDU erhalten wurde.

- **garantierte/unzuverlässige Übertragung**:

  Ist der garantierte Modus aktiviert (z.B. durch das Service Specific Connection-Oriented Protocol - SSCOP der SAR-Schicht), so werden die jeweiligen fehlerhaften oder fehlenden Zellen erneut übertragen.

- **Point-to-Point/Point-to-Multipoint Verbindung**:

  Bei AAL 3/4 können mehrere Sitzungen vom selben Host aus über den gleichen virtuellen Kanal gemultiplext werden und anschließend am Ziel getrennt werden (z.B. Remote-Logins). Die Point-to-Multipoint Verbindungen werden durch die CPCS bereitgestellt.

Die Regelung der Flußkontrolle (Flow Control) geschieht durch das EFCI-Bit (Expilicit Forward Congestion Indicator) im PTI-Feld des ATM-Headers, das, wenn es durch einen überlasteten Switch gesetzt wird, das Endsystem dazu veranlaßt, protokollmäßig zu reagieren (beispielsweise durch Herabsetzen der Zellenrate).

AAL-Typ 5 Wie oben erwähnt wurde AAL 5 von der Industrie entwickelt. Es ähnelt den Definitionen von AAL 3/4, jedoch wurde versucht, den Protokoll-Overhead und damit die Ineffizienz zu vermeiden. Außerdem war damals AAL 3/4 noch nicht ausreichend spezifiziert. Genau wie AAL 3/4 dient AAL 5 zur Übermittlung von verbindungsorientierten und verbindungslosen Datenpaketen variabler Länge und unterstützt ebenfalls sowohl den Streaming- als auch den Message-Modus (garantiert oder unzuverlässig). Die Vereinfachung liegt darin, daß man viele Dienste von der SAR-Schicht in die Convergence Sublayer (SSCS und CPCS) verlegt hat. So wurde zum Beispiel das Multiplexen für Point-to-Multipoint Verbindungen in die SSCS verlegt.

AAL 5 wird heutzutage aufgrund seiner Praxisrelevanz und Effizienz am häufigsten für den allgemeinen Datenverkehr verwendet. Da es ein Typ ohne großen Protokoll-Overhead ist, gibt es bei AAL-Typ 5 keine Flußkontrolle. Zusatzfunktion wie Flußkontrolle, Fehlerkorrektur etc. müssen deshalb in höheren Schichten realisiert werden. Neben AAL 5 zählt wohl AAL 1 im CBR Real-Time Bereich zu den häufigsten Protokollen, obwohl auch immer häufiger komprimiertes Video und Audio über AAL 5 übertragen wird.

2.4.5 Die ATM-Schicht

Die Hauptaufgabe der ATM-Schicht ist die transparente Übertragung der ATM-Zellen. In dieser Schicht wird das Zellformat festgelegt und die Verbindungen aufgebaut. Außerdem fällt ihr die Überwachung der Netzauslastung und der vereinbarten Übertragungsparameter zu. Die ATM-Schicht unterstützt zwei Schnittstellen: das **User-Network-Interface (UNI)** und das **Network-Network-Interface (NNI)**. UNI wird bei der Verbindung zwischen einem Endgerät (Host) und einem ATM-Netzwerk benötigt, während NNI die Schnittstelle für Kommunikation zwischen verschiedenen Netzen, zum Beispiel zwei verschiedenen Providern, definiert.

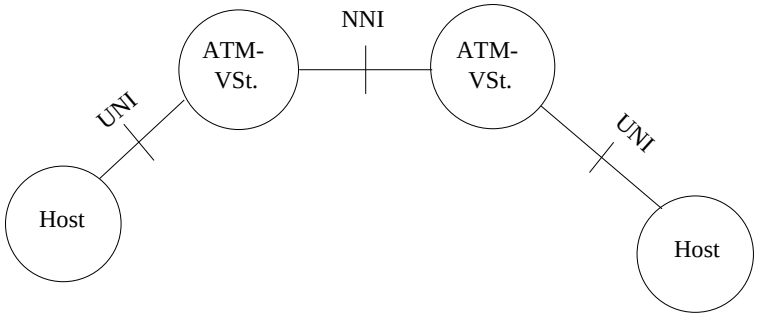


Abbildung 33: UNI/NNI-im ATM-Netzwerk

Zur Unterscheidung hat der ATM-Zellenheader verschiedene Felder. Beim NNI enthält der Zellheader ein Virtual Path Identifier-Feld (VPI) und ein Virtual Channel Identifier(VCI) zur Adres-

sierung, ein Payload Type-Feld zur Bestimmung der Verkehrsart, ein Cell Loss Priority-Feld zur Bestimmung der Priorität sowie ein Header Error Control-Feld, das die Prüfsumme für den Header enthält. Der UNI-Header hat genau die gleichen Felder, nur ist das VPI-Feld um vier Bits kleiner und es kommt ein zusätzliches Generic Flow Control-Feld (GFC) hinzu, das für die lokale Flußkontrolle bis zum ATM-Switch benötigt wird und z.B. Provider-spezifische Informationen enthält. Kommt die Zelle beim ersten ATM-Switch an, so wird im Header das GFC-Feld vom zwölf Bit großen VPI-Feld überschrieben.

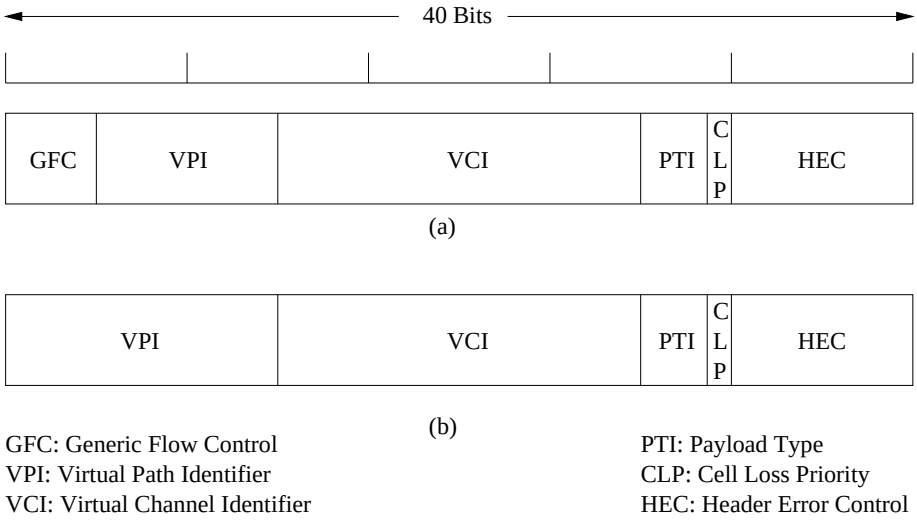


Abbildung 34: Format des ATM-Zellheaders: UNI (1) und NNI (2)

Neben den normalen Datenzellen gibt es noch besondere Zellen, die für die Signalisierung und Kontrolle wichtig sind. Diese Zellen fließen im Datenstrom mit und werden OAM-Zellen genannt (Operation, Administration and Maintenance). OAM-Zellen werden wie alle anderen Zellen durch ihr PTI-Feld identifiziert. OAM-Zellen werden von den Switches erzeugt und dienen ausschließlich zur Signalisierung zwischen den einzelnen Switches.

2.4.6 Traffic Shaping und Policing

Traffic Shaping (Nutzlastformung) und Policing (Verkehrslastüberwachung) sind zwei Techniken zur Optimierung der Auslastung des Netzwerks. Beim Traffic Shaping wird die durchschnittliche Rate der Datenübertragung reguliert. Das bedeutet, daß der Betreiber einer Netzwerkverbindung die fristgerechte Zusendung der Daten garantiert, solange der Benutzer vertragskonform (innerhalb der ausgehandelten Parameter) sendet [132].

Traffic Shaping verwendet zur Realisierung der Netzlastkontrolle den sogenannten "Generic Cell Rate Algorithm", der auch als "Leaky Bucket" bekannt ist.

Es gibt zwei verschiedene Arten mit denen man versucht, durch Erkennung von nicht vertragskonformen Verbindungen die Netzlast zu regulieren. Zum einen eine Regulierung bei der Aufnahme der Verbindung (Connection Admission Control - CAC) und zum zweiten die Steuerung der Benutzerkenngrößen (Usage Parameter Control - UPC).

Bei der Connection Admission Control prüft das Netz vor der Aufnahme jeder neuen ATM-Verbindung die zur Verfügung stehenden Netzressourcen jedes Knoten, über den die Verbindung läuft. Dafür werden zwischen dem Benutzer und Netzwerk Informationen bezüglich Da-

tenverkehrsvolumen, Datenart, QoS-Parameter sowie mögliche Toleranzen ausgetauscht. Stellt die CAC fest, daß die angeforderte Verbindung momentan wegen mangelnder Netzressourcen nicht angenommen werden kann, so wird die Anfrage verworfen.

CAC-Strategien sind nicht genormt, sondern herstellerspezifisch. Zwar gibt es als eine von vielen Möglichkeiten auch einen Vorschlag des ATM-Forums, der jedoch keinerlei Verbindlichkeit hat. Aufgrund der Schwierigkeit, einen Mittelweg zwischen Vermeidung von Überlast und der optimalen Ausnutzung des Netzes zu finden, ist eine Normung auch nicht gewünscht [59].

Die zweite Technik, Usage Parameter Control, kann durch Markierung von Zellen das Netz vor übermäßiger Belastung bewahren. Dazu stehen UPC drei Möglichkeiten zur Verfügung:

1. Passing:

   Alle Zellen verhalten sich wie im Verkehrskontrakt vereinbart. Dann werden die Zellen durchgelassen.

2. Tagging:

   Einige Zellen verstoßen gegen den Verkehrskontrakt, dem Netz stehen jedoch noch ausreichend Ressourcen zur Verfügung. Daher werden die betreffenden Zellen markiert, um im Falle eines auftretenden Engpasses verworfen zu werden.

3. Discarding:

   Zellen, die gegen den Vertrag verstoßen, werden unverzüglich verworfen.

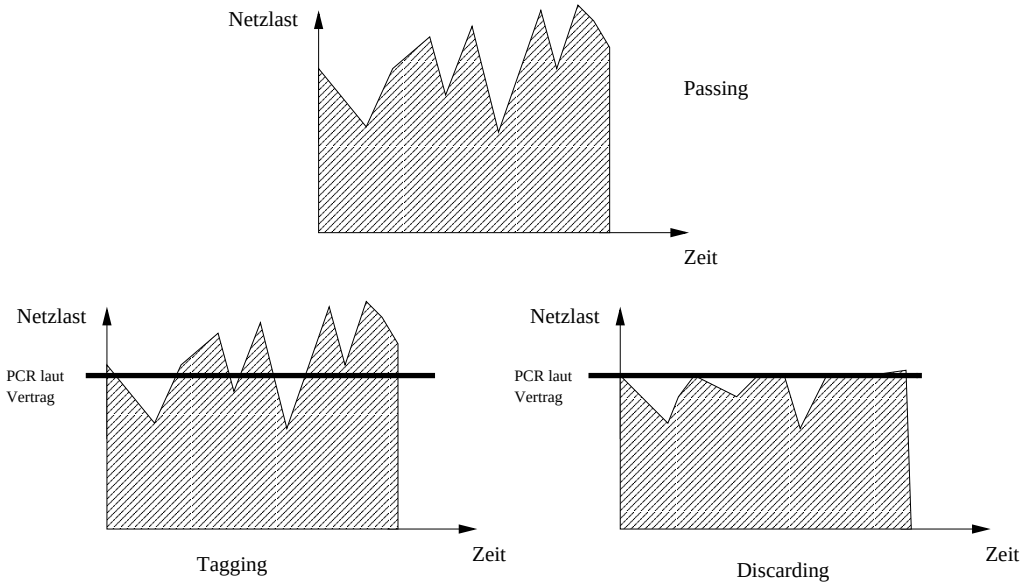


Abbildung 35: Passing, Tagging und Discarding von ATM-Zellen

Traffic Shaping ist wie CAC nicht genormt. Die Auswahl der Algorithmen zur Überlastkontrolle ist vielseitig und setzt an unterschiedlichen Punkten an. So gibt es Implementierungen im Bereich der Reduzierung der Zellspitzenrate, Burstlängen oder Zellverzögerungsschwankungen.

2.4.7 Die Bitübertragungsschicht

Die physikalische Schicht gliedert sich beim ATM-Referenzmodell in zwei Teile - die TC-Schicht (Transmission Convergence). Auf der Senderseite sendet die TC-Schicht die zu übertragenden Zellen an die PMD. Auf der Empfängerseite muß sie die ankommenden Bitströme in Zellströme konvertieren. Auch die Aufteilung, wo innerhalb des Stromes Zellen beginnen und enden, werden in dieser Teilschicht geregelt. Die PMD-Teilschicht (Physikal Medium Dependent) realisiert nun die eigentliche Schnittstelle zum physikalischen Medium. Sie ist für den eigentlichen Transport der Bits sowie das Timing der Bits (Bitzeitgabe) verantwortlich.

2.5 Routing

Beim Asynchronen Verkehrsmodus werden die Verbindungen geroutet. Da ATM verbindungsorientiert ist, wird das Routing nur beim Verbindungsaufbau durchgeführt. Kommt die Verbindung zustande, so muß nicht weiter geroutet werden, was den Vorteil hat, daß der Arbeitsaufwand wesentlich geringer als beim Routen jeder einzelnen Zelle ist. Die Tatsache, daß ATM nur mit virtuellen Kanälen und Pfaden arbeitet, erleichtert das Routing ebenfalls, da man die Einträge der Indextabelle beim Umleiten einzelner Kanäle im selben Pfad von 2^{28} (Länge des VCI-Feldes plus Länge des VPI-Feldes) auf 2^{12} reduzieren kann (Länge des NNI-VCI-Feldes). Ein weiterer Vorteil ist, daß man durch die Virtualisierung und Bündelung zu Pfaden durch Umleitung eines virtuellen Pfades bis zu 65535 virtuelle Kanäle gleichzeitig umleiten kann und nicht jeden Kanal einzeln routen muß.

Dennoch hat das ATM-Routing auch Nachteile: Steht eine Verbindung, so kann nachträglich nichts mehr daran verändert werden. Fällt ein Switch aus, so werden alle Verbindungen, die über diesen Switch gelaufen sind, unterbrochen. Im Nachhinein läßt sich auch nichts mehr an QoS-Parametern ändern. Natürlich gibt es auch beim ATM-Routing ähnlich wie bei SDH Backup-Strategien, die eine Verbindung in Sekundenschnelle umleiten kann, um zu vermeiden, daß der Ausfall eines Switches ganze Teile von Verbindungen zu Erliegen bringt.

Das Prinzip des Routens ist bei ATM statisch. Jeder Router hat eine feste Indextabelle, in der statische Einträge stehen. Diese Tabelle ist durch den Netzwerk-Administrator vordefiniert und enthält in einer Spalte die Eingangspfade und in der anderen die Ausgangspfade. Steht also beispielsweise in einer Tabelle als Eingangs-/Ausgangspaar VPI=5/VPI=7, so wird jeder Kanal, der über VPI 5 ankommt, statisch zu VPI 7 weitergeleitet.

Die Adressierung von ATM-Zellen geschieht über 20 Byte große ATM-Adressen, die, wie in Abbildung 36 dargestellt, aufgebaut sind.

Der erste Teil, der Domain Specific Part (DSP), umfaßt die ersten 13 Bytes und wird verwendet, um auch in hierarchisch tiefer gelegene Stufen innerhalb der Netzwerktopologie zu verzweigen. Der darauf folgende 6 Byte große zweite Teil, der End System Identifier (ESI), spezifiziert das Endgerät und ist somit vergleichbar mit der MAC-Adresse in einem normalen Ethernet. Das letzte Byte, der sogenannte Selektor (SEL), wird beim Routing nicht beachtet. Er spezifiziert beispielsweise einzelne Einheiten in einem Endgerät wie einzelne Einzelgeräte innerhalb einer Telefonanlage. Dieser von der ITU definierte Standard E.164 ist jedoch nicht ATM-spezifisch und wird auch für Telefonnummern verwendet [59].

2.5.1 ILMI

Das ILMI-Protokoll (Integrated Local Management Interface) wird im ATM-Netz zur Identifizierung der ATM-Geräte verwendet. Jedes ATM-Gerät verfügt eine Datenbank (Management

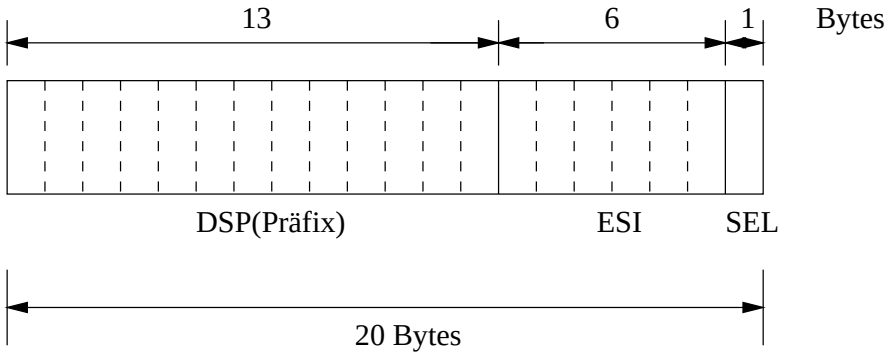


Abbildung 36: ATM-Adressierungschema

Information Base), in der die ATM-Spezifikationen nach dem Schlüssel - Datensatz-Prinzip abgelegt sind. Außerdem hat jedes ATM-Gerät eine Interface Management Entity (IME), in der Informationen über die Interface-Indizes für die Physical Layer, die ATM-Layer, die Virtual Path Connection, die Virtual Channel Connection, Adressen etc. stehen. Diese IMEs müssen an den Enden der ATM-Verbindung synchronisiert werden, damit vor der Übertragung alle Komponenten definiert sind. Diese Aufgabe übernimmt ILMI mit Hilfe des SNMP-Protokolls (Simple Networks Management Protocol). SNMP ist ein Peer-To-Peer-Protokoll, was bedeutet, daß immer nur zwei Partner in einem Master-Slave-Modus miteinander kommunizieren können. Da der Slave nur auf Anfrage des Masters handelt, einigte man sich bei ILMI darauf, daß beide Kommunikationspartner beide Aufgaben (Master und Slave) wahrnehmen, also jedes Gerät als Master die Datenbank des anderen abfragt. Bei der Kommunikation zwischen einem ATM-Endgerät und einem Switch, erfährt zum Beispiel das Endgerät durch ILMI seine vollständige Endadresse und der Switch weiß nun, an welchem Interface das ATM-Gerät hängt. Durch ILMI kann die Adressregistrierung automatisiert werden.

2.5.2 IISP

Das "Interim Inter-switch Signaling Protocol" (IISP) ist ein provisorisches ("Interim") Routing-Protokoll. Es routet hop-by-hop, was bedeutet, daß jeder Switch beim Verbindungsaufbau nur jeweils zu einem seiner Nachbarn routet und nicht darüber hinaus. Das Routing geschieht, wie oben erwähnt, mittels fester Routing-Tabellen innerhalb der einzelnen Switches. Jeder Eintrag besteht aus einer 20 Byte langen ATM-Adresse, einem Adresslängenfeld, das die Werte 0 bis 104 oder 152 annimmt, sowie einem Portfeld, in dem ein Indikator für einen physikalischen Port oder die logische Verbindung zu einem anderen Switch steht. Die Integerwerte spezifizieren ein ATM-Endgerät (152 Bits), eine Domain (104 Bits oder weniger) oder die Defaultroute (0 Bits). IISP wurde provisorisch am Anfang der ATM-Technologie entwickelt und wurde mittlerweile durch P-NNI ersetzt.

2.5.3 P-NNI

Das Private-Network-Network-Interface (P-NNI) Version 2.0 übernimmt die Routingaufgaben innerhalb eines ATM-Netzes. Im Gegensatz zu IISP realisiert P-NNI ein Source-Routing. Das bedeutet, daß der erste ATM-Switch die Netzroute planen muß. Dadurch bietet P-NNI Features

wie automatische Umgehung ausgefallener Switches, eine hohe Skalierbarkeit und die automatische Distribution von erreichbaren Adressen.

Um aber ein Source-Routing durchführen zu können, benötigen die Switches eine gewisse Kenntnis des Netzwerk-Aufbaus, also der Topologie des Netzes, aber auch Informationen über Bandbreiten oder die Anzahl der Verbindungen pro Switch. Eine weitere wichtige Information ist der Lastzustand des Netzes, im speziellen, wieviele Verbindungen ein einzelner Switch noch aufnehmen kann.

Die Technik zur Weitergabe dieses Wissens an die Switches wird **Topologiedistribution** genannt. Topologiedistribution erfolgt im ATM-Netz wie folgt: Die Adressen seiner Endgeräte sind jedem ATM-Switch durch ILMI bekannt. Um in einem großen Netzwerk wichtige Informationen auszutauschen, ohne damit das Netz durch eine Flut von Informationen zu gefährden, wird eine logische Hierarchie errichtet. Dazu werden zunächst mehrere benachbarte Switches zu sogenannten "Peergroups" zusammengefaßt. Diese Aufgabe fällt dem Netzwerkadministrator zu. Innerhalb jeder Peergroup wird nun ein "Peergroup-Leader" ermittelt, der quasi die Schnittstelle der Peergroup zum übrigen Netz bildet. Informationen innerhalb einer Peergroup werden mittels PTSEs (PNNI-Topology State Elements) ausgetauscht, so daß jeder Switch eine genaues Bild über die Verbindungen innerhalb seiner Peergroup hat.

Der Peergroup-Leader hat nun die Aufgabe, der nächsthöheren Hierarchiestufe eine vereinfachte Darstellung seiner Peergroup zu übermitteln. Dabei wird die Peergroup als ein Knoten dargestellt. Haben zwei Peergroups mehrere Verbindungen untereinander, so werden sie für die nächsthöhere Stufe als **eine** Peergroup mit angepaßten Eigenschaften (Bandbreite etc.) dargestellt. Durch weitere Bündelung auf der nächsten übergeordneten Hierarchiestufe, kann die Netzwerkkomplexität weiter reduziert werden.

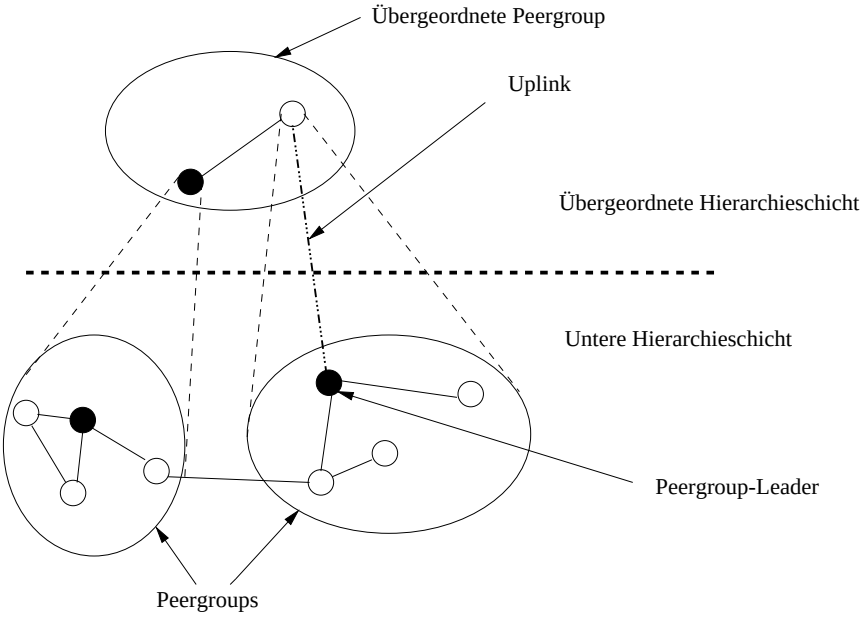


Abbildung 37: Topologiedistribution im ATM-Netz

Die wichtigste Aufgabe kommt den Peergroup-Leadern zu, da sie die gesammelten Informationen nach oben und unten weitergeben und somit sowohl ihrer Peergroup als auch den oberen Schichten einen vereinfachten Aufbau des Netzes übermitteln. Zur Verbindung mit den nächsthöheren

Schichten gibt es sogenannte Uplinks, die für das Routing logische Verbindung zwischen den Hierarchiestufen darstellen. Über Uplinks lassen sich auch benachbarte Peer-Groups ansprechen, die sonst keine Kenntnisse voneinander hätten. Abbildung 37 zeigt die Topologiedistribution in einem Beispielnetz.

Obwohl P-NNI 2.0 mittlerweile vollständig standardisiert ist, gibt es keine konkreten Standards für Routing-Strategien. Dieses Gebiet bleibt ein großes Forschungsthema und zur Zeit dominieren verschiedene, qualitativ zum Teil gleichwertige, herstellerspezifische Routingalgorithmen. Wie bei CAC ist eine einheitliche Normung auch hier nicht vorgesehen. Auch das ATM-Forum hat einen Routingalgorithmus vorgeschlagen, der jedoch nichts anderes als eine Empfehlung ist. Die Realisierung von echtem QoS-sensitivem Routing bleibt nach wie vor ein weites Betätigungsfeld der aktuellen und zukünftigen Forschung.

2.6 Anwendungsprotokolle im ATM-Netz

ATM hat sich durch seine Flexibilität und seine durch Multiplexing enormen Bandbreiten als Netzwerktechnologie im Hochgeschwindigkeitsbereich durchgesetzt. Dennoch war man immer bemüht, bestehende, im Betrieb befindliche Dienste zu integrieren. Die drei wichtigsten Protokolle sind dabei:

- Classical IP over ATM
- LANE
- MPOA

2.6.1 Classical IP over ATM

Die Integration IP-basierter Netze in ATM wird mit Hilfe des von der "Internet Engineering Task Force" (IETF) standardisierten "Classical IP over ATM"-Protokoll realisiert. Sinn dieses Protokolls ist es, das ATM-Netz vor IP zu verschleiern und eine normales IP-Netz zu simulieren um ein ATM-Routing zu ermöglichen. Da diese Verschleierung jedoch nicht vollständig ist, ist "Classical-IP" das einzige Protokoll, das einige ATM-Eigenschaften nutzen kann [118]. Ein "Classical IP over ATM"-Netz untergliedert sich in sogenannte "Logical IP Subnets" (LIS). Innerhalb dieser LIS können die einzelnen Clients ähnlich wie in einem reinen IP-Netz kommunizieren. In jedem LIS gibt es einen Server, der eine vollständige Tabelle aller im LIS befindlichen IP-Nummern und deren dazugehörige ATM-Adressen gespeichert hat. Zur Kommunikation zweier LIS benötigt man einen echten IP-Router. Beim Aufbau der Kommunikation zweier Clients holt sich der Client nun vom Server die ATM-Adresse seines Partners und stellt eine SVC (Switched Virtual Circuit) - Verbindung her. Obwohl alle Dienstklassen (CBR, VBR, UBR, ABR) möglich sind, handelt es sich standardmäßig um eine ABR-Verbindung. Basiert das IP auf Ethernet, so wird zunächst durch das Address Resolution Protocol (ARP) die Medium Access Control (MAC)-Adresse ermittelt. Im ATM-Bereich existiert dafür analog das ATMARP (ATM -Address Resolution Protocol).

2.6.2 LAN-Emulation (LANE)

LANE (Local Area Network Emulation) ist eine Reihe von Protokollen, die das Betreiben jedes ISO/OSI-Schicht 3-Protokolls über ATM ermöglichen.

Den einzelnen Protokollen bleibt ATM dabei vollständig verborgen. Nachteil von LANE ist, daß dabei keinerlei ATM-Eigenschaften ausgenützt werden können. Analog zu "Classical IP" werden bei LANE virtuelle Teilnetze (Emulated LANs - ELANs) generiert, die ebenfalls nur über externe Router miteinander in Verbindung treten können. Innerhalb eines Teilnetzes müssen sich die LANE-Clients (LECs) beim LANE-Server (LES) anmelden. Dabei senden die zu emulierenden MACs und erhalten vom LES die "Broadcast and Unknown Services" (Bus)-Adresse und die LECs-Adressen.

Das Teilnetz hat noch einen "Broadcast and Unknown Services"-Server (BUS). Zu diesem Server werden alle Pakete mit unbekanntem Ziel gesendet, worauf der BUS zu jedem LEC Verbindung aufnimmt und die Pakete weiterschickt. Dies verursacht zum Teil erheblichen Datenverkehr.

Im LANE gibt es noch einen dritten Server, den LANE Configuration Server (LECS), der die Zugehörigkeit der einzelnen LECs zu verschiedenen ELANs regelt. LANE ist aufgrund seines großen Protokoll-Overheads relativ fehleranfällig, obwohl durch LANE 2.0 eine Verbesserung der Ausfallsicherheit erzielt wurde.

2.6.3 Multiprotocol over ATM (MPOA)

Mit Hilfe von MPOA (Multi Protocol over ATM) versucht man, Eigenschaften von "LANE" und "Classical IP" zu kombinieren. Ziele sind dabei die direkte Kommunikation zwischen den einzelnen LIS bzw. ELANs ohne externe Router. Dafür wurde das "Next Hop Resolution Protocol" (NHRP) entwickelt, das es zwei MPOA-Clients ermöglicht, eine eigene direkte Verbindung aufzubauen, selbst wenn diese in zwei verschiedenen ELANs liegen [118]

2.7 Ausblick - Standardisierungen

In den Anfängen der Daten- und Telekommunikationstechnik gab es eine Vielzahl von verschiedensten herstellerspezifischen Techniken zur Regelung der Netzwerke im Bereich der Daten- und Telekommunikation. Man erkannte bald die Notwendigkeit der Normung, um damit Integrität und Interoperabilität der einzelnen Dienste zu gewährleisten. Es haben sich zwei Arten von Standards durchgesetzt. Zum einen Standards, die aufgrund ihrer allgemeinen Akzeptanz übernommen wurden, sogenannte *de facto -Standards*, zum anderen Standards, die auf formellen Gesetzesnormen basieren, sogenannte *de jure - Standards*. Ebenfalls lassen sich die Normungsanstalten in freiwillige Gruppen und staatliche Vertragsgruppen einteilen. Die wichtigsten Gruppen im ATM Bereich sind:

- ITU

  Die "International Telecommunications Union" ist eine Organisation, die sich seit 1947 mit der Standardisierung im Bereich der Telefon- und Datenkommunikationssysteme befaßt. Von 1956-1993 hieß die ITU CCITT(Committé Consultatif International Télégraphique et Téléphonique) , bevor sie 1993 umorganisiert und umstrukturiert wurde. Von der ITU-T (ITU-Telecommunication Standardization Sector) ausgearbeitete Standards sind reine Empfehlungen und technische Vorschläge, die von den einzelnen Ländern verwendet oder abgelehnt werden können.

- IETF

  Die Internet Engineering Task Force wurde 1989 ins Leben gerufen, als man die Notwendigkeit der Standardisierung des Internets erkannte. Die IETF befaßt sich mit kurzfristigen

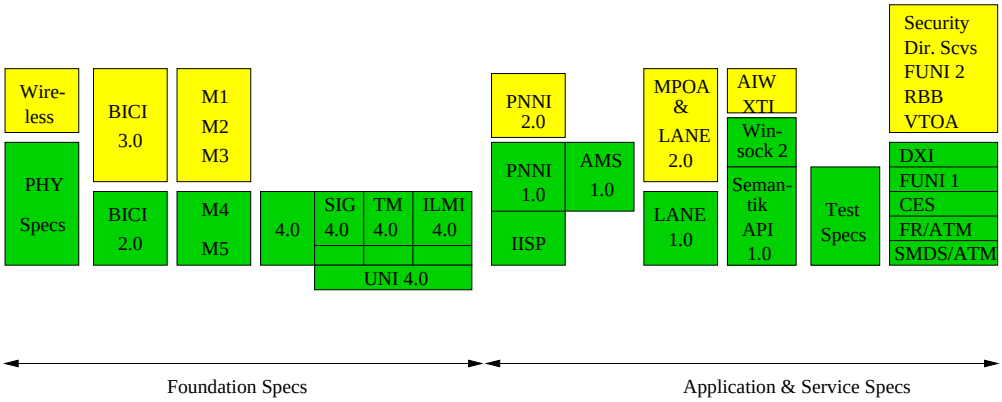


Abbildung 38: Aktuelle ATM Standards (Stand Mai 1999)

technischen Fragen und gibt technische Berichte, sogenannte “Request for Comments - RFC” heraus. Derzeit existieren über 2000 solcher RFCs). Bei genügendem Interesse entstehen daraus Standard-Entwürfe (Draft Standards), die dann nach ausreichendem Testen einer funktionierenden Implementierung zu “Internet Standards” erhoben werden.

- ATM-Forum

  Das ATM-Forum ist eine Organisation, bestehend aus Vertretern der Wissenschaft und Vertretern der Daten- und Telekommunkationsbranche, die sich zum Ziel gesetzt hat, die Technik im ATM-Bereich zu vereinheitlichen. Im ATM-Bereich wurde bereits eine Menge Arbeit geleistet, große Teile des ATM-Managements und des Referenzmodells sind bereits genormt. Das ATM-Forum gibt jedoch auch nur Empfehlungen heraus, die nicht zwingend eingehalten werden müssen.

Trotz der Tatsache, daß die einzelnen Organisationen nur Empfehlungen vorschlagen, läuft der Standardisierungsprozeß aufgrund der Isolationsgefahr (andere Technik als alle anderen) zügig. Allein die ITU-T gibt jährlich ca. 5000 Seiten an Empfehlungen heraus. Abbildung 38 zeigt eine Auflistung aktueller ATM-Standards.

ATM wird aufgrund seiner Flexibilität und der vielseitigen Verwendungsmöglichkeiten mit verschiedensten Datenströmen sowie QoS-Parametern als die Technik der Zukunft gepriesen. Und obwohl noch eine Menge im Bereich der Standardisierung zu tun ist, hält der asynchrone Transfermodus bereits einen Teil der an ihn gestellten Anforderungen ein und führt die Daten- und Telekommunikationstechnik in Bereiche, die vor ein paar Jahren noch undenkbar gewesen wären.

2.8 Abkürzungen

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
B-ISDN	Broadband Integrated Services Digital Network
BUS	Broadcast and Unknown Server
CAC	Connection Admission Control
CBR	Constant Bit Rate
CCITT	Committé Consultatif International des Télégraphique et Téléphonique
CPCS	Common Part Convergence Sublayer
CS	Convergence Sublayer
ELAN	Emulated LAN
GCRA	Generic Cell Rate Algorithm
GFC	General Flow Control
HEC	Header Error Control
IETF	Internet Engineering Task Force
ILMI	Intergrated Local Management Interface
IP	Internet Protocol
ITU	International Telecommunications Union
LANE	LAN Emulation
LEC	LAN Emulation Client
LECS	LANE Configuration-Server
LES	LANE-Server
LIS	Logical IP Subnet
MAC	Medium Access Control
MIB	Management Information Base
MPOA	Multiprotocol over ATM
NHRP	Next Hop Resolution Protocol
NNI	Network-Network-Interface
OAM	Operation, Administration and Maintenance
OC-n	Optical Carrier-n
PDU	Protocol Data Unit
P-NNI	Private-Network-Network-Interface
PT	Payload Type
QoS	Quality of Service
RFC	Request for Comment
SAR	Segmentation and Reassembly
SCR	Sustainable Cell Rate
SDH	Synchronous Digital Hierarchy
SDU	Service Data Unit
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SSCOP	Service Specific Connection-Oriented Protocol
SSCS	Service Specific Convergence Sublayer
STM	Synchronous Transfer Mode
STS-n	Synchronous Transport Signal-n

SVC	Switched Virtual Circuit
TC	Transmission Convergence
UBR	Unspecified Bit Rate
UNI	User-Network Interface
UPC	Usage Parameter Control
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier

3 EEE 802.x - LAN Technologien

3.1 Einführung

Lokale Netze (engl. Local Area Networks - LAN) zeichnen sich durch eine geringe Ausdehnung aus (aus einigen hundert Metern) und relativ hohe Übertragungsgeschwindigkeiten (im MBit/s-Bereich). Sie grenzen sich damit von den Wide Area Networks (WAN) ab, die zur Verbindung geographisch weit entfernter Netze dienen und sich bis zu einigen hundert Kilometern hinweg erstrecken.

Das Gremium 802 des IEEE[9] (Institute of Electrical Electronics Engineers) bemüht sich seit 1983 um die Standardisierung von LANs und MANs (Metropolitan Area Networks). Die wichtigsten IEEE-Standards wurden von der ISO übernommen (ISO/IEC 8802 u.a.) und standardisiert.

3.2 Überblick IEEE 802.x

Die IEEE 802 Taskforce ist in 14 Gremien aufgeteilt, die an folgenden Projektion arbeiten bzw. gearbeitet haben:

- **LAN/MAN Bridging & Management (802.1)** Overview – Architecture – LAN/MAN Management – Media access control (MAC) bridging – Virtual Bridge LANs
- **Logical Link Control (802.2)** Sicherungsschicht im LAN
- **CSMA/CD Access Method (802.3)** Ethernet
- **Token-Passing Bus Access Method (802.4)**
- **Token Ring Access Method (802.5)**
- **DQDB Access Method (802.6)** Distributed Queue Dual Bus – MAN
- **Broadband LAN (802.7)**
- **Fiber Optics Integrated Services (802.9)**
- **LAN/MAN Security (802.10)** Interoperable LAN/MAN Security (SILS) – Secure Data Exchange (SDE)
- **Wireless (802.11)** Kabellose LANs
- **Demand Priority Access Method (802.12)** V(oice)G(rade)-AnyLAN – Zwitter zwischen CSMA/CD und Token-Ring auf niederwertigen Kabel
- **Cable TV (802.14)**

[9] `http://grouper.ieee.org/groups/802/`

3.3 ISO/OSI-Referenzmodell

Schicht 1 – Physical Layer Schicht 1 spezifiziert das Übertragungsmedium und die Regeln für die Übertragung von einzelnen Bits.

Schicht 2 – Data Link Layer Die Sicherungsschicht hat die Aufgabe, eine sichere Übertragung zwischen zwei direkt benachbarten Stationen zu garantieren. Dazu werden die übertragenen Bits in *Frames* zusammengefaßt und mit einer Prüfsumme versehen. Dadurch ist eine Fehlererkennung möglich. In LANs wird die zweite Schicht in zwei Teilschichten aufgeteilt: Schicht 2a als *MAC-Schicht (Media Access Control)* regelt den Zugriff auf das Übertragungsmedium. Schicht 2b als *LLC-Schicht (Logical Link Control)* stellt die eigentliche Sicherungsschicht in LANs dar.

Schicht 3 – Network Layer Diese Schicht baut Ende-zu-Ende-Verbindungen auf. Zu diesem Zweck muß für die einzelnen Datenblöcke ein Weg *(Route)* durch das Netz festgelegt werden. Die innerhalb von Schicht 3 übertragenen Blöcke werden oft *Pakete* genannt.

Schicht 4 – Transport Layer Die Transportschicht hat die Aufgabe, eine virtuelle Ende-zu-Ende-Verbindung für den Transport von Daten in Form von festgelegten Paketen zwischen den Endsystemen bereitzustellen. Die Aufgaben bestehen vor allem in der Korrektur der Übertragungsfehler.

Schicht 5, 6 und 7 – Session Layer, Presentation Layer, Application Layer Die obersten drei Schichten sind anwendungsorientiert. Hier befinden sich Synchronisation zwischen Kommunikationsprozessen (5), Umsetzung der Informationen auf einheitliche Formate (6) und die Anwendungsprogramme selbst (7).

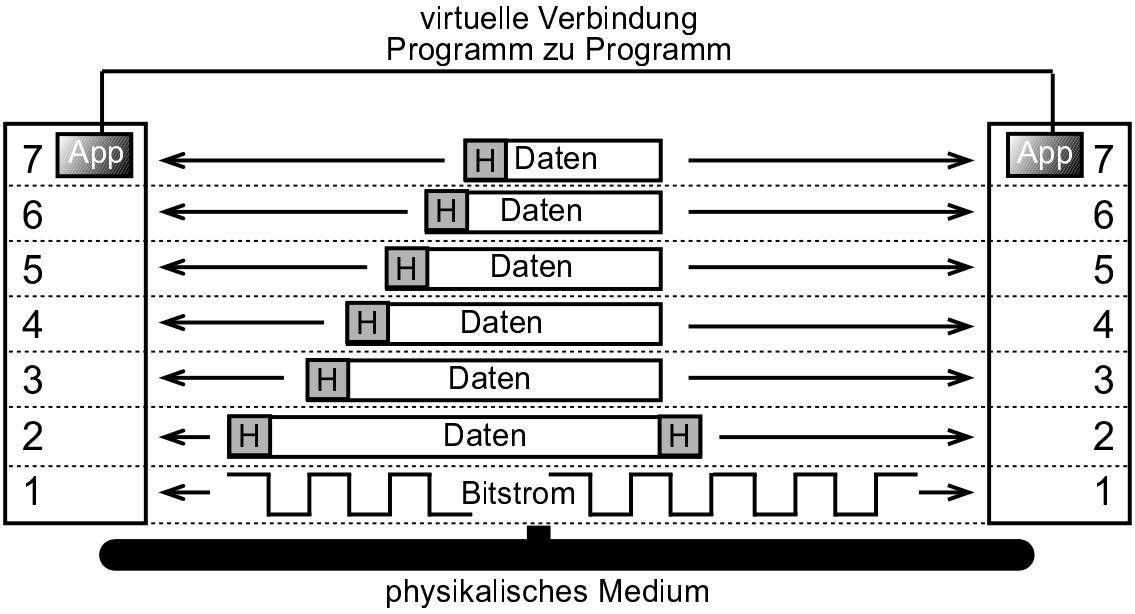


Abbildung 39: ISO/OSI-Referenzmodell

3.4 IEEE 802.3 – Ethernet

3.4.1 CSMA/CD

Das klassische IEEE 802.3 besitzt logisch – und meist auch physikalisch – eine Bus-Struktur. Der Zugriff auf das physikalische Medium erfolgt bei IEEE 802.3 durch das CSMA/CD-Verfahren *(Carrier Sense Multiple Access with Collision Detection)*. Das Prinzip setzt viele beteiligte Sender voraus *(Multiple Access)*, die vor dem Senden in den Kanal hineinhören *(Carrier Sense)* und auch während der Datenübertragung den Kanal überprüfen *(Collision Detection)*.

Tritt nun eine Übertragungspause ein, dann darf jeder Teilnehmer jedem beliebigen Teilnehmer ohne Umwege ansprechen. Dabei kann es allerdings zu einer Überlagerung von mehreren Sendern auf dem Medium geben *(Collision)*. Dies bemerken selbstverständlich alle Beteiligten und brechen die Kommunikation vorerst ab. Um eine erneute Kollision zu vermeiden, startet jede Station nach einer über einen Zufallsgenerator gesteuerten Zeit einen erneuten Versuch.

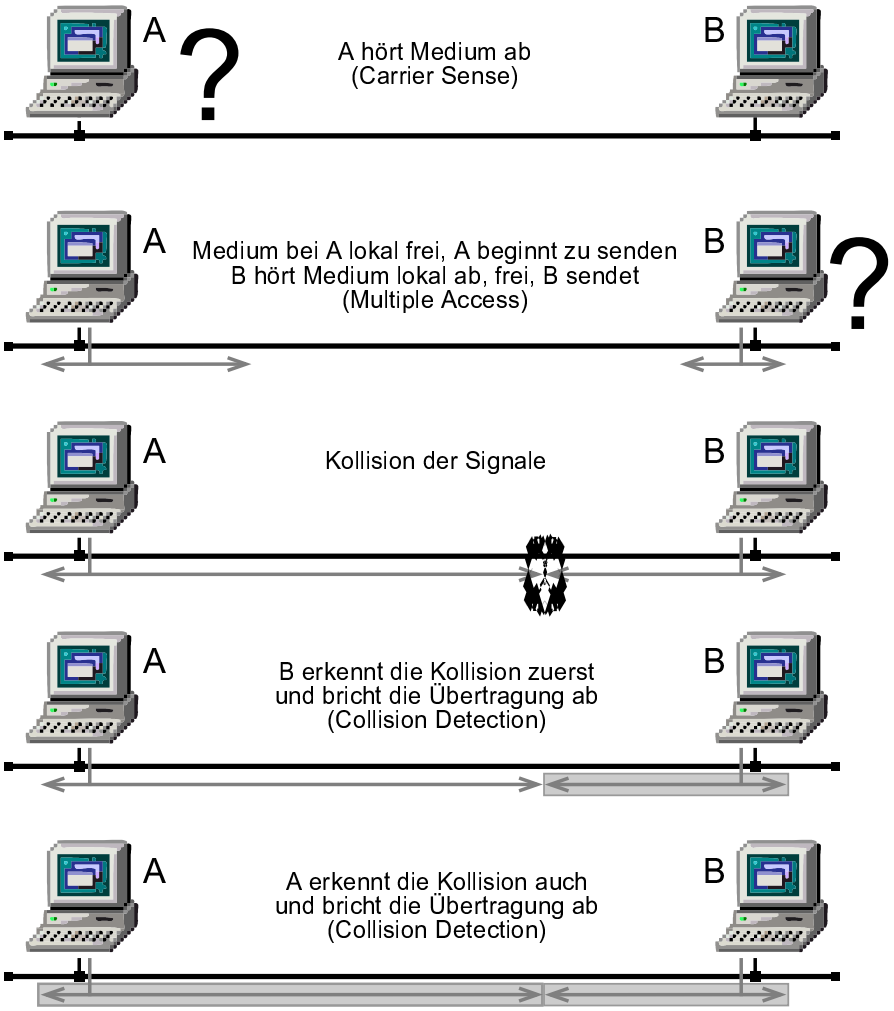


Abbildung 40: CSMA/CD-Verfahren

3.4.2 Ethernet Technologien

Mit dem Begriff *Ethernet* ist heute eine Ansammlung von Standards verbunden. Unter Beibehaltung des charakteristischen Eigenschaften den CSMA/CD Verfahrens, gliedert sich die Ethernet-Technologie in

- 10Base 5 (Ethernet) (IEEE802.3r),
- 10Base 2 (Cheapernet),
- 10Base T (IEEE802.3i),
- 10Base F (IEEE802.3j),
- 100Base TX (IEEE802.3u),
- 100Base FX,
- 100Base T4,
- 1000Base SX,
- 1000Base LX,
- 1000Base CX (IEEE802.3z),
- 1000Base T (IEEE802.3ab)

Die erste Zahl gibt an, mit welcher Übertragungsgeschwindigkeit im LAN gearbeitet wird (10 = 10 MBit/s, 100 = 100 MBit/s, 1000 = 1 GBit/s), *Base* steht für Basisbandübertragung. Die letzte Zahl macht eine Aussage über die Charakteristik des Übertragungsmediums:

- T(x) – Twisted Pair mit x Adernpaare,
- F(x), S(x), L(x) – Fiber Optic,
- C(x) – Copper Link,
- 5 – 500 m Segmentlänge,
- 2 – 200 m Segmentlänge

IEEE 802.3 spezifiziert die unterste Schicht des ISO-OSI-Modells (Physical Layer), Schicht 2 (Logical Link Layer) wird von IEEE 802.1 und IEEE 802.2 beschrieben.

3.4.3 Ethernet – 10Base

Alle 10 MBit/s-Varianten von IEEE 802.3 setzen auf einen Bus als Verkabelung auf, auf dem sich alle Stationen die Übertragungsgeschwindigkeit statistisch teilen.

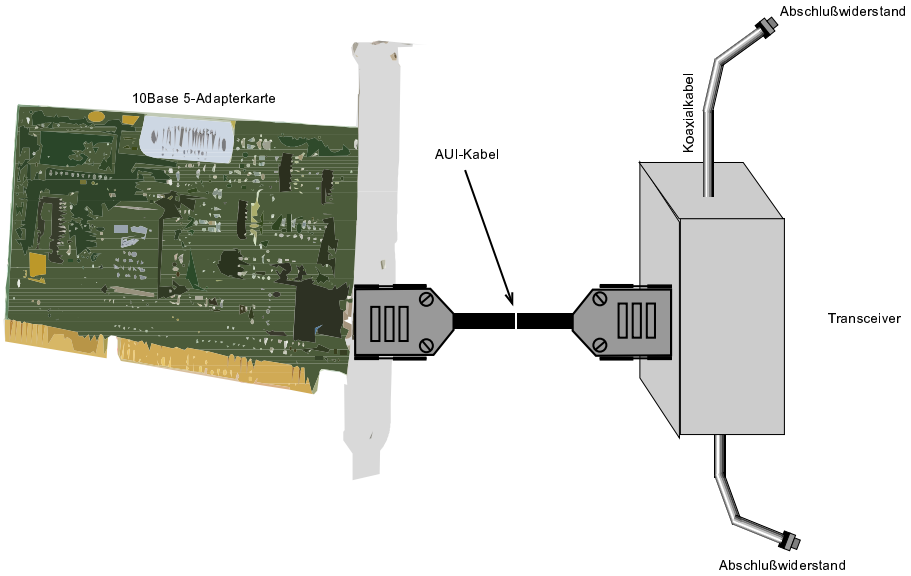


Abbildung 41: Anschlußtechnik bei 10Base 5

10Base 5 Die Hauptkomponenten und die Anschlußtechnik von 10Base 5 sind in Abbildung 41 gezeigt. Als Übertragungsmedium dient hier ein Koaxialkabel mit 50 Ohm Wellenwiderstand und einem Durchmesser von einem Zentimeter. Dieses Kabel ist zweimal mit einem Drahtgeflecht und zwei weiteren Metallfolien geschirmt. Dieses Koaxialkabel wird wegen seiner Mantelfärbung auch *Yellow Cable* genannt.

Der Anschluß erfolgt mit einem externen Transceiver, der direkt auf das Kabel montiert wird, auf dem im Abstand von 2,5m Markierungen als Anhaltspunkte für die Transceiver-Montage angebracht sind. Die Länge eines Ethernet-Segments beträgt maximal 500 m.

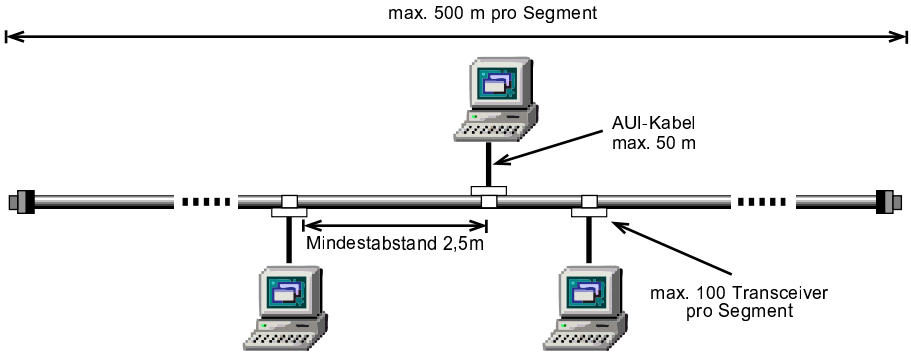


Abbildung 42: 10Base-5-Basis-Konfigurationen

10Base 2 Die bisher größte Verbreitung der Varianten von Ethernet/IEEE 802.3 hat das als *Cheapernet* bekannte 10Base 2. Abbildung 43 zeigt die 10Base-2-Basiskonfiguration. Das Koaxialkabel hat ebenfalls einen Wellenwiderstand von 50 Ohm, jedoch einen geringeren

Max. Segmentlänge	500 m
Übertragungsmedium	Koaxialkabel; Wellenwiderstand 50 Ohm
Max. Anzahl von Anschlüssen pro Segment	100
Anschlußmöglichkeiten	Transceiver-Klemme auf Yellow Cable
Min. Abstand zwischen zwei Anschlüssen	2,5 m
Netztopologie	Bus

Tabelle 10: Wichtige 10Base 5-Parameter

Kabeldurchmesser von unter 5 mm. Im Vergleich zum 10Base-5-Segment hat man beim 10Base-2-Segment die Verringerung der maximalen Segmentlänge auf 185 m sowie eine Limitierung auf höchstens 30 Anschlüsse pro Segment. Das 10Base-2-Konzept wird auch als *Thin Ethernet* bezeichnet. Die 10Base-2-Anschlußtechnik ist in Abbildung 44 gezeigt. Beim

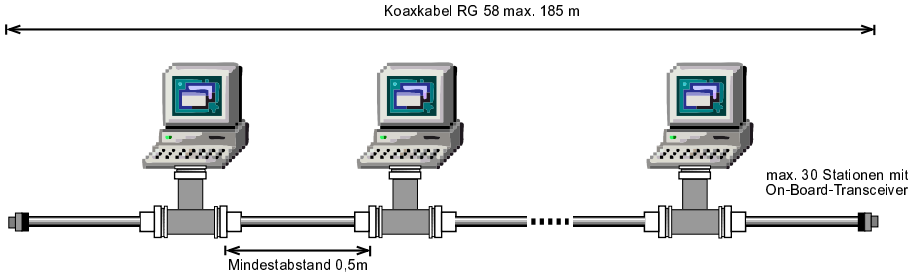


Abbildung 43: 10Base-2-Basis-Konfigurationen

10Base-2-Segment ist die MAU[10] *(Transceiver)* im allgemeinen auf der Adapterkarte im Rechner untergebracht. Damit entfällt hier ein Äquivalent zum AUI[11]-Kabel des 10Base-5-Segments. Jede Station enthält eine BNC-Buchse für den Anschluß an das Übertragungsmedium.

Max. Segmentlänge	185 m
Übertragungsmedium	Koaxialkabel; Wellenwiderstand 50 Ohm
Max. Anzahl von Anschlüssen pro Segment	30
Anschlußmöglichkeiten	BNC-Steckerverbinder bzw. T-Stücke
Min. Abstand zwischen zwei Anschlüssen	0,5 m
Netztopologie	Bus

Tabelle 11: Wichtige 10Base 2-Parameter

10Base T Die Basistopologie des 10Base-T-LANs ist ein physikalischer Stern. Wie Abbildung 45 zeigt, werden die Kabel ausgehend von einem zentralen 10Base-T-Verteiler (10Base-T-Hub, kurz Hub) sternförmig zu den einzelnen Stationen verlegt. 10Base T ist aber dennoch

[10] Media Access Unit
[11] Attachment Unit Interface

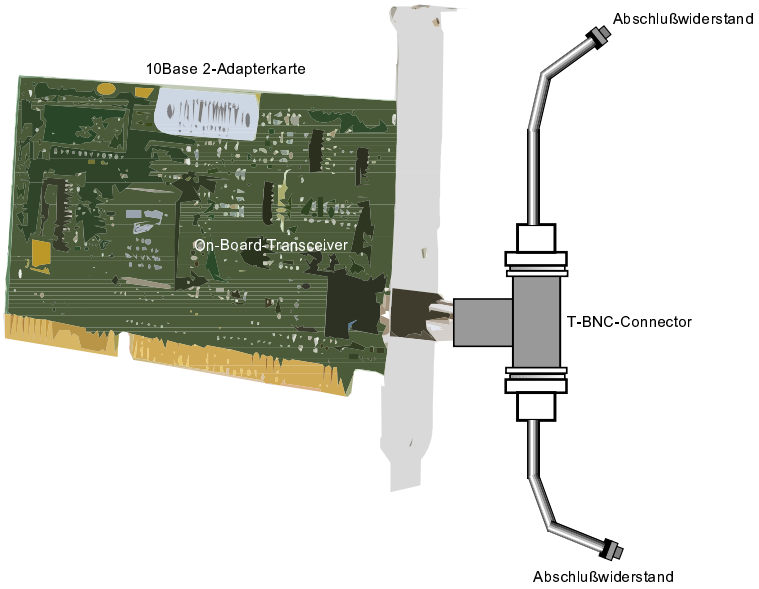


Abbildung 44: 10Base-2-Anschlußtechnik

ein logischer Bus, so daß das Zugriffsverfahren CSMA/CD realisiert wird. Der Standard sieht für 10Base T eine paarweise verdrillte Leitung (UTP[12]) mit einem Wellenwiderstand von ca. 100 Ohm vor. Für jede Station werden zwei Adernpaare benötigt, wobei ein Paar als Sende- und das andere als Empfangsleitung verwendet wird. Diese Leitung darf nach dem Standard maximal 100 m lang sein. Der Hub trennt – im Falle einer fehlerhaften

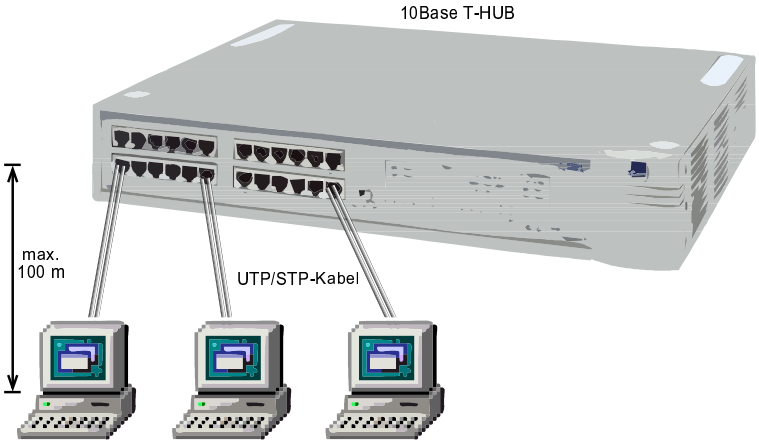


Abbildung 45: 10Base-T-Basis-Konfiguration

Station oder eines defekten Kabels – die Station vom übrigen Ethernet-LAN. Ein Hub stellt somit eine *Collision Domain* dar und gewährleistet einen einwandfreien Netzbetrieb auch bei Störungen auf einzelnen Anschlüssen.

[12] *Unshielded Twisted Pair*

Max. UTP/STP-Leitungslänge	100 m
Anschlußkabel	UTP/STP[13]-Kabel; Wellenwiderstand 100 Ohm
Max. Anzahl von Anschlüssen pro Segment	1024
Anschlußstecker	RJ-45-Stecker
Netztopologie	Stern oder Punkt-zu-Punkt

Tabelle 12: Wichtige 10Base T-Parameter

10Base F Um IEEE-802.3-LANs, die räumlich sehr weit voneinander entfernt sind (bis zu mehrere Kilometer) verbinden zu können, wurde der Standard 10Base F normiert, der über zwei getrennte Glasfaserkabel (jeweils eins zum Senden und Empfangen; *Simplex-Übertragung*) überträgt. Abbildung 46 zeigt eine mögliche 10Base-F-Topologie. Sie besitzt an den Knotenpunkten sogenannte Sternkoppler als optische Verteiler.

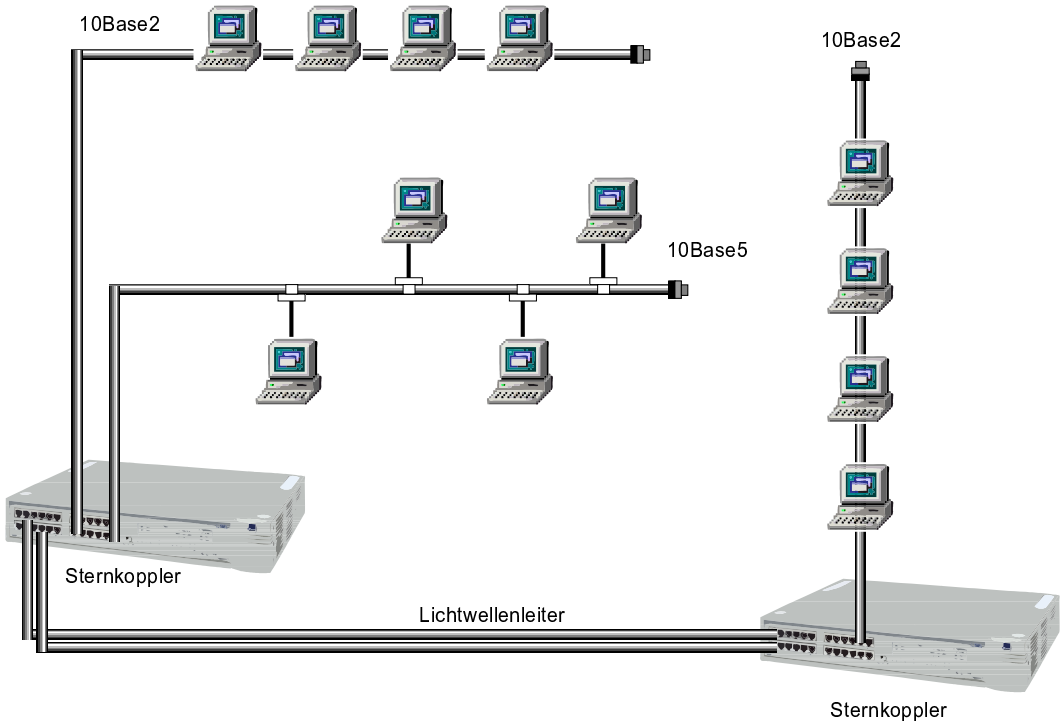


Abbildung 46: Beispiel für den Einsatz von 10Base F

3.4.4 Fast Ethernet – 100Base

Die Fast-Ethernet-Technologie versteht sich als Fortführung der IEEE-802.3-CSMA/CD-Technologie im Rahmen der Arbeitsgruppe IEEE 802.3u mit den Zielen:

- CSMA/CD-Übertragung mit Bitrate 100 MBit/s,
- identisches MAC-Format zum IEEE-802.3-Standard,

Max. UTP/STP-Leitungslänge	500 m / 2000 m
Anschlußkabel	LWL-Kabel ($50/125\mu m$ oder $62.5/125\mu m$)
Anschlußmöglichkeiten	ST, FSMA u.a. Steckerverbinder
Netztopologie	Stern oder Punkt-zu-Punkt

Tabelle 13: Wichtige 10Base F-Parameter

- physikalische Medien sind Twisted Pair und Glasfaser (MMF[14]),
- Interoperabilität von 10Base-T- und 100Base-Tx-Komponenten.

Um die notwendige Anpassung an die physikalische Übertragungsschicht zu erzielen, gliedert sich 100Base X in folgende medienspezifische Technologien:

- **100Base Fx** für die Übertragung auf Multimode-Glasfaser (MMF),
- **100Base Tx** für die Übertragung auf Twisted-Pair-Kabeln der Kategorie 5 (UTP) bzw. über STP Kabel vom IBM Typ 1,
- **100Base T4** für eine Twisted-Pair-Verkabelung auf Basis der Kategorie 3 unter Nutzung aller vier Adernpaare.

Die Unterschiede zwischen 100Base Tx und 100Base T4 betreffen in erster Linie die medienspezifischen Funktionen beider Protokolle.

Der 100Base-X-Standard setzt eine Hub-Technologie voraus, d.h. im Gegensatz zum klassischen Ethernet, wo die physikalische und logische Vernetzung ein Bussystem darstellt, basiert 100Base X ausschließlich auf einer physikalischen Stern-Topologie. Die hierzu notwendigen Hubsysteme müssen in einer gemischten Umgebung in der Lage sein, aufgrund der ankommenden Signalart zu unterscheiden, ob die sendende Station 10Base-T-, 100Base-Tx- oder 100Base-T4-Standards entspricht. Diese Komponenten werden *Class II* Fast-Ethernet-Repeater genannt, während *Class I* Fast-Ethernet-Repeater die Repeating-Funktion lediglich für Ports mit gleichartigem Medienanschluß bereit stellen. Der Fast-Ethernet-Standard unterstützt auch den Full Duplex Übertragungsmodus. Dies ermöglicht eine Anbindung der Endgeräte mit einer Gesamtgeschwindigkeit von 200 MBit/s.

Der Auto Negotiation-Prozeß

Der Full Ethernet-Standard unterstützt den Halbduplex- oder den Vollduplex-Modus. Dies ermöglicht eine Anbindung von Geräten mit Geschwindigkeiten von 10 und 100 MBit/s im Halbduplex- bzw. 20 und 200 MBit/s im Vollduplex-Modus. Der Standard sieht im Bereich der Twisted-Pair-Kabel ein automatisches Konfigurieren der Link-Segmente mit Hilfe des Negotiation-Prozesses vor. Dadurch kann der Benutzer ohne große Probleme in einem Netz sämtliche Fast Ethernet- oder 10 MBit/s-Produkte installieren und muß sich nicht um die spezifischen Konfigurationen bereits installierter Komponenten kümmern. Der Auto Negotiation-Prozeß ermöglicht es zwei Komponenten, die an einem Link-Segment angeschlossen sind, untereinander Parameter auszutauschen und sich mit Hilfe dieser Parameter auf die jeweils unterstützten Eckwerte der Kommunikation einzustellen. Der Mechanismus muß sicherstellen, daß er auch bei Störungen (Noise) auf dem UTP-Kabel zu keinen Fehlfunktionen führt.

[14] *Multi Mode Faser*

Fast Ethernet auf Twisted Pair-Leitungen (100Base Tx) Der 100BaseTx-Standard legt zur Übertragung die Kabel der Kategorie-5 (gemäß ISO/IEC 11801) zugrunde. Gegenüber den Kategorie-3- oder den Kategorie-4-Kabeln weisen die Kategorie-5-Kabel ein wesentlich besseres Übertragungsverhalten und Übersprechen auf. Der 100BaseTx-Standard schreibt die Nutzung von zwei Aderpaaren für die Übertragung der Daten fest. Die 100 MBit/s-Datenrate wird auf den zwei Aderpaaren durch die MLT-3-Kodierung auf 33,333 MHz reduziert. Dadurch ist gewährleistet, daß die amerikanischen und die noch strengeren europäischen Vorschriften zur elektromagnetischen Abstrahlung eingehalten werden.

Die Länge eines Twisted Pair-Segments beträgt maximal nur 100 m. Als Standardverbinder wurde beim 100BaseTx-Standard die RJ45-Technologie festgeschrieben. Als Standard-100BaseTx-Interface steht eine 8-polige RJ45-Buchse zur Verfügung (siehe Abbildung 47).

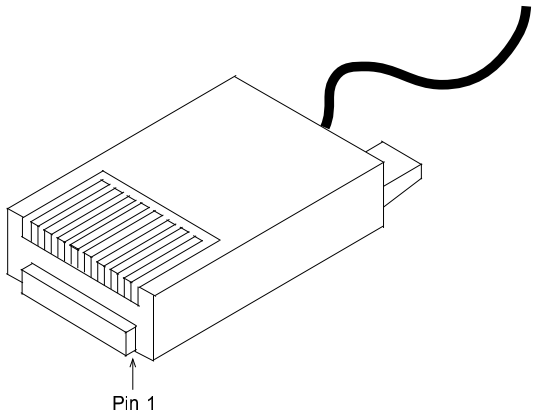


Abbildung 47: RJ45-Stecker

Dieser Stecker ist aus der Telefontechnik bekannt. Er ist sowohl in geschirmter als auch in ungeschirmter Ausführung verfügbar. Tabelle 14 zeigt die Belegung eines 8-poligen RJ45-Steckers.

Kontakt	**Signal**	**Kontakt**	**Signal**
1	Transmit+	5	Nicht benutzt
2	Transmit-	6	Receive-
3	Receive+	7	Nicht benutzt
4	Nicht benutzt	8	Nicht benutzt

Tabelle 14: Belegung der Kontakte beim 8-poligen RJ45-Stecker (100Base Tx)

Fast Ethernet auf Glasfaser (100Base Fx) Der 100BaseFx-Standard legt zur Übertragung der Daten die Glasfasertechnik zugrunde. Benutzt wird ein 2-adriges Glasfaserkabel ($62,5/125\mu m$ oder $50/125\mu m$). Die Länge eines Glasfasersegments beträgt 400 m. Als Standardverbinder stehen beim 100BaseFx-Standard eine Reihe unterschiedlicher Verbinder zur Verfügung:

- Duplex SC-Stecker gemäß ANSI X3T9.5 LCF-PMD Revision 1.3
- Media Interface Connector (MIC). Der MIC-Stecker muß beim 100BaseFx-Standard immer als M-Verbinder kodiert werden.

- ST-Stecker

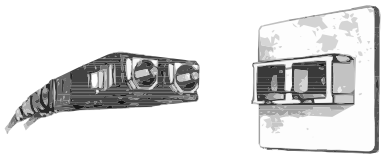


Abbildung 48: Duplex-SC Stecker

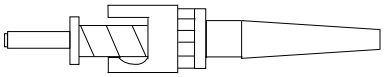


Abbildung 49: ST-Stecker

Fast Ethernet auf Kategorie-3-Kabel (100Base T4) Der 100BaseT4-Substandard gehört zu den neuen Ethernet-Spezifikationen, die im Zuge der Fast-Ethernet Aktivitäten festgeschrieben wurden. Einige bereits aus der 10BaseT-Spezifikation bekannten Strukturen und Definitionen (Twisted-Pair-Verkabelung, RJ45-Stecker) wurden in den 100BaseT4-Standard übernommen. Die Bezeichnung T4 definiert die Anforderungen, die an das Übertragungskabel gestellt werden. Der 100BaseT4 legt zur Übertragung die Kabel der Kategorie-3 (gemäß ISO/IEC 11801) zugrunde. Gegenüber den Kategorie-5-Kabeln weisen die Kategorie-3-Kabel ein wesentlich schlechteres Übertragungsverhalten und Übersprechen auf. Aus diesem Grund schreibt der 100BaseT4-Standard die Nutzung von vier Aderpaaren für die Kommunikation vor. Zur Übertragung wird ein 8B6T-Code verwendet. Jeweils acht Bit werden dabei in einen sechsstelligen Code umgewandelt. Jede Codegruppe wird separat auf einer der drei Datenleitungen übertragen. Die effektive Datenrate auf jeder Datenleitung beträgt somit 33,333 MBit/s. Durch den 6/8-Code wird die 100 MBit/s-Datenrate auf den drei Aderpaaren in 25 MBit/s-Kommunikationskanäle unterteilt. Durch die Verteilung der Datenübertragung auf mehrere parallele Adern ist gewährleistet, daß die Vorschriften zur elektromagnetischen Abstrahlung eingehalten werden. Die Datenübertragung auf dem Kabel erfolgt zusätzlich unidirektional. In der Praxis kann der 100BaseT4-Standard immer nur in Punkt-zu-Punkt-Verbindungen eingesetzt werden. Eine Station kann entweder senden oder empfangen, nie beides gleichzeitig.

Als Übertragungsmedium wurde für den 100BaseT4-Standard ein Unshielded Twisted Pair-Kabel (UTP) mit einer Impedanz von 100 Ohm bzw. 120 Ohm der Kategorien 3, 4, und 5 festgeschrieben. Die Länge eines Twisted Pair-Segments beträgt wie beim 100BaseTx-Standard maximal 100 m. Als Standardverbinder wird ebenfalls die RJ45-Technik (siehe Abbildung 47) verwendet. Tabelle 15 zeigt die Belegung eines 8-poligen RJ45-Steckers.

Full-Duplex-Ethernet Das CSMA/CD-Protokoll wurde ursprünglich auf dem Hintergrund spezifiziert, daß nur ein gemeinsamer Übertragungskanal (Koaxialkabel) zum Senden und Empfangen der Signale zur Verfügung steht. Dies ist bei den modernen Verkabelungssystemen nicht mehr der Fall. Die Nutzung getrennter physikalischer Übertragungsstrecken *(FDX: Full Duplex)* hat für die Ethernet-Technologie und für die Ethernet-Spezifikation erhebliche Konsequenzen:

Kontakt	Signal	Kontakt	Signal
1	TX_D1+	5	BI_D3-
2	TX_D1-	6	RX_D2-
3	RX_D2+	7	BI_D4+
4	BI_D3+	8	BI_D4-

Tabelle 15: Belegung der Kontakte beim 8-poligen RJ45-Stecker (100Base T4)

- Die Protokolle 100Base Fx und 100Base Tx sind bereits in ihrer Grundstruktur Full-Duplex fähig. Das Aushandeln der FDX-Übertragung findet hierbei über den Auto-Negotiation-Prozeß statt, den alle 100Base-X-Produkte beherrschen müssen.
- Zusätzlich muß die durch den CSMA/CD-Mechanismus vorgenommene (segmentweite) *Flußkontrolle (Flow Control)* beim FDX-Ethernet durch lokale Steuerungsverfahren, d.h. zwischen den beteiligten Endkomponenten ersetzt werden (siehe Abbildung 50).
- Problematisch bei der FDX-Ethernet-Übertragung ist, daß diese Funktion lediglich von Endgeräten und Switches wahrgenommen werden kann. Aufgrund des Wegfalls der CSMA/CD-Kompatibilität sind Repeater in einem FDX-Umfeld nicht geeignet.
- Der Einsatz einer Full-Duplex-Übertragung beim Ethernet bedeutet letzlich eine Abkehr vom CSMA/CD-Mechanismus.

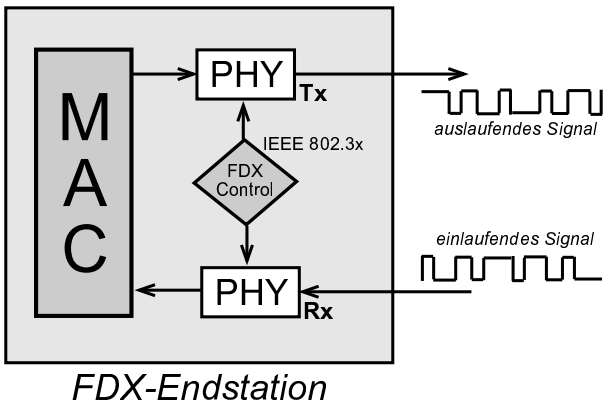


Abbildung 50: FDX-Ethernet-Station mit zwei PHY- und einer FDX-Kontrollinstanz

3.4.5 Gigabit Ethernet – 1000Base

Nachdem für viele Anforderungen LANs mit einer Übertragungsgeschwindigkeit von 10 MBit/s oder 100 MBit/s nicht mehr ausreichen, wurde der neue Ethernet-Standard mit 1000 MBit/s definiert. Die Standardisierung der IEEE-802.3z-Gruppe ist inzwischen abgeschlossen. Beim Gigabit-Ethernet wurde die MAC (Media Access Control) Layer modifiziert. Dies hat direkte Auswirkungen auf die maximale Ausdehnung des Netzes. Aufgrund der Geschwindigkeit wurden neue Anforderungen an die Verkabelung definiert.

Der 1000BaseX Standard unterstützt sowohl die Übertragung von 1000 MBit/s Daten über Glasfaserstrecken (1000Base SX und 1000Base LX) als auch über Twinax-Kabel (1000Base CX). Aufgrund von technischen Schwierigkeiten und einer schnellen Verfügbarkeit des Gigabit Ethernet Standards wurde die Festschreibung des 1000Base-TX-Standards in die IEEE802.3ab-Gruppe abgegeben.

Die Ziele der 802.3z Gigabit Ethernet Task Force waren es, einen Gigabit Ethernet Standard zu entwickeln, der Halb- und Voll-Duplex-Betrieb mit 1000 MBit/s erlaubt, das 802.3 Ethernet Frame Format benutzt, das CSMA/CD-Zugriffsverfahren benutzt und einen Repeater pro Collision Domain erlaubt, rückwärtskompatibel zu 10Base-T und 100Base-T ist.

1000Base SX Bei der Glasfaser-Übertragung des Gigabit Ethernets mit Hilfe der Short Wavelength Technik (850nm Wellenlänge) können die Komponenten mit relativ preiswerten LED-Dioden ausgerüstet werden. Die Short Wavelength Komponenten definieren jedoch nur die Multimode-Glasfaser. Die maximale Reichweite ist je nach verwendeter Faser 260-550m.

1000Base LX Bei der Glasfaser-Übertragung des Gigabit Ethernets mit Hilfe der Long Wavelength Technik (1300nm) werden Laserdioden eingesetzt. Dadurch ist die Übertragung sowohl über Multimode- als auch Monomode-Glasfaserkabel möglich. Mit 1300nm Lasers ist die Reichweite auf dem Faser erheblich besser, weil das Glasfaserkabel bei 1300nm eine geringere Dämpfung und eine geringere Dispersion (Signalverzerrung) als bei der Übertragung mit 850nm aufweist. Die maximale Reichweite ist je nach verwendeter Faser 440-3000m.

Der 1000Base FX-Stecker Grundsätzlich wird bei den Gigabit Ethernet Glasfaserkomponenten der Duplex SC Stecker gemäß den Spezifikationen IEC 61754-4 und IEC 61754-4 Part 4.2 verwendet. Der Duplex-Stecker ermöglicht die Kopplung von zwei LWL-Fasern (Receive und Transmit) in einem Gehäuse. Zwei Keys stellen sicher, daß die Verbindung verwechslungssicher angekoppelt (eingesteckt) werden kann.

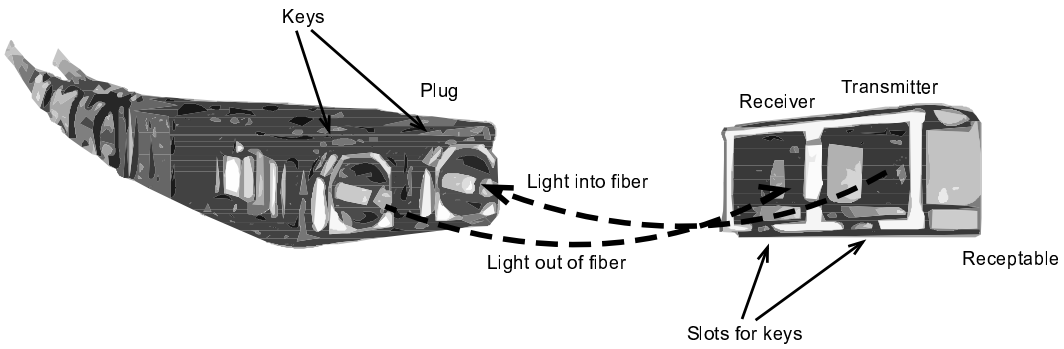


Abbildung 51: Duplex SC Stecker

1000Base CX Neben dem Glasfaserkabel kommt beim Gigabit Ethernet wieder das altbekannte Twinax-Kabel zu neuen Ehren. Mit Hilfe des 1000Base-CX Standards lassen sich ohne komplizierte Kodierverfahren Reichweiten von bis zu 30m über ein Kupferkabel erzielen. Durch die relativ günstige Technik lassen sich die Kosten erheblich unter die Preise von Glasfaserkomponenten drücken. Es wird ein geschirmtes 150 Ohm Balanced Cable nach der

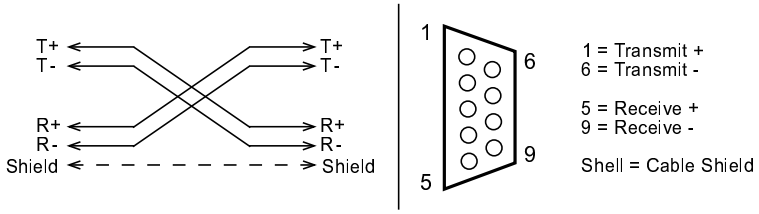


Abbildung 52: Balanced Cable Wiring / 9-polige Sub-D Stecker

Spezifikation ISO/IEC 11801:1995 verwendet. Die Kabel des 1000Base-CX Standards sind immer gekreuzt auszuführen. Als Stecker werden immer 9-polige Sub-D Stecker eingesetzt.

Jedoch wird die 1000Base CX Technik von Fachleuten nur als Übergangslösung angesehen, die durch den 1000Base T Standard (1000 MBit/s auf Kategorie 5 Twisted Pair Kabel; Reichweite 100m) abgelöst wird.

1000Base T 1999 fertiggestellt von der IEEE-Task Force 802.3ab wurde der 1000Base T Standard, der 1 GBit/s über Unshielded Twisted Pair-Kabel der Kategorie 5 überträgt. Damit kann bereits bestehende Kategorie-5-Verkabelung, wie sie in den meisten Unternehmen eingesetzt wird, weiterbenutzt werden. 1000Base T benutzt wie 100Base T ein symbolische Transferrate von 125 Mbaud/s (wegen der 4B5B-Codierung), sendet und empfängt allerdings auf allen 4 Adernpaaren gleichzeitig. Das ergibt die effektive Rate von 1 GBit/s.

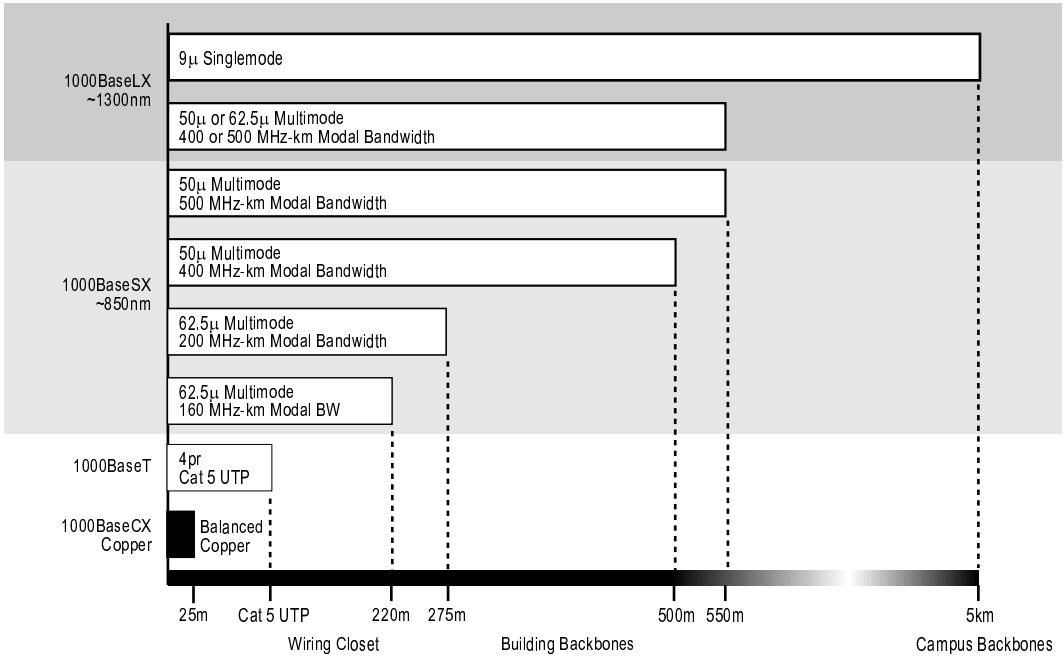


Abbildung 53: Reichweiten-Übersicht 1000BaseX

Weitere Informationen zu Gigabit Ethernet finden sich u.a. auf der Homepage der Gigabit Ethernet Alliance (`http://www.gigabit-ethernet.org`).

3.5 Ethernet-Komponenten

Neben den Netzwerkkarten *(NIC; Network Interface Card)* und dem Kabel gibt es eine Reihe weiterer Komponenten im Ethernet-Umfeld, die zum Aufbau eines Netzes notwendig oder empfehlenswert sind.

3.5.1 Transceiver

Die Bezeichnung Transceiver wird aus den Begriffen *Trans*mitter (Sender) und Re*ceiver* (Empfänger) gebildet. Der Transceiver repräsentiert das Verbindungsglied zwischen dem Übertragungskabel und dem Endgerät. Ein Transceiver läßt sich logisch in drei Funktionseinheiten aufteilen:

- **AUI Interface** Die Verbindung zwischen Transceiver und Endgerät erfolgt immer über das Attachment Unit Interface (AUI). Als Anschlußkabel zum Ethernet Controller des Endgeräts wird ein Transceiver-Kabel verwendet. In den IEEE 802.3-Spezifikationen wurde diese Schnittstelle als 15-polige Sub-D-Steckverbindung mit Schiebeverriegelung festgeschrieben. Die Länge des Transceiver-Kabels ist auf 50 m begrenzt.
- **Transceiver-Logik** Der Ethernet Transceiver enthält einen Leitungstreiber, einen Leitungsempfänger und eine spezielle Schaltung zur Kollisionserkennung. Ein Transceiver gewährleistet darüber hinaus auch noch eine galvanische Trennung der Endgeräte vom Übertragungsmedium. Dadurch wird sichergestellt, daß Störimpulse (Schaltspitzen, Blitzschlag) im angeschlossenen Endgerät keinen Schaden anrichten
- **Physikalisches Netzwerk-Interface/Netzschnittstelle** Bei der Netzschnittstelle unterscheiden sich die Transceiver entsprechend dem verwendeten Netztyp. Man unterscheidet im Basisbandbereich drei Anschlußtypen: Koax-Ethernet, Twisted Pair und Glasfaser.

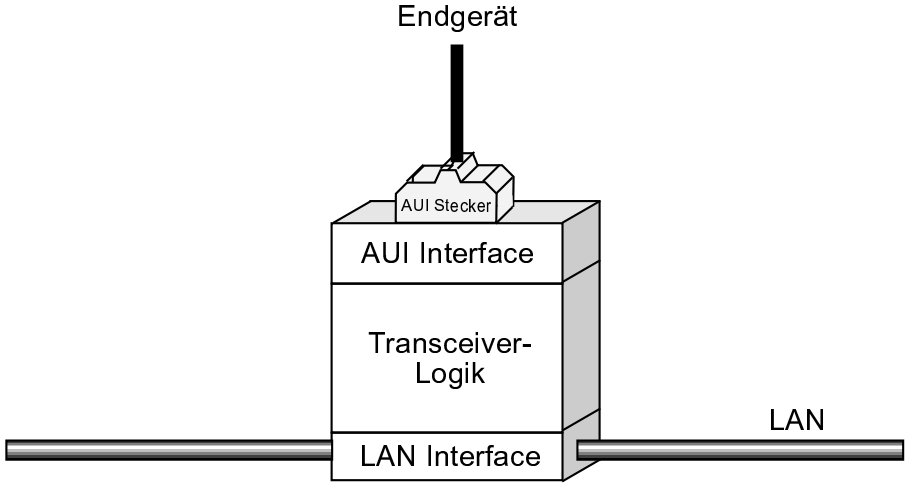


Abbildung 54: Funktionseinheiten eines Transceivers

Funktionen des Transceivers
Der Transceiver erfüllt als Funktionseinheit zwischen dem Endgerät und dem Übertragungsmedium verschiendene Aufgaben:

- **Senden und Empfangen der seriellen Bitströme** Das Endgerät überprüft vor dem Sendevorgang, ob das Übertragungsmedium zur Datenübermittlung frei ist. Bei belegtem Medium wird die Übermittlung der Informationen zurückgestellt. Alle Daten, die vom Medium empfangen werden, werden vom Transceiver direkt auf die Empfangsleitung gegeben und über das Ethernet Dropkabel an das Endgerät weitergeleitet.
- **Kollisionserkennung** Durch den CSMA/CD-Mechanismus kann es geschehen, daß zwei oder mehrere Stationen gleichzeitig feststellen, daß das Medium frei ist. Danach greifen diese Stationen auf das Medium zu und übermitteln ihre Daten. So überlagern sich zwangsläufig die elektrischen Signale auf dem Medium. Die auf das Kabel gesendeten Informationen gehen durch die Überlagerung der Signale verloren. Das führt dazu, daß sich der Strom und die Spannung auf dem Kabel erhöht. Diese Erhöhung wird von der Kollisionserkennung im Transceiver ausgewertet.
- **Heartbeat** Der Heartbeat eines Transceivers dient dazu, einem Endgerät mitzuteilen, ob der jeweilige Transceiver noch funktioniert. Dieses Signal wird im Abstand von $0,6\mu s$, nachdem ein Datenpaket auf das Medium übertragen wurde, über die Kollisionsleitung an das Endgerät übermittelt.

In den meisten Ethernet-Technologien ist der Transceiver auf der Netzwerkkarte untergebracht, lediglich bei 10Base5 ist die Trennung Netzwerkkarte/Transceiver tatsächlich physikalisch existent.

3.5.2 Repeater

Beim Übergang zwischen zwei Ethernet-Substandards (z.B. 10Base5 $\leftrightarrow$ 10Base2, 10Base5 $\leftrightarrow$ 10BaseT) muß gemäß dem IEEE 802.3-Standard die Kopplung durch einen Repeater erfolgen. Ein Repeater arbeitet auf der untersten Schicht, der physikalischen Schicht, des OSI-Referenzmodells; sie sind demnach hardware-orientierte Produkte. Zum Betrieb eines Repeaters werden keine Software-Komponenten benötigt. Es erfolgt nur die reine Signalregenerierung der Bitströme. So kann ein Repeater auch nicht zur Kopplung unterschiedlicher Zugriffsverfahren (z.B. Ethernet $\leftrightarrow$ Token Ring) verwendet werden. Diese Kopplung erfolgt mit Hilfe einer auf der Schicht 2 arbeitenden Translation Bridge.

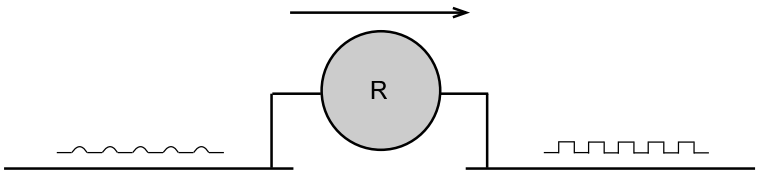


Abbildung 55: Aufbereitung der Signale

Jedes Signal wird bei einem Repeater – ohne Rücksicht auf Verluste – auf die angeschlossenen Netzsegmente übertragen. Ein Repeater dient ausschließlich der Anpassung und der Regenerierung von Signalen. Repeater werden auch zur Verlängerung von Ethernet-Segmenten verwendet. Dadurch lassen sich innerhalb einer Kollisionsdomäne die reinen Kabelrestriktionen umgehen. Mit Repeatern können auch mehrere Segmente miteinander verschaltet werden. Bei diesen Systemen handelt es sich um *Multiport Repeater*. Um Netzfehler zu separieren, können Repeater defekte Netzsegmente automatisch abschalten. Dies verhindert die Beeinflussung anderer Segmente.

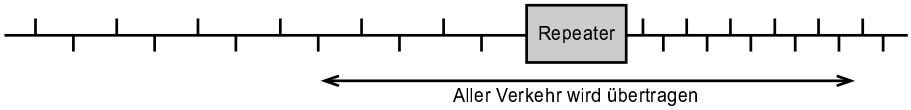


Abbildung 56: Verlängerung der physikalischen Netzsegmente

Repeater werden in zwei Funktionsgruppen eingeteilt: Lokale Repeater und Remote Repeater.

Lokale Repeater
Zur Verlängerung von Ethernet-Segmenten auf der untersten Ebene (10Base5 und 10Base2) können lokale Repeater eingesetzt werden. Zur Kopplung von Netzsegmenten mit Hilfe von lokalen Repeatern gelten zur Ermittlung der maximalen Distanz zwischen zwei Ethernet-Endgeräten diese Regeln:

- Es dürfen maximal fünf Koaxialkabel-Segmente (10Base5-Standard: maximal 500 m) auf dem Kommunikationsweg liegen.
- Zwei der fünf Koaxialkabel-Segmente dürfen nur als reine Link-Segmente benutzt werden (siehe unten).
- Zwischen zwei Ethernet-Endgeräten dürfen maximal vier lokale Repeater auf dem Kommunikationsweg liegen.
- Die Länge der Transceiver-Kabel darf jeweils (bei Endgeräten und Repeatern) maximal 50 Meter betragen.

Remote Repeater
Auch über größere Entfernungen lassen sich Ethernet-Segmente mit Hilfe von Repeatern verbinden. Die Verbindung erfolgt hier über Remote Repeater. Der IEEE 802.3-Standard ermöglicht die Verbindung zweier Koaxsegmente über eine Punkt-zu-Punkt-Verbindung. Diese Verbindungen werden als Link-Segmente bezeichnet. Die Erweiterung des IEEE 802.3-Standards aus dem Jahre 1986 gestattet Glasfaserstrecken zur Realisierung der Link-Segmente. Diese werden dann als *Fibre Optic Interrepeater Link (FOIRL)* bezeichnet. Bei Remote-Repeatern wird die Repeater-Funktion in zwei Repeater-Hälften (Half Repeater) aufgeteilt. Die beiden Repeater-Hälften und das Link-Segment erscheinen als ein einziger Repeater.

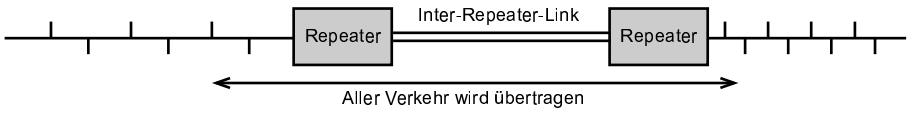


Abbildung 57: Remote Repeater im LAN

Remote Repeater werden eingesetzt, wenn zwei Kabelsegmente über größere Distanzen miteinander verbunden werden sollen. Bei Ethernet-Netzwerken, die mit lokalen und mit Remote Repeatern gekoppelt werden sollen, bestehen zusätzlich zu den o.g. folgende Richtlinien:

- Die Summe aller Längen der Link-Segmente darf 1000 m nicht überschreiten.

- Es dürfen maximal zwei Remote Repeater-Paare auf dem Kommunikationsweg liegen.

Fast Ethernet Repeater
Auch im Fast Ethernet-Standard sind die Funktionen von Repeatern festgeschrieben. Die Fast Ethernet Repeater arbeiten auf der physikalischen Schicht. Sie dienen zur Verbindung von Fast Ethernet-Segmenten (100BaseTx, 100BaseT4 und 100BaseFx). Die maximale Ausdehnung der Segmente hängt in erster Linie von der *Round Trip Propagation-Zeit* ab. Dieser Wert definiert, welche maximale Ausdehnung ein Netzwerkkonstrukt haben darf, damit eine Kollision innerhalb des Sendezeitfensters (Kollisionsfenster) noch als gültiger Wert erkannt wird. Dies wird auch als Kollisionsdomäne oder Collision Domain bezeichnet. Unterschiedliche Kollisionsdomänen, die aus Fast Ethernet- oder Standard-Ethernet-Komponenten aufgebaut sind, werden mit Hilfe von Bridges oder Switches verbunden.

Der Fast Ethernet-Standard unterscheidet zwei Repeater-Klassen:

- **Klasse-I-Repeater** Als Klasse-I-Repeater werden Geräte bezeichnet, die zwischen dem Eingangsport und dem Ausgangsport eine maximale Verzögerungszeit von 168 Bit-Zeiten aufweisen. Die Klasse-I-Repeater werden eingesetzt, wenn unterschiedliche physikalische Standards (z.B. 100BaseTx $\leftrightarrow$ 100BaseFX; 100BaseTx $\leftrightarrow$ 100BaseT4) miteinander kommunizieren sollen. In einem Kommunikationspfad zwischen zwei Fast Ethernet-Endgeräten darf bei Ausnutzung der maximalen Kabellängen immer nur ein Repeater der Klasse I zwischengeschaltet sein.
- **Klasse-II-Repeater** Als Klasse-II-Repeater werden Geräte bezeichnet, die zwischen dem Eingangsport und dem Ausgangsport eine maximale Verzögerungszeit von 92 Bit-Zeiten aufweisen. Die Klasse-II-Repeater werden in Konfigurationen eingesetzt, in denen nur ein physikalischer Standard (z.B. 100BaseTx) verwendet wird. Aufgrund der geringeren Laufzeiten von Repeatern der Klasse II dürfen in einem Kommunikationspfad zwischen zwei Fast Ethernet-Endgeräten – unter Ausnutzung der maximalen Kabellängen – zwei Repeater der Klasse II zwischengeschaltet sein.

Durch die Verkürzung der Kabelstrecken zwischen den Komponenten läßt sich die maximale Verzögerung so weit enschränken, daß weitere Repeater-Komponenten auf dem Kommunikationspfad zwischen zwei Fast Ethernet-Endgeräten geschaltet werden können. Nähere Informationen über die Berechnung der Längen findet man in [69], S. 313ff.

3.5.3 Bridges

Ethernet LANs arbeiten grundsätzlich nach dem Broadcast-Verfahren. Dies bedeutet für die Praxis, daß alle Informationen über das gesamte Netzsegment zu allen Stationen übermittelt werden. Nur die Station, die durch ihre Hardware-Adresse angesprochen wird, wertet die Information aus. Dieser Mechanismus führt dazu, daß der Datenverkehr mit der Anzahl der angeschlossenen Stationen ansteigt. Eine Überlastung des Netzes ist die Folge. In der Vergangenheit genügte es, die einzelnen Ethernet-Segmente über Repeater zu verbinden. Heute werden LAN-Segmente durch den Einsatz von Bridges gekoppelt.

Bridges arbeiten auf der Media Access Control- (MAC) Ebene und teilen ein Datennetz in kleinere, besser überschaubare Einheiten auf. In der Ethernet-Welt werden in der Regel nur transparente Bridges eingesetzt, um LANs zu koppeln. Die Datenpakete werden bei der Übermittlung über Ethernet-Bridges ohne jede Änderung der Datenstruktur weitergeleitet.

Da Ethernet Bridges auf der Schicht 2 arbeiten, übertragen diese Bridges – im Gegensatz zu Repeatern – nicht den gesamten Datenverkehr auf das angeschlossene Netzwerk. Wie in der folgenden Abbildung dargestellt, unterteilen die Bridges das Netz in Kollisionsdomänen

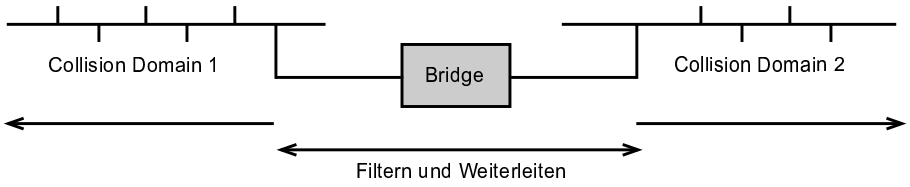


Abbildung 58: Aufteilung in Kollisionsdomänen

Store-and-Forward-Mechanismus
Alle MAC Level Bridges arbeiten auf Basis einer Store-and-Forward-Technologie. Eine Bridge hört alle Datenpakete auf den angeschlossenen LANs mit. Jedes Datenpaket wird vom Ethernet Controller eingelesen und in einem Zwischenspeicher kopiert. Anschließend überprüft die Bridge bei jedem empfangenen Paket die Destination-Adresse. Anhand der Destination-Adresse entscheidet die Bridge, ob dieses Datenpaket an ein angeschlossenes LAN weitergeleitet werden muß, oder ob es sich um lokalen Datenverkehr handelt. Muß ein Datenpaket an ein anderes LAN-Segment der Bridge weitergegeben werden, so wird diese Information and das Memory des Sende-Ethernet-Controller weitergeleitet. Dieser Controller sendet das Datenpaket, sobald das Netzwerk für eine Übermittlung zur Verfügung steht. Die Store-and-Forward-Funktion der Bridge benötigt zur Bearbeitung relativ viel Zeit. Diese Verzögerung wird als *Latency* bezeichnet. Bei normalen Bridges beträgt die Verzögerungszeit etwa 150 - 300 ms.

Learning, Filtering, Forwarding
Eine Ethernet Bridge übermittelt die Datenpakete anhand von gespeicherten Adreßlisten, die durch einen Adressenalgorithmus gebildet werden. Die Bridge liest alle Datenpakete auf den angeschlossenen LANs mit. Bei der Untersuchung der Datenpakete liest die Bridge alle darin enthaltenen Sendeadressen aus. Diese Adressen werden in den jeweiligen Adreßlisten der Ports abgespeichert und als Transporttabellen für die Datenpakete verwendet. Da die Adreßlisten durch das Mitlesen der Quelladressen aller Datenpakete auf den angeschlossenen Subnetzen automatisch gebildet werden, wird dieser Mechanismus auch als *Learning*-Mechanismus bezeichnet. Bridges mit dieser Funktionalität werden auch als selbstlernende Bridges bezeichnet.

Sendet ein Gerät ein Datenpaket auf das Netz, so liest die Bridge diese Informationen ein. Die im Paket enthaltene Destination-Adresse wird mit den Einträgen in den gelernten Tabellen verglichen. Befindet sich ein Eintrag in der lokalen Tabelle, so stellt die Bridge fest, daß sich der Empfänger auf dem lokalen Netz befindet und das Datenpaket wird nicht weitergeleitet. Dieser Vorgang wird als *Filtering* bezeichnet. Findet dieses Modul die Adresse in einem der anderen Adreßtabellen, wird das Datenpaket an den entsprechenden Ethernet Controller der Bridge weitergegeben. Dieser Ethernet Controller vermittelt das Paket auf das lokale Netzsegment. Dieser Vorgang wird als *Forwarding* bezeichnet. Wird kein Eintrag gefunden, so wird eine Kopie des Datenpakets an alle Ethernet Controller der Bridge weitergeleitet. Antwortet ein unbekanntes Gerät auf das empfangene Datenpaket, so wird die darin enthaltene Source-Adresse in die Adreßliste aufgenommen.

Da Ethernet Bridges auf der Schicht 2 (MAC Layer) arbeiten, entkoppeln diese Geräte auf der logischen Ebene zwei Netzsegmente in zwei unabhängige Kollisionsdomänen. Tritt eine Kollision in einem Netzsegment auf, so wird dieses Signal nicht über die Bridge übertragen. Außerdem sind die Signallaufzeiten immer nur für eine Kollisionsdomäne relevant. Im Grunde können Bridges

endlos kaskadiert werden und damit die Reichweite von Ethernet-Netzwerken um ein Vielfaches vergrößert werden. Letztendlich hängt der Timeout der Datenkommunikation dann nur noch von den Timern der Endgeräte ab.

Lokale Bridges
Eine lokale Bridge verbindet zwei oder mehr Ethernet-Segmente. Diese Segmente befinden sich innerhalb eines geographisch eng begrenzten Raums. Lokale Bridges können sowohl physikalisch gleichartige Netzwerke verbinden, als auch Übergänge zwischen verschiedenen Ethernet-Medien schaffen, z.B. Ethernet/Thin Ethernet, Ethernet/Glasfaser-Ethernet.

Remote Bridges
Ähnlich wie Remote Repeater verbinden Remote Bridges entfernt liegende Datennetze. Sie dienen zur transparenten Verbindung entfernt liegender Teilnetze über festgeschaltete Verbindungen (privates oder öffentliches Netz) oder Wählleitungen. Die Datengeschwindigkeit kann je nach Anwendung – und nach Anforderung – zwischen 9,6 KBit/s und 2 MBit/s betragen.

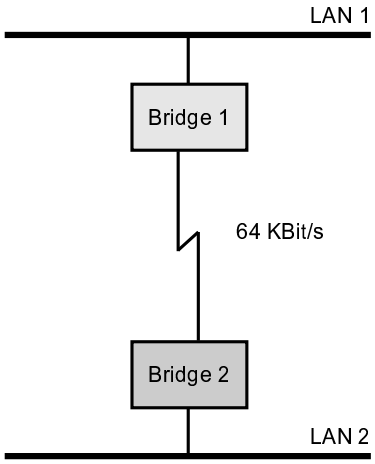


Abbildung 59: Verbindung zwischen LANs über Remote Bridges

Zur Verbindung auf der Schicht 2 zwischen andersartigen LANs (FDDI[15], Token Ring) und dem Ethernet werden aufgrund unterschiedlicher Adreß-, Protokoll- und Paketformate nur Encapsulation Bridges oder Translation Bridges verwendet.

Encapsulation Bridges
Eine Encapsulation Bridge wird nur dann eingesetzt, wenn das Zwischennetz (z.B. FDDI) zwischen zwei Ethernets als reines Transit-LAN verwendet werden soll. Diese Bridges verzichten dann auf die Analyse und Interpretation des Datenverkehrs. Statt dessen werden die empfangenen Datenpakete komplett in ein Datenpaket mit dem anderen Format verpackt und im Transit an eine Ziel-Bridge weitergeleitet. Die Ziel-Bridge analysiert das empfangene Paket und entnimmt das Ethernet-Paket aus dem Datenfeld. Dieses Paket wird anschließend unverändert auf das angeschlossene LAN-Segment weitergegeben. **Translation Bridges**
die direkte Umsetzung von LAN-Datenformaten auf der Schicht 2 erfolgt über Translation Bridges. Jedes Ethernet-/IEEE 802.3-Paket kann grundsätzlich in ein FDDI- oder Token Ring-Paketformat übersetzt werden. Der umgekehrte Weg (FDDI/Token Ring nach Ethernet/IEEE 802.3) bringt jedoch aufgrund der unterschiedlichen Paketlängen einige Probleme mit sich. Token Ring oder FDDI Frames werden daher bei der Übermittlung auf ein Ethernet auf die maximale Größe der Ethernet-Pakete begrenzt.

[15] *Fibre Distributed Data Exchange*

Funktion	Repeater	Bridge
Arbeitsebene	Schicht 1	Schicht 2
Verzögerungszeit	gering	höher
Maximale Kaskadierung	4	unbegrenzt
Lastentkopplung	nein	ja
Redundante Strecken	nein	ja
Fehlerentkopplung	nein	ja
LAN/WAN-Verbund	nein	ja
Filtermechanismen	nein	ja

Tabelle 16: Vergleich zwischen Repeater- und Bridge-Funktionen

3.5.4 Switches

Da neue Technologien relativ teuer sind und oftmals nicht mit den bereits installierten Techniken harmonisieren, werden heute zur Erhöhung der Performance-Anforderungen die traditionellen LANs in mehrere kleinere LAN-Segmente unterteilt. Das heißt, die verfügbare Bandbreite in einem segmentierten LAN setzt sich aus der Summe der einzelnen Bandbreiten in den jeweiligen Segmenten zusammen. Beim Switching erfolgt die Verbindung zwischen den einzelnen LAN-Segmenten über MAC-Level-Devices. Das Ethernet gehört von seinem Übertragungsverfahren her zu der Halbduplex-Übertragungstechnik. Das beim Ethernet eingesetzte CSMA/CD-Verfahren ist in der Lage, alle Kollisionen zu erkennen, jedoch verhindern kann das Verfahren die Kollisionen nicht. Bei Netzen mit vielen Stationen kann es deshalb schon ab einer Last von 40%-50% zu einer erheblichen Zunahme der Antwortzeiten führen.

Bei Ethernet-Technologien, wie 10BaseT, 10BaseF, Fast-Ethernet oder Gigabit-Ethernet befindet sich an einem Kabel durch die Punkt-zu-Punkt-Struktur immer nur ein Empfänger und ein Sender. Diese Funktion wird beim Einsatz von Switches genutzt. Im Prinzip handelt es sich bei Switches um schnelle Multiport-Bridges. Jeder Port verfügt dabei über eine separate Bridge-Funktion. Da der Switch alle an den Ports angeschlossenen Adressen lernt, kann er entsprechend der Ziel- und Absende-Adressen des Datenpaketes eine direkte Verbindung schalten. Jeder Client-Server-Beziehung steht somit ein exklusiver kollisionsfreiher Datenkanal zur Verfügung. Nur so kann auch die Vollduplex-Übertragung genutzt werden. Durch das Multiplexen mehrerer Verbindungen auf einem schnellen internen Bus im Switch (auch *Backplane* genannt) kann die Durchsatzrate der angeschlossenen Endgeräte um ein Vielfaches erhöht werden. Oft beziehen sich die Produktbezeichnungen (z.B. *Gigabit Switch*) auf die Bandbreite der Backplane.

Die Switching-Technologie hat sich in mehrere unterschiedliche Richtungen entwickelt. Die im Markt verfügbaren Switches können in Store-and-Forward- und Cut-Through-Forwarding-Switches unterschieden werden.

Store-and-Forward-Switches
Die auf der Store-and-Forward-Technologie aufbauenden Switches benutzen die gleiche Forwarding-Funktion wie die Bridges. Ein empfangenes Datenpaket wird erst nach dem vollständigen Einlesen weiter verarbeitet. Das resultiert zwangsläufig in einer variablen Einlesezeit und ist außerdem abhängig von der Gesamtlänge des Paketes.

Cut-Through-Forwarding-Switches

Die Cut-Through-Switches starten den Forwarding-Prozeß, sofort nachdem die sechs Byte lange Destination-Adresse von dem Switch-Controller gelesen wurde. Diese Switching-Methode reduziert die Verzögerungszeit zwischen dem Empfangs- und Sendeport dadurch, daß der gesamte Datenrahmen niemals komplett zwischengespeichert werden muß. Die ersten auf diese Technik verfügbaren Switches arbeiteten anhand eines Cross-Point-Matrix-Schemas. Durch dieses Konzept werden mehrere parallele Kommunikationswege zwischen LAN-Segment-Paaren ermöglicht. Der Nachteil dieser Technik zeigt sich bei Punkt-zu-Multipunkt-Kommunikationsbeziehungen (Multicast, Broadcast). Bei Cut-Through-Switches können keine Datenpakete ausgefiltert werden, da diese Switches mit dem Forwarding-Prozeß bereits beginnen, bevor das gesamte Datenpaket empfangen wurde.

Die meisten Switches haben zusätzlich zu den normalen Ports einen designierten *Uplink-Port*. Dieser bietet meist eine höhere Bandbreite als die restlichen und eignet sich vor allem zum Anschluß von Servern oder anderen Switches.

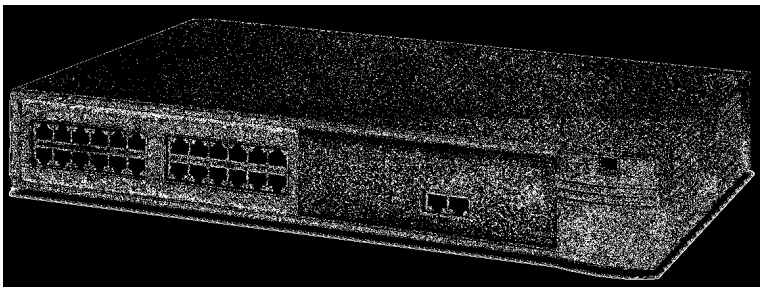


Abbildung 60: 3Com SuperStack II Switch 3300

Layer-3-Switches
Normalerweise wird bei Switches der Datentransport und die Entscheidung, zu welchem Zielport die Daten vermittelt werden sollen, ausschließlich auf der Schicht 2 getroffen. Zur Transportentscheidung wurde die Zieladresse in Form der physikalischen MAC-Adresse genutzt. Da Switches nur flache – von der physikalischen Schicht abhängige Netzstrukturen zuließen, wurden die virtuellen Netze *(VLANs)* eingeführt. Mit der Bildung von virtuellen Netzen war es möglich, Netze unter logischen Gesichtspunkten zu strukturieren. Unter dem Aspekt der Unternehmensorganisation war es beispielsweise möglich, alle Mitarbeiter einer Abteilung zu einer Netzgruppe zusammenzufassen, auch wenn sie auf unterschiedliche Gebäude verstreut waren. Layer-3-Switches treffen nun ihre Transportentscheidung auf Basis der Network Layer. Sie sind daher protokollspezifisch (IP, IPX, AppleTalk, ...) und übernehmen alle Aufgaben eines Routers. Daher werden sie auch *Routing Switch* genannt. Ein großer Vorteil von Layer-3-Switches liegt im Bereich Multicast/Broadcast, da sich deren Ausbreitung nun viel zielgruppenspezifischer einschränken läßt. Für mehr Informationen über Layer-3-Switching sei [36] empfohlen.

3.5.5 Router

Auf der Schicht 3 werden mehrere voneinander getrennte Netzwerke zu einem logischen Gesamtnetzwerk gekoppelt. Es ist Aufgabe dieser Schicht, die dafür notwendigen Adreßfunktionen und die Wegefindung (Routine) zwischen den Datennetzen bereitzustellen. So können logisch strukturierte, hierarchische Netzwerke aufgebaut werden. Bei allen Datennetzen (Ethernet, FDDI, Token Ring) sind nur die beiden unteren Schichten im jeweiligen Standard festgelegt. Ab Schicht 3 werden die Funktionen von den höheren Protokollen, ihren Normen und Spezifikatio-

nen abgedeckt. Zu den bekanntesten Protokollen gehören das *Internet Protocol* (IP), das *Novell Netware-Protokoll* (IPX) und *AppleTalk*. Alle Router arbeiten nur mit einem auf der Schicht 3 angesiedelten Protokoll.

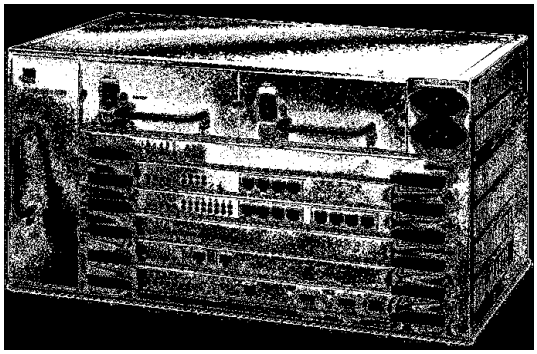


Abbildung 61: 3Com PathBuilder S600

Zur Grundfunktion eines Routers gehört das Auffinden von Wegen innerhalb eines vermaschten Netzwerks. Die Router finden den Weg zu den Nachbar-Routern und zu den Zielnetzen anhand der Routing-Informationen. Diese Routing-Informationen können manuell oder dynamisch über Router-to-Router-Protokolle in den Routing-Tabellen eingetragen werden. In der TCP/IP-Welt können große, vermaschte Netze in einzelne Routing-Domänen unterteilt werden. Innerhalb einer Routing-Domäne verwenden die Router eigene *Interior Gateway Protocols* (IGP). Die bekanntesten IGP-Protokolle sind das *Routing Information Protocol* (RIP) und das *Open Shortest Path First-Protokoll* (OSPF). Die Routing-Domänen propagierten untereinander die Erreichbarkeit von Netzen über Exterior Gateway-Protokolle. Dazu zählen das *Exterior Gateway Protocol* (EGP) und das *Border Gateway Protocol* (BGP). Durch die Aufteilung in verschiedene Routing-Domänen reduzieren sich die Routingupdates zwischen den einzelnen Domänen erheblich.

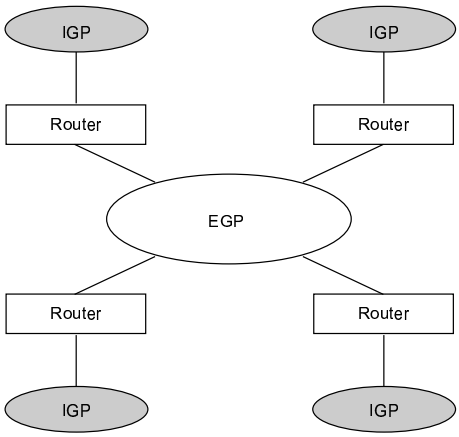


Abbildung 62: Aufteilung in Routing-Domänen

Einsatzgebiete von Routern

Ein Router verbindet zwei oder mehr Datennetze miteinander, indem er auf der Netzwerkschicht eine Adressierung (Anpassung der Adressen) über physikalisch und logisch getrennte Netze hinweg vornimmt. Der Router erscheint den angeschlossenen Geräten als ein selbstständiger Netzknoten. Beim Senden und Empfangen paßt der Router die Datenpakete den netzspezifischen

Gegebenheiten (z.B. Paketlänge, maximale Übertragungszeit) an. Die Daten in einem Router werden nicht einfach transparent durchgereicht, sondern zwischengespeichert und erst in einem weiteren Schritt an den Empfänger weitergereicht. Zur Anbindung von Ethernet und Token Ring an ein FDDI-Netz ist der Einsatz von Routern die effektivste Art der Netzverbindung. Router transportieren – im Gegensatz zu Bridges – keine Hardware-spezifischen Broadcasts auf angeschlossene Geräte.

Weitere Informationen über Routing-Algorithmen und -Protokolle finden sich in [69], S. 401-431.

Funktion	**Bridge**	**Router**
Arbeitsebene	Schicht 2	Schicht 3
Unabhängig vom Netzwerkprotokoll	nein	ja
Abhängig vom höheren Kommunikationsprotokoll	nein	ja
Verbindung Ethernet $\leftrightarrow$ FDDI	möglich	möglich
Verbindung Token-Ring $\leftrightarrow$ FDDI	problematisch	möglich
Verbindung LAN/WAN	problematisch	möglich
Ausfiltern von Netzwerk-Broadcasts	nein	ja

Tabelle 17: Vergleich zwischen Bridge- und Router-Funktionen

3.6 Strukturierte Vernetzung

Durch strukturierte Datennetze wird heute eine universell einsetzbare Kabelinfrastruktur geschaffen. Die Strukturierung erfolgt so, daß innerhab verschiedener Hierarchieebenen Gruppen gebildet werden, die topologisch oder administrativ zusammengehören. Diese Verkabelung ist sowohl bei EN 50173 als auch bei ISO/IEC 11801 standardisiert. Im **Primärbereich** (Gelände-Backbone) werden die einzelnen Gebäude eines Campus über Kabeltrassen verbunden. Der Gelände-Backbone beginnt und endet in sogenannten Gebäudeverteilern. Der **Sekundärbereich** erstreckt sich über den gesamten Gebäude-Backbone, also über die Datenverbindungen, die die Etagenverteiler mit dem Gebäudeverteiler verbindet. Die **Tertiär-Verkabelung** (Endgeräteverkabelung) erfolgt im arbeitsplatznahen Bereich zwischen dem Etagenverteiler und den Endgeräten (Entfernung bis 100 m). Die Endgeräte auf den einzelnen Stockwerken werden im Tertiärbereich über spezielle Anschlußschnüre mit den Datensteckdosen verbunden. Die Datendosen selbst sind mit dem installierten Übertragungskabel Bestandteil der Kommunikationsinfrastruktur. Als Übertragungsmedium setzt man heute in der Anschlußebene ein Übertragungskabel ein, das für den Betrieb der meisten LAN-Übertragungsverfahren geeignet ist, um eine applikationsunabhängige Kommunikationsinfrastruktur realisieren zu können. Die einzelnen Verkabelungshierarchien werden in festgelegten Schnittpunkten miteinander verbunden. Die in den Schnittpunkten eingesetzten Geräte bezeichnet man als Kabelkonzentratoren oder Hub-Systeme. Die heute im Markt verfügbaren Gerätekonzeptionen lassen sich in folgende Komplexitätskategorien einteilen: Stackable-Hubs und modulare Highend-Hubs.

Bezeichnung	**USA**	**Europa**
Geländeverkabelung	campus backbone	Primärbereich
Stockwerksverkabelung	building backbone	Sekundärbereich
Etagenverkabelung	horizontal subsystems	Tertiärbereich

Tabelle 18: Bezeichnungen für Gebäudeverkabelungsstandards

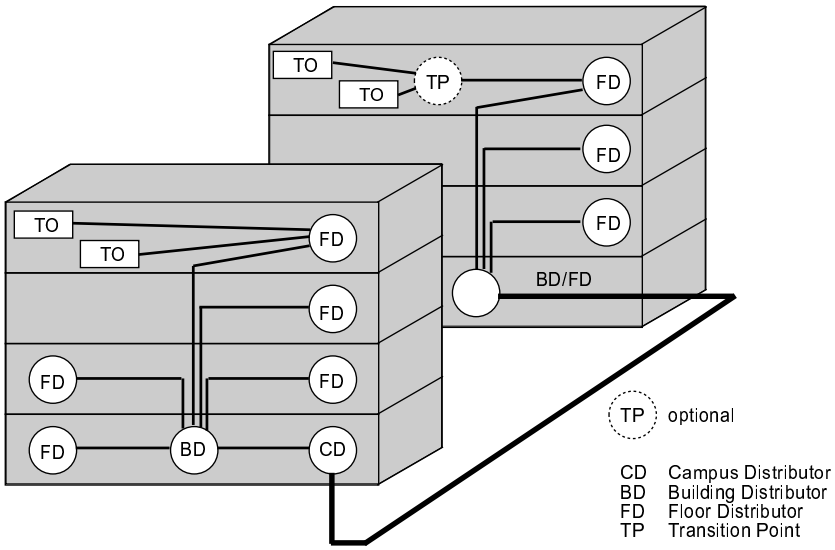


Abbildung 63: Mögliche Ausprägung eines strukturierten Verkabelungssystems

In Abbildung 63 sind die funktionalen Elemente des Verkabelungssystems als Kreise dargestellt. Dies sind die Verteiler der verschiedenen Hierarchieebenen und die Anschlußdosen, die durch die Verbindung untereinander in logisch selbstständige Subnetzwerke aufgeteilt werden. Die Anbindung der Subnetzwerke an das Backbone-Netz erfolgt über Bridges oder Router, die in den Verteilern realisiert sind. Hierdurch ergeben sich folgende Vorteile:

Optimale Nutzung der Backbone-Übertragungskapazität, da nur der subnetzübergreifende Datenverkehr den Backbone belastet. So wird eine Verbesserung des Antwortzeitverhaltens erzielt, die bei Überlastsituationen von Vorteil ist.

Das strukturierte Netz kann durch das Hinzufügen weiterer Netzsegmente problemlos erweitert werden.

Störungen, die in einem Netzsegment auftreten, bleiben auf dieses begrenzt und beeinflussen deshalb die Funktionalität des Backbone-Netzes oder anderer Subnetzwerke nicht. Die Lokalisierung von Fehlerquellen wird wesentlich vereinfacht. Auch bei einem Ausfall des Backbone-Netzes bleiben die lokalen Kommunikationsfunktionen in den Subnetzen erhalten.

Die Leitungslängen für den Primärbereich (CS bis BD) wurden mit 1500 m, für den Sekundärbereich (BD bis FD) mit 500 m und für den Tertiärbereich (FD bis TO) mit 90 m spezifiziert.

3.6.1 Stackable-Hubs

Im LAN-Markt haben sich die Stackable-Hubs aufgrund der Kosten eindeutig durchgesetzt. Der Anwender kann heute Workgroups oder auch kleinere Endgerätekonfigurationen über – im Vergleich zu modularen Hub-Systemen – wesentlich günstigere Stackable-Hubs anbinden. Die Komponenten verfügen über acht bis 24 feste Twisted-Pair oder BNC-Ports. Bei allen Stackable-Hubs werden die einzelnen Geräte über ein separates Kabel miteinander verbunden. Der Vorteil dieser Anbindung besteht darin, daß alle Geräte im Stapel, inklusive aller Ports nach außen nur als ein Repeater wirken. Damit können auf engstem Raum eine Vielzahl von Endgeräten angeschlossen

werden, ohne daß Repeater-Kaskadierungsprobleme auftreten. Bis zu 10 Hubs können in einem Stack mit maximal 260 Ports zusammengefaßt werden. Hierbei können die einzelnen Hubs bzw. Hub-Ports in einzelne voneinander unabhängige Segmente aufgeteilt werden. Auf diese Weise lassen sich potentielle Engpässe schon von Beginn an vermeiden.

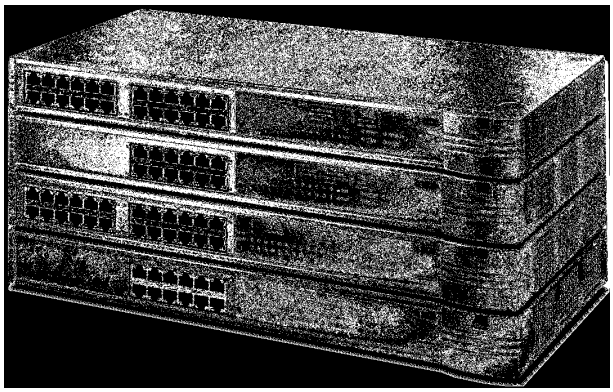


Abbildung 64: 3Com SuperStack II DualSpeed Hub 500

3.6.2 Modulare Highend-Hubsysteme

Die Kategorie der modularen Hubs werden in Datennetzen mit bis zu mehreren hundert Benutzern eingesetzt. Die meisten Hubs in dieser Produktkategorie unterstützen mehrere parallele LANs (Ethernet, Token-Ring, FDDI, ATM). Der Aufbau der Backplane ermöglicht es, die Einschubmodule an mehrere, voneinander unabhängige Bussysteme anzuschließen. So können mehrere physikalisch getrennte Netze über eine Backplane betrieben werden.

Die modularen Konzentrator-Systeme können mit unterschiedlichen Busrückwandsystemen, Stromversorgungen und Modulen bestückt werden. Durch das modulare Design der Grundgehäuse können die Konzentratoren flexibel auf die aktuellen Bedürfnisse zugeschnitten werden.

Das Ganze soll am Beispiel des modularen Switches CoreBuilder 9000 von 3Com[16] verdeutlicht werden (siehe Abbildung 65):

Skalierbarkeit Die Backplane-Kapazität des CoreBuilder 9000 beträgt 560 GBit/s, ein CoreBuilder 9000-Chassis kann 187 Millionen Pakete pro Sekunde verarbeiten. Ein vollausgerüstetes 16-Slot-Chassis unterstützt bis zu 126 Gigabit Ethernet-Ports, 504 Fast Ethernet-Ports, 22 OC-12c oder 88 OC-3c ATM-Ports.

Management Subsystem Simple Network Management Protocol (SNMP) Management Information Bases (MIBs) bieten Zugriff auf detaillierte Informationen über Puffermanagement, Traffic Statistiken, Switch/Router Status Informationen, etc.; Remote Monitoring (RMON)-Unterstützung; HTTP-Server für Browser-gestütztes Management mit grafischem User-Interface.

Verfügbare Module MultiLayer-Switch-Modul (4-12 Ports), Layer-2-Gigabit-Ethernet-Modul (2-9 Ports), Layer-2-Ethernet-Modul (10-36 Ports), ATM-Interface-Modul (2-8 Ports)

[16] `http://www.3com.com/solutions/documents/guides/400346.html`

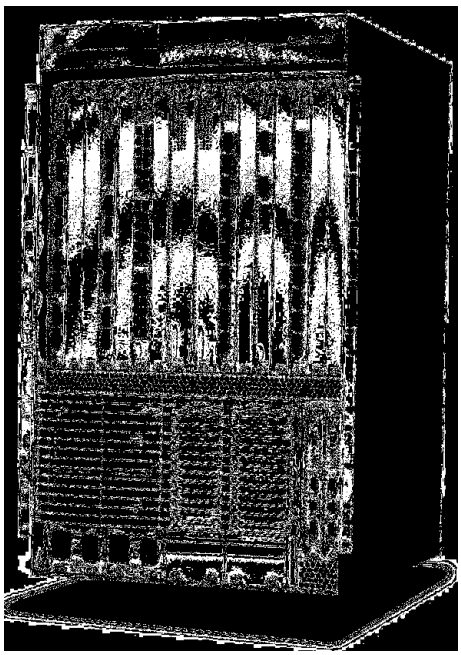


Abbildung 65: 3Com CoreBuilder 9000

Das Haupteinsatzgebiet von solchen Highend-Switches ist sicherlich der Backbonebereich. Das spiegelt sich auch in den Preisen wieder. Tabelle 19 zeigt einen Auszug aus der Preisliste (alles ca.-Verkaufspreise):

16-slot chassis	20.000 DM
820 W AC power supply for 16-slot and 8-slot chassis	6.000 DM
9-port Gigabit Ethernet switch fabric module	13.000 DM
2-port 1000BASE-SX interface module	8.000 DM
9-port 1000BASE-SX switching module	27.000 DM
36-port 10/100BASE-TX switching module	18.000 DM
ATM switch fabric module	37.000 DM

Tabelle 19: Auszug aus der Preisliste CoreBuilder 9000

3.6.3 Beispiel einer Firmenverkabelung

Um nun den praktischen Einsatz der kennengelernten Technologien und Komponenten zu zeigen, sei folgendes fiktives Szenario gegeben:

Die Entwicklungs-Abteilung in München benötigt ihren eigenen Server, da sie viele Daten verarbeitet und hohe Geschwindigkeit benötigt. Jedoch muß die Technik in Hamburg jederzeit auf diesen Server Zugriff haben und evtl. sogar Fehler diagnostizieren. Und natürlich wollen alle Mitarbeiter Zugriff auf das Internet haben.

Wie vernetzt man nun die Abteilungen und Filialen nach derzeitigem Stand miteinander, wenn man auf Zukunftssicherheit, Erweiterbarkeit und Rentabilität achten muß?

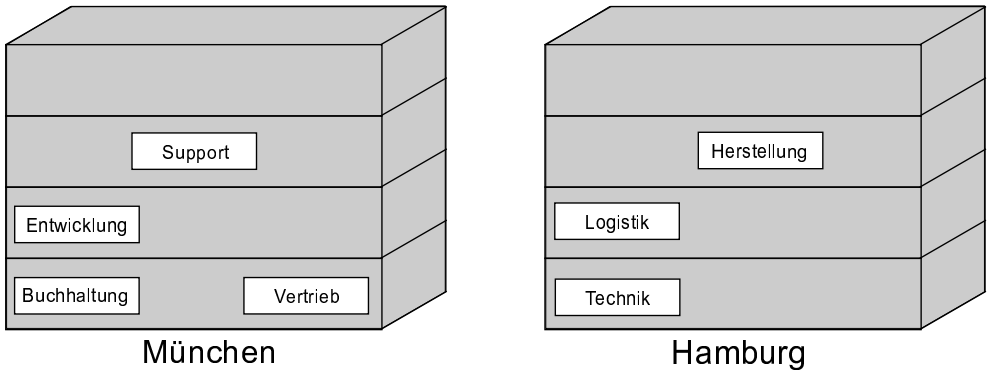


Abbildung 66: Fiktives Unternehmen

Interne Vernetzung
Beschäftigen wir uns zunächst mit der Vernetzung der einzelnen Filialen: Wir haben uns entschlossen, in München zwei und in Hamburg einen Server aufzustellen. Die Arbeitsplatzrechner werden über 100Base Tx angeschlossen (Kosten pro Arbeitsplatz ca. 100 DM). Zusätzlich wird in jeder Abteilung ein Stackable Fast Ethernet Switch (Kosten pro Port ca. 100 DM) mit 1000Base SX-Modul (ca. 2000 DM) aufgestellt. Die Arbeitsplatzrechner werden dann über Kategorie-5 UTP-Kabel an den Switch angeschlossen, die Switches untereinander über Glasfaserkabel (Gigabit-Ethernet) an den Backbone-Switch (Gigabit-Ethernet) vernetzt (pro Port ca. 1000 DM), an dem auch der Hauptserver angeschlossen ist.

Externe Vernetzung
Die beiden Filialen lassen sich über ATM verbinden, z.B. T-ATM von der Deutschen Telekom mit Bandbreiten von 0,5 MBit/s bis 155 MBit/s[17]. Dazu muß in die Backbone-Switches je ein ATM-Modul eingebaut werden (Kosten je ca. 5000 DM). Über T-ATM ist ebenfalls eine Highspeed-Anbindung an das Internet möglich.

Abbildung 67 zeigt nun die fertige Vernetzung des Unternehmens.

Erweiterbarkeit der Vernetzung
Neue Arbeitsplatzanschlüsse lassen sich einfach durch Erweitern der Stackable Switches erreichen, neue Abteilungen lassen sich über zusätzliche Switches problemlos in den großzügig dimensionierten Gigabit Ethernet-Backbone einbinden.

Bei Bedarf kann die Bandbreite der ATM-Verbindung/Internet-Anbindung bei ausreichend finanziellen Mitteln bis auf 155 MBit/s ausgebaut werden. Hierzu ist keinerlei lokale Hardwaremodifikation des Switches/ATM-Moduls nötig. Die ATM-Verbindung eignet sich auch für Echtzeitanwendungen wie Videokonferenzen, da ATM von sich aus eine Quality of Service-Kontrolle besitzt.

In ferner Zukunft können bei Bedarf auch die Arbeitsplatzrechner per 1000Base T ohne Neuverkabelung an die Switches angeschlossen werden. Hierzu müssen lediglich die Network Interface Cards der Rechner ausgetauscht werden (z.Zt. Kosten von ca. 1200 DM je Rechner) und die Switches durch Gigabit-Ethernet-Switches ersetzt werden.

[17]Preise siehe `http://www.dtag.de/angebot/datenkomm/verm_netze/t_net/pdf/preise_atm.pdf`

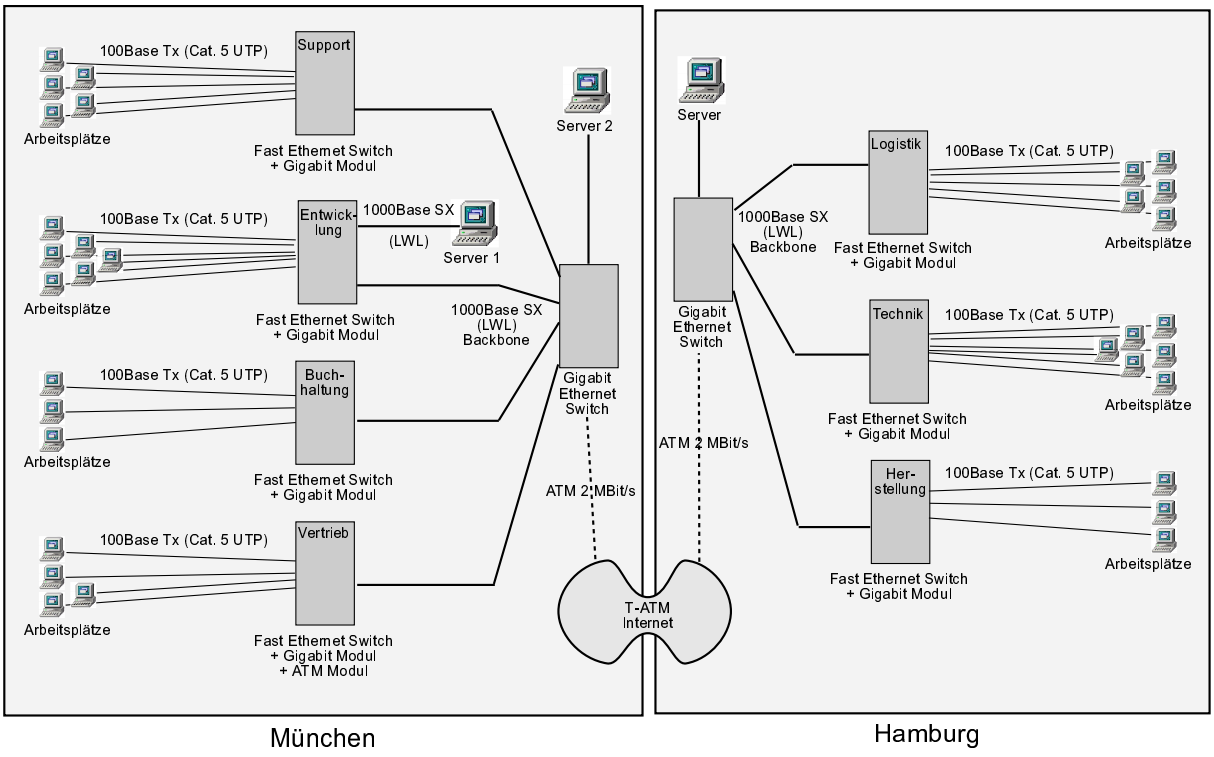


Abbildung 67: Vernetzung des fiktives Unternehmen

3.7 Quality of Service

In der Mitte der 90er-Jahre forcierte sich der Bedarf an garantierter Bandbreite und geringer Verzögerung von Seiten des Netzwerks durch Anwendungen wie Sprach- und Videoübertragung über LANs und WANs, Multicast Software Distribution, usw. Die Standardisierungsorgane reagierten darauf mit neuen Definitionen wie RSVP (Resource Reservation Protocol) und den aktuellen Arbeiten der IEEE 802.1p- und IEEE 802.1Q-Gremien.

Wieso braucht man *Quality of Service*? Solange das Netz nicht überlastet ist, mitunter also noch genügend Bandbreite zur Verfügung stellt, steht einem ja die volle Leistung zur Verfügung. Doch selbst dann kann in ungünstigen Situationen eine zu hohe Verzögerungszeit entstehen, wenn z.B. durch einen Filetransfer ein großes Datenpaket vor dem eigenen Paket in der Warteschlange eines Switches oder Routers hängt. Das kann dann ein Abreißen des Videostroms zur Folge haben. Es geht hier also weniger darum, für seine zeitkritischen Applikationen die gesamte Bandbreite zur Verfügung zu haben, als vielmehr darum, eine garantierte Mindestbandbreite und eine maximale Verzögerungszeit zu haben. Um diesen Anforderungen Rechnung zu tragen, muß der Datenverkehr also priorisiert werden, damit z.B. Pakete von zeitkritischen Anwendungen bevorzugt weitergeleitet werden. Hier sind zwei Ansätze festzustellen:

Bei RSVP schickt die Anwendung eine Anforderung über das Netz, um einen bestimmten QoS-Service zu reservieren, bevor dann der eigentliche Datenverkehr stattfindet. RSVP gewinnt immer mehr Akzeptanz in der Industrie als bevorzugte Methode, Qualität über Netzverbindungen anzufordern und bereitzustellen. Um einer Anwendung mittels RSVP eine gleichbleibende Qualität zu liefern, muß jede Netzkomponente in dem Kommunikationsweg zwischen Server und

Client RSVP unterstützen.

802.1p und 802.1Q bewerkstelligen *Quality of Service* über eine Kennzeichnung der Pakete mit Prioritäts- oder Serviceklasseninformationen. Diese Kennzeichnung erlaubt es der Anwendung, mit anderen Geräten die Priorität der Pakete auszuhandeln. RSVP-Unterstützung kann erreicht werden, indem man RSVP Sessions in 802.1p-Serviceklassen umsetzt.

Quality of Service-Anforderungen/Signalisierungen werden immer über Layer 3 erreicht und sind daher Protokoll-spezifisch. Bis jetzt konzentrieren sich alle Anstrengungen auf das Internet Protokoll (IP), das den Layer-3-Protokollbereich dominiert. Die spezifischen Hardware-Implementationen, wie die tatsächliche *Quality of Service*-Realisierung stattfindet, sind implementationsspezifisch. Cisco z.B. benutzt *WFQ* (Weighted Fair Queueing) und *WRED* (Weighted Random Early Detection).

4 IPv6 & MPLS - Internetprotokolle

4.1 IPv6

4.1.1 Einführung : Hintergründe und Übersicht

Das einheitliche Adressierungsschema des IP-Protokolls ist durch das Internet vorgegeben. Durch die schnelle Verbreitung der TCP/IP-Protokolle und das explosive Wachstum des Internet entstanden jedoch Probleme, die beim Design der TCP/IP-Protokolle vor 25 Jahren nicht absehbar waren. Damals waren Rechnernetze den großen Organisationen vorbehalten. Diese Organisationen verfügten über die nötigen Finanzmittel, um sich einen entsprechenden Rechnerpark leisten zu können. Den Urhebern der IP-Spezifikationen schien aus diesem Grund eine 32-Bit-Adresse absolut ausreichend zu sein. Da sich zu diesem Zeitpunkt niemand vorstellen konnte, daß einmal eine TCP/IP-Workstation auf fast jedem Schreibtisch stehen würde, erschien der Adreßraum als so groß, daß eine Aufteilung in Adreßklassen angeraten schien. Durch diese Aufteilung des Adreßraumes werden die Routing-Tabellen klein gehalten, da nur ein Eintrag pro Netz vorgenommen wird. In der Praxis schränkt dieser Mechanismus die zur Verfügung stehenden Adreßräume jedoch unnötig ein.

Ein Klasse B-Netz verfügt zum Beispiel über maximal 65.534 adressierbare Rechner. In der Realität sind an den Klasse-B-Netzen jedoch wesentlich weniger Rechner angeschlossen. Bei Untersuchungen in Deutschland hat man festgestellt, daß durchschnittlich weniger als 2.500 Rechner an diesen Netzen angeschlossen sind. In der Konsequenz bedeutet dies, daß ein Großteil des zur Verfügung stehenden Adreßraumes verschenkt wurde.

Da die Wachstumsrate des Internet weiter ansteigt und Klasse-B-Adressen kaum noch verfügbar sind, entschlossen sich die für die Adreßvergabe verantwortlichen Behörden nur noch Blöcke von Klasse-C-Adressen zu vergeben. Der Nachteil dieser Verfahrensweise ist, daß für jedes dieser Klasse-C-Netze ein eigener Eintrag in den Routingtabellen notwendig ist. Die Routingtabellen wachsen dadurch stark an und belasten die Router überdurchschnittlich.

Die neue Version des IP-Protokolls trägt den offiziellen Namen IPv6 (auch IPnG genannt). Dieses neue Protokoll entstand aus einer Notlage heraus, da das alte 32-Bit-Adressierungsschema der IPv4 mittelfristig dazu führen würde jedes Wachstum im Internet drastisch zu begrenzen. Aus diesem Grund ist das IPnG (IP Next Generation) der logische Schritt auf dem Weg der IP-Evolution. IPv6 kann jederzeit als reiner Software-Update auf den IP-Komponenten eingerichtet werden. Die Betreiber des Internet sorgten dafür, daß die bisherige IP-Version weiter betrieben werden kann, und nicht zu einem bestimmten Datum die Migration vollzogen sein muß. Die IPnG-Protokollspezifikation kann sowohl auf schnellen Datennetzen (z.B. ATM) als auch langsamen Medien (z.B. Funk-LAN's) eingesetzt werden. Darüber hinaus wurde eine Reihe von Funktionen integriert, die die für eine zukünftige Internet-Plattform von Bedeutung sind.

4.1.2 IPv6 und IPv4 im Vergleich

Die neuen Funktionen von IPv6([48]) beseitigen einige Engpässe, die sich im Betrieb des alten IPv4-Protokolls ergeben haben. Bestimmte Funktionen, die das IPv4 unterstützte, die jedoch aus praktischen Gründen in keiner Implementation unterstützt wurden, sind in der IPv6-Version nicht mehr enthalten. Die wesentlichen Unterschiede gegenüber der alten Version beziehen sich auf folgenden Punkte:

- Erweiterte Routing- und Adressierungsfunktionen

Die IP-Adressen werden beim IPnG von 32 Bits auf 128 Bits vergrößert. Dadurch werden hierarchische Adreßschemata unterstützt. Innerhalb der Adreßgruppe kann dadurch eine wesentlich größere Zahl an Rechnern unterstützt werden. Durch einen neuen Adreßtyp, die sogenannten Cluster-Adressen, können die Netze in topologische Regionen unterteilt werden.

- Vereinfachung des Header-Formats

  Bereits in der IPv4-Version wurden einige Header-Felder nur selten benutzt. Um die Übermittlung der IP-Daten notwendige Bandbreite so gering wie nur möglich zu halten, wurden in der neuen IPnG-Version alle unnötigen Header-Felder eliminiert. Obwohl in der IPnG-Version die Adreßfelder viermal länger sind als bei der alten Version, ist der gesamte Header nur doppelt so lang wie bei IPv4.

- Flexibilität bei der Unterstützung von Optionen

  Die IP-Header-Optionen können in der Zukunft wesentlich einfacher integriert werden. Durch einfache Erweiterungen des Header-Formats können neue Optionen jederzeit eingeführt werden.

- Quality-of-Service

  Durch neue Steuerungsfelder im Header können die Datagramme zwischen dem Sender und dem Empfänger anhand bestimmter Qualitätsparameter gesondert übermittelt werden. Dies wirkt sich besonders bei der Übermittlung von Multimedia-Applikationen (Real-Time-Anwendungen) aus.

- Authentication und Privacy

  In der neuen IPnG-Version wurden die Bedürfnisse der heutigen Kommunikationsstrukturen berücksichtigt. Aus diesem Grund wurden Funktionen wie z.B. Authentication, Datenintegrität und Sicherheit implementiert.

4.1.3 IPv6-Adressen

Die allgemeinen Adressierungskonzepte des IPv6-Protokolls bleiben gegenüber IPv4 unverändert. Jedes IP-Paket wird für sich adressiert und unabhängig von den anderen übertragen[18]. Das IP-Datagramm hat eine maximale Länge von 65.535 Byte. Der richtige Empfang eines IP-Datagramms wird nicht bestätigt, was auch als nicht zuverlässige Übertragung bezeichnet wird. Eine Bestätigung des Empfangs eines Paketes kann aber von der oberen Schichten übernommen werden.

Das IP-Protokoll sichert eine Übertragung eines Paketes zum Computer des Empfängers, der durch seine IP-Adresse identifiziert wird. Diese Adresse zeigt die Werte der vier Bytes, die im Header des IPv4-Paketes die Adresse des Absenders bzw. des Empfängers in binärer Form darstellen. Der Empfänger eines IP-Datagramms wird durch das Interface der IP-Schicht zur darunterliegenden Link-Schicht identifiziert. Dadurch wird zugelassen, daß ein Computer über mehrere Interfaces verfügt.

Eine IPv6-Adresse ist demzufolge ein Identifikator eines Interfaces oder einer Gruppe von Interfaces. Es existieren drei IPv6 Adreßtypen:

[18] Es wird noch weiter unten das Konzept der «Flow Labels» erläutert, bei deren Verwendung einzelne Datagramme nicht mehr voneinander unabhängig übertragen werden

- Unicast

  Dieser Adressentyp stellt einen Identifikator für ein Interface dar. Ein Datagramm an eine Unicast-Adresse wird an das durch die Adresse identifizierte Interface zugestellt. Jedes Interface einer Station kann zu ihrer Identifizierung genutzt werden.

- Anycast

  Der Adressentyp ist ein Identifikator für eine Gruppe von Interfaces. Ein Datagramm an eine Anycast-Adresse wird an eines der Interfaces aus der Gruppe zugestellt, normalerweise an das Interface mit dem kleinsten Abstand laut Routingtabelle. Dadurch läßt sich ein Service auf mehreren Computer implementieren, wobei über Anycast eine Aufteilung der Service-Anforderungen (Lastausgleich) erzielt werden kann.

- Multicast (Rundsenden)

  Dieser Adressentyp stellt einen Identifikator einer Gruppe von Interfaces dar. Ein Datagramm an eine Multicast-Adresse wird an alle Interfaces dieser Gruppe zugestellt.

Die IPv6-Adressen werden nicht dem Computer zugeordnet, sondern einem oder mehreren Interfaces. Einem Interface können aber mehrere IPv6-Adressen zugeordnet werden.

Routing ist eine weitere Funktion der IP-Schicht, die in enger Verbindung mit der Adressierung steht. IPv6 behält das Routingkonzept von IPv4 bei. Der lokale Computer weiß normalerweise nicht welchem Computer die angegebene IP-Adresse gehört. Deshalb delegiert er das IP-Datagramm zu einem lokalen Standort-Router des Netzes. Wenn der Router mit dieser Adresse nichts anfangen kann, wird das Datagramm zu einem der Router der benachbarten Netze weitergeleitet usw.

Allgemeine Form IPv6 hat die IP-Adresse auf 16 Byte erweitert. eine IPv6-Adresse([71]) wird normalerweise als Folge von acht 16-Bit-langen Zahlen dargestellt, z.B.

0000:0000:0000:3210:0123:4567:89AB:CDEF

oder

7100:0000:0000:3210:0123:4576:89AB:CDEF

Wenn eine oder mehrere sequentielle Zahlen am Anfang, am Ende oder in der Mitte der Adresse den Wert 0 haben, können sie einmal durch zwei Doppelpunkte ersetzt werden:

::3210:0123:4576:89AB:CDEF

7100::4576:89AB:CDEF

Eine IPv4-Adresse kann in einem IPv6-Format auf zwei verschiedenen Wegen umgesetzt werden:

1. IPv4-kompatible IPv6-Adresse:

   Die Station unterstützt IPv6, wird aber über IPv4-Netze und Router erreicht. Es wird dynamische Tunneling von IPv6-Datagrammen, eingepackt in IPv4-Datagrammen, vorausgesetzt. Die IPv4-kompatiblen IPv6-Adressen werden durch Setzen der ersten sechs 16-Bit-Zahlen auf 0 dargestellt, z.B.:

   0:0:0:0:0:0:C1AE:1AA1

   oder

   ::C1AE:1AA1

2. IPv4-mapped IPv6-Adresse

   Die Station unterstützt keine IPv6-Adressen, d.h. sie ist eine pure IPv4-Station. Die IPv4-mapped IPv6-Adresse wird durch Setzen der ersten fünf 16-Bit-Zahlen auf 0 und der sechsten 16-Bit-Zahl auf FFFF dargestellt, z.B.:

   0:0:0:0:0:FFFF:C1AE:1AA1

   oder

   ::FFFF:C1AE:1AA1

Die Verwendung der Loopback-Adresse für TCP/IP-Kommunikation zwischen den Programmen eines Computers hat die gleiche Bedeutung wie bei IPv4, lautet aber :

0:0:0:0:0:0:0:1 (::1) statt 127.0.0.1

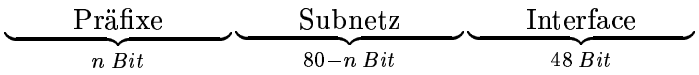
Präfixe Die IPv4-Adresse weist keine Struktur auf. Die IPv4-Adresse wird ferner als undurchsichtig bezeichnet, da der Router keine Hierarchie von Netzen erkennen kann: er leitet das Datagramm weiter und hofft, daß ein weiterer Router die entsprechende Netzwerkadresse kennt. Die anwenderfreundlichere Adreßform über Internet-Namen (z.B. www.informatik.tu-muenchen.de), weist dagegen eine in den meisten Fällen geographische Struktur auf. Solche Adressierung ist aber für den Anwender bestimmt und erfordert den Zugriff auf ein DNS-Server der ihre Übersetzung in die numerische Form übernimmt. Der Router erkennt also diese Struktur nicht.

In ihrer allgemeiner Form sind IPv6-Adressen nicht strukturiert. Eine Strukturierung kann über sogenannte Präfixe erfolgen. Ein Präfix umfaßt die linken Bits der IPv6-Adresse wobei ihre Anzahl durch /(slash) und eine Zahl angegeben wird. Zum Beispiel bedeutet

4567:89AB:CDEF::/40

daß der Präfix 40 Bit umfaßt, d.h. 4567:89AB:CD. Die vordefinierten Präfixe bilden eine Ausnahme - mehr als 80% der IPv6-Adressen sind ohne Struktur, d.h. undurchsichtig.

Zum Beispiel wird in einem LAN die MAC-Adresse als Interface-Identifikator benutzt. Es werden ferner ein Subnetz-ID und weitere Präfixe ermittelt. Die entsprechende IPv6-Adresse wird dann folgende Struktur erhalten:



Beispiel einer Strukturierung einer IPv6-Adresse

Die allgemeine Form einer Strukturierung kann dann mehrere Ebenen beinhalten. Ähnlich wie bei der Strukturierung über Subnetze, wird die Kenntnis der Router über die Strukturierung unterschiedlich sein und von ihrer Position in der Hierarchie abhängen.

Eine Strukturierung kann aber über vordefinierte Adreßtypen - die sogenannten Spezialadressen erfolgen. Die strukturierten Spezialadressen tragen zur Entlastung des Routers und zur Reduzierung des Umfangs der Routingtabelle bei. Die Einführung von geografischen Unicast-Adressen würde weiterhin den Routern erlauben, auf dem kürzesten Weg das Datagramm zur entsprechenden geografischen Region zu leiten. Folgende Unicast-Adressen verdienen in diesem Zusammenhang eine besondere Beachtung:

- Anbieter-basierte Unicast-Adressen:

  Diese Adressen bieten eine grobe geografische Aufteilung.

- Link-lokale Adressen

  Diese Adressen werden für die Kommunikation innerhalb eines LAN's verwendet und spielen bei der Autokonfiguration eine zentrale Rolle.

- Standort-lokale Adressen.

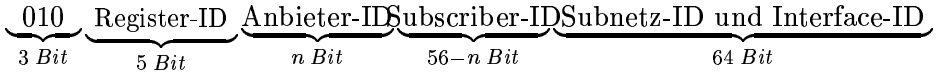
  Diese Adressen sind nur innerhalb eines Standortes gültig und gewinnen im Kontext von betriebsinternen TCP/IP-Netzen besondere Bedeutung.

Anbieter-basierte Unicast-Adressen Die Anbieter-basierten Unicast-Adressen werden bei normalen Point-to-Point Kommunikation benutzt. Diese Adressen werden von einem Register einer großen Region verwaltet. Als Beispiel für ein solches Register kann InterNIC erwähnt werden.

Ein Register-ID bekommt einen Teil des gesamten Adreßraumes. Ein Teil davon wird wiederum einem Anbieter zugewiesen, der seinerseits einen Teil einem Subscriber zuweist.

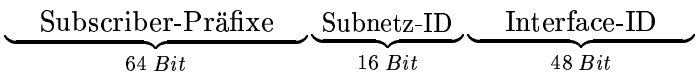
Der Provider-ID wird vorläufig mit n Bits definiert. Dadurch kann das Register selbst entscheiden, welcher Teil seines Adreßraums einem Anbieter zur Verfügung gestellt wird.

Der Subscriber-ID kann wiederum in regionale Subscriber-IDs aufgeteilt werden. Dies kann dem Anbieter erlauben, mehrere topologisch benachbarte Subscriber zusammenzufassen, was zu einem effizienterem Routing führt.



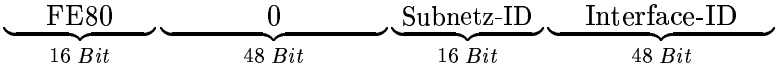
Anbieter-basierte Unicast-Adresse

Der IntraSubscriber-ID kann dann in ein Subnetz-ID, der den physikalischen Link identifiziert, und ein Interface-ID aufgeteilt werden, wie das auch bei IPv4 üblich war. Bei einem IntraSubscriber-ID auf der Basis einer MAC-Adresse nach IEEE-802 werden zwangsläufig 48 Bit für Interface-ID verwendet, so daß die restlichen 16 Bit ein Subnetz-ID ergeben:



Bits-Zuweisung an die Intra-Subscriber-ID auf der Basis einer MAC-Adresse

Linklokale und standortlokale Adressen IPv6-Datagramme mit solchen Adressen können nicht durch das Internet verschickt werden. Die Standort-lokalen Adressen bestehen aus einem 64 Bit-langem Subnetz- und Interfacefeld und können nur zur Kommunikation innerhalb einer Subscriber-ID, d.h innerhalb eines Netzes, genutzt werden.



Standort-lokale IPv6-Adresse

Die Link-lokalen IPv6-Adressen haben nur innerhalb des Adreßraumes des unterliegenden Netzwerkes eine Verwendung. Dies könnte für eine sichere Kommunikation innerhalb eines Bereiches genutzt werden. Die Datagramme werden von keinem Router bearbeitet und weitergeleitet.

Link-lokale IPv6-Adresse

Multicast Durch eine IPv6-Multicast-Adresse ist ein Rechner in der Lage, eine fest definierte Gruppe von Rechnern zu adressieren. Die Multicast-Adressen haben folgendes Format:

IPv6-Multicast-Adresse

Das Flags-Feld dient zur Unterscheidung zwischen permanenten (von IANA vorgegebenen) und temporären Multicast-Adressen.

Der Scope-Identifikator definiert die Bedeutung der Multicast-Gruppe (z.B. global-scope, intra-link-scope, intra-node-scope).

Die vordefinierten Multicast-Adressen werden in folgende Gruppen aufgeteilt:

- All Nodes-Adressen

  FF01::1 - Multicast an alle innerhalb eines Rechners

  FF02::1 - Multicast an alle innerhalb eines Links

- All Router-Adressen

  FF01::2 - Multicast an alle innerhalb eines Rechners

  FF02::2 - Multicast an alle Router innerhalb eines Links

- DHCP-Server/Relay-Agent

  FF02::C - Multicast an alle DHCP-Server und Relay-Agents innerhalb eines Links.

- Solicited Node-Adress

  FF02::1:XXXX:XXXX - Solicited Multicast für Nachbarentdeckung innerhalb eines Links.

Anycast Eine Station, die zu einer Anycast-Gruppe gehört, muß das dem lokalen Router explizit mitteilen. Ein IPv6-Datagramm an die Anycast-Adresse wird dann einer der Stationen dieser Gruppe zugestellt. Dies erlaubt, z.B. einen Dienst auf mehreren Stationen anzubieten, so daß die Clients nur eine auswählen können.

Die Anycast-Adressen bilden einen Teil des Unicast-Adreßraumes, wobei eines der Unicast-Formate genutzt wird, d.h. die Anycast-Adressen sind Unicast-Adressen die explizit konfiguriert wurden. Eine Anycast-Adresse darf nicht als Sender-Adresse in einem IPv6-Datagramm auftreten.

Die Konfiguration von Anycast-Adressen setzt voraus, daß ein gemeinsamer Präfix die Region der Wirkung der Anycast-Adresse definiert wird. Dann wird jede der Anycast-Adressen als separate Eintragung in den Routing-Tabellen auftreten.

Die Anycast Adresse für Subnetz-Router ist vordefiniert und hat folgendes Format:

$$\underbrace{\text{Subnetz-Präfix}}_{n\ Bit}\ \underbrace{0\ldots0}_{128-n\ Bit}$$

Das Format einer Anycast-Adresse

4.1.4 Optionale Erweiterungsheader

Der IPv6 Header ist wie folgt aufgebaut:

Version	Flow-Label	
Payload Length	Next Header	Hop Limit
Source - Adress		
Destination - Adress		

Zum Vergleich wird hier der alte IPv4-Header angeführt:

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment-Offset
Time to Live	Protocol		Header Checksum	
Source Adress				
Destination Adress				
Options				Padding

Das Versionsfeld hat bei IPv6-Datagrammen den Wert 6.

Das Feld «Flow Label» identifiziert einen Strom (flow), d.h. eine Kette von zusammenhängenden Paketen mit gleichem Sender und gleichem Empfänger, die von den Routern gesondert behandelt werden sollen. Solche gesonderte Behandlung könnten z.B. Garantien für QoS oder für Real-Time-Verkehr sein. Die Art dieser Behandlung kann explizit über ein spezielles Protokoll oder durch die Pakete mit dem Flow Label selbst erfolgen. Ein Beispiel dazu wäre die Verwendung des Hop-by-Hop-Headers, um spezielle Steueraktionen zu initiieren.

Das Feld «Payload-Length» bestimmt die Länge des Rests des Paketes nach dem IP-Header, und nicht, wie bei IPv4, die Länge des gesamten Datagramms. Das Feld wird mit 16 Bit kodiert, was einer maximalen Paketlänge von 64 KByte entspricht. Die «Jumbo-Payload»-Option erlaubt es allerdings, Datagramme, die länger sind als 64 KByte, zu übertragen.

Das Feld «Next Header» spezifiziert den Typ des Headers nach dem IPv6-Header. Bei IPv6 werden die sogenannten Erweiterungs-Header verwendet, die nur dann in das Feld «Next Header» einbezogen werden, wenn sie gebraucht werden.

Aufbau Die Erweiterungs-Header sind optional, sie werden aber miteinander verkettet: Jeder Header gibt den Typ und den Abstand zum nachfolgenden an. Der Typ-Code des Headers im Feld «Next Header» wird in RFC 1700 definiert.

Die Erweiterungs-Header können auch semantisch miteinander verbunden sein. Deshalb ist die Reihenfolge der Erweiterungs-Header nach dem IPv6-Header wie folgt festgelegt.

1. Hop-by-Hop-Options-Header

   Nur dieser Header wird, falls vorhanden, von jedem Router behandelt. Bis jetzt wird nur die Jumbo-Payload-Option verwendet.

2. Routing-Header

   Es wird für Source-Routing in IPv6 verwendet.

3. Fragment-Header

   Der Fragment-Header wird nicht von den Routern berücksichtigt und dient nur zur Übertragung von Fragmentierungsinformation zum Empfänger, Er unterstützt dadurch eine Fragmentierung von größeren Paketen nur durch den Sender.

4. Authentication-Header

   Wird zur Übertragung von fälschungssicherer Unterschrift zur Authentifizierung des Senders verwendet.

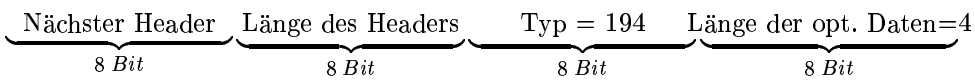
5. Encrypted security payload

   Das ist der letzte der verketteten Header, der teilweise noch im Klartext erscheint. Alle nachfolgenden Daten werden verschüsselt.

6. Destination-Option-Header

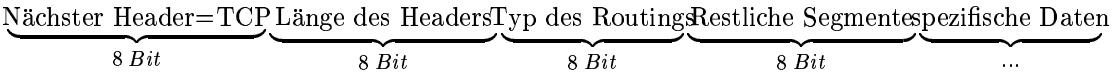
   Es sind nur zwei Felder vorgegeben : nächster Header und Länge des Headers. Alle anderen Felder werden von Anwendungen bestimmt.

Jumbo-Payload Der Jumbo-Payload-Option-Header ist der einzige bis jetzt definierte Hop-by-Hop-Header. Diese Option wird zur Übertragung von Datagrammen mit der Länge größer als 64 KB verwendet. Das Format sieht wie folgt aus:



Jumbo-Payload-Option-Header

Source-Routing Der Routing-Header kann für Source-Routing verwendet werden. Dabei werden ein oder mehrere Zwischenknoten aufgelistet, über die das Datagramm geleitet wird. Der Routing-Header hat folgendes Format:



Der Routing-Header

Zur Zeit wird nur der Routing-Mechanismus mit dem Typ 0 spezifiziert. Die spezifischen Routing-Daten beinhalten eine Strict/Loose Bit-Maske und eine Liste von Router-Adressen, wobei die Adresse des nächsten Routers als Empfängeradresse in den IP-Header eingetragen wird.

Dieses Routing-Konzept stellt eine wesentliche Leistungsverbesserung gegenüber dem IPv4-Source-Routing dar. Der Routing-Header wird nur dann von einem Router bearbeitet, wenn seine eigene Adresse in der Liste ist, und wenn er seine eigene Adresse im Emfängeradressenfeld des IP-Headers erkennt. Er überprüft dann, ob weitere Routeradressen in der Liste vorhanden sind:

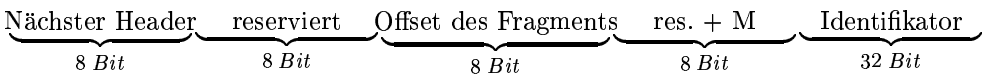
- Wenn weiter keine Router aufgelistet sind, wird mit der Bearbeitung des nächsten Erweiterungs-Header fortgefahren.
- Wenn weitere Router eingetragen sind, wird die nächste Router-Adresse aus der Liste mit der Empfängeradresse im IP-Header ausgetauscht und das Datagramm weitergeleitet. Wenn das Bit 0 im Feld Strict/Loose den Wert 1 hat, muß diese Adresse eine Nachbaradresse sein.

Fragmentierung Eine Fragmentierung von IP-Datagrammen wird vorgenommen, wenn eines der Netzsegmente auf der Route kleinere Pakete als das Datagramm übertragen kann, so daß es zusätzlich in kleinere zusammenhängende Fragmente aufgeteilt wird.

Beim IPv6-Konzept ist nur eine Ende-zu-Ende-Fragmentierung vorgesehen. Der Sender führt, falls notwendig, die Fragmentierung eines Datagramms durch und übergibt entsprechende Informationen an den Empfänger über den Fragment-Header. Der Fragment-Header wird nicht von den Routern berücksichtigt, was eine wesentliche Leistungsverbesserung gegenüber IPv4 darstellt.

Der IPv6-Fragmentierungsalgorithmus ist einfach. Falls ein Segment auf der Route Pakete dieser Länge nicht durchläßt, wird das Paket annulliert und eine ICMP-Fehlermeldung «Packet Too Big» zum Sender mit der Information über die erforderliche Länge zurückgesendet. Der Sender führt dann die erforderliche Fragmentierung durch, trägt sie in den Fragment-Header und sendet erneut das Paket in Form von mehreren Datagrammen. Jedes Datagramm hat den gleichen IPv6-Header, gefolgt von dem Fragment-Header, der das Fragment beschreibt. Für diesen Zweck wird ein 32-Bit-langer Identifikator erzeugt, der die zusammenhängenden Datagramme mit den Fragmenten eindeutig markiert. Jedes Fragment wird unabhängig geroutet.

Der Fragment-Header sieht wie folgt aus:



Der Fragment-Header

In IPv6 erfolgt die Fragmentierung in den Bereichen von über 576 Byte langen Paketen durch die Endknoten. Bei Netzen, die kleinere Pakete als 576 Byte erfordern, sollte die erforderliche Fragmentierung auf der Link-Schicht erfolgen. IPv6-Datagramme dürfen die 576 Byte Grenze nicht unterschreiten. Das Feld «Offset des Fragments» gibt den Offset der Daten in diesem Datagramm bezüglich des Anfangs der fragmentierten Daten in Bytes an. Das letzte Bit M markiert ggf. das letzte Fragment.

Path-MTU-Discovery Oft wird eine Fragmentierung umgangen, indem die obere Schicht, die für die Aufteilung in Pakete verantwortlich ist, sich an die maximal zulässige MTU entlang der Route anpaßt. Dieses wird «Path MTU Discovery»([102]) genannt und wird sowohl bei Unicast- als auch bei Multicast-Adressen auf der Basis des ICMP-Message «Packet too big» durchgeführt. Dadurch wird weiterhin gesichert, daß die Paketlänge aus der oberen Schicht mit der maximal möglichen MTU auf der Route erzeugt wird, was zur Erhöhung der Effizienz beiträgt. Da sich die zulässige MTU der Route dynamisch vergrößern kann, wird periodisch der Versuch unternommen, Pakete mit größeren MTU zu verschicken, um dies zu entdecken. Deshalb muß die IPv6-Schicht die UDP/TCP-Schicht über Veränderungen in der MTU entlang der Route informieren.

4.1.5 Anpassung von höheren Schichten der TCP/IP-Protokollfamilie

Die Änderungen in der IP-Schicht haben ihre Auswirkungen auch in der oberen Schichten der TCP/IP-Protokollfamilie. Außerdem wurde das ICMP-Protokoll um die Funktionalitäten von IGMP erweitert. Dadurch entstand die neue Version von ICMP mit dem Namen ICMPv6.

Die Auswirkung von IPv6 auf die oberen Schichten kann man in zwei wesentliche Gruppen aufteilen:

- Probleme des Übergangs, die bei der Verwendung der bestehenden Dienste mit IPv6 entstehen: Sie sind vor allem mit den Unterschieden in den ICMP-Meldungen, beim Broadcast durch IGMP, bei den Optionen und bei längeren Adressen in IPv6 in Verbindung zu setzen.

  Die Bearbeitung der ICMP-Meldungen erfolgt in vielen Fällen auf der oberen Schicht. Das bedeutet, daß die oberen Schichten, die ICMPv4 nutzen, an die Besonderheiten von ICMPv6 angepaßt werden müssen.

  Der neue Typ «Hop Limit» soll statt «Time To Live» verwendet werden.

- Erweiterte Funktionalität, die IPv6 bietet: Die speziell für IPv6 entwickelten Dienste können deren Vorteile vollständig nutzen. Damit die Anwendungen die volle Funktionalität von IPv6 nutzen können, müssen die Erweiterungen, die IPv6 bietet, berücksichtigt werden.

Die Veränderungen auf der Vermittlungsebene haben auch Veränderungen auf der Transportebene hervorgerufen. Es müssen z.B. größere IP-Adressen berücksichtigt werden, wenn die Prüfsumme der Transportebene berechnet wird. Als weitere Beispiele könnten die Bearbeitung von der neuen ICMP-Meldungen(z.B. Hop Limit statt Time To Live) und Berechnung der Maximum Segment Size als Gegenstand der Verhandlung auf der TCP-Ebene genannt werden.

4.1.6 Duale IP-Stacks und Tunneling

Voraussetzung für den Erfolg von IPv6 ist seine Kompatibilität mit der riesigen Menge von IPv4-Computern und Anwendungen. Die volle Rückwärtskompatibilität wird durch eine Reihe von Mechanismen in den Routern und in den Stationen gewährleistet, die gleichzeitig beide Protokolle, IPv4 und IPv6, betreiben. Diese Mechanismen sind:

- Einführung einer dualen IP-Schicht, die sowohl IPv4 als auch IPv6 unterstützt. Das Interface zu den beiden Protokollstacks wird über zwei verschiedene Socket-APIs gewährleistet.

Das Feld ≪Version≫ im IP-Header des eingetroffenen Pakets gibt an, welcher Protokollstack es bearbeiten soll. Die Anwendung kann die beiden API unterstützen durch Umschalten zwischen den APIs, die gleichzeitig von der Anwendung implementiert werden, bzw. durch Umwandlung eines Socket-Typs in den anderen.

- Einführung von Mechanismen für Tunneling von IPv6 über IPv4(s. [45]). Dabei werden IPv6-Pakete in IPv4-Pakete eingekapselt und über IPv4-Netzwerke übertragen. Die entfernte IPv6-Station erhält das IPv6-Paket wieder. Es werden zwei Tunneling-Arten definiert: konfigurierte und automatische.

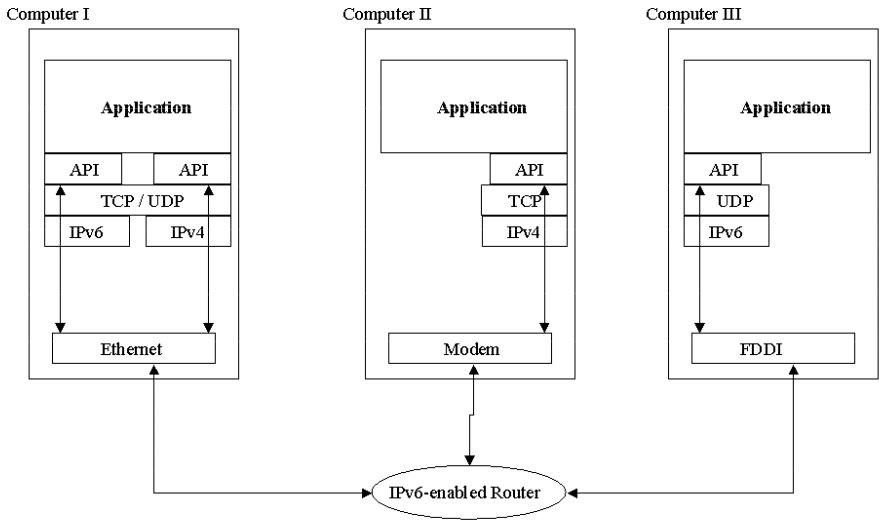


Abbildung 68: Verwendung von dualen IP-Stacks

Die Stationen werden in der Übergangsperiode sowohl das IPv4- als IPv6-Protokoll für Kommunikation über IPv6-Pakete implementieren.

Die IPv6-Stationen können weiterhin kein Tunneling erlauben, vorausgesetzt daß der unterliegende Internet-Router beides, IPv4 und IPv6, unterstützt. Wenn aber einer oder mehrere Router auf der Route nur IPv4 unterstützen, muß ein konfiguriertes und/oder automatisches Tunneling durchgeführt werden.

Die IPv6-Pakete werden bei dem Tunneling in IPv4-Pakete eingekapselt, über das IPv4-Netzwerk übertragen und bei dem IPv6-Empfänger wiederhergestellt. Dieses Szenario stellt ein Ende-zu-Ende-Tunneling mit folgenden Fällen dar:

- Die Sender- und Empfänger-Adressen sind IPv4-kompatible Adressen(z.B. 0::123.2.23.123)
- Die Ende-Adressen des Tunnels sind IPv4-Adressen. Deshalb können die Endpunkte des Tunnels automatisch ermittelt werden.

Es sind drei weitere Arten des Tunneling möglich:

1. Station-zu-Router:

   Wenn das erste Segment nur IPv4 unterstützt, werden beim Sender IPv6-Datagramme in IPv4-Datagramme eingepackt. Der Endpunkt des Tunnels läßt sich nicht aus der IPv4-Adresse ableiten und muß deshalb explizit konfiguriert werden. Dieser Vorgang wird auch als konfiguriertes Tunneling bezeichnet.

2. Router-zu-Router:

   Wenn zwei IPv6-fähige Router über ein IPv4-Netzwerk verbunden sind, können die IPv6-Datagramme in IPv4-Pakete eingekapselt und zum nächsten Router übertragen werden. Der Tunnel hat in diesem Fall die Länge eines Segments (Hops). Diese Art von Tunneling mit den entsprechenden IPv4-Endpunkten des Tunnels wird in den Routern konfiguriert.

3. Router-zu-Station:

   Wenn das letzte Segment ein IPv4-Netzwerk ist, können die IPv6-Datagramme in IPv4-Pakete eingekapselt und zum Empfänger übertragen werden. Der Tunnel hat in diesem Fall die Länge eines Segments. Diese Art von Tunneling mit den entsprechenden IPv4-Endpunkten des Tunnels wird in den Routern konfiguriert.

Diese drei Arten von konfiguriertem Tunneling erfordern, daß an jedem Endpunkt des Tunnels die IPv4-Adresse des anderen Endpunktes bekannt ist, so daß diese Adresse bei der Einkapselung des IPv6-Paketes in den IPv4-Header als Empfänger eingetragen wird. Welches der IPv6-Pakete entsprechend eingekapselt werden soll, wird über die Eintragung in der Routing-Tabelle entschieden. Wenn eine IPv4-Station die Adresse des Routers zum nächsten Backbone-Netzwerk kennt, kann sie eine Default-Route für alle IPv6-Pakete in die Routing-Tabelle eintragen und sie über den Tunnel in das Backbone einführen. Wenn aber mehrere IPv6-Backbone Router bekannt sind, kann eine IPv6-Anycast-Adresse an alle Router verwendet werden, was zu Lastausgleich und Fehlertoleranz des Backbones beitragen kann.

Bei der Einkapselung wird in das Feld «Protokolltyp» des IPv4-Headers 41 eingetragen, die auch für das andere Ende des Tunnels als Indikation verwendet wird, um dieses IPv4-Paket auszupacken und ein IPv6-Paket zu erhalten.

4.1.7 Sicherheit

Die Sicherheitsdienste bei IPv6 werden durch zwei Header gesichert:

- Authentication-Header (AH)

  Dieser Header sichert Integrität und Authentizität, ohne Vertraulichkeit der IP-Datagramme über Verschlüsselung. Dadurch wird erreicht, daß die Einschränkungen mancher Länder für Export oder Verwendung von bestimmten Verschlüsselungsverfahren nicht verletzt werden. Der Router mit einer AH-Implementierung kann dabei einen Sicherheits-Gateway zu einer Sicherheitszone darstellen.

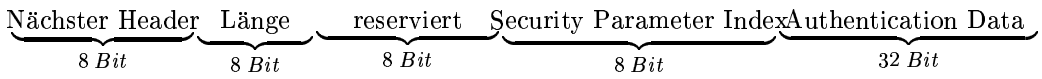
- Encapsulating Security Payload (ESP)

  Dieser Header sichert Integrität, Authentizität und Vertraulichkeit der IP-Datagramme, die zwischen zwei oder mehreren Stationen und Routern ausgetauscht werden. Eine verschlüsselte Kommunikation zwischen zwei Gateways könnte zur Verbindung von zwei Sicherheitsinseln verwendet werden. Dies schließt aber die gleichzeitige Verwendung einer Station-zu-Station-Verschlüsselung nicht aus. Der Router mit einer ESP-Implementierung

kann dabei einen Sicherheitsgateway zu einer Sicherheitszone darstellen. Wenn in einer verschlüsselten Ende-zu-Ende-Kommunikation die Router die Verschlüsselung nicht unterstützen, kann man nur den Inhalt des Datagramms (z.B. TCP- bzw. UDP-Daten) verschlüsseln.

Die beiden Sicherheitsmechanismen können getrennt oder gemeinsam verwendet werden.

Authentication-Header Der IP-Authentication-Header([14]) beinhaltet Information, die zur Authentifizierung des IP-Datagramms dient. Für diesen Zweck wird eine verschlüsselte Signatur über das ganze Datagramm mit einem geheimen Schlüssel berechnet. Bestimmte Felder, die bei Routern verändert werden, werden bei dieser Berechnung nicht berücksichtigt. Der rechtmäßige Empfänger kann diese Signatur entschlüsseln und dadurch die Integrität und die Authentizität der Nachricht feststellen. Um eine Rückwärtskompatibilität zu den älteren Systemen ohne Authentication-Header-Unterstützung zu gewährleisten, wird die Signatur ins eigene Feld übertragen. Die älteren Systeme können dann diese Daten ignorieren.



Der Authentication-Header

IP-Encapsulating Security Payload Der IP-Encapsulating Security Payload ([15]) sichert Integrität, Authentizität und Vertraulichkeit der IP-Datagramme, indem entweder das ganze IP-Datagramm, d.h. dessen Nutzlast (Payload), oder nur die Pakete der Transportschicht in ein ESP eingekapselt werden. Der ESP wird dann verschlüsselt. Im ersten Fall spricht man von einem Tunnel-Modus, im zweiten von einem Transport-Modus.

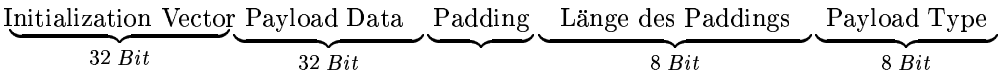
Im Tunnel-Modus bildet das originale Datagramm den verschlüsselten Teil von ESP, wobei der ganze ESP dann über ein Datagramm mit unverschlüsseltem Header übertragen wird.

Im Transport-Modus wird ein ESP-Header direkt nach dem IP-Schicht-Header plaziert. Die IP-Header oder Optionen werden demzufolge nicht verschlüsselt.

Die Verschlüsselung erfolgt auf der Basis eines Schlüssels, der auf der Basis eines Key-Management-Mechanismus vor der Verschlüsselung vereinbart werden soll. Falls der Empfänger über keinen Schlüssel für diese Sicherheitssitzung verfügt, wird die verschlüsselte ESP annulliert und der Fehler in einem Log gespeichert. Der Empfänger antwortet nicht mit einer Fehlermeldung, um eine Dienstblockade seitens eines Eindringlings zu umgehen.

Am ESP kann ein IP-Pseudo-Header angehängt werden, der im Klartext übertragen und von den Routern wie ein normaler IP-Header interpretiert wird. ESP kann zwischen Stationen, einer Station und einem Router oder zwischen zwei Routern betrieben werden. Die Nutzung von ESP ist immer mit einer Leistungsminderung verbunden, die von der konkreten Implementierung, von dem verwendeten Verschlüsselungsverfahren und von der Länge des Schlüssels abhängt. ESP überläßt die Wahl des Verschlüsselungssystems den Anwendern. Alle Systeme im Internet müssen allerdings DES unterstützen.

Der ESP-Header



Der Opaque Transform Data - Feld

4.2 MPLS

4.2.1 Einführung und Motivation

Multiprotocol Label Switching (MPLS [33]) wurde ursprünglich zur Steigerung der Routinggeschwindigkeiten entwickelt und ist zur Zeit eine Technologie, die neue Möglichkeiten für große skalierbare Netzwerke bietet. Einige Beispiele der Bereichen, auf denen MPLS erfolgreich eingesetzt werden kann, sind Traffic Engineering und Unterstützung von virtuellen privaten Netzen.

Es werden an der Stelle einige Beispiele der Anwendung von MPLS näher betrachtet, um einen Überblick über die Möglichkeiten der Technologie zu verschaffen.

Flow-Labels-Konzept bei IPv6 Nun soll ein neues Feature von IPv6 erwähnt werden, das zur MPLS-Unterstützung auf der IP-Ebene verwendet werden könnte.

Das «Flow Label»-Feld (s. auch [107]) des IPv6-Headers kann von einem Sender zur speziellen Markierung bestimmter Pakete verwendet werden. Ein Router im Kommunikationspfad hat dadurch die Möglichkeit, die Route schneller zu ermitteln und die Pakete mit einer entsprechender Priorität zum Empfänger weiterzuschicken. Die Funktion der Flow-Control bzw. der Priorisierung von IPv6 ist eine Neuerung von IP.

Als Flow wird eine Paketsequenz bezeichnet, die von einem bestimmten Senderrechner an eine Unicast- bzw. Multicast-Adresse gesendet wird und deren Senderrechner vorschreibt, daß ein im Kommunikationspfad liegender Router diese Paketsequenz speziell verarbeiten muß. Man kann sich z.B. eine FTP-Session vorstellen, bei der eine große Datei übertragen wird. An der Stelle könnte das Flow-Konzept zum Einsatz kommen, um die Übertragungszeiten zu reduzieren.

Diese spezielle Behandlung kann zwischen dem Sender und den Routern mit Hilfe eines Kontrollprotokolls oder durch Informationen (z.B. als Hop-by-Hop-Option) vereinbart werden, die in das jeweilige Flow-Paket codiert werden. Zwischen einem Sender und einem Empfänger können in der Praxis mehrere parallele Datenströme bestehen. Einige Datenströme enthalten besonders gekennzeichnete Daten (Flows), während anderen Daten kein Flow zugeordnet wurde. Als Flow wird ein individueller Identifikator bezeichnet, der aus der Source-Adresse und dem Flow-Label besteht. Alle Pakete eines Flows werden immer mit dem gleichen «Flow Label» von der gleichen Senderadresse zur gleichen Empfängeradresse übertragen.

Im Feld «Flow Label» können MPLS-Labels untergebracht werden. Durch das «Flow-Label»-Feld ist also eine Unterstützung des Label-Konzeptes von MPLS auf der IP-Ebene gewährleistet.

Weiterleitung Bei MPLS kann Forwarding auf einer exakten Übereinstimmung der (kurzen) Labels basieren, und nicht auf der Übereinstimmung von langen Adressen. Außerdem sind Label-Header, die dabei analysiert werden, klein gehalten. All das führt zur Entlastung der Routern und Steigerung der Übertragungsgeschwindigkeit.

Effizientes explizites Routing Explizites Routing ist eine mächtige Technik, die zu verschiedenen Zwecken genutzt werden kann. Bei konventionellen Routing-Protokollen werden allerdings mit jedem Datagramm sämtliche Angaben zu der Route übertragen, was den Paket-Overhead ziemlich stark vergrößern kann. MPLS erlaubt es jedoch, die explizite Route-Information nur einmal (zur Konfigurationszeit der Route) zu übertragen, die nachfolgenden Datagramme werden mit dem gleichen Label, das das erste Paket erhalten hat, versehen und entsprechend auf dem gleichen Weg weitergeleitet. Dadurch werden die Router auf dem Kommunikationspfad stark entlastet, da weniger Daten verarbeitet werden müssen.

Traffic Engineering Der Begriff «Traffic Engineering» bezieht sich auf Pfadselektierung, in Abhängigkeit von der Auslastung der einzelnen Routen, um einen Lastausgleich (load balance) im Netz zu gewährleisten. «Traffic Engineering» kann in den Netzen, bei denen es mehrere parallele bzw. alternative Wege gibt (z.B. Internet), sehr wichtig sein.

Bei einer großen Anzahl von alternativen Pfaden ist es sehr schwer einen Lastausgleich basierend auf den Metriken, die beim Hop-by-Hop-Routing verwendet werden, zu bewerkstelligen.

MPLS erlaubt es Datenströme von einem Knoten zu einem anderen einzeln zu identifizieren und stellt einen Mechanismus zur Messung der Auslastung zwischen zwei Knoten zur Verfügung. Außerdem ist bei MPLS ein effizientes explizites Routing gegeben.

4.2.2 MPLS-Funktionalität

Die Idee von MPLS besteht in der Generierung von kurzen Labels, die eine fixierte Länge haben. Ein solches Label ist eine kurze Darstellung von dem entsprechenden IP-Header. Man könnte sich ein Label als eine Art PLZ vorstellen, die zur Kurzrepräsentation der gesamten Postanschrift dient. Anhand eines Labels werden dann entsprechend Entscheidungen über die Weiterleitung getroffen.

IP-Pakete enthalten in jedem Datagramm Adressfelder, die von jedem Router bearbeitet werden. In MPLS wird jedes IP-Paket vom sogenannten Edge-LSR (einem MPLS-fähigen Eingangsrouter) samt Label-Daten in ein Datagramm eingekapselt. Der Edge-LSR analysiert den IP-Header des eingehenden IP-Paketes und ordnet dem Paket ein entsprechendes Label zu. Diese Zuordnung kann nicht nur auf der Empfänger-Adresse des Paketes basieren (das könnte z.B. auch QoS sein). Bei allen nachfolgenden Routern im Netz wird das verkapselte Paket anhand des dem Paket zugeordneten Labels weitergeleitet. Sobald das Paket das Netz verläßt wird bei dem letzten MPLS-Router (edge router) das Label wieder entfernt und das Paket in der ursprünglichen Form aus dem Netz weitergeleitet.

In der MPLS-Terminologie heißt jeder Knoten, der MPLS-fähig ist, d.h. die Labels entsprechend behandeln kann, Label Switched Router (LSR).

Es gibt zwei Kategorien von LSR's. An der Grenze des Netzwerkes werden sehr performante Router benötigt, die die ein- bzw. aus-gehenden Pakete schnell klassifizieren und den Paketen entsprechende Labels zuordnen können. Diese Art von Routern werden als Edge-Router bezeichnet. Im Inneren des Netzwerkes werden sogenannte Core-LSR's verwendet, deren Aufgabe es ist, Pakete anhand eines Labels bei extrem hoher Bandbreite weiterzuleiten.

Labels, Label-Stacks und Weiterleitung Ein Label ist, wie erwähnt, eine Kurzdarstellung der Empfängeradresse, die auch einige Parameter (wie z.B. QoS) berücksichtigen kann.

Der Wert eines Labels hat einen streng lokalen Wirkungsbereich, d.h. ein Label hat nur zwischen zwei benachbarten Knoten eine Bedeutung. Die Entscheidungen über die Verwendung von einem Label können allerdings auf globalen Informationen basieren (um z.B. Schleifen zu vermeiden bzw. Ressourcenanforderungen zu befriedigen).

Im Allgemeinen werden Labels verwendet, um die Funktionsweise des System zu optimieren, sie werden aber nicht zur Kontrolle über das System verwendet. Z.B. bestimmt ein Router den Pfad auf dem ein Paket weitergeleitet wird. Die Verwendung von Labels kann den Pfad selbst nicht beeinträchtigen. Sie stellt allerdings solche Möglichkeiten wie «load balancing» und effizientes explizites Routing zur Verfügung.

Der Begriff «Forwarding Equivalence Class» (FEC) wird verwendet, um eine Menge von Paketen, die in der selben Art und Weise weitergeleitet werden, zu bezeichnen. Ein FEC ist also eine Menge von Paketen, die auf das gleiche Label abgebildet werden. Es kann jedoch vorkommen, daß ein FEC auf verschiedene Labels abgebildet wird[19].

Eine einfache Weiterleitungsoperation besteht in der Analyse des eingehenden Labels, um das ausgehende Label und einige zusätzliche Informationen zu bestimmen. Dies wird als «Label Swap» bezeichnet. Wenn ein Datagramm eine MPLS-Domäne betritt, wird mit dem Datagramm ein Label in einem Paket eingekapselt. Dies wird als « Label Push» bezeichnet. Wenn ein Paket die MPLS-Domäne verläßt, wird das Label aus dem Paket entfernt. Diese Operation wird als «Label Pop» bezeichnet. Es wird also von einem Label-Stack gesprochen.

Einkapselung Bei einem Label-basierten Forwarding werden verschiedene Informationen benötigt, z.B. Label bzw. Label-Stack und einige zusätzliche Informationen, wie z.B. TTL-Wert. In manchen Fällen werden diese Informationen in einem MPLS-Header untergebracht, sie können aber auch in Layer2- bzw. Layer3-Headern eingekapselt werden. Die in das Paket eingekapselten Informationen können folgenden Felder enthalten:

- Label
- TTL
- class of service
- stack indicator
- next header indicator
- checksum

Ein TTL-Feld könnte z.B. zur Terminierung von Schleifen benutzt werden. Ein Beispiel zum Einsatz von «class of service»-Feld (COS) wäre die Möglichkeit mehrere Service-Classes in einem Label zu unterbringen. Das MPLS-Header kann auch benutzt werden, um Tunneling zu gewährleisten. Im MPLS-Header muß signalisiert werden, daß mehrere MPLS-Header vorhanden sind. Dies wird durch das «next header indicator»-Feld erreicht. «Stack indicator» und «next header indicator» können optional in einem Feld gehalten werden. Das «checksum»-Feld ist optional.

[19] wenn z.B. kein «stream merge» benutzt wird

Label-Switching (Forwarding- und Steuerung-Komponenten) Ein Label kann auf verschiedene Arten einem Paket zugeordnet werden. An der Grenze eines MPLS-Netzes werden eingehende Pakete klassifiziert und entsprechend weitergeleitet. Alle nachfolgende Knoten im Netz verwenden dann das Label, um entsprechende Forwardingentscheidungen zu treffen. Das Label wird normalerweise bei jedem LSR geändert. An der Grenze des Netzes werden (an einem Edge-Router) bei den ausgehenden Paketen die Labels entfernt und anhand der IP-Adresse weitergeleitet. Falls ein Core-LSR (ein LSR im Inneren des Netzes) ein Paket erhält, wird das Label als Index in der Forwarding-Tabelle verwendet. Falls das Label vorhanden ist, wird das Paket mit einem neuen Label versehen und entsprechend weitergeleitet. Label Switching Forwarding-Tabellen können auf der Knoten-Ebene (eine Tabelle per Knoten) bzw. auf der Interface-Ebene eingesetzt werden (eine Tabelle per Interface).

Das Wichtigste bei einem Label-basierten Forwarding ist, daß es nur einen Forwarding-Algorithmus für alle Switching-Typen gibt, der zur Steigerung der Geschwindigkeit auf Hardware-Ebene realisiert werden kann.

Labels werden bei einem «upstream LSR» einem Paket zugeordnet. Der «downstream LSR», der die Pakete erhält, muß dabei wissen, was er mit den Paketen zu tun hat. Diese Aufgabe wird von der «Switching Control»-Komponente übernommen, dabei werden die Inhalte der Forwarding-Tabelle gebraucht. Diese Komponente ist für die Verbreitung der Routing-Informationen in einer konsistenter Form und die Konvertierung dieser Informationen in die Forwarding-Tabelle zuständig.

Um die Kommunikation mit den konventionellen Routing-Protokollen zu sichern, muß die «Label Switching Control»-Komponente eine Abbildung zwischen FEC's und entsprechenden Adressen zur Verfügung stellen. Zusätzlich muß ein LSR folgende Punkte realisieren:

- Anlegen von Abbildungen zwischen FEC's und Labels
- Verteilung von dieser Abbildungen an andere LSR's.
- Anlegen einer eigenen Forwarding-Tabelle

Die Bindung von einem FEC an ein Label kann entweder daten- (data-driven) oder kontrollgesteuert (control-driven) erfolgen. Bei einer datengesteuerten Bindung wird eine Abbildung erst dann angelegt, wenn sie unmittelbar gebraucht wird. Kontrollgesteuerte Bindung basiert auf den Management-Informationen, die aus den Routing- und Ressourcenallokation-Prozessen gewonnen werden.

Verteilung von Label-Informationen Jeder Eintrag der Forwarding-Tabelle muß Informationen über das nächste Interface (der nächste LSR) und ein Label, das einem FEC von dem LSR zugeordnet wird, beinhalten. Zusätzlich könnte sie z.B. auch einen Indikator für eine Warteschlange enthalten. Einem eingehende Label kann nur ein Eintrag aus der Tabelle entsprechen. Einem Label, das von dem LSR verteilt wird, muß ein Eintrag aus der Tabelle zugeordnet werden. Diese Zuordnung kann entweder von dem LSR selbst unternommen werden oder sie wird von einem anderen LSR verteilt. Die gegenwärtige Version von MPLS benutzt die lokal gebundenen Labels als eingehende und die von anderen LSR's verteilten Labels als ausgehende Labels. Dies wird als «downstream bounding» bezeichnet.

Die Informationen über die Abbildung zwischen den lokal gebundenen Labels und FEC's müssen an benachbarte LSR's verteilt werden, damit die benachbarten LSR's ihre eigene Forwarding-Tabellen aufbauen können. Diese Informationen müssen auch bei Änderungen konsistent gehalten werden.

4.2.3 Case Study

Im folgenden werden Anwendungen von MPLS anhand einiger Beispiele erläutert.

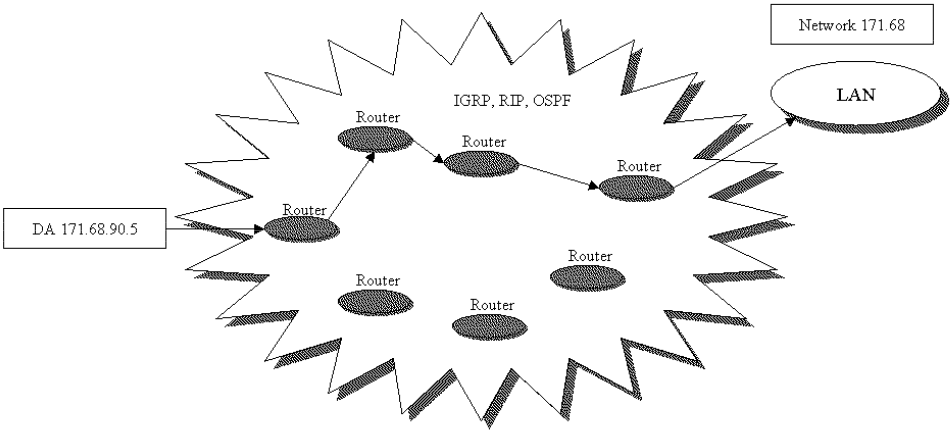


Abbildung 69: Dynamisches Routing

Traffic Engineering Die Dienstanbieter bestimmen immer neue Services, bei denen keine ausreichenden Leistungen in einer IPv4-Umgebung(mit Hilfe von konventionellen Routing-Protokollen)erzielt werden können. Für einen Netzwerkadministrator muß z.B. das Routing-Konzept eine Möglichkeit bieten, den Datenstrom zu kontrollieren. Für explizites Routing kann MPLS eingesetzt werden. Dies kann mittels eines «Label Switched Path» (LSP) realisiert werden. Unter LSP kann man sich einen transparenten Tunnel vorstellen, durch den Datagramme verschickt werden. Der Datenstrom fließt durch den Tunnel in einer Richtung. Dies verschafft den Netzwerkadministratoren eine Kontrolle über den Datenfluß im Netz.

Im Beispiel initialisiert der Rechner «Ennovate Envoy 1600» einen LSP und schickt Datagramme durch das MPLS-Netz an ein LAN.

Virtuelle Private Netzwerke Der Markt der virtuellen privaten Netzwerke entwickelt sich rasant. Die neuen Dienste, die VPNs mit sich bringen, verdrängen die existierenden «line»- und «frame-relay»-Netze.

Es gibt eine Reihe von MPLS-Features, die zur Steigerung der Effizienz beim Einsatz von VPN's beitragen könnten. Einige davon sind z.B.:

- Quality of Service. Die Vorteile des expliziten Routings können den Dienstanbietern eine Abhilfe zur Kontrolle über das Netz verschaffen.
- Viele Firmen verfügen über keine global eindeutigen IP-Adressen, die das IP-Protokoll voraussetzt. Dadurch werden die Kommunikation und das Routing durch öffentliche globale Netze unmöglich. MPLS kann solche nicht eindeutige Adressen in eindeutige Labels verkapseln, und so die Datagramme weiterleiten.

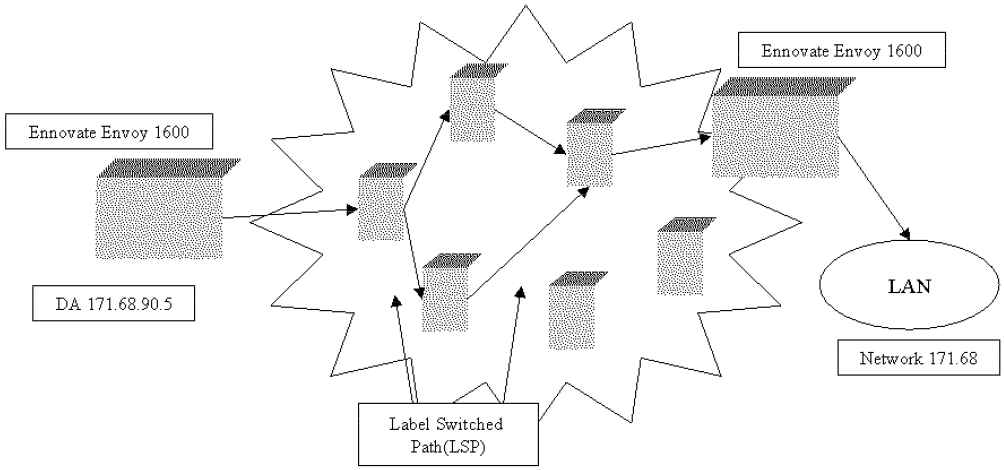


Abbildung 70: Traffic Engineering

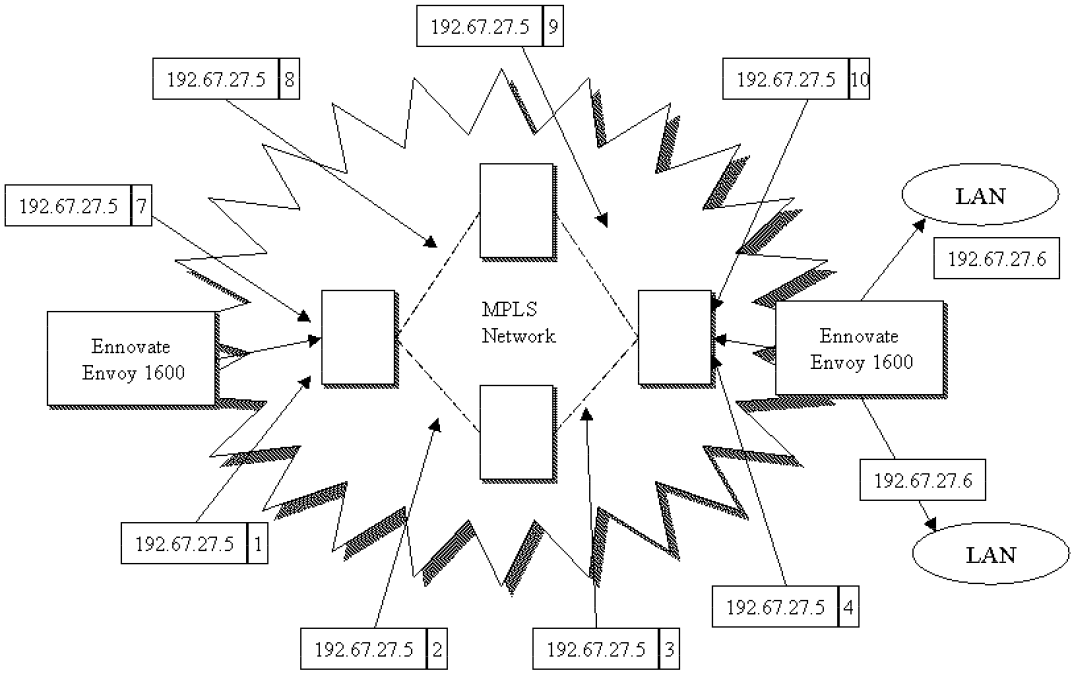


Abbildung 71: Verwendung von MPLS auf VPN's

5 RSVP & IP over ATM - QoS Management

5.1 Einführung

Die Struktur des Internets ist durch seine Entwicklung und die damaligen Anforderungen durch das U.S Department of Defense (DoD) Anfang der 70er Jahre geprägt. Lange Zeit wurde das Internet hauptsächlich für Text orientierte Anwendungen wie Virtual Terminal Sessions oder für non-realtime Aufgaben wie e-Mail oder Dateiübertragung genutzt. Anfang der 90er Jahre wuchs die Anzahl der Rechner und auch der Benutzer im Internet stark an. Diese Entwicklung wurde vor allem durch die Nutzung des WWW mit graphisch orientierten Browsern angetrieben. Anfangs wurden nur Text und Bilder unterstützt, doch durch Erweiterungen der Browser ist es heutzutage möglich, Audio und Video zu empfangen.

Diese Anwendungen stellen allerdings neue Anforderungen an die Leistungsfähigkeit des Internets. Die heutige Internet Architektur TCP/IP transportiert Datenpakete nach dem *best-effort* Prinzip. Im Vordergrund steht die zuverlässige Übertragung der Daten. Quantitativer Quality of Service spielt eine eher untergeordnete Rolle. An Routern werden Datenpakete ohne Priorisierung behandelt. Warteschlangen werden in der Regel nach dem FIFO Verfahren abgearbeitet.

Bei einer starken Belastung des Netzes kommt es zu Verzögerungen, die bei der Abarbeitung der Warteschlangen in den Routern entstehen. Kommt es zu einer Überlastung, d.h. Pakete können nicht mehr in die vollen Warteschlangen aufgenommen werden, dann werden diese Pakete verworfen und müssen erneut übertragen werden, wodurch noch größere Verzögerungen entstehen.

Die große Bandbreite zukünftiger Anwendungen und deren verschiedenartige Anforderungen an das Netzwerk erfordern eine differenzierte Behandlung von Datenpaketen. Zum Beispiel ist bei der Übertragung von Ton und Bild in realtime der Verlust einzelner Pakete zu verkraften, größere Verzögerungen oder der Abriß des kontinuierlichen Datenstroms jedoch gravierend. Im Gegensatz zu Anwendungen wie e-mail oder FTP, die eine zuverlässige Übertragung erfordern, Verzögerungen aber in Kauf genommen werden können.

In dieser Arbeit sollen zunächst die in der heutigen Internet Architektur TCP/IP verwendeten Konzepte zur Realisierung von best-effort Übertragung beschrieben werden. Anschließend wird eine mögliche Erweiterung der Internet Architektur, die sog. *Integrated Services*, erläutert. Dabei liegt der Schwerpunkt auf einer Teilkomponente, dem *Resource Reservation Protocol* (RSVP). Im letzten Abschnitt zu RSVP werden mögliche Vorteile und Probleme bei einer Realisierung von RSVP mit IP über ATM dargestellt.

5.2 Quality of Service in TCP/IP

Wenn TCP/IP auch grundsätzlich dem best-effort Konzept entsprechend entworfen ist, gibt es in IPv4 Ansätze, Pakete für die Abarbeitung in Routern Prioritäten zu verleihen und dadurch einen qualitativen Quality of Service zu realisieren.

5.2.1 Priorisierung von IP Paketen

In IP wird Priorisierung durch das *Type of Service* Feld im Header eines IP Datagrammes ermöglicht ([109]). Damit können verschiedene Stufen von Geschwindigkeit und Zuverlässigkeit angefordert werden. Pakete mit einer höheren Priorität werden in Routern bevorzugt behandelt. Bei Überlastung werden Pakete erst ab einer gewissen Priorität verarbeitet.

Im Type of Service Feld wird die Priorität in 8 Bit festgelegt, von denen 2 Bit für zukünftige Verwendung reserviert sind.

Bits 0-2 In diesem *Precedence Field* kann die Priorität mit einer Zahl zwischen 0 (normal) und 7 (Network Control) gesetzt werden.

Bit 3 Dieses Flag muß mit 1 belegt werden um eine niedrige Verzögerung zu erzielen. Eine Belegung mit 0 bedeutet normale Verzögerung.

Bit 4 Der Datendurchsatz kann mit diesem Flag erhöht werden (1=hoher Durchsatz, 0=normaler Durchsatz).

Bit 5 Die Zuverlässigkeit wird durch dieses Flag geregelt (1=hohe Zuverlässigkeit, 0=normale Zuverlässigkeit).

Die Benutzung eines der Flags Verzögerung, Durchsatz und Zuverlässigkeit ist mit gewissen Kosten verbunden. So hat in den meisten Netzwerken eine bessere Leistung einer der Parameter eine schlechtere Leistung der übrigen Parameter zur Folge.

Das Konzept des Type of Service dient dazu, die Behandlung der Datagramme während ihrer Übertragung durch das Internet zu spezifizieren. Jedem Netzwerk bleibt es jedoch überlassen, wie die Prioritätsangaben umgesetzt werden. In [133] wird beschrieben, daß heutige Router das Type of Service Feld ignorieren und erst mit IPv6 das Type of Service Feld von Routern ausgewertet werden wird.

Im folgenden Abschnitt wird die grundlegende Funktionsweise einer TCP Verbindung, insbesondere das Konzept des *Sliding Window* kurz skizziert und danach die Konzepte der Flußsteuerung zur Vermeidung von Überlastung beschrieben. Eine ausführlichere Beschreibung des TCP Protokolls ist in [128] zu finden.

5.2.2 Funktionsweise von TCP

Auf die von IP angebotene Dienstschnittstelle setzt TCP auf und realisiert eine verbindungsorientierte und zuverlässige Übertragung. Ein wichtiger Bestandteil von TCP ist die Flußsteuerung, die die Reihenfolge der IP Pakete überwacht, bei Paketverlusten eine erneute Übertragung durchführt und den Datenfluß der aktuellen Bandbreite des Netzwerkpfades anpaßt, um Netzwerküberlastung zu verhindern.

Daten werden in TCP als Segmente übertragen. Die Größe der Segmente, die *Maximum Segment Size* (MSS) , wird beim Verbindungsaufbau festgelegt. In der MSS ist die Größe des fixen TCP Headers (20 bytes) nicht berücksichtigt.

Die MSS kann zwischen beiden Kommunikationspartnern vereinbart werden oder wird andernfalls auf einen "Standardwert" gesetzt. Da TCP Segmente jeweils als ein IP Paket verschickt werden und da kein Rechner IP Pakete größer als 576 bytes akzeptieren muß, wird die MSS mit 576 bytes − 20 bytes (IP Header) − 20 bytes (TCP Header) = 536 bytes standardmäßig festgelegt. Größere Segmente sind effektiver, allerdings nur wenn sie nicht aufgeteilt werden. Deshalb ist es wichtig, daß die *Maximum Transfer Unit* (MTU) nicht überschritten wird. Für Ethernet bedeutet dies zum Beispiel, daß MSS bis zu 1460 bytes möglich sind[20].

Die Reihenfolge von Segmenten wird durch Sequenznummern geregelt. Die Nutzdaten (Inhalte des Datenteils eines Segments) einer TCP Verbindung werden durchgehend byteweise numeriert.

[20] bei manchen TCP Implementierungen sind nur MSS als Vielfache von 512 erlaubt

Jedes Segment wird durch eine Sequenznummer im Header identifiziert. Diese Sequenznummer entspricht der Nummer des ersten Bytes im Datenteil.

Da TCP eine zuverlässige Verbindung garantiert, müssen Segmente anhand der Sequenznummern bestätigt werden. Der Segmentheader enthält eine *Acknowledgment* Nummer, die der Sequenznummer des Segments entspricht, das vom Empfänger als nächstes erwartet wird. Damit werden auch alle Segmente mit niedrigeren Sequenznummern bestätigt. Segmente, die als Bestätigung verschickt werden, transportieren aus Effizienzgründen auch Nutzdaten, falls vorhanden (*Piggyback*). In der Hoffnung, Acknowlegments mit Daten füllen zu können bzw. zusätzliche Segmente mit dem selben Acknowledgement bestätigen zu können, ist es laut [28] erlaubt ein Acknowledgement bis zu 500 ms zu verzögern. Die meisten TCP Implementierungen warten maximal 200 ms.

Um das Netz effizient zu nutzen, muß nicht für jedes Segment vom Empfänger eine Bestätigung geschickt werden, und der Sender darf trotzdem Segmente verschicken, obwohl Bestätigungen ausstehen. Wieviele Segmente der Sender verschicken darf, ohne eine Bestätigung für vorhergehende Segmente erhalten zu haben, wird ihm vom Empfänger als sogenannte Window Größe mitgeteilt.

Reduziert sich die Pufferkapazität des Empfängers, dann setzt der Empfänger die Window Größe herab. Dieser Mechanismus wird als ***Sliding Window*** bezeichnet. Durch Veränderung der Window Size kann aber nicht nur Einfluß auf die Flußsteuerung bezüglich der Empfängerkapazität genommen werden, sondern auch bezüglich der Netzkapazität, wie in den folgenden Abschnitten gezeigt wird.

Beim Senden eines Segments wird der *Retransmission Time Out* (RTO) gestartet. Ist nach dessen Ablauf das Segment nicht bestätigt worden, gilt dieses Segment als verloren und die Übertragung dieses Segments wird wiederholt. Als Grundlage zur Abschätzung des RTO dient die *Round Trip Time* (RTT). Zur genauen Berechnung des RTO siehe 5.2.7. Der Verlust eines Pakets kann zwei Ursachen haben:

1. Es liegt ein Übertragungsfehler vor
2. Das Netz ist überlastet und das Paket wurde wegen mangelnder Pufferkapazität gelöscht

Die Wahrscheinlichkeit eines Paketverlusts aufgrund eines Übertragungsfehlers kann bei Netzwerkpfaden in Festnetzen als $\ll 1\%$ angenommen werden. Deshalb gilt ein Segmentverlust als ein Indiz für Netzwerküberlastung (siehe dazu 5.2.3). Diese Annahme gilt nicht in Funknetzen, da dort mit höheren Verlustraten durch Übertragunsfehler gerechnet werden muß.

Jacobson beschreibt in [76] wie im Oktober 1986 das Internet den ersten "Überlastungskollaps" erlebte, so daß die Bandbreite fast um den Faktor 1000 abfiel, zwischen Rechnern die nicht mehr als 300 m und zwei Hops von einander entfernt waren.

Als Folge dieser Feststellung wurde in TCP der Slow Start Algorithmus und Congestion Avoidance eingeführt, sowie Modifikationen bei der Berechnung des RTO vorgenommen, um eine Netzüberlastung zu verhindern.

5.2.3 Slow Start

Die Flußsteuerung von TCP ist durch das Sliding Window Konzept ein selbstgetaktetes System. Im Netz befindet sich immer eine konstante Anzahl von Paketen[21]. Ein neues Paket kann nur

[21] Die Anzahl dieser Pakete entspricht der Window Größe (s. 5.2.2)

dann vom Sender ins Netz eingespeist werden, wenn ein anderes Paket das Netz verlassen hat: Das Netz befindet sich im "Gleichgewicht".

So gut dieses System eine Verbindung am Laufen hält, so kritisch verhält es sich beim Start. Existiert im Pfad einer TCP Verbindung ein Flaschenhals, der die verfügbare Brandbreite stark herabsetzt, dann wird beim Start ein großer Teil von Paketen am Router vor dem "Flaschenhals" verworfen. Der Verlust dieser Pakete hat einen Timeout beim Sender zur Folge und bedeutet die erneute Übertragung dieser Pakete. Dadurch ist die ohnehin kleine Bandbreite des Flaschenhalses auch noch durch eine große Anzahl von erneuten Übertragungen belastet.

Das Konzept des Slow Starts beseitigt diesen Schwachpunkt, indem nach dem Verbindungsaufbau die Window Größe nicht wie vom Empfänger vorgeschlagen festgelegt wird, sondern mit einer Segmentgröße beginnend gesteigert wird.

Die Implementierung von Slow Start gestaltet sich folgendermaßen:

- Eine neue Zustandsvariable `cwnd` (Congestion Window) wird beim Sender eingeführt. `cwnd` wird als bytes gespeichert[22]. Die Anzahl der Segmente ergibt sich aus dem ganzzahligen Anteil, der Division $cwnd/MSS$.
- Beim Start wird `cwnd` auf eine Segmentgröße gesetzt und beim Empfang einer Bestätigung um eine Segmentgröße erhöht.
- Die Anzahl der Segmente, die ohne Bestätigung gesendet werden dürfen, wird durch das Minimum der vom Empfänger verlangten und durch `cwnd` begrenzten Window Größe ermittelt.

Slow Start ist beendet, wenn die Verbindung abgebrochen wird. Ansonsten wird Slow Start fortgesetzt, d.h. `cwnd` wird so lange erhöht bis die Kapazität des Netzes erreicht ist und ein Router beginnt, Pakete zu verwerfen. Dies signalisiert dem Sender, daß das Congestion Window zu groß geworden ist. Wie die Flußsteuerung des Senders auf Paketverluste reagiert, wird in 5.2.4 beschrieben. Zuvor soll Slow Start anhand eines Beispiels verdeutlicht werden.

Abbildung 72 zeigt den Start einer TCP Verbindung zwischen zwei PCs (Linux 2.0.33), die über ein 10 Mbps Ethernet und eine 64 kbps PPP Leitung miteinander verbunden sind (s. Abb. 73). Im Rahmen des Verbindungsaufbaus wird von Rechner2 das SYN Segment 2 bestätigt und damit `cwnd` auf zwei Segmentgrößen erhöht. Die MSS beträgt 1460 bytes. Rechner1 sendet zwei Segmente (Nr. 4, 5). Diese werden beide bestätigt, `cwnd` wird auf drei Segmentgrößen (=4380 bytes) gesetzt. Rechner1 kann drei Segmente senden (Nr. 7, 8, 9), es werden jedoch nur die Segmente 7 und 8 bestätigt. `cwnd` beträgt nun 4mal die MSS, da aber das Segment 9 noch unbestätigt ist, können nur drei Segmente (Nr. 11, 13, 14) von Rechner1 ins Netz eingespeist werden. Die nächste Bestätigung, die Rechner2 schickt, umfaßt nur die Segment 9 und 11. Obwohl die Größe von `cwnd` es jetzt ermöglicht, daß 5 Segmente verschickt werden dürfen, ohne auf eine Bestätigung zu warten, können von Rechner1 nur wieder drei neue Segmente (Nr. 16, 17, 18) gesendet werden, da die Bestätigung für noch zwei Segment (Nr. 13 und 14) aussteht.

Wie in diesem Kapitel beschrieben, wird eine TCP Verbindung durch Slow Start nach dem Verbindungsaufbau in einen der Netzwerkkapazität angepaßten, funktionsfähigen Zustand überführt. Wie im weiteren Verlauf einer Verbindung auf eine eventuelle Überlastung reagiert wird, erläutert das nächste Kapitel.

[22] Die Speicherung von `cwnd` scheint jedoch je nach TCP Implementierung zu variieren. In Linux 2.0.33/TCP 1.0.16 ist cwnd als Anzahl der Segmentgrößen implementiert, entgegen der Beschreibung von [128]

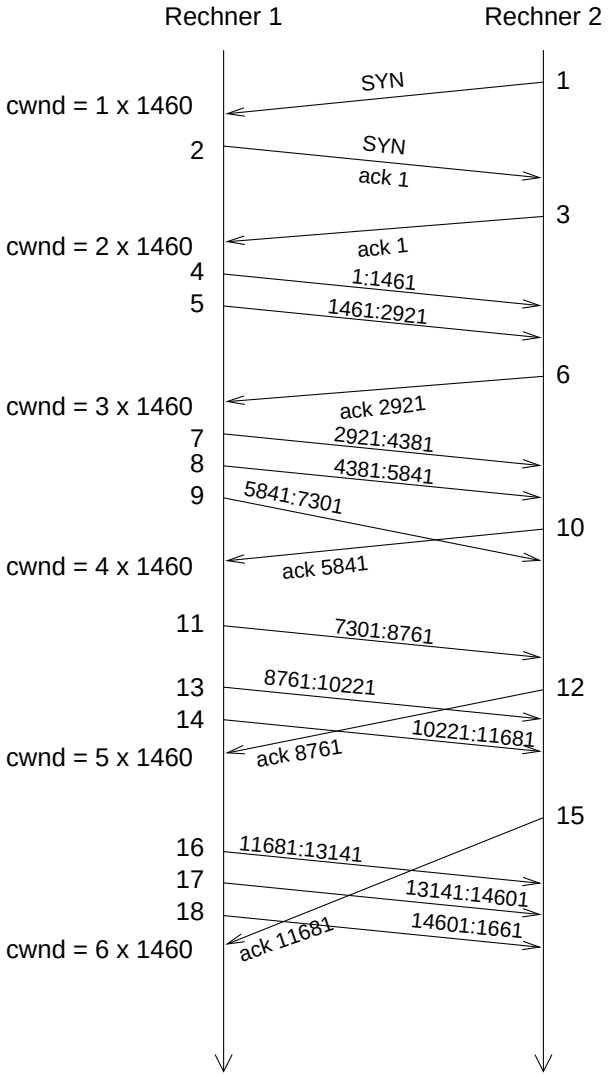


Abbildung 72: Beispiel Slow Start (als Grundlage für diese Abbildung dient die Ausgabe des Werkzeugs *tcpdump*)

5.2.4 Congestion Avoidance

Aufgabe von Congestion Avoidance ist es, auf eine Überlastung des Netzes zu reagieren und den Datenfluß entsprechend anzupassen. Wie Slow Start ist Congestion Avoidance in [76] beschrieben.

Als Indiz für eine Überlastung des Netzes dient, wie in 5.2.2 beschrieben, das Auftreten von Paketverlusten. Paketverluste bemerkt der Sender durch einen Timeout. Trifft bis zum Auslaufen des RTO keine Bestätigung für ein TCP Segment ein, gilt das Segment als verloren.

Eine weitere Möglichkeit einen Paketverlust zu erkennen, besteht in einer differenzierten Auswertung, duplizierter Bestätigungssegmente[23]. Erreichen den Sender duplizierte Bestätigungen,

[23]Mit duplizierten Bestätigungen werden Bestätigungen beschrieben, die das gleiche Segment bestätigen

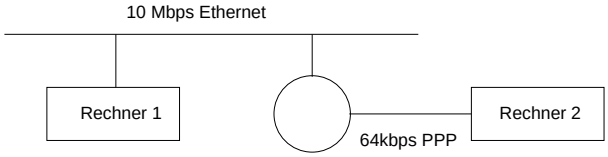


Abbildung 73: Netzwerkkonfiguration

bedeutet dies, daß beim Empfänger Segmente in falscher Reihenfolge eingetroffen sind. Bei mehr als zwei duplizierten Bestätigungen kann, wie in [128] beschrieben, angenommen werden, daß keine Neuordnung der Segmente beim Empfänger erfolgte, sondern ein Segment von einem Router wegen Überlastung verworfen wurde.

Die Behandlung einer Überlastung erfolgt differenziert:

- Wird die Überlastung durch einen Timeout angezeigt, dann wird die Window Größe (`cwnd`) auf eine Segmentgröße zurück gesetzt und mit Slow Start wieder bis zu einer gewissen Grenze (*Slow Start Threshold*) gesteigert. Danach wird Congestion Avoidance angewandt, d.h. die Window Größe moderater angehoben (s. Abb. 74).
- Wird die Überlastung jedoch durch duplizierte Bestätigungen registriert, wird kein Slow Start durchgeführt, da sich hinter duplizierten Bestätigungen mehr Information verbirgt als nur die Anzeige eines Segmentverlusts:

  Der Empfänger kann nur duplizierte Bestätigungen erzeugen, wenn nach dem Verlust eines Segments trotzdem nachfolgende Segmente eingetroffen sind. Dies bedeutet, daß nur eine moderate Überlastung vorliegt (s. S.970, [144]) und der bestehende Datenfluß nicht abrupt durch Slow Start gestoppt werden muß[24].

Congestion Avoidance und Slow Start sind zwar unterschiedliche Algorithmen, werden aber zusammen eingesetzt. Congestion Avoidance und Slow Start in Kombination benötigen zwei Zustandsvariablen zur Verwaltung der Window Größe für jede TCP Verbindung:

- `cwnd`, das im Slow Start verwendete Congestion Window
- `ssthresh` (*Slow Start Threshold*)

Mit folgenden Schritten wird durch Einsatz von Slow Start und Congestion Avoidance die Window Größe bei Überlastung reguliert:

1. `ssthresh` wird auf die Hälfte der aktuellen Window Größe gesetzt[25]. Wird die Überlastung durch einen Timeout angezeigt, wird `cwnd` auf eine Segmentgröße gesetzt und damit Slow Start eingeleitet. Bei duplizierten Bestätigungen, wird wie oben beschrieben, nicht mit Slow Start, sondern nur mit Congestion Avoidance auf die Überlastung reagiert, d.h. `cwnd` wird nicht auf eine Segmentgröße, sondern auf die Hälfte der aktuellen Window Größe gesetzt.

[24] Dies gilt nur für Festnetze. Wie in 5.2.3 erläutert, können in Funknetzen Paketverluste nicht als Indiz für Netzüberlastung gelten

[25] Die aktuelle Window Größe wird aus dem Minimum von `cwnd` und der vom Empfänger begrenzten Window Größe berechnet

2. Wenn neue Segmente vom Empfänger bestätigt werden, wird `cwnd` erhöht. Wie `cwnd` erhöht wird, hängt davon ab, ob sich der Sender in Slow Start befindet oder in Congestion Avoidance. Ist `cwnd` $\leq$ `ssthresh`, dann handelt es sich um Slow Start, ansonsten wird Congestion Avoidance angewendet.

   Im Slow Start Zustand wird `cwnd` jeweils um eine Segmentgröße erhöht, in Congestion Avoidance wie folgt:

$$cwnd \longleftarrow cwnd + \frac{\text{Segmentgröße}}{cwnd} * \text{Segmentgröße};$$

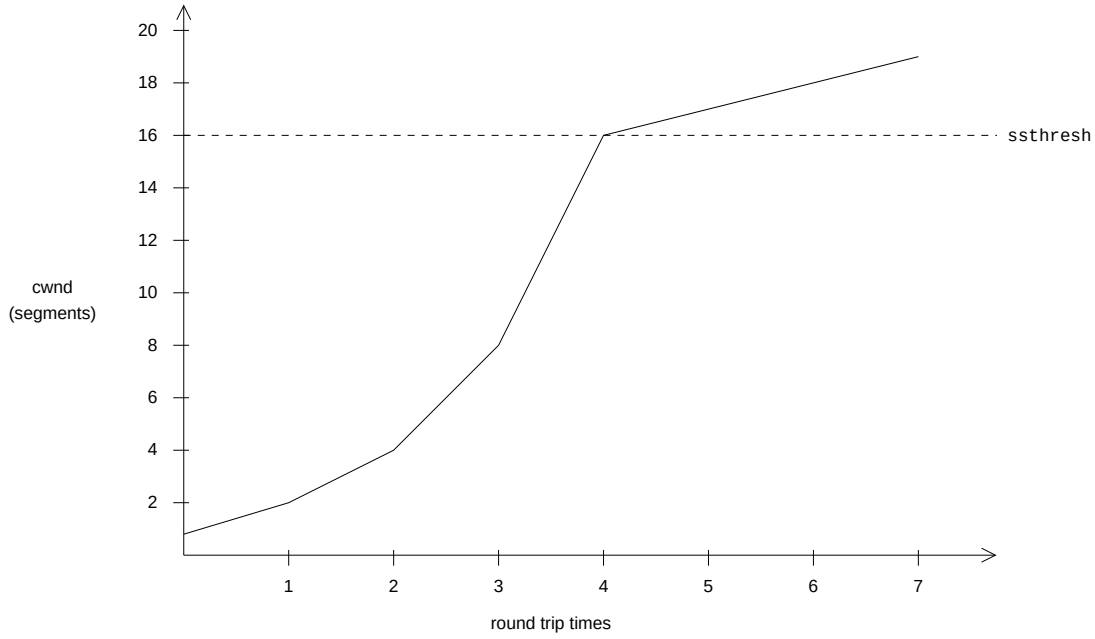


Abbildung 74: Congestion Avoidance

Abbildung 74 zeigt das Zusammenwirken von Slow Start und Congestion Avoidance im Falle eines Timeouts: Durch Slow Start wird der Datenfluß bei einem `cwnd` von 32 Segmenten gestoppt, danach exponentiell[26] zur RTT bis zu `ssthresh` gesteigert, dann beginnt Congestion Avoidance das Congestion Window nur noch additiv zu erhöhen.

Modifikationen dieses Verfahrens bei duplizierten Bestätigungen wurden in [75] unter den Schlagwörtern Fast Retransmit und Fast Recovery vorgeschlagen.

5.2.5 Fast Retransmit und Fast Recovery

Wie in 5.2.4 erläutert, bedeutet der Empfang von 3-4 duplizierten Bestätigungen einen Segmentverlust. Die erneute Übertragung des vermutlich verlorenen Segments, ohne auf den Timeout zu warten, wird als *Fast Retransmit* bezeichnet. Daran schließt sich eine modifizierte Version des Congestion Avoidance Algorithmus. Diese Version, der *Fast Recovery*, ist üblicherweise folgerndermaßen realisiert:

[26] Wenn mehrere Segment durch ein Acknowledgment bestätigt werden, dann ist die Steigerung nicht mehr exponentiell

1. Nach Empfang der dritten doppelten Bestätigung wird **ssthresh** auf die Hälfte der aktuellen Window Größe gesetzt (s. 5.2.4)
2. Das verlorene Segment wird erneut übertragen.
3. **cwnd** wird folgendermaßen modifiziert (ack_{dupp} ist die Anzahl doppelter Bestätigungen):

$$cwnd \longleftarrow ssthresh + ack_{dupp} * Segmentgröße$$

4. Jedes Mal, wenn nun eine doppelte Bestätigung eintrifft, wird **cwnd** um eine Segmentgröße erhöht.
5. Trifft eine Bestätigung für neue Segmente ein, d.h. Segmente die noch nicht bestätigt wurden, dann wird **cwnd** der Wert von **ssthresh** zugeordnet. Mit dieser Bestätigung sollten alle Segment bestätigt werden, die zwischen dem verlorenen Segment und seiner erneuten Übertragung gesendet wurden.

Der letzte Schritt des Fast Recovery beseitigt die Netzüberlastung, da die Übertragung auf die Hälfte der Rate vor dem Paketverlust verringert wird. Die Veränderungen des Congestion Windows während dieses modifizierten Congestion Avoidance wird in [75] unter anderem algebraisch beschrieben.

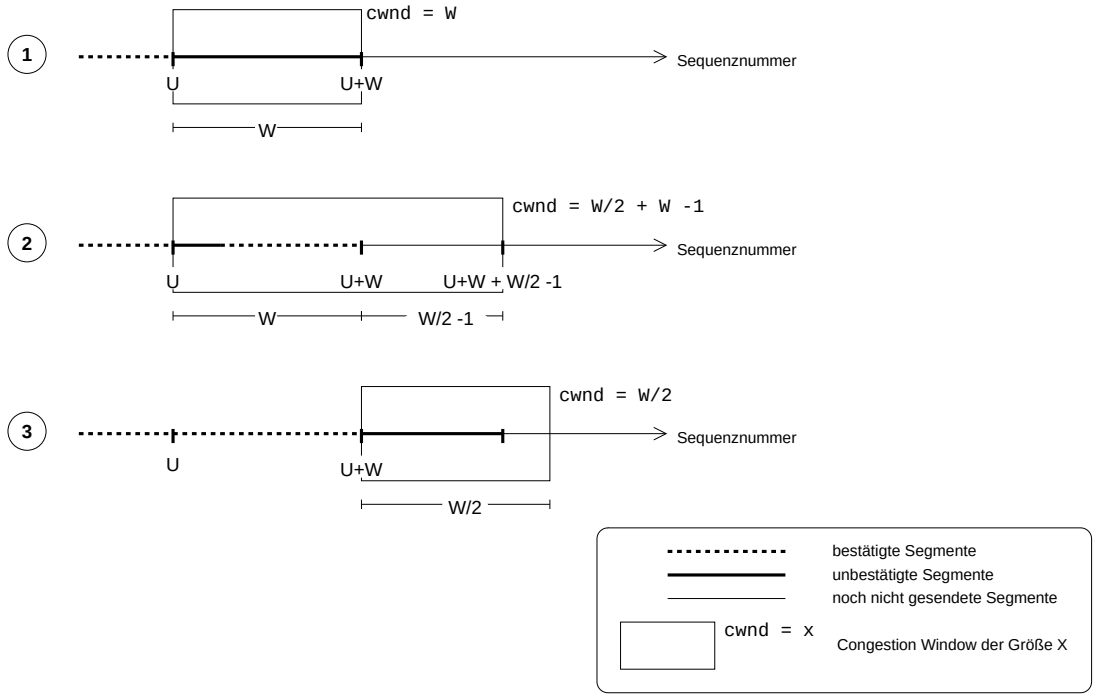


Abbildung 75: cwnd während Fast Retransmit und Fast Recovery

Abbildung 75 zeigt die Veränderung von **cwnd** mittels Jacobsons algebraischer Beschreibung in drei Schritten:

1. U sei die erste unbestätigte Sequenznummer und W die Größe des Congestion Window. Die Segmente $[U, \ldots, W + U]$ werden übertragen.

2. U ging wegen Überlastung verloren, die Segmenten $[U+1,\ldots,U+W]$ werden durch $W-1$ duplizierte Acknowlegments bestätigt. Dadurch wird der Verlust von U registriert, die Übertragung sofort wiederholt (*Fast Retransmit*) und `cwnd` auf $W/2$ gesetzt. Von den Segmenten $[U+1,\ldots,U+W]$ ist wegen der doppelten Bestätigung bekannt, daß sie beim Empfänger eingetroffen sind und das Netz verlassen haben. Deshalb kann `cwnd` um die Anzahl der doppelten Bestätigungen $W-1$ erhöht werden ($\Longrightarrow cwnd = W/2 + (W-1)$).

   Subtrahiert man von `cwnd` die Anzahl der unbestätigten Segmente $[U,\ldots,U+W]$, erhält man die Anzahl der Segmente, die neu verschickt werden dürfen:

$$cwnd - W = W/2 + (W-1) - W = W/2 - 1$$

3. Die Bestätigung "neuer Daten", d.h. der Segmente $[U,\ldots,U+W]$, ist nun eingetroffen(*Fast Recovery*), daher wird `cwnd` auf die Hälfte seines Wertes vor dem Verlust des Segments U gesetzt ($\Longrightarrow cwnd = W/2$).

   Da die Bestätigungen der Segmente, die zwischen dem Entdecken des Verlust und dem Eintreffen der "Recovery" Bestätigung gesendet wurden, d.h. die Segmente $[U+W,\ldots,U+W+W/2-1]$, noch nicht vorliegen, kann nur ein neues Segment verschickt werden:

$$cwnd - (W/2-1) = W/2 - (W/2-1) = 1$$

   Dadurch ensteht an einem potentiellen Flaschenhals kein plötzlicher Schwall von Segmenten, nach dem Retransmit.

Der Fast Retransmit Algorithmus wurde zum erstenmal in 4.3BSD Tahoe implementiert, wurde aber fälschlicher Weise durch einen Slow Start fortgesetzt. Die Kombination von Fast Retransmit und Fast Recovery erschien zum ersten Mal in der 4.3BSD Reno Release.

5.2.6 ICMP Source Quench Error

Neben der Signalisierung von Überlastung durch Paketverlust gibt es auf IP Ebene die Möglichkeit, daß ein Router, der keine Pakete mehr annehmen kann, die ICMP (Internet Control Message Protocol) Nachricht Source Quench Error schickt. Dadurch wird bei einer TCP Verbindung Slow Start eingeleitet, der durch kein `ssthresh` begrenzt wird, sondern die Window Größe so lange steigert, bis entweder die vom Empfänger begrenzte Window Größe erreicht ist oder eine Überlastung entsteht.

Ein Rechner muß diese Nachricht nicht generieren und nach derzeitigem Stand ist diese Methode veraltet, da sie Bandbreite verbraucht und ein ineffektiver und unfairer Behelf ist, um Überlastung zu behandeln ([128]). Daher wird die Überlastungsbehebung durch eine Source Quench Meldung hier nicht näher ausgeführt.

5.2.7 Retransmission Time Out

In den vorhergehenden Abschnitten wurden Konzepte beschrieben, die eine Überlastung durch die Modifizierung der Window Größe regulieren. Im Zusammenhang mit Netzüberlastung spielt jedoch auch die Optimierung des RTO eine wichtige Rolle.

Eine gute Abschätzung für den RTO ist für die Ausgewogenheit des Netzes notwendig (s. 5.2.3), d.h. es darf kein neues Paket gesendet werden, so lange kein Paket vom Empfänger aus dem Netz genommen wurde. Ist der RTO zu kurz, werden erneute Übertragungen eingeleitet, obwohl die

entsprechenden Pakete nicht verloren gegangen sind, sondern sich aufgrund von Verzögerungen, z. B. bei hoher Belastung, noch im Netz befinden. Dadurch wird das Netz mit der Übertragung von Paketkopien zusätzlich unnötig belastet.

Zur Abschätzung des RTO kann kein fester Wert angenommen werden, da die Übertragunszeit je nach Verbindung, in Abhängigkeit von Bandbreite oder Anzahl der Hops, stark variiert. Als Grundlage der RTO Abschätzung wird für jede Verbindung jeweils die gemessene RTT verwendet. Da jedoch auch während einer Übertragung sich die Round Trip Time wegen einer modifizierter Route oder Verkehrszu- bzw. abnahme ändern kann, muß die RTT wiederholt gemessen und der RTO entsprechend angepaßt werden.

In der Original TCP Spezifikation [110] wird für die Abschätzung der mittleren RTT ein Tiefpaßfilter vorgeschlagen:

$$R \longleftarrow \alpha * R + (1 - \alpha) * R_{gem}$$

wobei R die mittlere RTT Abschätzung ist, R_{gem} die gemessene RTT vom letzten bestätigten Segment und α der Zunahmefilter mit einem vorgeschlagenen Wert von 0.9.

Nach der Aktualisierung von R wird der RTO auf $\beta * R$ gesetzt, wobei vorgeschlagen wird, $\beta = 2$ zu setzen.

Nach [76] eignet sich diese Abschätzung nur für Netzwerklasten bis zu 30%. Bei einer Netzbelastung oberhalb dieser Grenze reagiert TCP mit erneuten Übertragungen von Paketen, obwohl die Übertragung der Pakete nur verzögert wurde.

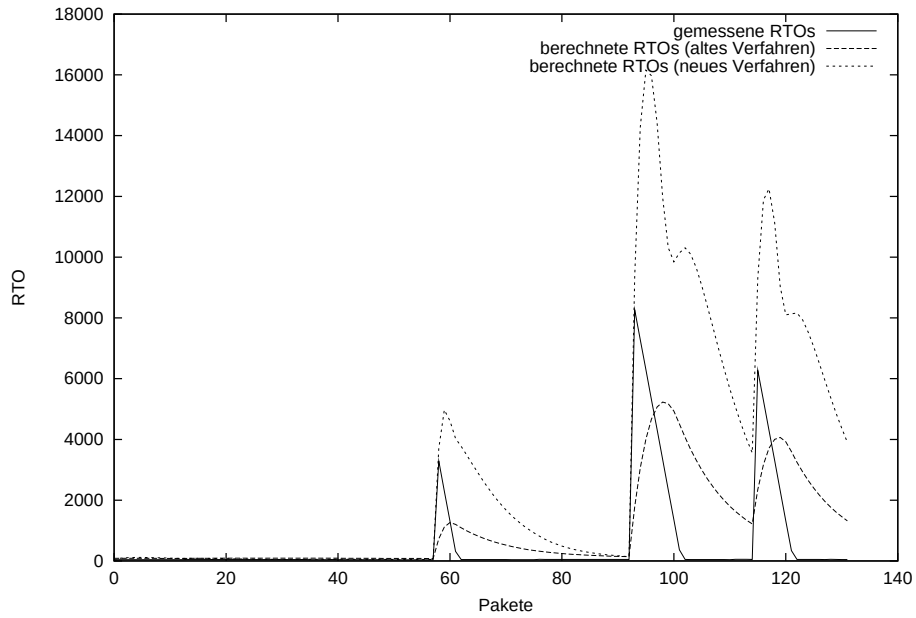


Abbildung 76: Beispiel für RTO Abschätzungen; zur Simulation realistischer RTTs wurden die Zeitangaben aus einer "Ping Messung" zwischen Rechner1 und Rechner2 (s. Abbildung 73) verwendet.

Die Lösung diese Problems wäre die Einbeziehung der Standardabweichung der RTT in die Abschätzung der RTO. Die Berechnung der Standardabweichung erfordert zur Quadratberechnung eine kostspielige Integer Multiplikation mit der Gefahr eines Integer Overflows. Wie ebenfalls in [76] beschrieben, eignet sich die mittlere Abweichung als Näherung für die Standardabweichung. Dies führt zu folgenden Gleichungen zur Berechnung des RTO:

$$\begin{aligned} \delta_{err} &= R_{gem} - R \\ R &\longleftarrow R + g * \delta err \\ D &\longleftarrow D + h * (|\delta err| - D) \\ RTO &= R + 4 * D \end{aligned}$$

mit δ_{err}, der Differenz zwischen der gemessenen RTT und der aktuellen Abschätzung für die RTT und D der mittleren Abweichung. Der Zunahmefaktor h wird zur Berechnung der mittleren Abweichung auf 0.25, der Zunahmefaktor g zur Berechnung der mittleren RTT auf 0.125 gesetzt.

Abbildung 76 zeigt die unterschiedlichen Wirkungsweisen der alten und und der neuen Abschätzung des RTO.

5.3 Resource Reservation Protocol (RSVP)

Die in 5.2 geschilderten Mechanismen realisieren das heutige Service Modell des Internets: Point-to-Point und best-effort Service. Datenpakete werden unter Ausnutzung der maximal vorhandenen Netzwerkbandbreite so gut wie möglich, d.h. mit möglichst geringer Verzögerung und Verlustrate, von einem Sender zu einem Empfänger befördert. Kein Paket wird bevorzugt behandelt, das Paket, das als erstes am Router eintrifft, wird als erstes weiterverarbeitet.

Dieses Modell ist vollkommen ungenügend für die Anforderungen zukünftiger Anwendungen wie zum Beispiel Video-on-Demand, Multimedia Konferenzen oder auch Internet Telefonie. Derartige realtime Anwendungen benötigen Verbindungen mit niedrigen Vezögerungszeiten, um sinnvoll genutzt werden zu können. Die Lösung liegt in der Spezifikation von Quality of Service Anforderungen, die durch Reservierung von Netzwerkressourcen realisiert werden. Dies kann jedoch nicht vom bestehenden best-effort Modell geleistet werden und erfordert eine erweiterte oder auch neue Architektur.

Die zweite Eigenschaft des bestehenden Internet Service Modells, die Spezialisierung auf Point-to-Point Verbindungen, widerspricht ebenfalls der Anforderung der oben bereits genannten Anwendungen, die meist zur Kommunikation mehrerer Teilnehmer bestimmt sind. Bei Konferenzen gibt es mehrere "Sender", die auch als "Empfänger" fungieren können, und umgekehrt mehrere "Empfänger", die als "Sender" auftreten können.

5.3.1 Integrated Services Packet Network

Die Entwicklung neuer Netzwerkarchitekturen und Service Modelle, die den oben geschilderten Anforderungen moderner Applikationen genügen, war in den letzten Jahren Gegenstand intensiver Forschungstätigkeit. Ein Ergebnis ist eine Erweiterung der bestehenden Internet Architektur, die als *Internet Integrated Services* (ISS) bezeichnet wird. Ein Netzwerk, das diese unterstützt, wird als *Integrated Services Packet Network* (ISPN) bezeichnet. Eine ausführlichere Beschreibung ist in [30] zu finden.

Das ISPN ermöglicht Anwendungen, einen Quality of Service für eine Verbindung anzufordern. Dieser QoS wird durch Reservierung von Netzwerkressourcen entlang des Netzwerkpfades und in den Endgeräten für die Verbindung realisiert. Für ISPN sind folgende Komponenten notwendig:

Flow Spezifikation Zur Charakterisierung des Datenflusses dient die Flow Spezifikation. Damit kann der Sender seine Anforderungen an das Netzwerk definieren und das Netzwerk

im Gegenzug den Quality of Service angeben, den es zur Verfügung stellen kann. Die Flow Spezifikation, sog. *Flowspec*, wird jedoch hauptsächlich von den Anwendungen dazu benutzt, ihre Anforderungen bezüglich Quality of Service an das System zu stellen. In [145] und [123] werden zwei Quality of Service Klassen zur Flow Spezifikation beschrieben.

Routing Das Routing Protokoll steuert, auf welchem Weg die Pakete im Netz transportiert bzw. verteilt werden. Um Multipoint-to-Multipoint Anwendungen zu unterstützen, muß das Routing Protokoll nicht nur unicast, sondern auch *mulitcast* unterstützen. Als Routing Protokoll kann zum Beispiel das derzeitige Internet Protokoll (IP) verwendet werden.

Resource Reservation Zur Realisierung eines quantitativen Quality of Service für einen Datenstrom, müssen gewisse Betriebsmittelkapazitäten für diesen Strom vom Netzwerk reserviert werden. Die Resource Reservation ermöglicht, Ressourcen entlang eines Verbindungspfades zu reservieren und die vorgenommenen Reservierungen zu verwalten. Zwei Ansätze zur Resource Reservation sind das *Proposed Internet Stream Protocol* und das *Experimental Internet Stream Protocol*. In dieser Arbeit wird ein drittes Konzept beschrieben, das *Resource Reservation Protocol* (RSVP).

Admission Control Da die Netzkapazität begrenzt ist, kann nicht jede Reservierungsanfrage genehmigt werden. Die Verwaltung der Ressourcen ist Aufgabe der Admission Control. Ein Beispiel für einen Admission Control Algorithmus wird in [77] beschrieben.

Policy Control Während die Admission Control Komponente über die Zulassung einer Reservierung gemäß der Verfügbarkeit von Ressourcen entscheidet, wird durch die Policy Control Komponente der administrative Aspekt einer Reservierung abgedeckt. Das System entscheidet, ob es dem User bzw. der Anwendung erlaubt ist, die Reservierung zu erhalten. Dies kann zum Beispiel durch die Benutzerverwaltung des Betriebssystems geregelt werden.

Packet Scheduler Die Umsetzung der genehmigten Reservierung, d.h. die Steuerung der Paketverteilung wird durch den Paket Scheduling Algorithmus realisiert. [44] beschreibt eine mögliche Implementierung. Durch den Packet Scheduler wird der verlangte Quality of Service umgesetzt.

Packet Classifier Die Aufgabe des Packet Classifiers ist es, die Datenflüsse für den Packet Scheduler in entsprechende Klassen einzuordnen. Die Klassen werden durch Reservierungsfilter dem Packet Classifier vom Reservierungs Protokoll mitgeteilt.

Packet Scheduler und Classifier realisieren die Weiterleitung der Datenpakete und werden deshalb als *Traffic Control* zusammengefaßt.

Abbildung 77 zeigt die Komponenten des ISPN, das streng modular aufgebaut ist. Die Implementierung der Admission Control Komponente ist zum Beispiel für die Resource Reservation Komponenten unerheblich. Ebenso sind die Inhalte der Flow Spezifikationen, die zur Reservierung transportiert werden, der Resource Reservation Komponente verborgen. Es ist für die Resource Reservation Komponente nur wichtig, ob die Reservierung durch Admission Control und Policy Control zugelassen wird oder nicht.

5.3.2 RSVP Architektur

Eine Realisierung der Resource Reservation Komponente ist das *Resource Reservation Protocol* (RSVP). Das Konzept von RSVP wird erstmals in [146] vorgestellt. In [31] werden weitere

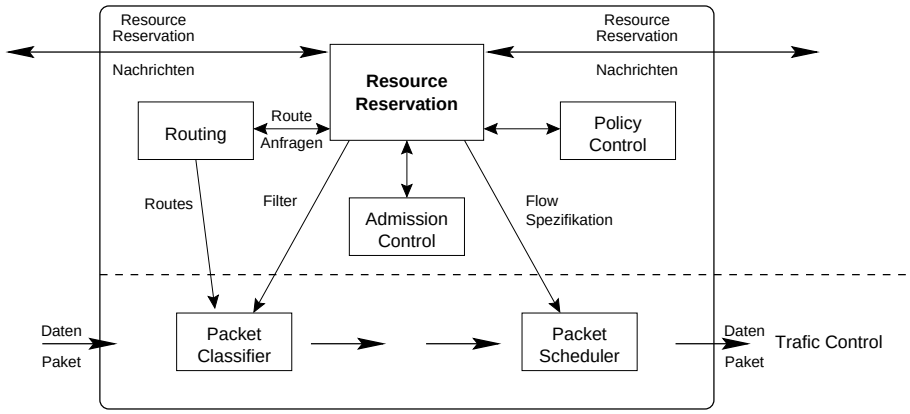


Abbildung 77: ISPN Komponenten

technische Aspekte geschildert. Das RSVP als Internet Protokoll wird in [29] beschrieben. RSVP zeichnet sich durch folgende grundlegende Eigenschaften aus:

- Empfänger orientierte Reservierung
- Unterstützung von Multipoint-to-Multipoint Anwendungen
- Verschiedene Reservierungs Styles
- Soft State in Routern

RSVP Reservierungen werden durch den Empfänger aufgebaut. Dies hat den Vorteil, daß heterogene Empfänger individuell den gewünschten Quality of Service entsprechend ihrer Verarbeitungskapazitäten wählen können. Die Festlegung des Quality of Service durch den Empfänger ist auch hinsichtlich einer zukünftigen Bezahlung von QoS Leistungen sinnvoll.

Reservierungen werden nur für unidirektionale Verbindungen aufgebaut. Ein Sender kann für die Dauer einer Reservierung niemals als Empfänger, sondern immer nur als Sender agieren. Das Analoge gilt für Empfänger. Allerdings können Empfänger Reservierungen für mehrere Sender vornehmen und Sender können gleichzeitig an mehrere Empfänger Daten über reservierte Pfade verschicken (*Multipoint-to-Multipoint Verbindungen*, s. Abb. 78). Empfänger werden in Multicastgruppen zusammengefaßt.

Wie Reservierungen bei Multipoint-to-Multipoint Verbindungen die Ressourcen nutzen, wird durch *Styles* festgelegt.

Die Robustheit und Flexibilität von RSVP wird durch *Soft States* in den Routern erreicht, d.h. Reservierungen werden periodisch erneuert, um die Reservierung aufrecht zu halten. Dadurch kann sowohl auf Änderungen des Pfades reagiert werden, indem im neuen Pfad Reservierungen aufgebaut werden, als auch vom Empfänger in bestehenden Reservierung der Sender gewechselt werden.

Die periodischen Nachrichten zur Aufrechterhaltung der Reservierungen werden “Hop by Hop” weitergeschickt. Vom Empfänger ausgehend wird immer nur eine Reservierung auf die Verbindung zum nächsten Knoten angefordert. Liegen an einem Knoten Reservierungsanforderungen

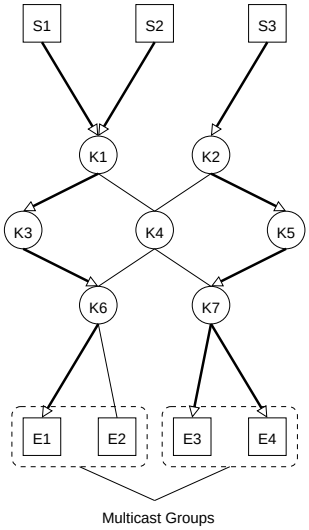


Abbildung 78: RSVP Multipoint-to-Multipoint

mehrerer Empfänger für den selben Sender vor, dann können diese je nach Style zu einer Reservierung zusammengefaßt werden, die allen zusammengefaßten Reservierungsanforderungen genügt.

RSVP Session Verbindungen (DataFlow) entlang eines reservierten Pfades werden von RSVP durch zwei Teile definiert: Einer *Filter Spec* und einer Session Definition. Die Session Definition beschreibt die Empfänger, die Filter Spec den "Rest" (hauptsächlich Information über die Sender). Eine RSVP Session wird durch ein Tripel identifiziert:

(Empfänger Adresse, IP Protokoll ID, Empfänger Port)

Die *Empfänger Adresse* ist im Multicast Fall die Adresse einer Multicast Gruppe und bei Unicast die Adresse eines Rechners. *IP Protokoll ID* beschreibt das Transportprotokoll, das zur Übertragung verwendet wird. Das optionale Feld *Empfänger Port* entspricht einem TCP oder UDP Port. RSVP ist zwar entwickelt worden mit der Absicht, für andere Protokolle leicht erweiterbar zu sein, die hier und auch in [29] beschrieben Version von RSVP unterstützt grundsätzlich nur TCP und UDP.

RSVP Nachrichten Elementarer Baustein für den Aufbau und die Verwaltung von Reservierungen sind die RSVP Nachrichten, die nicht nur unidirektional entsprechend der Richtung der Datenpakete verschickt werden, sondern bidirektional. Die wichtigsten Nachrichten sind die *Path Message* und die *Resv Message*, die zum Aufbau und der Aufrechterhaltung der Reservierungen dienen.

- Path Message

  Bevor ein Empfänger eine Reservierung aufbauen kann, muß er wissen zu welchem Sender und für welchen Quality of Service. Dazu schicken die Sender periodisch *Path Messages* an eine Gruppe (Multicast) oder einzelne Rechner (Unicast). Eine Path Message enthält folgende Informationen:

  - Die *TSpec*, eine Beschreibung des Datenflusses,
    der vom Sender gesendet wird. Folgende Parameter sind in der TSpec enthalten:
    * Token Bucket Rate
    * Token Bucket Size
    * Peak Data Size
    * Minimum Policed Unit
    * Packet Size
  - Die *AdSpec*, die Angaben über die Netzwerkressourcen des Pfades enthält:
    Damit ist dem Empfänger bekannt, welcher QoS überhaupt reserviert werden kann. Dazu werden folgende Parameter gespeichert und an jedem Router, der ISPN unterstützt, von der Traffic Control Komponente aktualisiert:
    * NON IS Hop Count:
      Information über Netzwerkkomponenten im Pfad die kein QoS unterstützen.
    * Available Path Bandwith: verfügbare Bandbreite im Pfad
    * Minimum Path Latency:
      Kleinste mögliche Verzögerung, die beim Weiterleiten eines Pakets entstehen kann.
    * Path MTU:
      Diese MTU wird für den Pfad jeweils aus der lokalen IP MTU berechnet

    Eine genauere Beschreibung der einzelnen Parameter ist in [124] zu finden.
  - Ein Sender Template:
    Das *Sender Template* beschreibt das Format der Daten, die gesendet werden. Seine Form entspricht der Filter Spec und sollte vom Empfänger bei der Reservierungsanforderung als Filter für den Sender verwendet werden.
  - Information über den letzten Knoten:
    Um den Pfad zurück zum Sender verfolgen zu können, hinterlegen die Path Messages in jedem Knoten auf dem Weg zum Empfänger Information über den vorhergehenden Knoten.

- Resv Message

  Resv Messages werden regelmäßig von Empfängern generiert und wandern entgegen der Richtung der Datenpakete zum Sender, um Reservierungen aufzubauen. Zu welchem Knoten sie geschickt werden, ist aus der abgelegten Pfadinformation der entsprechenden Path Message bekannt. Zum Reservierungsaufbau werden in Resv Messages folgende Informationen transportiert:

  - Adresse des nächsten Knoten im Pfad
  - Die *FlowSpec*: Die FlowSpec besteht enthält die TSpec des Senders, die den Datenstrom beschreibt und eine RSpec, die den gewünschten QoS definiert.
  - Eine Liste von *FilterSpecs*: Eine *FilterSpec* beschreibt den Sender, für dessen Datenpakete eine Reservierung aufgebaut werden soll.
  - Reservierungs Style

- ResvTear Message und PathTear Message

  Obwohl RSVP durch Soft State verwaltet wird, gibt es die *ResvTear Message* und die *PathTear Message*, um explizit Reservierungen abzubauen.

- ResvErr Message und PathErr Message

  Zur Fehlerverarbeitung dienen die *ResvErr Message* und die *PathErr Message*, die Fehler bei der Bearbeitung einer Resv Message bzw. Path Message an den Empfänger bzw. an den Sender melden.

Styles Styles sind Attribute von Reservierungsanforderungen. Die aktuelle Version von RSVP ([29]) unterstützt zwei Attribute:

Das eine Attribut legt fest, wie Sender ausgewählt werden: *Explizit* bedeutet, daß in der Liste der FilterSpecs jeder Sender einzeln durch eine FilterSpec angegeben wird. Bei einer *Wildcard* Auswahl sind alle Sender ausgewählt. Wenn neue Sender auftreten, dann wird die Auswahl um die neuen Sender automatisch erweitert.

Das andere Attribut bestimmt, auf welche Weise Reservierungen verschiedener Sender innerhalb derselben RSVP Session (s. 5.3.2) behandelt werden: Entweder wird für alle Sender eine Reservierung vorgenommen (*Shared*) oder jeder Sender erhält eine eigene Reservierung (*Distinct*).

	Reservierung	
Sender Auswahl	Distinct	Shared
Explizit	FF Style	SE Style
Wildcard	(nicht definiert)	WF Style

Tabelle 20: RSVP Reservierungs Styles

Aus diesen Attributen ergeben sich folgende Kombinationen (s. Tab. 20):

- Wildcard-Filter (WF)

  Der *WF* Style impliziert Shared Reservierung und Wildcard Sender Auswahl, d.h. eine Reservierungsanforderung mit WF Style erstellt *eine* Reservierung für *alle* Sender.

- Fixed-Filter (FF)

  Der *FF* Style beinhaltet Distinct Reservierung und Explicit Sender Auswahl. Eine derartige Reservierungsanforderung erstellt für *jeden* aufgelisteten Sender eine *eigene* Reservierung.

- Shared Explizit (SE)

  Eine Reservierungsanforderung mit *SE* Style enthält wie eine FF Reservierungsanforderung eine Liste mit *explizit* aufgelisteten Sendern, für die jedoch nur eine *gemeinsame* Reservierung aufgebaut wird.

In früheren Versionen von RSVP war noch ein zusätzlicher Style vorgesehen, der *Assured Style*, der ebenso wie die nicht definierte Distinct Wildcard Kombination, aufgrund der Komplexität nicht beibehalten wurde. Bei jedem Style handelt es sich um einen Kompromiß zwischen Funktionalität, Komplexität und Overhead.

5.3.3 Funktionsweise von RSVP

Anhand einer einfachen Netzwerkkonfiguration, die in Abbildung 79 dargestellt ist, soll die Funktionsweise von RSVP erläutert werden. Abbildung 79 zeigt die Sender S1-S3, die Router R1-R3 und die Empfänger E1-E3. Die Verbindungen zwischen den Komponenten sind mit L1-L8 bezeichnet. Zur Vereinfachung wird angenommen, daß für alle Reservierungsanforderungen ausreichend Netzwerkressourcen zur Verfügung stehen. Weiterhin wird vorrausgesetzt, daß sich alle Empfänger in derselben Multicastgruppe befinden, bisher noch keine Reservierungen vorgenommen wurden und kein Sender Datenpakete verschickt hat.

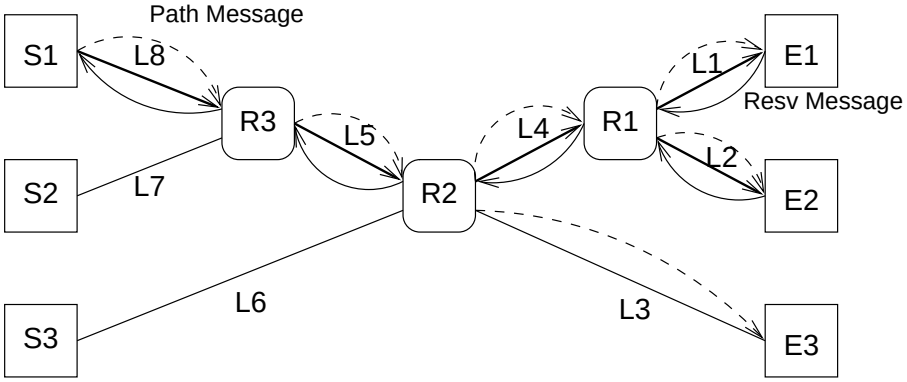


Abbildung 79: RSVP Beispiel

Der Sender S1 will senden und verschickt daher Path Messages an die Empfänger E1-E3. In den Routern R3, R2 und R3 werden in einer Tabelle die Pfadinformationen aus der eingetroffenen Path Message abgelegt:

Router	R1	R2	R3
Eingehende Verbindungen (Sender)	L4	L5	L8
Ausgehende Verbindungen (Empfänger)	L1,L2	L4,L3	L5

Die Empfänger E1 und E2 wollen Datenpakete von Sender S1 über eine reservierte Verbindung empfangen und schicken je eine Resv Message mit Reservierungsstyle WF an Router R1. Der Einfachheit halber sei die FlowSpec eine Vielfache der Ressourceneinheit B. Der Empfänger E1 fordert einen QoS von $3B$ an und Empfänger E2 nur $2B$. Nach Überprüfung der Reservierungsanforderung durch Policy Control und Admission Control wird im Router R1 folgende Reservierung aufgebaut.

	R1	
Eingehende Verbindungen (Sender)	L1(3B)	L2(2B)
Ausgehende Verbindungen (Empfänger)	L4(3B)	

Die Reservierung von Empfänger E2 über $2B$ wird durch die größere Reservierung von Empfänger E1 abgedeckt und da beide Reservierungen mit dem Style WF versehen sind, können die Reservierungsanforderungen von E1 und E2 vom Router R1 zusammengefaßt werden und als Reservierungsanforderung von $3B$ an die Router R2 und R3 weitergeschickt werden:

	R2	R3
Eingehende Verbindungen (Sender)	L4($3B$)	L5($3B$)
Ausgehende Verbindungen (Empfänger)	L5($3B$)	L8($3B$)

Damit besteht eine reservierte Verbindung vom Sender S1 zu den Empfängern E1 und E2. Alle Datenpakete, die von Sender S1 verschickt werden und die dem in der Reservierung angegebenen Filter entsprechen, werden in den Routern von der Traffic Control Komponente gemäß der Reservierung bevorzugt behandelt.

5.4 RSVP über ATM

Die Nutzung der leistungsfähigen ATM Technologie als Link Layer zur IP Übertragung ist weitgehend ausgereift und ermöglicht dadurch die Unterstützung von QoS für IP Verbindungen. Den von ATM realisierten QoS durch ATM auch für RSVP zu benutzen ist daher naheliegend, jedoch aufgrund der unterschiedlichen Konzepte von RSVP und ATM nicht unproblematisch. RSVP QoS Definitionen müssen auf ATM QoS Parameter abgebildet werden und RSVP Verbindungen auf ATM Virtual Circuits (VC). In [24] wird die Problematik der QoS als unkritisch betrachtet, da beide QoS Konzepte ähnlich seien, und daher vornehmlich mögliche Lösungen des VC Managements für RSVP Verbindungen diskutiert. In [125] wird die Übertragung der QoS Parameter als größtes Problem bei RSVP und IP über ATM angesehen und dementsprechend der Schwerpunkt auf dieses Themengebiet gelegt. Im folgenden werden beide Problembereiche erläutert.

5.4.1 Übertragung von RSVP QoS auf ATM QoS Parameter

Ein wesentlicher Unterschied zwischen RSVP QoS Klassen ist die Ausrichtung auf Verzögerungszeiten, während bei ATM nach den Charakteristika der Datenströme (konstant, bursty, etc.) die Serviceklassen gebildet werden. Tabelle 21 zeigt ein mögliche Abbildung der ATM Klassen auf RSVP Klassen.

In [125] wird vorgeschlagen RSVP Reservierungen der *Guaranteed Quality of Service* Klasse (s. [123]) bei einer in der TSpec mit eins angegeben *Token Bucket Depth* als konstanten Datenstrom der *Constant Bit Rate* (CBR) ATM Klasse zuzuordnen. Bei einer Token Bucket Depth größer eins, soll die *Variable Bit Rate real time* (VBR-RT) ATM Klasse verwendet werden. Beide ATM Klassen, CBR und VBR-RT, erfüllen die Anforderungen der Guaranteed Quality of Service Klasse bezüglich zugesicherter Bandbreite und festgelegter End-to-End Verzögerung.

Für die *Predictive Service* Klasse ist die VBR non realtime (VBR-NRT) Klasse geeignet. Diese garantiert zwar keine End-to-End Verzögerung, gibt aber eine erwartete End-to-End Verzögerung an.

Die *Controlled Delay* Klasse[27] fordert einen Quality of Service, der von einem unbelasteten Netzwerk als Best-Effort angeboten wird.

Wie aus 21 ersichtlich ist es unmöglich, alle ATM QoS Parameter in RSVP Parameter zu übersetzen. Eine Übersetzung der Traffic Parameter scheint sogar noch schwieriger. Doch nicht nur die Übertragung der Qos Parameter ist bei der Nutzung von ATM für RSVP/IP Netze problematisch, auch das Management der ATM VCs zur Realisierung von RSVP Verbindungen

[27] Diese in [125] erwähnte Klasse scheint der in [145] als *Controlled-Load Network Element Service* bezeichneten Klasse zu entsprechen

ATM			RSVP	
QoS Class			Service Class	
CBR	QoS	CLR CDV Max CTD	Guaranteed Service	n/a n/a n/a
	Traffic	PCR		Average Token Rate (RSpec)
VBR-RT	QoS	CLR CDV Max CTD		n/a n/a n/a
	Traffic	PCR SCR MBS		n/a Average Token Rate (R of RSpec) Token Bucket Depth
VBR-NRT	QoS	CLR Mean CTD	Predictive Service	n/a Delay as part of RSpec
	Traffic	PCR SCR MBS		n/a Average Token Rate (TSpec) Token Bucket Depth
ABR	QoS	CLR	Controlled Delay	n/a
	Traffic	PCR MCR		n/a Average Token Rate (TSpec)
UBR	Traffic	PCR	Best Effort	No declarations are necessary

Tabelle 21: RSVP und ATM Service Klassen

ist ein zusätzlicher Problembereich. Im folgenden Abschnitt werden dazu einige Lösungsansätze geschildert.

5.4.2 Abbildung von RSVP Verbindungen auf ATM VC

RSVP Verbindungen können auf verschiedene Weise auf ATM VCs abgebildet werden. Zwei davon werden in [24] beschrieben und hier kurz dargestellt.

Einzelner VCs pro RSVP Verbindung Ein Lösung, um RSVP Verbindungen als ATM VCs zu realisieren, besteht darin, für jede RSVP Verbindung, d.h. für jeden reservierten Verbindungspfad einen eigenen VC zuzuordnen. Dabei ensteht das Problem, daß von verschiedenen Empfängern verschiedene QoS angefordert werden. Diese Heterogenität wird gelöst, indem von allen Reservierungsanforderungen das Maximum als Gundlage für den QoS beim VC Aufbau dient.

Da RSVP durch seine Soft State Eigenschaft dynamische QoS Anforderung ermöglicht, dies aber dem Konzept von ATM VCs widerspricht, da hier ein QoS für die gesamte Dauer einer Verbindung vereinbart wird, müßte bei einem Wechsel des QoS in RSVP der VC abgebaut und wieder neu aufgebaut werden. Der Abbau und erneute Aufbau von ATM VCs ist eine komplexe Operation und erfordert ein nicht geringes Maß an Rechenzeit, verbunden mit entsprechender Verzögerung. Um erhebliche Belastung durch diesen Verwaltungsaufwand im ATM Netz zu vermeiden, wird ein Timer benutzt, der Veränderung des QoS auf ATM Ebene nur nach festgelegten Zeitintervallen zuläßt.

Abbildung 80 zeigt eine Konfiguration mit einem Sender S1, der über ein ATM Netz an die

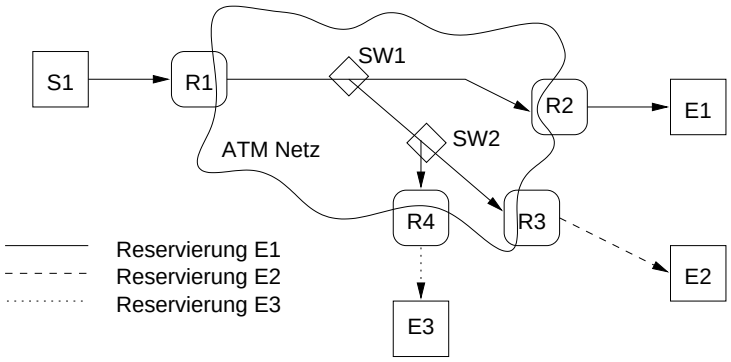


Abbildung 80: RSVP über ATM mit einem VC pro RSVP Verbindung

Empfänger E1-E3 Daten sendet. Empfänger E1 fordert den größten QoS an, so daß die VC Äste zu den Empfängern E2 und E3 ebenfalls den höheren QoS von E1 bieten.

Durch das Prinzip, allen Empfängern den gleichen QoS zuzuordnen, entsteht das Problem des *Free Ride*, den Empfängern über das ATM Netz nutzen, die einen kleineren QoS angefordert haben als den umgesetzten. Ein weiteres Problem liegt im Konzept des "einzelnen VCs pro RSVP Verbindung", wenn ein Empfänger eine existierende VC Verbindung nutzen will, aber nicht genügend Netzwerkressource zur Verfügung steht. Dann ist es dem Empfänger auch nicht möglich, eine Verbindung mit Best-Effort aufzubauen. Zur Lösung dieser beiden Probleme ist ein Modell nötig, das eine RSVP Verbindung auf mehrere VCs abbildet, wie im nächsten Abschnitt beschrieben wird.

Mehrere VCs pro RSVP Verbindung Das vorhergehende Modell, das einen einheitliche Festlegung des QoS impliziert, ist zwar einfach, aber ermöglicht nicht, verschiedene Stufen von QoS auf einer Verbindung umzusetzen. Folgende Modelle können heterogene Reservierungsanforderung umsetzen:

- Zwei VCs pro RSVP Verbindung

  Dieses Modell ermöglicht begrenzte Heterogenität bzgl. QoS Stufen. Über einen VC wird eine Best-Effort Verbindung angeboten und über den anderen ein homogener Quality of Service.

  In Abbildung 81 wird für Empfänger E3 eigens ein zweiter VC aufgebaut, der Best-Effort Service unterstützt. Die restlichen Empfänger E1 und E2 benutzen einen VC mit dem höheren angeforderten QoS von Empfänger E1.

- n VCs pro RSVP Verbindung

  Bei dieser Variante ist der Empfänger nicht auf zwei Stufen von QoS festgelegt, sondern kann beliebig einen QoS anfordern, der durch einen eigenen VC realisiert wird. Ein Nachteil dabei ist der höherer Bedarf an Netzwerkressourcen, da auf jedem VCs Kopien von Paketen befördert werden.

  Dies zeigt Abbildung 82: über den selben Pfad zwischen Router R1 und ATM Switch SW1 transportiert ein VC für Empfänger E2 als auch ein VC Empfänger für E1 identische Pakete.

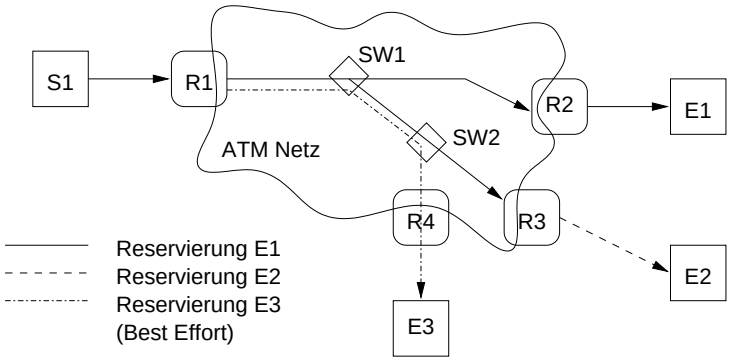


Abbildung 81: RSVP über ATM mit zwei VC pro RSVP Verbindung

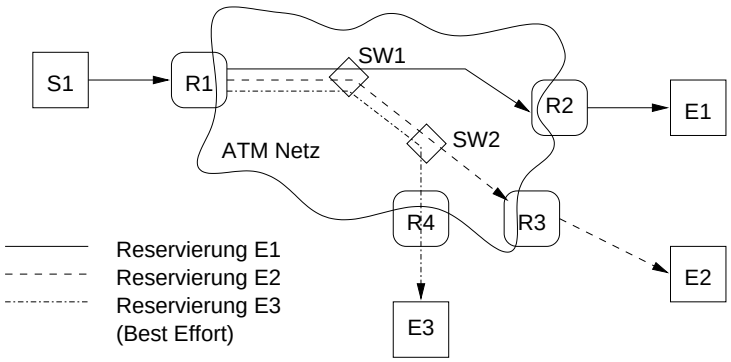


Abbildung 82: RSVP über ATM mit n VC pro RSVP Verbindung

6 xDSL, Cable und Powerline

6.1 Einführung

6.1.1 Der Kampf um die letzte Meile

Durch die Liberalisierung des Telefonmarktes in Deutschland ist auch hierzulande der Kampf um die Kunden voll entbrannt. Doch es geht schon lange nicht mehr nur um das Telefongeschäft. Telefonanbieter, Kabelnetzbetreiber und sogar Energieerzeuger haben erkannt, dass eine zunehmende Vernetzung der Haushalte die Zukunft ist. Auch das zuletzt explosionsartige Wachstum des Internets deutet darauf hin, dass ein Bedarf an schnellen Netzzugängen für Haushalte bereits heute besteht.

Schon vor Jahren wurden Dienste wie Video-on-Demand, Bildtelefonie, interaktive Archive, Fernlernen und, nicht zu vergessen, Telecommuting als die zukünftigen Zugpferde der Computer und Telekommunikationsindustrie ausgemacht. Neu hinzugekommen ist nun der schnelle Internetzugriff, für den es bereits heute eine enorme Nachfrage gibt. Die Vorzüge und Chancen, die diese Dienste bieten, wurden auf vielen Messen und in Fachblättern immer wieder angepriesen. In der Vergangenheit scheiterte die Realisierung solcher Technologien allerdings oft an der noch nicht weit genug entwickelten Computertechnologie, die oben genannte Dienste zwar technisch möglich, jedoch unverhältnismäßig teuer gemacht hätte. Dieser Zustand hat sich grundlegend geändert, und so sind heute die Defizite eher bei der Telekommunikation zu suchen.

Ein kleiner Vergleich sollte dies verdeutlichen. Vor etwa 15 Jahren waren V.22 Modems der Stand der Technik, welche Datenübertragungsraten von 2.4 Kbps über analoge Telefonleitungen ermöglichten. Die heutigen Modems schaffen 56 Kbps oder, im Falle von ISDN (Integrated Digital Services Network) mit Kanalbündelung, 128 Kbps. Dies ist eine Steigerung um den Faktor 50, wenn wir die damaligen Modems mit dem heute durchaus gängigen ISDN messen. An diesem vergleichsweise geringen Fortschritt ist allerdings weniger die Modemtechnologie, sondern vielmehr die Telefonleitung als historischer Flaschenhals schuld. Die Computertechnologie hat sich im gleichen Zeitraum wesentlich stärker entwickelt. So nahm etwa die Speicherfähigkeit, die ja als ein Ausdruck der Leistungfähigkeit eines Computersystems gelten kann, von 256Kb auf 64MB bei Arbeitsspeicher bzw. von 20MB auf 8GB bei Plattenspeichern zu. Dies ist ein Zuwachs um den Faktor 256 bzw. 409. Wir können also konstatieren, dass die Speicherfähigkeit der Computersysteme bei weitem stärker gewachsen ist als die Übertragungskapazität. Bei der Rechenleistung ergibt sich ein noch schärferes Bild, auf das wir hier nicht näher eingehen wollen. Aus diesem Vergleich wird deutlich, dass es im Bereich Datenübertragung deutlichen Nachholbedarf gibt. Die unzulängliche Vernetzung der Haushalte ist der Grund für die fehlende oder nur schleppende Realisierung der oben angesprochenen Dienste.

Für die Austattung von Haushalten mit breitbandigen Netzanschlüssen gibt es zahlreiche Ansätze. Zur Auswahl des geeignetsten Ansatzes sollte man sich allerdings zuerst Gedanken über die ungefähr benötigte Bandbreite machen. In der Vergangenheit wurde als Maßstab immer Video-on-Demand mit einem Bandbreitenbedarf von etwa 1.5 Mbit/sek. gehandelt. Dies gilt im Prinzip immer noch, jedoch sind in den letzten Jahren auch andere Dienste wie HDTV und vor allem schneller Internetzugang hinzugekommen, für die prinzipiell gilt: Je mehr Bandbreite desto besser. Um die notwendige Bandbreite nun bereitzustellen, bedarf es neuer Verteilernetze. Dabei gibt es verschiedene Alternativen, die sich grundlegend unterscheiden. Zum einen gibt es da die Ansätze FTTH (Fiber to the Home) und FTTC (Fiber to the Curb). Beide zielen darauf ab, Glasfaserkabel möglichst nahe zum Endkunden zu bringen. Dies ist zwar technisch gesehen die „ultima ratio“, da durch den Einsatz von Glasfaser eine sehr hohe Übertragungsbandbrei-

te in beide Richtungen erzielt werden kann, aber die immens hohen Investitionskosten machen diese Lösung impraktikabel. Außerdem würde es lange dauern, um damit eine flächendeckende Erschließung zu erreichen. Deshalb kommen diese Ansätze vielleicht mittel- bis langfristig in Frage, nicht aber in der näheren Zukunft.

Um schneller realisierbare und vor allem billigere Lösungen zu finden, führt kein Weg an der Nutzung der bereits vorhandenen Telekommunikationsinfrastrukturen vorbei. So ist fast jedes Haus, zumindest in Deutschland, an das Telefonnetz angeschlossen oder kann binnen weniger Tage angeschlossen werden. Alternativ dazu gibt es noch Strom und Kabelnetze, die theoretisch auch zum Datentransport eingesetzt werden können. Die verschiedenen Anbieter buhlen nun darum, die Haushalte über ihr Medium an ein breitbandiges Datennetz anzuschließen, um so die oben genannten Dienste anbieten zu können. Im Moment kann das in Deutschland nur die Telekom, die ja bekanntlich über die einzigen derzeit nutzbaren Datenleitungen (Telefon und Kabel) verfügt. Dies wird sich hoffentlich ändern.

In den folgenden Kapiteln wollen wir die Technologien, die den schnellen Transport von Daten über die Telefonleitung, das Fernsehkabel und Stromkabel ermöglichen, genauer untersuchen. Den Anfang wird xDSL machen, welches eine Technik darstellt, die hohe Datenraten über verdrillte Kupferkabel, wie sie im Telefonnetz verwendet werden, überträgt. Wir werden dabei sowohl auf die technischen Grundlagen als auch auf konkrete Standards eingehen. Im zweiten Kapitel wird dann die breitbandige Datenübertragung über das TV-Kabel beleuchtet. Dabei werden wir auch auf die zwei führenden Kabelmodemstandards, nämlich IEEE 802.14 und MCNS (Multimedia Cable Network System) eingehen. Das folgende Kapitel beschäftigt sich mit der DPL (Digital Powerline) Kommunikation. Aufgrund des Fehlens von Standards als auch Produkten wird hier mehr auf die technischen Möglichkeiten von DPL eingegangen. Das letzte Kapitel widmet sich konkreten Produkten und den Marktchancen dieser drei Technologien. Der Schwerpunkt wird dabei auf die Situation in Deutschland gesetzt.

6.2 xDSL

Zuerst gilt es einmal das Akronym xDSL zu erklären. DSL steht für Digital Subscriber Line, was soviel heißt wie digitaler Teilnehmeranschluss. Das x steht für die verschiedenen Ausprägungen von DSL, die sich bezüglich Technik, Übertragungsrate und Einsatzgebiet partiell bis erheblich unterscheiden. Der Vollständigkeit halber seien die gängigsten DSL Technologien im Folgenden erwähnt. Sie sind ISDN (auch IDSL genannt), ADSL (Asymmetric Digital Subscriber Line), HDSL (High bitrate Digital Subscriber Line), SDSL (Symmetric Digital Subscriber Line), UDSL (Universal Digital Subscriber Line) und VDSL (Very high bitrate Digital Subscriber Line). Eine ausführliche Diskussion all dieser Techniken würde den Rahmen dieser Arbeit sprengen, weshalb wir hier zuerst einige Prinzipien, die all diesen Techniken zugrunde liegen, behandeln wollen, um anschließend ADSL etwas konkreter zu explizieren. Um uns ein Bild von der Leistungsfähigkeit sowie der Limitationen der DSL Ausprägungen zu verschaffen, sei auf die Tabelle 22 verwiesen.

Nach dieser Erklärung des Akronyms xDSL, bleibt aber die Frage offen, was denn nun ein digitaler Teilnehmeranschluss eigentlich ist. Diesen wollen wir definieren als Leitung, an deren beider Enden ein Transceiver zum Empfang und Senden digitaler Daten angeschlossen ist. Diese Definition sollte auch zeigen, warum wir oben ISDN als xDSL Technologie aufgeführt haben. An einem Ende der ISDN Leitung ist das Vermittlungssystem, am anderen ein NT (Netzwerk Terminator) angeschlossen, durch die digtiale Daten übertragen werden.

Bis jetzt haben wir bezüglich xDSL meistens nur von Leitungen gesprochen. Was xDSL so interessant macht und was hier vielleicht noch einmal betont werden sollte ist, dass alle xDSL

Technologie	*Übertragungsrate*	*Entfernungslimitation*
ISDN	128 Kbps + 16 Kbps[a]	ca. 6 km[b]
ADSL Lite	1 Mbps Downstream [c], 512 Kbps Upstream [d]	ca. 6 km
ADSL/R-ADSL	1,5 - 8 Mbps Downstream, bis 1,544 Mbps Upstream	4 - 6 km
HDSL	1,544 - 2,048 Mbps voll duplex[e]	4 - 5 km
VDSL	13 - 52 Mbps Downstream, 1,5 - 2,3 Mbps Upstream	0,3 - 1,5 km

[a] Outband Signalisierungskanal
[b] kann durch Verstärker verlängert werden
[c] bezeichnet Richtung vom Dienstanbieter zum Teilnehmer
[d] vom Teilnehmer zum Dienstanbieter
[e] verwendet 2 - 3 Kupferdoppeladern

Tabelle 22: Leitungsfähigkeit der verschiedenen xDSL Ausprägungen

Technologien über normale, unkonditionierte, verdrillte Kupferdoppeladern, wie etwa die Telefonleitung, funktionieren und somit eine logische Alternative für die schnelle und kostengünstige Anbindung von Haushalten an breitbandige Datennetze darstellen. Die Frage, die sich nun natürlich stellt ist, wie so viele Daten über ein Kupferkabel übertragen werden können, welches lediglich für die Sprachübertragung konzipiert wurde. Um dies zu verstehen, müssen wir zuerst einmal einen Blick auf die Funktionsweise von POTS (Plain Old Telephony Service), also das analoge Telefonsystem werfen. Dazu soll uns erst einmal Abbildung 83 dienen. Wie zu ersehen, ist jeder Teilnehmer über eine einfache Kupferleitung mit einer Teilnehmervermittlungsstelle verbunden. Bei modernen Telefonnetzwerken, wie sie inzwischen eigentlich üblich sind, läuft das Signal von der Vermittlungsstelle aus digital über Glasfaserkabel weiter. Die analoge Strecke, die es sozusagen zu digitalisieren gilt, verläuft nur von der Vermittlungsstelle zum Teilnehmer. Diese wird auch oftmals als Subscriber Loop oder Local Loop bezeichnet. Bei POTS wird diese Leitung also genutzt, um analoge Sprachsignale zu übertragen. Diese haben eine ungefähre Bandbreite von 3,3 kHz. In der Vermittlungsstelle, wo diese Daten digitalisiert werden müssen, wird dem durch einen Tiefpassfilter Rechnung getragen, der alle höheren Frequenzen herausfiltert. Wenn wir nun einen Rauschabstand von 40 dB annehmen, so können wir laut Shannon nie mehr als 40 Kbps, was etwa der Leistung eines 56K Modems auf durchschnittlichen Telefonleitungen entspricht, übertragen. Der Trick von xDSL liegt nun darin, eine größere Bandbreite des Kupferkabels zu nutzen. Bei ISDN liegt dies bei etwa 120 kHz, bei ADSL handelt es sich um Bandbreiten im Megahertz-Bereich. Wie wir im Folgenden sehen werden, ist eine beliebige Erhöhung der Übertragungsbandbreite aber nicht so ohne weiteres möglich. Störungen sowie die nicht gerade optimalen elektrischen Eigenschaften des Kupferkabels gestalten eine fehlerfreie Übertragung solch großer Datenmengen sehr schwierig. Erst der Einsatz aufwändiger Übertragungsverfahren und Echokompensatoren macht dies möglich.

6.2.1 Die Eigenschaften von Kupferkabel

Wie bereits erwähnt, ist das beim Telefonsystem verwendete Kupferkabel nicht so ohne weiteres zum Transport großer Datenmengen einzusetzen. Der Grund dafür ist sowohl in der Inhomogenität von Telefonleitungen als auch in deren grundlegenden elektrischen Eigenschaften zu suchen. Letzteres kann durch die Grundeigenschaften einer Leitung, den Widerstand, die Induktivität, die Kapazität und die Ableitung beschrieben werden. Diese Grundgrößen hängen vom Aufbau

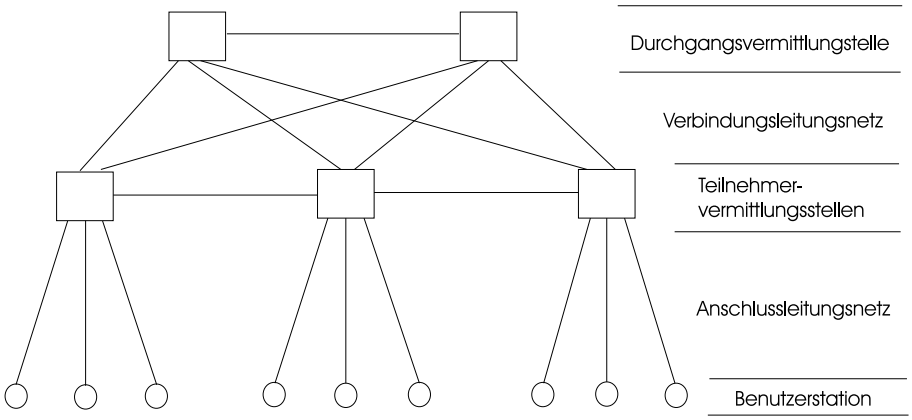


Abbildung 83: Aufbau des Telefonnetzes

der Leitung, den Abmessungen, der Ummantelung, dem Material, der Frequenz und der Temperatur ab. Eine genauere und vor allem mathematische Behandlung all dieser Größen würde den Rahmen dieser Arbeit bei weitem übersteigen und würde zudem einiges an nachrichtentechnischen Vorkenntnissen erfordern, welche wir hier nicht voraussetzen. Von diesen Grundgrößen können aber, mit Hilfe der Leitungstheorie, der Wellenwiderstand und die Dämpfung abgeleitet werden. Die Bedeutung dieser Größen für die Datenübertragung ist recht intuitiv, weshalb wir sie herausgreifen wollen, um die Übertragungseigenschaften von Kupferleitungen zu erklären.

Der Wellenwiderstand ergibt sich aus den vier oben genannten Grundgrößen und ist vor allem wichtig für die Anpassung der Leitung an den Sender und Empfänger. Richtig dimensionierte Abschlusswiderstände an den Leitungsenden verhindern Reflexionen, die die Datenübertragung stören bis unterbrechen können. Das Problem bei den als Telefonleitung verwendeten Kabeln ist eine teilweise Inhomogenität, die einen wechselnden Wellenwiderstand zur Folge hat. Dies erschwert natürlich die Datenübertragung. Typische Werte für den Wellenwiderstand sind 50 - 75 Ω. Aus den hier genannten Gründen sind auch die Abschlusswiderstände bei Ethernet und Koaxialverkabelung notwendig.

Die Dämpfung eines Leiters ist abhängig von der Frequenz. Daraus ergibt sich der Zusammenhang zwischen Distanz und Bandbreite, der in der Einleitung bei den verschiedenen DSL Techniken bereits angesprochen wurde. In Abbildung 84 ist zu sehen, wie die Dämpfung bei einem normalen verdrillten Leitungspaar bei höheren Frequenzen stark ansteigt. Dies limitiert die nutzbare Bandbreite bei einer gegebenen Leitungslänge, oder umgekehrt, die Leitungslänge bestimmt die nutzbare Bandbreite.

Die nun eingeführten Grundgrößen ermöglichen uns, die Übertragungseigenschaften von Leitern, in unserem speziellen Fall von verdrillten Kupferleitungen, quantitativ zu untersuchen und mit Hilfe von Shannon Aussagen über die Übertragungskapazität zu machen. Dazu fehlt uns aber noch ein Parameter, den wir bisher vernachlässigt haben, nämlich das Rauschen. Hierbei kann man in zwei Bereiche gliedern, nämlich Känale ohne und mit äußeren Störungen. Bei den nicht von außen kommenden Störungen sind vor allem Reflexionen und Verzerrungen zu nennen, die durch die Inhomogenität des Leiters und dessen inhärente Eigenschaften hervorgerufen werden. Außerdem ist in diesem Zusammenhang noch das Hintergrundrauschen oder AWGN (Additive White Gaussian Noise) zu nennen, welches durch die regellose, thermisch bedingte Bewegung von Ladungsträgern in Widerständen und Transistoren hervorgerufen wird.

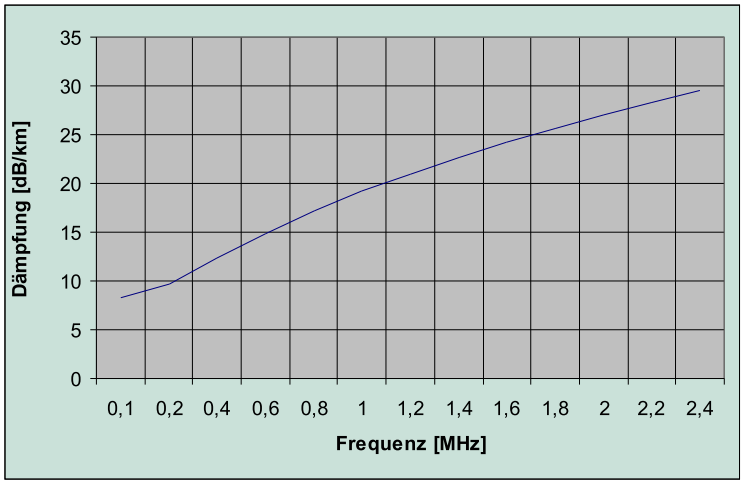


Abbildung 84: Dämpfung bei Telefonkabeln

Die Situation verkompliziert sich erheblich, wenn wir Kanäle mit äußeren Störungen betrachten. Verdrillte Leitungspaare werden ja nicht einzeln im luftleeren Raum, sondern zu Hunderten auf engstem Raum verlegt, was eine induktive und kapazitative Kopplung dieser Adern zur Folge hat. Dies wiederum kann zu Störungen bei der Datenübertragung führen. Diese Störungen werden Nebensprechen genannt. Die räumliche Nähe folgt aus der Zusammenfassung von Kupferadern zu Gruppen und dieser Gruppen zu Kabeln. Bei dieser Zusammenfassung gibt es verschiedene Techniken, nämlich Lagerverseilung und Bündelverseilung. Eine detaillierte Abhandlung ist in [64, 111] zu finden. Hier sei nur erwähnt, dass die Art der Verseilung die Störeinflüsse stark beeinflusst.

Man unterscheidet vor allem zwei Arten von Nebensprechen, nämlich NEXT (Nahnebensprechen, Near-end-Crosstalk) und FEXT (Far-end-Crosstalk). NEXT bezeichnet den Einfluß eines von einem Sender erzeugten Signals auf das für einen Empfänger am gleichen Leitungsende bestimmte Signal. FEXT bezeichnet analog den Einfluß eines Senders auf das Emfangssignal eines falschen Empfängers am anderen Leitungsende.

Andere Störeinflüsse sind Impulsstörungen und RFI (Radio Frequency Interference). Impulsstörungen sind plötzliche kurzzeitige Spannungsschwankungen, die durch äußere oder innere Einflüsse hervorgerufen werden können. Solche Störungen sind oft sehr schwierig zu vermeiden und auch sehr folgenschwer, da sie zu einem totalen Verlust führen. Durch neuere Methoden wie FEC (Forward Error Correction) lässt sich aber ein gewisser Schutz vor solchen Störungen erreichen. RFI kommt vor allem bei Überlandleitungen und in der Nähe von starken Sendeeinrichtungen in Betracht. RFI ist nicht so wichtig wie die anderen Störungsarten, sei jedoch der Vollständigkeit halber erwähnt.

Mit Hilfe der behandelten Grundeigenschaften und der genannten Störungen ist es nun möglich, ein mathematisches Kanalmodell auszuarbeiten, welches das Übertragungsmedium Telefonleitung analytisch beschreibt. Dieses Modell kann dann dazu benutzt werden, Übertragungsverfahren auszuarbeiten, welche die Leitung bestmöglich ausnutzen. Obwohl wir hier aus Platzgründen auf die mathematische Behandlung dieses Kanalmodells verzichtet haben, sollte nun trotzdem klar werden, wie schwierig die Entwicklung eines Übertragungsverfahrens wie ADSL ist und wie

viele Gegebenheiten berücksichtigt werden müssen. Die Auswahl eines Modulations- oder Fehlerkorrekturverfahrens wurde deshalb nicht etwa nach eigenem Gutdünken getroffen, sondern nach akribischer Ausarbeitung eines Kanalmodells und vieler Tests mit diesem Modell. Die verwendeten Verfahren wollen wir nun anhand von ADSL[28] untersuchen, wobei wir immer wieder Bezug auf diesen Abschnitt nehmen wollen.

6.2.2 Grundlagen von ADSL und ADSL Referenzmodell

In diesem Abschnitt werden wir die physikalischen Eigenschaften des Kabels außen vor lassen und mehr auf die Frage eingehen, wie auf diesem Kanal Daten übertragen werden. ADSL lässt sich grob in das OSI Modell als ein Datenübertragungsverfahren klassifizieren, das die Schichten 1 und 2 abdeckt. Demnach ist ADSL also ein gesicherter Bitübertragungsdienst. Vom ADSL Forum wurde allerdings ein eigenes ADSL Referenzmodell entwickelt (siehe Abbildung 85). Wie aus dem Referenzmodell zu entnehmen, wurde beim Design von ADSL vor allem darauf Wert gelegt, dass ADSL parallel zu POTS bzw. auch ISDN funktioniert. Dies wird bei ADSL durch den Einsatz von Filtern, sogenannten Splittern erreicht, welche die Frequenzen des Basisbandes von den höheren, für ADSL verwendeten, trennen. Dadurch ist der Zustand des Telefondienstes völlig unabhängig und unberührt von der Funktion des ADSL Systems. Dies wiederum bedeutet, dass beispielsweise auch telefoniert werden kann, wenn ADSL ausfällt, was von enormer Wichtigkeit für die praktische Anwendbarkeit ist (z.B. Notruf). Um die Kosten und die Komplexität der Installation weiter zu reduzieren, wurde auf Drängen einiger Hersteller auch die Möglichkeit eines splitterlosen ADSL in Betracht gezogen. Diese Variante wird G.Lite oder ADSL Lite genannt. Die Leistung liegt natürlich deutlich unter der des „normalen“ ADSL. Auch wird die Sprachübertragung im Basisband durch ein Einstreuen der hochfrequenten ADSL-Signale hörbar beeinträchtigt. Trotzdem könnte, aufgrund der gewonnenen Bequemlichkeit, ADSL Lite die Nachfolge analoger Modems antreten.

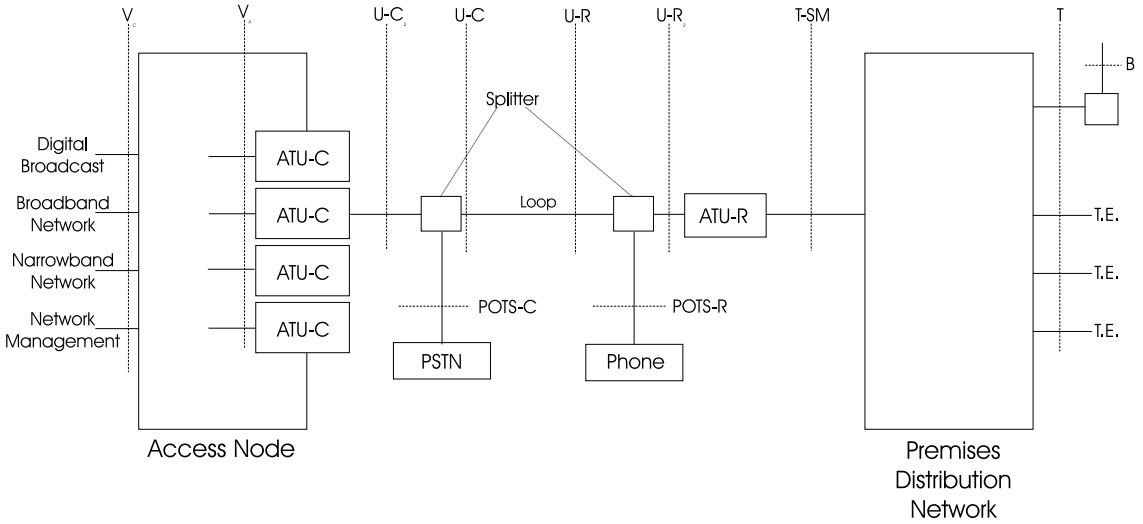


Abbildung 85: ADSL Referenzmodell

Wie im Referenzmodell zu sehen, ist die ADSL Strecke[29] zu beiden Seiten hin abgeschlossen. Das Kopfende wird dabei durch einen sogenannten ATU-C (ADSL Termination Unit-Central

[28] wir halten uns bei der Diskussion von ADSL Spezifika an den ANSI, ETSI Standard T1.413
[29] im Referenzmodell Loop genannt

site), das Teilnehmerende durch einen ATU-R (ADSL Termination Unit-Remote site) abgeschlossen. Bei einem ATU-R wird es sich in der Regel um ein bereits mehrfach erwähntes ADSL Modem handeln. Der ATU-C steht beim Dienstanbieter, welcher ADSL im allgemeinen über DSLAMs (DSL Access Multiplexer), also mehrere Modems in einem Gerät vereint, anbietet. Diese DSLAMs sind wiederum über Switches mit einem breitbandigen Backbone verbunden. Dabei könnte es sich beispielsweise um ATM (Asynchronous Transfer Mode) handeln.

6.2.3 Die Bitübertragungsschicht bei ADSL

ADSL, wie sein Name schon sagt, überträgt asymmetrische Datenströme. Wie bereits oben ausgeführt, ist die Downstream (vom Anbieter zum Kunden) Datenrate erheblich höher als die vom Teilnehmer zur Vermittlungsstelle. Die Gründe dafür sind zweierlei. Der technische Grund ist im NEXT zu suchen. Durch die Bündelung der verdrillten Kupferkabel ist NEXT bei symmetrischen Übertragungstechniken, wie etwa HDSL, bandbreitenlimitierend, während die Asymmetrie NEXT dadurch vermeidet, dass an einem Ende nicht gleichzeitig mit einer hohen Datenrate gesendet und empfangen wird. Das Nahnebensprechen fällt bei xDSL Techniken deshalb so ins Gewicht, weil zur Trennung der Upstream und Downstream Datenströme nicht das Frequenzmultiplexverfahren, sondern Echokompensation verwendet wird. Wie in Abbildung 86 zu sehen, belegen dadurch beide Übertragungsrichtungen das gleiche Frequenzband. Dies ist nur durch den Einsatz von adaptiven Echokompensatoren möglich, welche das gerade gesendete Signal vom empfangenen separieren und dadurch das Signal der Gegenstelle zurückgewinnen. Die technischen Feinheiten dieses Vorgehens sind in [35] nachzuschlagen. Es sei erwähnt, dass sich diese Echokompensation bei ADSL aufgrund der asymmetrischen Datenraten relativ schwierig gestaltet. Glücklicherweise ist das Nutzungsprofil der meisten Datenleitungen auch asymmetrischer Natur. Man denke dabei etwa an den schnellen Internet Zugang, wo verhältnismäßig kleinen Anfragen größere Downstream Datenmengen entgegenstehen, so dass diese Asymmetrie auch vom Nutzungsstandpunkt durchaus wünschenswert ist.

Um nun die Daten de facto auf die Leitung zu bringen, bedarf es einer Modulation. Bei der Standardbildung wurden dafür das CAP (Carrierless Amplitude Modulation) Verfahren und DMT (Discrete Multitone Modulation) ins Auge gefasst. CAP gehört zur Klasse der althergebrachten Einträgerverfahren. CAP ist dem bekannten QAM [111] sehr ähnlich, da die zur Übertragung eines Bitmusters erzeugten Sendesignale identisch sind. Der Unterschied liegt in der Signalerzeugung, bei der QAM einen Träger durch Oszillatoren moduliert, während CAP eine trägerlose Signalerzeugung durch Bandpassfilter spezifiziert. DMT ist im Gegensatz dazu ein neueres Vielträgerverfahren, welches eine weitaus bessere Ausnutzung der Bandbreite zulässt. Dies wird durch eine Aufteilung des vorhandenen Sendespektrums in 256 Unterkanäle erreicht. DMT gleicht damit dem parallelen Einsatz vieler Einträgersysteme, die sich das vorhandene Sendespektrum im FDM (Frequency Divison Multiplex) Verfahren teilen. Der große Vorteil dieses Ansatzes liegt in der Flexibilität, über gestörte Unterkanäle weniger oder gar keine Daten zu übertragen. Außerdem kann die Sendeleistung pro Kanal angepasst werden, was eine bessere Annäherung an das Optimum zulässt als bei CAP. Bei ADSL werden nun in jedem der Unterkanäle pro Schritt und abhängig von den Eigenschaften des Kanals zwischen 2 und 15 Bits übertragen. Die ankommenden Datenbits werden hierfür mittels festgelegter Konstellationsmuster[30] auf Symbole abgebildet. Es werden auf diese Weise also bis zu 256 Symbole parallel erzeugt, welche nun zur Übertragung bereitstehen. Dafür werden die Symbole als ein Symbolvektor komplexer Frequenzen interpretiert. Über eine IDFT (Inverse Diskrete Fouriertransformation) wird dieser Vektor in Abtastwerte eines Zeitsignals transformiert. Dieses wird

[30] abhängig von den Kanaleigenschaften zwischen 2^2 und 2^{14} Symbole pro Muster

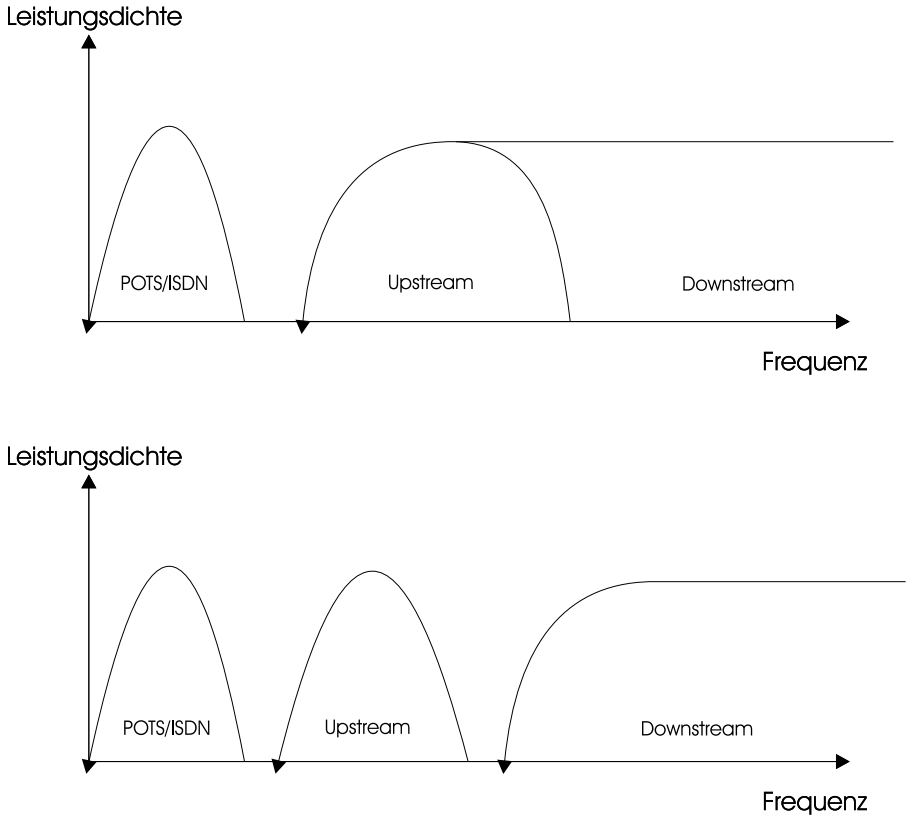


Abbildung 86: xDSL Spektrum

seriell an einen D/A-Wandler gegeben, der die digitalen Abtastdaten in analoge Spannungspegel konvertiert. Dieses Signal kann dann über die Leitung übertragen werden, um auf der anderen Seite mittels eines A/D-Wandlers und einer DFT (Diskreten Fourier Transformation) den Symbolvektor zurückzugewinnen.

6.2.4 Die Sicherungsschicht bei ADSL

Wie bereits mehrfach erwähnt, sind die Telefonkabel alles andere als ein ideales Übertragungsmedium. Um trotzdem hohe Datenraten mit tolerablen Fehlerraten zu erreichen, bedient sich ADSL ausgefeilter, fehlererkennender und fehlerkorrigierender Codes. Hierbei gilt es bei ADSL zwei Übertragungsmodi zu unterscheiden, den Fast-Modus und den Interleaved-Modus, welche sich bezüglich der Fehlerkorrektur und der Übertragungsverzögerung[31] (Latency) unterscheiden [35, 64]. Wie später zu sehen ist, werden Daten im Fast-Modus sofort übertragen, während beim Interleaved-Modus zuerst eine Codespreizung vorgenommen wird. Diese verteilt im Bytestrom aufeinanderfolgende Bytes so, dass sie bei der Übertragung in verschiedene Codeworte fallen. Dadurch wird eine größere Unempfindlichkeit gegen burstartige Fehler erreicht [35]. Nachdem der Empfänger die Daten wieder in die richtige Reihenfolge gebracht hat, treten die Fehler einzeln in verschiedenen Codeworten auf. Diese lassen sich dank des Einsatzes eines fehlerkorrigierenden Codes in aller Regel leicht beheben. Bei ADSL wird dafür ein sogenannter Reed-Solomon Code

[31] beträgt beim Interleaved Modus etwa 20ms

verwendet. Die Reed-Solomon-Codierung basiert auf erweiterter Galois Körper Arithmetik in $GF(2^8)$. Für eine weitreichendere Erklärung von Reed-Solomon Codes sei auf [64, 35] verwiesen. Reed-Solomon Codes können mehr Fehler erkennen und beheben als die bekannten CRCs (Cyclic Redundancy Code) [134]. So können bei einem Overhead von R Bytes, $\frac{R}{2}$ Bytes korrigiert werden. Der daraus entstehende Datenstrom ist aber nicht sehr gut für die direkte Übertragung geeignet, weil es eine klare Grenze zwischen den Redundanzbits und den Datenbits gibt. Außerdem müssen nun aufgrund der Redundanz mehr Daten übertragen werden als ursprünglich. Um diese Effekte auszugleichen, kann bei ADSL sogenanntes Trellis Coding zum Einsatz kommen, welches die Bits im Datenstrom nach vorgegebenem Schema durcheinanderwürfelt. Die Dekodierung erfolgt nach dem maximum-likelihood Prinzip durch einen Viterbi Algorithmus [35]. Dies steigert den effektiven Signal/Rauschabstand um 4.2 dB, was wiederum eine Erhöhung der nutzbaren Bandbreite zur Folge hat.

Der ADSL Standard sieht sieben logische Kanäle zum Datentransport vor. Darunter sind bis zu sieben unabhängige Simplex-Kanäle zum Downstream Datentransport, genannt AS0 - 3 und LS0 - 2, sowie bis zu drei Duplex-Kanäle. Die Datenrate eines jeden Kanals muss ein Vielfaches von 32 Kbps sein mit Ausnahme von LS0, wo die Datenrate 16 Kbps betragen kann. Zusätzlich bietet ADSL aber einen Synchronisationsmechanismus, der auch Datenraten, die keine ganzzahligen Vielfachen von 32 Kbps sind, ermöglicht. Wie bereits oben kurz angesprochen, bietet ADSL zwei unterschiedliche Übertragungsmodi: den Fast-Modus und den Interleaved-Modus. Je nachdem, ob beide Modi parallel (Dual Latency) oder nur einer der beiden (Single Latency) unterstützt werden soll, ändert sich die Nutzung der Kanäle. Jedem logischen Kanal kann unabhängig eine Latency zugeordnet werden. Die Aufteilung der Gesamtbandbreite in logische Kanäle schlägt sich natürlich in der Rahmenbildung nieder. Zur Übertragung stellt ADSL die Daten in Rahmen (Frames) zusammen, welche wiederum in Superframes gruppiert werden. Der Aufbau eines Downstream Superframes ist Abbildung 87 zu entnehmen. Die Upstream Rahmenbildung funktioniert analog für die Kanäle LS0-2 und wird deshalb hier nicht näher erörtert (siehe [35]). Die Sichtweise der hier vorgestellten Konzepte ist also die des ATU-C. Ein Superframe besteht aus 68 Frames mit einem darauf folgenden Synchronisationssymbol. Die Übertragung eines Superframes dauert 17ms, was aus Benutzersicht einer Framerate von 4 kHz entspricht $(68 \cdot 250\mu s = 17ms)$. Die Übertragung des Synchronisationssymbols erfolgt für den Benutzer transparent. Aus Abbildung 87 ist auch der grobe Aufbau eines Frames ersichtlich. Es besteht aus einem Fast Buffer und einem Interleaved Buffer. Wie bereits erwähnt, kann jeder logische Kanal entweder dem Fast- oder dem Interleaved-Pfad zugeordnet werden. Die Zuordnung und die Datenrate pro logischem Kanal bestimmt das genaue Aussehen des Fast oder Interleaved Buffers. Der detaillierte Aufbau des Fast Buffers ist in Abbildung 88 zu sehen.

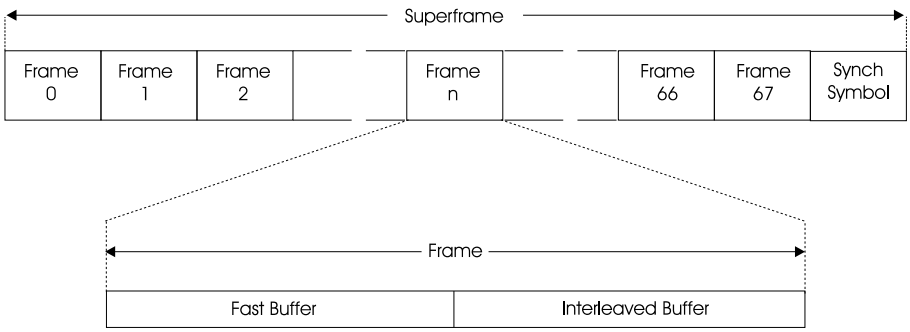


Abbildung 87: ADSL Superframe

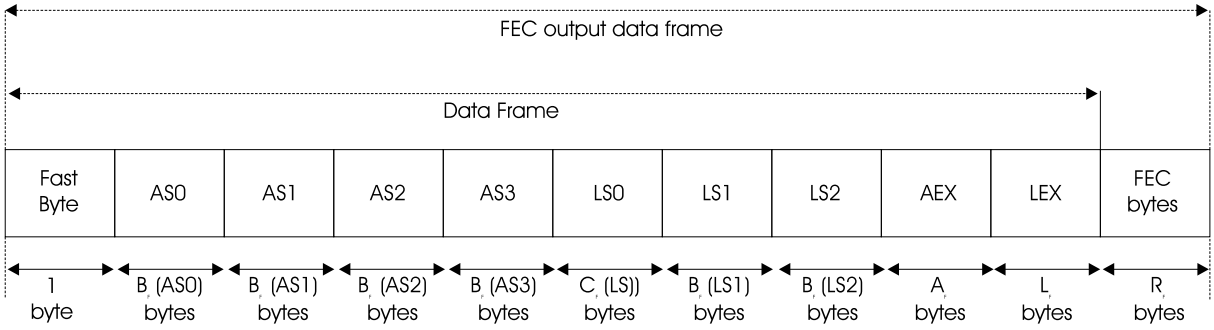


Abbildung 88: Downstream Fast Data Buffer

Die sieben logischen Kanäle werden im Zeitmultiplexbetrieb übertragen, weshalb für jeden Kanal ein Slot pro Frame existiert. Das Fast Byte enthält in Frame 0 eine CRC Prüfsumme über den Fast Buffer des vorhergehenden Superframes. In den übrigen Frames enthält es Informationen zum Betrieb und zur Wartung oder Synchronisationsinformation. Diese kann dazu verwendet werden, Datenraten, die keine Vielfachen von 32 Kbps sind, zu realisieren. Dafür kommen die AEX und LEX Bytes zum Einsatz, indem über sie versandte Bytes an bestimmten Stellen in den Datenstrom eingeschoben werden. Eine Beispielanwendung für diesen Mechanismus ist der Transport eines DS1 Signals mit 1,544 Mbps. Wenn man 48 Bytes pro Rahmen im AS0 Kanal versendet und zusätzlich ein Byte im AEX Feld jedes vierten Rahmens, so kommt man auf eine Datenrate von $48\frac{1}{4}\frac{Bytes}{Rahmen} \cdot 4000\frac{Rahmen}{s} = 1{,}544$ Kbps. Zur Reduktion des Overheads können die Synchronisationsfelder auch ignoriert werden. Das letzte noch zu erklärende Feld ist das FEC Feld, welches Paritätsbits zur Sicherung enthält. Die Paritätsbits werden derart berechnet, dass das entstehende Codewort ein gültiges Reed-Solomon-Codewort ergibt. Wie bereits oben erwähnt, wird im Fast-Modus allerdings keine Codespreizung vorgenommen. Diese zusätzliche Sicherheit bietet nur der Interleaved Modus.

Der Interleaved Buffer (siehe Abbildung 89) ist mit dem Fast Buffer beinahe identisch. Der große Unterschied besteht in der Funktionsweise des FEC-Codierers. Während beim Fast Buffer für jeden Rahmen das Paritätsfeld berechnet wird, erfolgt diese Berechnung beim Interleaved Buffer einmalig für Gruppen von X aufeinanderfolgenden Frames (siehe Abbildung 89). Dies bedeutet, dass immer X Frames zwischengespeichert werden müssen, wodurch sich die Übertragungsverzögerung erklärt. Die berechneten Paritätsbytes werden wieder auf die Frames verteilt und so versandt. Hiermit wollen wir es bei der Vorstellung von ADSL belassen. Viele Fragen wurden nur angeschnitten bzw. überhaupt nicht behandelt, da es aus Platzgründen nicht möglich ist, ADSL in all seinen Einzelheiten vorzustellen. Für eine eingehendere Betrachtung sei auf [64, 35] verwiesen.

6.2.5 Zusammenfassende Bemerkungen über xDSL

Im letzten Abschnitt wurden die technischen Einzelheiten von ADSL genauer vorgestellt. Viele der Probleme als auch der Lösungen, die für ADSL genannt wurden, sind so oder ähnlich auch für die anderen Ausprägungen von xDSL gültig. Dies gilt insbesondere für das in der Entwicklung befindliche VDSL, welches als das „Next Generation ADSL“ [35] betrachtet werden kann. Es erreicht die Datenratensteigerung fast ausschließlich durch die Erweiterung der Bandbreite

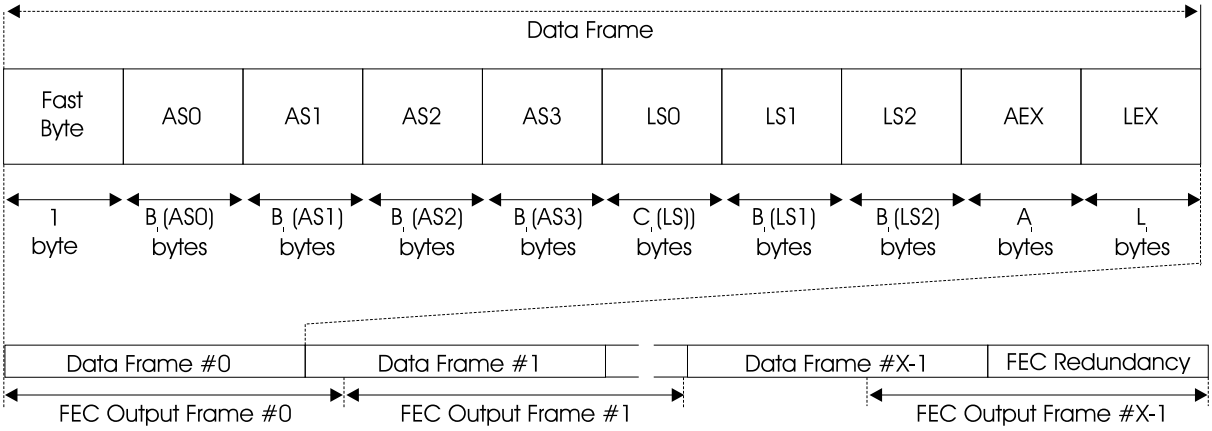


Abbildung 89: Downstream Interleaved Data Buffer

auf über 10 MHz mit einer damit verbundenen Verkürzung der Einsatzreichweite. Die enorme Komplexität von ADSL spiegelt die Schwierigkeiten wider, welche die Datenübertragung auf solch schlechten Medien wie Telefonkabeln bereitet. Es hat aber auch etwas mit den mannigfaltigen Problemen zu tun, die im praktischen Einsatz auftreten können. So musste ADSL auf Verträglichkeit mit vorhandenen Techniken wie POTS, ISDN, T1/E1, und HDSL getestet und abgestimmt werden. All dies musste bei der Spezifikation in Betracht gezogen werden. Es war also ein langer und steiniger Weg, bis ADSL zu einem Standard wurde, und es bedurfte vieler neuer Erkenntnisse in der Forschung, um ADSL zu entwickeln. Es ist also nicht verwunderlich, dass ADSL mehrere Jahre von der Erfindung bis zur Serienreife brauchte und es erst allmählich Verbreitung findet.

6.3 Cable

Die in diesem Abschnitt vorgestellte Data over Cable Technik bedient sich des Fernsehkabels und sogenannter Kabelmodems, um breitbandige Datenübertragung zu realisieren. Das Fernsehkabel bietet gegenüber den übrigen hier vorgestellten Medien den Vorteil, dass es ursprünglich für den breitbandigen Datentransport, wenn auch den analogen, entwickelt wurde. Praktischerweise ist es zumindest in den größeren Städten ebenfalls flächendeckend vorhanden. Das große Aufsehen, welches die Data over Cable Technologie in den Fachkreisen erregt hat, ist nicht alleine mit seinen technischen Eigenschaften zu erklären, obwohl diese durchaus überzeugen können. So sind zum Beispiel Downstream Datenraten von etwa 40Mbps denkbar. Upstream sind es nach dem heutigen Stand der Technik zwischen 0.32Mbps und 10Mbps. Data over Cable hat das Potential, wirklich multimediale Inhalte in jeden Haushalt zu liefern. Dazu könnte unter anderem auch ein Telefondienst zählen, welcher Kabelanbietern den lukrativen Telefonmarkt öffnen könnte. Gerade diese Möglichkeit war es, die vor allem in den USA die Entwicklung vorantrieb. In den letzten Jahren war die steigende Popularität des Internets natürlich ein weiterer positiver Faktor für die Entwicklung. Dies führte zu den zwei großen Kabelmodemstandards, dem IEEE 802.14 und dem MCNS. Wie wir später sehen werden, liegen die Unterschiede dieser beiden Standards vor allem beim Medienzugriffsverfahren, welches der vielleicht interessanteste Teilaspekt ist.

Nach dieser Einführung ist es nun an der Zeit, genauer auf die Architektur, die Protokollfragen und die Standards der Data over Cable Technologie einzugehen. Den Anfang soll dabei

ein Kurzüberblick über moderne Kabelnetze machen. Diese bestehen nämlich nicht nur aus Koaxialkabeln, sondern sie sind sogenannte HFC (Hybrid Fiber Coaxial) Netze, welche also teilweise aus Glasfaser- und teilweise aus Koaxialkabeln bestehen (siehe auch Abbildung 90). Am einen Ende dieses Netzes befindet sich die sogenannte Kopfstelle[32]. Dort werden die Signale der verschiedenen Fernsehstationen, Radiostationen und, bei der Data over Cable Technologie auch Daten auf das Kabel, den sogenannten Trunk, gemultiplext. Dieses Glasfaserkabel läuft zu einem Verteilerknoten und dann weiter zu einem Glasfaserknoten. Dort wird das Signal mittels eines opto-elektrischen Konverters in mehrere Koaxialkabel gespeist, welche wiederum die Häuser versorgen. Ein Trunk versorgt in etwa 500 Teilnehmer, obwohl die Zahl natürlich von Anbieter zu Anbieter variiert. Da diese Architektur keine Schaltelemente, sondern nur Verstärker und Opto-Elektrische Wandler enthält, sind die Kosten relativ niedrig. Wie bereits erwähnt, vereinfachen die elektrischen Eigenschaften von Koaxialkabeln die Datenübertragung erheblich. Die nutzbare Bandbreite eines modernen HFC Netzes liegt bei etwa 750 MHz [134], also ein enormes Potential, das natürlich nicht komplett für Data over Cable genutzt werden kann. Klassisches Radio und Fernsehen sowie neuerdings digitales Fernsehen müssen ja auf dem gleichen Kabel übertragen werden. Heute übliche Kabelmodems nutzen eine Bandbreite von 6 - 8 MHz, also genau jene eines Fernsehkanals. Als Modulationsverfahren werden in allen gängigen Kabelmodemstandards Downstream 64 oder 256 QAM verwendet. Upstream kommt das weniger leistungsfähige, dafür aber robustere QPSK zum Einsatz. Als Kodierung werden die von ADSL bekannten Reed-Solomon Codes verwendet.

Die bisherige Diskussion läßt uns zu dem Schluss kommen, dass im Gegensatz zum ADSL und der unten behandelten DPL die Probleme beim Data over Cable nicht bei der Bitübertragung zu suchen sind. In der Tat liegen die wahren Probleme in der Rückkanalfähigkeit und dem Medienzugriff. Das Telekabel wurde ursprüglich nur zur Übertragung von unidirektionalen Signalen von der Kopfstelle zum Kunden ausgelegt. Data over Cable verlangt aber einen bidirektionalen Kanal. Das HFC Kabelnetz muss also entsprechend aufgerüstet werden, also etwa durch den Einbau bidirektionaler Verstärker sowie Elektro-Optischer Wandler. Diese Aufrüstung sollte zumindest in Deutschland laut [121] bei einem Großteil der Teilnehmer relativ problemlos möglich sein. Die Rückkanalfähigkeit zieht aber weitere Konsequenzen nach sich. Da alle Rückkanalsignale spätestens im Trunk zusammenlaufen, muss ein Medienzugriffsverfahren zur Sychronisation der Kommunikation bereitgestellt werden. Hier liegt der große konzeptionelle Unterschied zu ADSL, welches ja immer eine Punkt-zu-Punkt Verbindung verwendet. Dies ist auch der Ansatzpunkt vieler Kritiker, die die Datensicherheit gefährdet sehen. Außerdem besteht natürlich die Möglichkeit der Überlastung durch simultanen, massiven Bandbreitenverbrauch vieler Benutzer. Das große konzeptionelle Problem bei Data over Cable ist also die Broadcast Natur des Mediums, welches die Stationssynchronisation auf Bit und Frame Ebene, ein Rückkanalzugriffsverfahren, eine Kollisionsresolution sowie Sicherheitsmaßnahmen zur Abhörsicherheit notwendig macht.

6.3.1 Die Standards IEEE 802.14 und MCNS

Die Industrie erkannte sehr schnell, dass es für eine breite Akzeptanz von Kabelmodems nötig sein würde, ihre Kabelmodems durch einen gemeinsamen Standard kompatibel zu machen. So wurde die IEEE 802.14 Gruppe bereits 1994 gegründet, hat es aber bis heute nicht fertiggebracht, einen verbindlichen Standard zu setzen. Die dauernden Verzögerungen brachten einige Hersteller[33] dazu, einen eigenen Standard, MCNS, zu kreieren. Während IEEE stets bestrebt war, einen

[32] auch Headend genannt

[33] dazu gehören unter anderen Cisco, 3Com, Motorola, Nortel, Com21, GE, Samsung, Thomson, Toshiba, Sony, Zenith, AT&T, Microsoft (@Home), Time Warner, TCI, Cox, Comcast,...

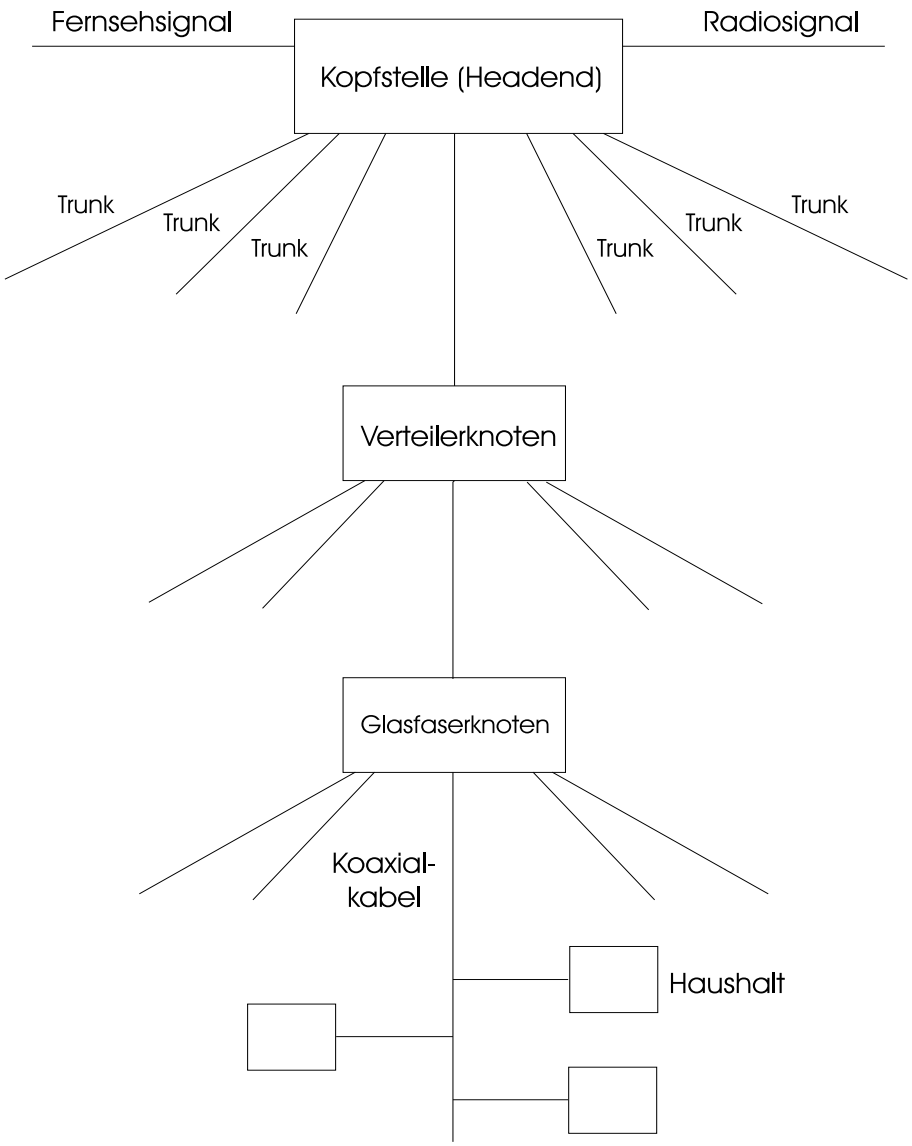


Abbildung 90: Aufbau des Kabelnetzwerks

zukunftssicheren Standard zu schaffen, wurde bei MCNS mehr Wert auf andere Gesichtspunkte wie etwa Time to Market oder die Kosten der Hardware gelegt. Dies führte natürlich zu teilweise erheblich unterschiedlichen Lösungen der oben genannten Probleme. Diese wollen wir jetzt der Reihe nach besprechen.

Beginnen wir mit dem Anschluss des Kabelmodems an das Netz. Das Modem muss zuerst einen Downstream Kanal finden, wozu es alle gültigen Frequenzen absucht. Nun muss es sich auf der Bit-Ebene synchronisieren um dann den Upstream Kanal zu finden, dessen Charakteristika periodisch übermittelt werden. Der Upstream Kanal wird durch Frequenzmultiplex und Zeitmultiplex Verfahren aufgeteilt. Da die Stationen den Upstream Kanal nicht abhören können, ist es notwendig, dass die Kopfstelle den Zugriff auf diesen steuert. Der Zugriff auf den Upstream Kanal funktioniert etwa nach folgendem Schema (siehe Abbildung 91).

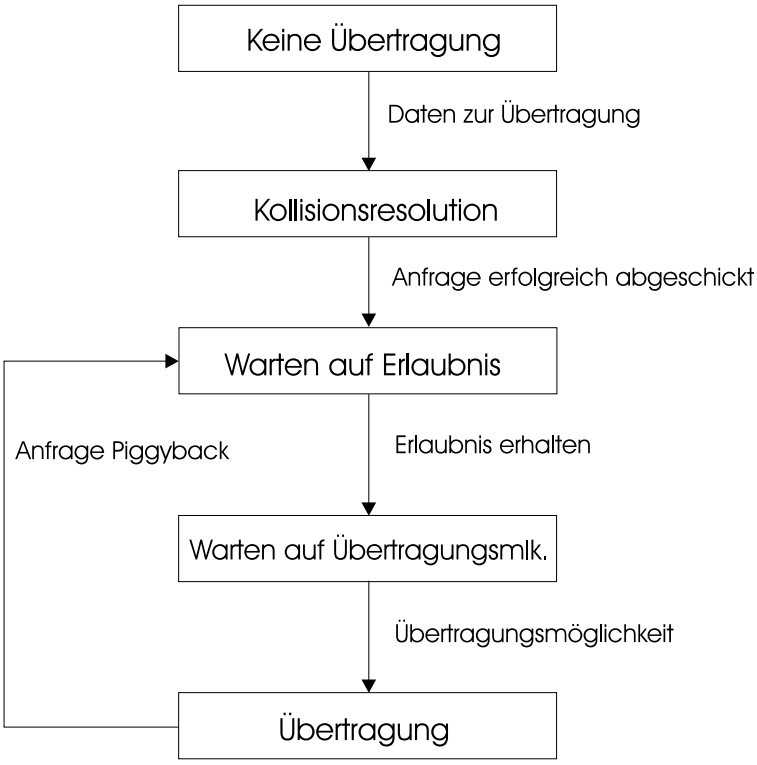


Abbildung 91: Zustandsdiagramm für Station

Wir sehen, dass bei diesem Rückkanalzugriffsverfahren Stationen immer zuerst Bandbreite reservieren müssen[34], bevor es ihnen erlaubt ist, zu senden. Dazu sammelt die Kopfstelle solche Anfragen in der „Bandwidthallocationmap“, welche periodisch im Downstream Kanal übertragen wird. Dadurch erfahren sendewillige Stationen, welche Zeitschlitze ihnen zugeteilt wurden. Der Upstream Kanal ist deshalb in Anfrageminislots und Datenminislots aufgeteilt. Um die Wahrscheinlichkeit von Kollisionen gering zu halten, wurden die Slots des TDM möglichst klein gewählt, daher der Name „Minislots“. Zur weiteren Reduktion der Kollisionswahrscheinlichkeit ist es einer gerade sendenden Station auch möglich, weitere Bandbreitenanfragen an einen Datenminislot anzuhängen (Piggybacking).

Bevor wir jetzt auf die hier noch offen gelassene Frage der Kollisionsresolution eingehen, müssen wir noch mit einer weiteren Eigenheit eines HFCs fertig werden, und zwar mit dem großen Propagation Delay. Wie oben gesehen, müssen Stationen Bandbreite reservieren, welche sie dann auch in Form mehrerer Minislots zugeteilt bekommen. Wenn die Kopfstelle aber nun einer Station A den Minislot i zuteilt, muss die Station A wissen, wann sie die Daten abzuschicken hat, damit sie zum richtigen Zeitpunkt ankommen. Dies ist schwierig, da praktisch alle Stationen verschieden weit von der Kopfstelle entfernt sind. Es muss also eine Synchronisation erfolgen, die diese Verzögerung kompensiert. Dies kann erreicht werden, indem jeder Station eine Zeit zugewiesen wird, die sie zu warten hat, bevor sie Daten versendet. Bei Stationen, die näher an der Kopfstelle liegen, ist diese Zeit natürlich länger, bei solchen, die weiter weg sind kürzer,

[34]beim MCNS Standard gibt es auch einen sog. Immediate Access Mode, der aber nur bei niedriger Auslastung des Netzes genutzt werden darf

während die am weitesten entfernte Station überhaupt nicht warten muss. Dieser Zeitfaktor wird als RTC (Round-Trip Correction) bezeichnet (vgl. Abbildung 92). MCNS und IEEE nutzen ähnliche Verfahren, um diese Zeit zu bestimmen, die in [96, 94] nachzulesen sind.

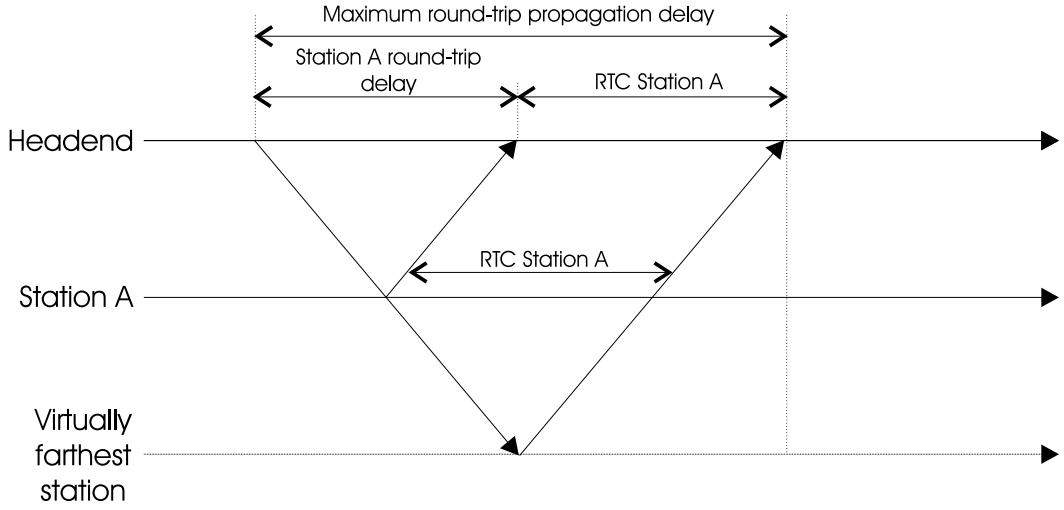


Abbildung 92: Round Trip Correction

Bei der oben besprochenen Reservierung von Bandbreite, kann es zu Kollisionen der Anfragepakete kommen. Diese müssen insbesondere deshalb auf möglichst effiziente Art und Weise gelöst werden, weil die Stationen im Gegensatz etwa zum Ethernet das Medium nicht abhören können und deshalb jedes Mal lange Zeit auf Antwort von der Kopfstelle zu warten haben. IEEE 802.14 und MCNS nutzen dafür erheblich unterschiedliche Kollisonsresolutionsalgorithmen. Der IEEE Standard verwendet hier ein recht kompliziertes Verfahren, welches aus einer Kombination von n-ary Tree (siehe[134, 111]) mit p-persistence (siehe[134, 111]) Algorithmen sowie mehreren parallel laufenden CREs (Collision Resolution Engines) besteht. Bei beiden Standards gibt es spezielle Minislots auf dem Upstream Kanal, die für die Reservierung von Bandbreite vorgesehen sind. Bei IEEE 802.14 sind diese Minislots durch Prioritäten und eine Admission Time Boundary, die sicherstellen soll, dass ältere Anfragen bevorzugt behandelt werden, weiter aufgeteilt. Wenn die vorliegende neue Anfrage die korrekte Priorität hat und bereits *alt* genug ist, kann sie laut der First Transmission Rule gesendet werden. Wenn es hierbei zu einer Kollision kommt, greift die Retransmission Rule, welche dann unter Verwendung von n-ary Tree und p-persistence Algorithmen diese Kollision zu lösen versucht. Eine detailliertere Abhandlung ist in [63, 96, 94] zu finden. Aus obiger Kurzbeschreibung ist bereits die Komplexität dieses Verfahrens ersichtlich, welches zwar technisch ausgeklügelt, aber eben auch schwierig zu implementieren und damit teuer ist. Genau diese Komplexität wird aber bei MCNS zu verhindern versucht, weshalb es nicht verwunderlich ist, dass hier ein anderes, viel simpleres Verfahren zum Einsatz kommt. MCNS verwendet einen elementaren Binary Exponential Backoff Algorithmus [134], der natürlich viel einfacher zu implementieren ist. Näheres hierzu findet man in [96].

Bisher haben wir immer von Stationen gesprochen, die Bandbreitenanfragen stellen und somit am Vielfachzugriff teilnehmen. Genauer betrachtet ist dies nicht genau zutreffend, da beide Standards Virtual Queues, eine weitere Multiplexebene, definieren. Jede Station hat eine eindeutige 48 Bit MAC (Medium Access Control) Adresse und eine oder mehrere 14 Bit Virtual Queue Adressen, die während der Initialisierung zugewiesen werden. Diese Adressen werden Local ID (IEEE) oder Service ID (MCNS) genannt und referenzieren eine Virtual Queue. Wie bereits

oben angedeutet, nimmt jede dieser Virtual Queue eigenständig am MAC Protokoll teil, was auch schon ihre Bedeutung impliziert. Sie können etwa für die Realisierung von Dienstgüten verwendet werden, indem die Kopfstelle die Bandbreitenvergabe je nach Dienstklasse einer Virtual Queue steuert. Außerdem ermöglichen sie die einfache Adressierung von Gruppen von Stationen (Multicasting). Bei IEEE 802.14 wurde ein noch mächtigerer Ansatz gewählt, wo zwischen die Station und einer Virtual Queue noch die Abstraktionsebene einer Virtual Station eingezogen wird. Diese weitere Abstraktion erlaubt eine noch feingranularere Differenzierung der zu transportierenden Daten, womit sich bessere Scheduling Algorithmen für die Bandbreitenvergabe entwickeln lassen (siehe auch [95]). Der Hauptgrund, warum dieser Ansatz in IEEE 802.14 gewählt wurde, ist allerdings die leichte Abbildbarkeit von aus dem Backend kommenden ATM PVCs (Permanent Virtual Circuits) und SVCs (Switched Virtual Circuits) auf diese Anordnung.

Wie bereits erwähnt, können bei HFCs immer alle Stationen den Downstream Kanal abhören. Es ist offensichtlich, dass die Sicherheit in einem so gearteten Netz von besonderem Interesse sein muss. Diese Sicherheit kann durch Verschlüsselung erreicht werden, wie das auch bei IEEE 802.14 und MCNS der Fall ist. Beide Standards verschlüsseln alle Nutzdaten mit DES [88]. Der Unterschied liegt lediglich im verwendeten Modus, nämlich ECB (Electronic Code Book) für MCNS und CBC (Cipher Block Chaining). Da DES ein symmetrisches Chiffrierverfahren ist, muss bei der Initialisierung zuerst ein Schlüsseltausch erfolgen. Dieser wird bei MCNS durch RSA [88] abgewickelt. IEEE 802.14 spezifiziert dafür den nicht weniger sicheren Diffie-Hellman Schlüsseltausch [88]. Die dadurch erreichte Sicherheit sollte bei beiden Standards für den Normalgebrauch ausreichend sein. Der Einschätzung des Autors nach liegt die größere Sicherheitsproblematik eher bei den verwendeten Diensten (z.B. Internet) als in der Data over Cable Technik.

6.4 Powerline

Dieser Abschnitt widmet sich der DPL (Digital Powerline) Technik, welche den Datentransport über gewöhnliche Stromkabel ermöglicht. Der große Vorteil des Stromkabels liegt in der flächendeckenden Verfügbarkeit sowie der Bequemlichkeit für den Nutzer. Ein DPL-Netz würde es erlauben, einen Computer nur an die Steckdose anzuschließen und sofort *loszulegen*. Dies wäre ein erheblicher Fortschritt in Sachen Benutzerfreundlichkeit, aber es hört sich in den Marketingbroschüren der Energieindustrie besser an als es dann in Wirklichkeit ist; da gibt es nämlich noch technische Probleme von einem Ausmaß, das durchaus Fragen nach der Zukunft dieser Technologie aufwirft.

Um DPL zu verstehen, müssen wir uns zuerst einen Überblick über den Aufbau des Stromnetzes verschaffen. Erzeugt wird der Strom natürlich im Kraftwerk, um dann in Hochspannungsleitungen in die Nähe des Verbrauchsortes, etwa eine Stadt, geführt zu werden. Dort verteilt ein Umspannwerk den Strom auf mehrere Mittelspannungsleitungen, welche dann die lokalen Trafostationen mit Strom versorgen. Diese Trafostationen transformieren den Strom auf die uns bekannten 230V. Über Niederspannungsleitungen werden dann die Haushalte an diese Trafostationen angeschlossen. Die Frage, die sich selbstverständlich stellt, ist, wo nun DPL ins Spiel kommt. Da Stromleitungen keine guten Datenübertragungsmedien sind, erscheint es logisch, die Daten nur so kurz wie möglich auf Stromleitungen zu transportieren. Die nächstgelegene Zentralstelle von den Haushalten aus gesehen sind die Trafostationen, welchen bei der DPL somit die Aufgabe der Dateneinkopplung zukommt.

Die Idee, Daten über das Stromnetz zu übertragen, ist eigentlich uralt. Bereits 1922 wurde die TFH (Trägerfrequenztechnik) auf Hochspannungsleitungen eingeführt. TFH eignet sich etwa zur Erfassung von Lastverteilungen an den Umspannstationen. Auf der Mittelspannungsebene gibt

es seit längerem TRT (Tonfrequenz-Rundsteuertechnik), die schmalbandigen Datentransport bis hinüber in die Niederspannungsebene erlaubt, was etwa dazu benutzt werden kann, Stromzähler bei Kunden zwischen Nacht- und Tagtarifen umzuschalten. Es gibt auch Anstrengungen der Energieerzeuger, diese Technik zu verbessern, um zum Beispiel bestimmte Haushaltsgeräte beim Kunden fernsteuerbar zu machen. Handlungsbedarf besteht bei der Niederspannungsebene, wo DPL jetzt den großen Durchbruch bringen soll. Bisher wurden hier im Wesentlichen die gleichen Technologien wie auf der Mittelspannungsebene verwendet, was natürlich keineswegs optimal ist. Durch Verbesserungen planen Firmen, Geschwindigkeiten von mehreren Megabit pro Sekunde zu erreichen. Bis es soweit ist gibt es aber noch eine Menge Probleme zu lösen.

Im Gegensatz zu xDSL und Data over Cable, ist DPL derzeit über Laborversuche und einzelne Pilotprojekte nicht hinaus gekommen. Die Schuld hierfür ist sowohl bei der Technologie selbst als auch bei der bürokratischen Reglementierung dieses Marktes zu suchen. So erlaubt die im Moment in der EU gültige CENLEC Norm EN500065 Datenübertragung nur in den Frequenzbereichen zwischen 3 und 148,5 kHz. Es ist trivial auszurechnen, dass sich über einen derart schmalen Kanal bei der schlechten Beschaffenheit von Stromkabeln laut Shannon bestenfalls 300 Kbps übertragen lassen, wobei dieser Wert schon eher optimistisch angesetzt ist. Dies würde bei angenommenen 150 Teilnehmern[35] pro Trafostation eine Bandbreite von 2 Kbps zulassen. Wie wir daraus bereits entnehmen können, handelt es sich bei DPL auch wieder um ein Broadcast Verfahren wie beim Kabel. Wenn die Trafostation, die bei DPL die Kopfstelle des Netzes ist, sendet, können alle angeschlossenen Stationen mithören. Zusätzlich muss nun auch wieder ein Rückkanal realisiert werden, welches ähnliche Probleme wie beim Kabel aufwirft und die schmale Bandbreite zusätzlich einschränkt. Außerdem gilt es nun, die gleichen Probleme wie beim Kabel zu bewältigen, also den Medienzugriff beim Rückkanal zu organisieren und die Datensicherheit zu gewährleisten. DPL scheint also die Nachteile von xDSL (schlechtes Medium) und Kabel (keine Punkt-zu-Punkt Verbindung) zu vereinen.

Die Gesetzeslage[36] macht die breitbandige Übertragung von Daten wie oben gesehen momentan zwar unmöglich, ist aber bei weitem nicht das einzige Problem. In anderen Ländern ist diese zumindest besser, trotzdem hat DPL den Durchbruch dort nicht geschafft. Ein Problem, das es auf jeden Fall zu überwinden gilt, sind die enormen Störungen, die gerade im niedrigeren Frequenzbereich, wo die Dämpfung erträglich ist, sehr stark sind. Abbildung 93 zeigt die Störungen, die einfache Haushaltsgeräte verursachen, und die bei der Datenübertragung zu burstartigen Fehlern führen.

Einige Firmen versuchen, die Probleme mit Störungen und limitierter Bandbreite zu umgehen, indem sie trotz der vorherrschenden Gesetzeslage auf höhere Frequenzen setzen. Diese Ansätze sind gestützt auf neue Erkenntnisse, die für Stromnetze eine ähnliche Beschaffenheit wie Koaxialnetze finden. Diese wiederum sind gut erforscht und beherrschbar. Leider gilt dies aber beim Stromnetz nur bis zu den sogenannten T-Stücken, hinter denen die Haushalte angeschlossen sind. Der Trick ist nun, dort einen Hochpassfilter zu installieren, um die bidirektionale Kommunikation durch Isolation von den im Haushalt entstehenden Störungen zu ermöglichen. Zusätzlich ist dann ein Tiefpassfilter notwendig, um das Haushaltstromnetz vor den Hochfrequenzsignalen zu schützen. Ein so konditioniertes Stromnetz nennt man HFCPN (High Frequency Conditioned Power Network), welches sich relativ gut zur Datenübertragung eignet. Nortel erzielte mit einer Testanlage im englischen Applerig, die nach diesem Prinzip arbeitet, bereits Geschwindigkeiten im Megabit Bereich. Konkret wurden dort im Frequenzbereich zwischen 1 und 10 MHz bei einer Entfernung von 250m Signal/Rauschabstände von 10 bis 40 dB erreicht. Die große Schwankung des Rauschabstandes bedeutet wiederum das Auftreten burstartiger Fehler, was ein weiteres

[35] siehe auch [100]

[36] Eine Änderung ist zwar absehbar, aber der Termin steht noch nicht fest.

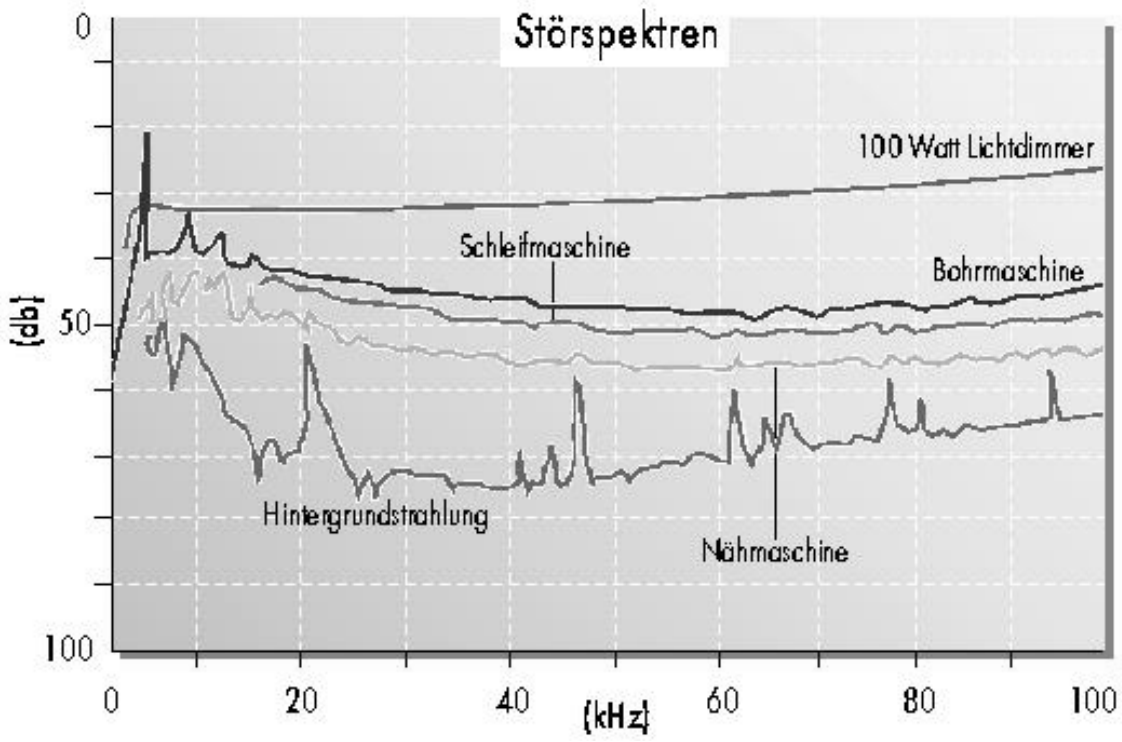


Abbildung 93: Störspektren verschiedener Haushaltsgeräte, aus [100]

Problem der DPL-Technik ist. Dadurch ist DPL zur Übertragung isochroner oder Echtzeit Datenströmen eher weniger geeignet. Die direkte Konsequenz daraus ist, dass das Telefonieren über DPL trotz weitaus größerer Bandbreite als ISDN nur mit Schwierigkeiten möglich sein wird. Gerade die Chance, als Telefonanbieter aufzutreten, war es aber, die viele Energieerzeuger zu Investments in die DPL bewogen hat.

Zusammenfassend lässt sich sagen, dass DPL eine sehr interessante Technologie ist, die allerdings noch nicht sehr weit gediehen ist. Sogar die Forschung steckt noch in den Kinderschuhen, obwohl sich viele Unternehmen darum bemühen. Wegen gesetzlicher und technischer Hürden lässt aber der große Durchbruch weiter auf sich warten. Um seine Chancen zu wahren, müssen für DPL in der nächsten Zeit Standards geschaffen werden, welche die Grundlage für einen zukünftigen Einsatz bilden. Die Möglichkeit, dass dies eintritt, erscheint sehr zweifelhaft, genau wie die Zukunft von DPL.

6.5 Konkrete Produkte und Marktchancen der Technologien

Die obige technische Betrachtung ist zwar wichtig und das primäre Ziel dieser Arbeit, aber gerade wenn man über zukünftige Technologien redet, ist eine kritische Betrachtung des Marktes notwendig. Eine Technik kann noch so vielversprechend sein, wenn dafür kein Markt vorhanden ist oder keiner das Geld für die Weiterentwicklung ausgeben will, ist sie zum Scheitern verurteilt. Gerade im Bezug auf xDSL, Data over Cable und DPL sind diese Gesichtspunkte von großer Relevanz.

xDSL ist in weiten Teilen Europas und den USA eine bereits sehr weit verbreitete Technologie. Die unterschiedlichen Varianten von DSL haben natürlich weitgehend verschiedene Kundengruppen. So wird HDSL bereits vielerorts gewerblich zum Ersatz der teuren E1 Leitungen verwendet. ADSL zielt hingegen klar auf den Massenmarkt ab. Im Juli diesen Jahres stellte die Deutsche Telekom AG ihr Produkt T-DSL vor, einen auf ADSL basierenden Dienst, der Downstream Übertragungsraten von bis zu 800 Kbps anbietet. Die Telekom zeigt damit klar ihre Ambitionen, in der Versorgung der Haushalte mit Hochgeschwindigkeitsnetzen eine führende Rolle zu spielen. T-DSL ist für den Kunden sicherlich ein Schritt voraus, weil es relativ preiswert und schnell ist. Ein Blick auf die USA beweist aber wieder, dass mehr Konkurrenz die Anbieter zwingt, mehr Leistung für weniger Geld zu bieten. Insgesamt lässt sich konstatieren, dass xDSL bei der Anbindung der Haushalte an schnelle Netze eine große Rolle spielen wird.

Bei Data over Cable sieht es mit Produkten nicht viel schlechter aus als bei xDSL. Hier gibt es auch Angebote in Deutschland, wie etwa Cablesurf in München, wo allerdings für Upstream Daten die Telefonleitung genutzt wird. In anderen Ländern, wie natürlich den USA, aber auch etwa Österreich, ist der bidirektionale Datentransport über Fernsehkabel bereits etwas Alltägliches. So gibt es in den USA schon heute über 1 Million Kunden, die im Genuss eines Internetzugangs über Kabel sind. Bis zum Jahr 2005 soll deren Zahl auf über 20 Millionen Nutzer ansteigen, wobei diese Zahl bei den jüngsten Wachstumsmeldungen des Internets eher als konservativ einzuschätzen ist. Die Kabelbetreiber wittern zweifellos einen riesigen Markt und eine Chance, in das stetig wachsende Geschäft der Telekommunikation einzusteigen. Dazu gehört gewiss die Telefonie über Kabel. Hier in Deutschland bietet das Kabel auch große Chancen, ist aber leider *noch* in der Hand der Telekom, welche kein Interesse hat, ihrem erfolgreichen ISDN Angebot Konkurrenz zu machen. Prinzipiell ist das deutsche Kabelnetz gut gerüstet, so dass binnen weniger Wochen [121] 90 Prozent des Netzes rückkanalfähig gemacht werden kann. Es lässt sich feststellen, dass Data over Cable in Zukunft einen erheblichen Marktanteil bei Hochgeschwindigkeits-Netzanbindungen von Haushalten spielen wird.

Bei der DPL ist noch keine kommerzielle Nutzung abzusehen. Dies liegt zum einen an der immer noch bestehenden CENELEC Normung, aber auch am kompletten Fehlen serienreifer Produkte, die eine Datenrate größer als im zweistelligen Kilobitbereich bewerkstelligen. Die einzige Firma, die in dieser Hinsicht etwas auf die Beine brachte, ist die Nortel Tochter Nor.Web, die testweise einigen Schulen einen 2 Megabit Internetzugang über DPL zur Verfügung gestellt hat. Am 7. September 1999 hat Nor.Web allerdings angekündigt, dass sie aufgrund insuffizienter oder zumindest zweifelhafter Marktchancen ihr Engagement im Bereich DPL ab sofort beendet. Da Nor.Web eine technische Vorreiterrolle zukam, ist es wahrscheinlich, dass andere Firmen es Nor.Web gleich tun. Die DPL dürfte zu wenig zu spät bieten, weshalb sie wahrscheinlich nur in Nischenmärkten eine Zukunft hat.

7 VLANs & VPNs - Virtuelle Private Netze

7.1 VLANs

7.1.1 Einführung

Motivation

Warum virtuelle Netze?

- Mitarbeiter aus verschiedenen Abteilungen sollen zu projektbezogenen und teamorientierten Arbeitsgruppen zusammengestellt werden können, ohne dass eine physikalische Umkonfigurierung des Netzes nötig ist.
- Integration von Tele- und Heim-Arbeitsplätzen. Benutzer sollen nicht aus Gründen ihres geographischen Standortes oder ihrer Entfernung untereinander in verschiedenen Subnetzen angeordnet sein.
- Problem Umzüge: Jeder Mitarbeiter zieht etwa alle zwei bis drei Jahre innerhalb des Unternehmens um und muss meist einem anderen physikalischen Subnetz zugeordnet werden. Sinnvoller wäre es, wenn das Netz jeden Umzug selbst registrieren, und der Umziehende weiterhin in seiner logischen Workgroup bleiben könnte.
- Weiterhin sind die Vorteile virtueller Netze dann gefragt, wenn man Server, die in zentralen Technikräumen untergebracht sind, räumlich entfernten Workgroups zuordnen will.
- Kosteneinsparung
- Broadcast - Reduzierung auf entsprechendes VLAN, Broadcast wird nicht auf alle Ports übertragen.

Bisher wurde die Segmentierung mittels teurer Router gelöst, was zur Verschwendung des IP-Adressraumes durch viele Subnetze beitrug und zu Zeitverzögerungen durch den langsameren Routingvorganges führte.

Was ist ein VLAN?

Um technisch zu verstehen, was ein virtuelles LAN ist, ist es nötig, sich noch einmal zu vergegenwärtigen, wie ein LAN funktioniert. LANs sind Bereiche, die durch ein gemeinsames Medium miteinander verbunden sind. Eine Nachricht, die eine Station innerhalb eines LANs aussendet, kann von allen an das Segment angeschlossenen Endgeräten empfangen und ggf. ausgewertet werden. LAN-Segmente können mittels Bridges miteinander verbunden sein, die entsprechende Nachrichten von einem LAN-Segment in ein anderes LAN-Segment weiterleiten.

Nachrichten, die von einem LAN in ein anderes LAN weitergeleitet werden sollen, müssen über einen Router gehen, der jetzt auf OSI-Ebene 3 die entsprechende Wegewahl vornimmt und die Nachricht entsprechend weiterleitet. Router sind aufwendiger als Bridges, da die Bestandteile einer Nachricht auf OSI-Ebene 3 verarbeitet werden müssen.

Bei VLANs wird nun die physikalische Sicht von der logischen Sicht getrennt. Grundlage für VLANs ist ein physikalisches Netz mit “intelligenten” Switchen, welches prinzipiell jedes Endgerät mit jedem anderen Endgerät verbinden kann. Durch eine entsprechende Konfiguration

werden nun Nachrichten von einem Endgerät nur an die Endgeräte weitergeleitet, die in einem "virtuellen" LAN konfiguriert sind. Für diese Stationen sieht es also so aus, als würden sie ein gemeinsames Netz, ein LAN, bilden, obwohl das LAN nur eine Teilmenge des physisch vorhandenen Netzes benutzt. Damit werden Broadcasts auf eine sinnvolle Anzahl von Endsystemen begrenzt, sowie die Sicherheit erhöht, da keine Station mehr den Verkehr von anderen, der nicht für das LAN bestimmt ist, mitgehört werden kann.

Definition VLAN:
Virtuelle Netze sind ein relativ neues technologisches Konzept zur logischen Vereinigung von Netzteilnehmern zu dynamischen Arbeitsgruppen innerhalb eines Netzes mittels Switches. Dieses soll transparent und ohne physikalische Veränderung des Netzes möglich sein. Ein virtuelles Netz stellt eine Broadcast Domäne dar. Routing ist zwischen VLAN's nötig, innerhalb des VLAN's nicht. [68]

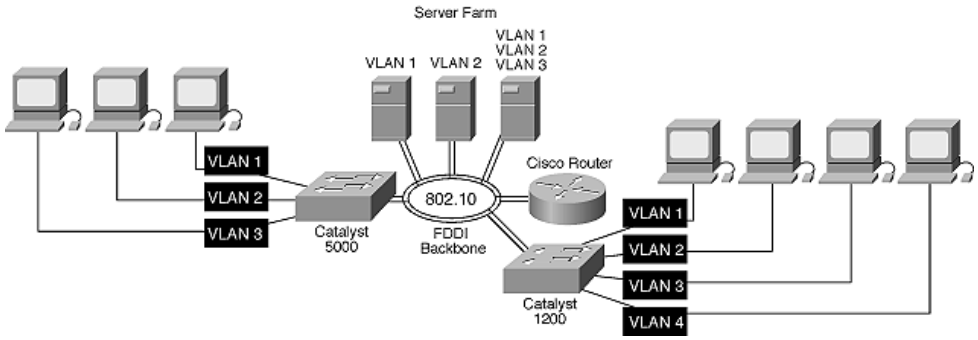


Abbildung 94: VLAN: Virtual LAN

Technische Rahmenbedingungen

Virtuelle Netze werden mittels Switches gebildet, die an jedem Port die maximal mögliche Bandbreite unterstützen und die Daten in der Regel viel schneller transportieren als dies Router tun. Beliebige Netzteilnehmer aus verschiedenen Segmenten können über ein Netzwerk-Managementsystem nach unterschiedlichen Kriterien zu einem virtuellen Netz vereint werden, ohne dass das Netzwerk physikalisch umstrukturiert werden muss. Bei komfortablen Systemen muss man hierzu einfach die Stationen am Bildschirm mit der Maus anklicken, die eine virtuelle Verbindung erhalten sollen.

Die Switches sorgen dafür, dass alle Daten, auch Broadcasts, in einem virtuellen Netz bleiben und nicht in andere virtuelle Netze gelangen. Damit entspricht ein virtuelles Netz einer Broadcast Domäne. Innerhalb eines virtuellen Netzes werden die Daten gebridged; Routertechnik wird nur benötigt, wenn man verschiedene virtuelle Netze miteinander verbinden will. Da man in der Regel mehrere Segmente in einem logischen Subnetz integriert, wird die Anzahl der zeitraubenden Routerübergänge damit reduziert.

Es muss beachtet werden, dass entsprechend auch alle aktiven Komponenten VLAN's unterstützen, d.h. eine Managementsoftware verfügbar ist (z.B. "Transcent" unter UNIX).

Virtuelle Netze vereinen die Vorteile von Brücken und Routern. Stationen lassen sich leicht ändern, hinzufügen oder entfernen. Trotzdem hat man den Vorzug der Systemtrennung und Strukturierung, ohne jedoch die Durchsatzprobleme von Brücken und die aufwendige Konfiguration großer Netze mit Routern hinnehmen zu müssen.

7.1.2 Technik

Technische Realisierungen für VLANs

Für die Realisierung von VLANs gibt es mehrere Möglichkeiten, jeweils mit eigenen Vor- und Nachteilen.

- Der Port an einem Switch bestimmt das zugehörige VLAN Eine Gruppe von Ports an einem Switch oder Router definieren gemeinsam ein LAN. Entspricht der "physikalischen" Schicht, da ein Stecker bestimmt, zu welchem LAN die Geräte gehören, die an einen Port angeschlossen sind.
- Die MAC-Adresse in einer Nachricht bestimmt das zugehörige VLAN. Dies entspricht OSI-Schicht 2. MAC-Adressen werden über Software einem VLAN zugeordnet.
- Teile der Informationen aus der Netzwerkschicht, also OSI-Schicht 3, wie z.B. die IP-Adresse (bzw. vergleichbare Bestandteile andere Protokolle) bestimmt das zugehörige VLAN.
- VLANs werden durch die Protokolle höherer Schichten bestimmt. Denkbar sind ein VLAN für Video-Übertragungen, ein VLAN für Email, ... (OSI-Schicht 4)
- Verschiedene Bereiche aus OSI-Schicht 1 bis 4 können kombiniert werden, um über Regeln ein VLAN zu bestimmen.

Schicht 1 VLANs

Schicht 1 VLANs sind die älteste und einfachste Form der Realisierung von VLANs. Ursprünglich aus der Idee von Intelligenten Hubs kommend, können verschiedene Ports zu einer Broadcast-Domain zusammengefasst werden. Sehr gut nachvollziehbar sind die Zuordnung der Stationen zu den einzelnen VLANs. Bei Bedarf muss man lediglich nachsehen, an welchem Port eine Station angeschlossen ist. Die Sicherheit ist hoch, da Verkehr wirklich nur an die an einem VLAN Beteiligten geht, alle Broadcasts sind nur am VLAN beteiligten Endgeräten empfangbar. Fehler können fast so einfach wie bei traditionellen LANs gesucht und gefunden werden.

Nachteilig ist, dass pro Port nur ein VLAN unterstützt werden kann. Falls Endgeräte in zwei unterschiedlichen VLANs kommunizieren wollen, müssen sie dies über einen Router tun, der Geld kostet, zwei Ports benötigt und auch noch zu konfigurieren ist. Die "Sparversion" ist die Verwendung von mehreren Netzwerkkarten an den Endgeräten, die mit mehreren VLANs kommunizieren wollen. Der Multicast-Support ist gering, jede Nachricht wird an alle Teilnehmer eines VLANs gesendet. Wenn ein Benutzer umzieht, müssen noch wirklich Kabel umgesteckt werden. Also ist diese Lösung noch nicht sonderlich flexibel.

Schicht 2 VLANs

Bei Schicht-2-VLANs dienen MAC-Adressen innerhalb der Pakete als Zugehörigkeitsmerkmal zu einem VLAN. Wenn also ein Benutzer umzieht, bemerkt dieses der Switch und passt automatisch seine Adresstabellen an, eine manuelle Umkonfiguration entfällt. Positiv ist ebenfalls, dass mehrere Endgeräte an einem Port zu verschiedenen VLANs gehören können. Allerdings ist dadurch die Sicherheit ggf. niedriger, da Endgeräte anderer VLANs einen Teil des Verkehrs

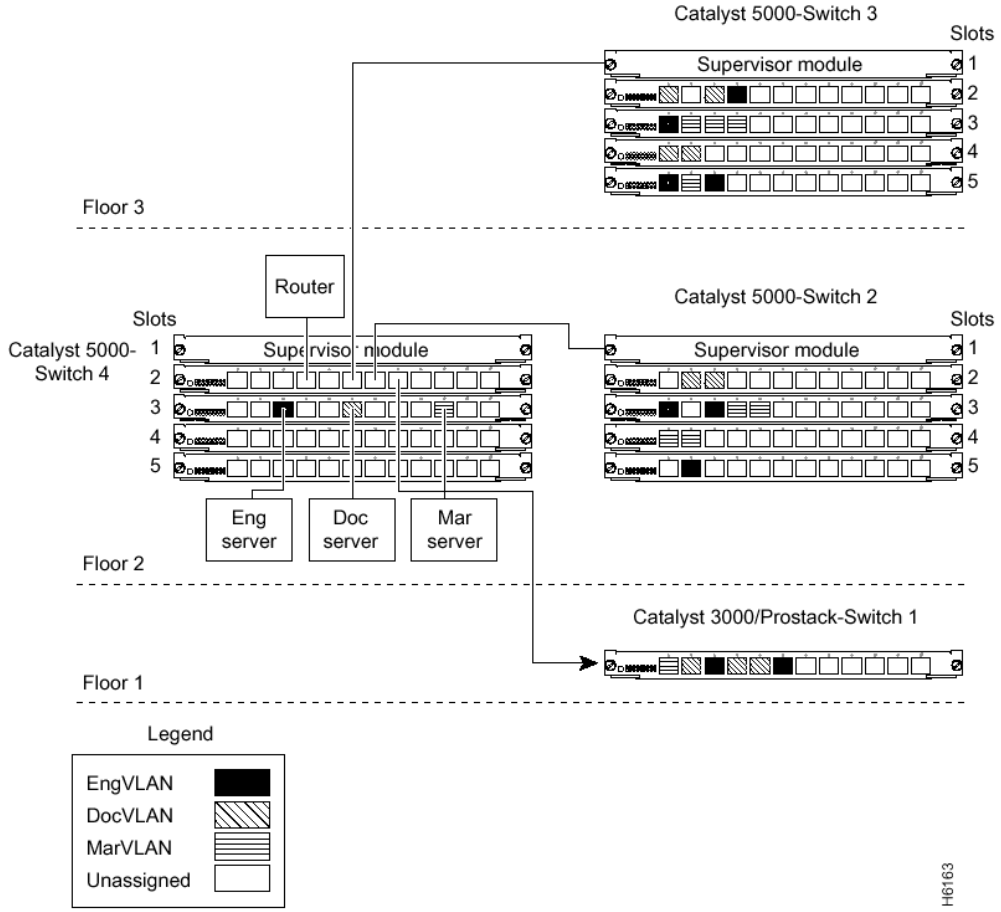


Abbildung 95: VLAN on Layer 1

des VLANs mithören können. Des weiteren unterstützen nicht alle höheren Protokolle mehrere VLANs pro Segment, da höhere Protokolle, wie z.B. IP, davon ausgehen, dass alle Stationen an einem Segment die gleiche Netzwerkadresse haben, was hier ja nicht mehr unbedingt zutreffen muss. Es gibt Switche, die aus diesem Grund automatisch die Netzwerkadresse entsprechend anpassen, um die sonstige "Kastration" auf einen Schicht-1-VLAN zu umgehen. Positiv ist auch, dass Verkehr nicht mehr an alle an einem VLAN beteiligten Geräte gesendet werden muss, da ja die MAC-Adresse eindeutig ist.

Falls ein Switch keine Auto-Konfiguration unterstützt, ist das Eingeben der MAC-Adressen in die Adresstabellen des Switches ein sehr mühseliger und fehleranfälliger Vorgang. Ausserdem muss man dafür sorgen, dass die Tabellen der verschiedenen Switches immer konsistent sind. Dazu müssen regelmäßig Informationen über das Netz übertragen werden. Genau an dieser Stelle trifft man auf eines der noch bestehenden wesentlichen Probleme der virtuellen LANs: So ziemlich jeder Hersteller verwendet für diese Informationsabgleichung proprietäre Verfahren, so dass man davon ausgehen kann, dass die wenigsten Komponenten verschiedener Hersteller sich auf Anhieb verstehen. Mindestens drei Verfahren findet man vor:

Regelmäßiger Austausch der Adresstabellen
Einige Switches tauschen spezielle Nachrichten aus, um ihre Adresstabellen abzugleichen. Be-

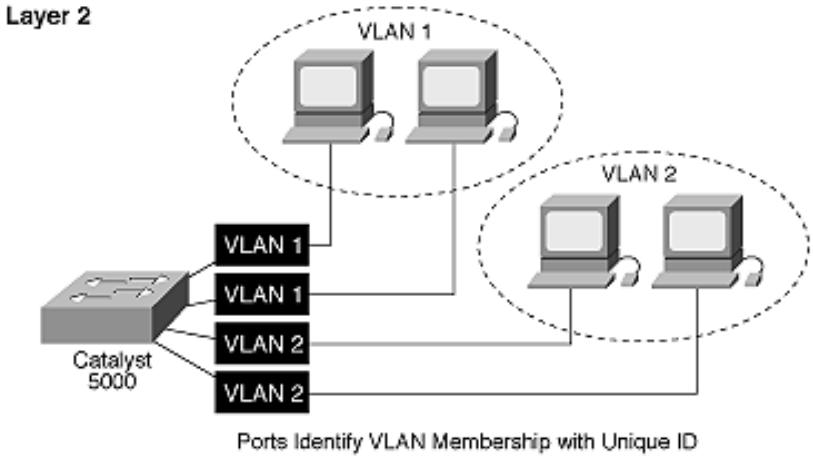


Abbildung 96: VLAN on Layer 2

vor eine neue Endstation zum ersten Mal Daten versenden darf, müssen alle Switches wissen, zu welchen virtuellen Netz diese Station gehört. Der nächstgelegene lokale Switch erkennt die Adresse des zugehörigen virtuellen Netzes am Port, über den er Verbindung zu der neuen Station erhält, da üblicherweise alle Stationen eines Segments genau einem virtuellen Netz zugeordnet sind. Dieser lokale Switch ergänzt seine Adresstabelle und sendet die neue Information (MAC - Adresse und Adresse des virtuellen LANs) mittels einer kurzen Nachricht hoher Priorität an alle anderen Switches. Dieser Nachrichtenaustausch ist nicht standardisiert, so dass hier jeder Hersteller andere Verfahren einsetzt. Erst wenn alle Switches die neue Endstation kennen, können deren Daten übertragen werden. Dieses Verfahren ist recht einfach zu implementieren, führt aber in großen Netzen schnell zu Synchronisations- und Überlastproblemen. Letzteres insbesondere auch deshalb, weil die Switches regelmäßig, etwa jede Minute, die kompletten Tabellen untereinander austauschen. Bei einer Tabellengröße von 1.000 Bytes und mehr kann man sich leicht ausrechnen, was hier an zusätzlichem Datenverkehr dazu kommt.

Frame Tagging

Eine weitere Möglichkeit des Informationsaustauschs ist das Frame Tagging. Jedem Datenpaket wird ein kurzes Datenfeld vorangestellt. Dieses Tag beschreibt, zu welchem virtuellen LAN das Datenpaket gehört. Der umständliche Austausch der Adresstabellen kann somit entfallen. Allerdings generiert auch dieses Verfahren einen erheblichen Overhead, da jedes Datenpaket um Synchronisationsinformation ergänzt werden muss. Außerdem bekommt man Probleme, wenn ein Datenpaket bereits die maximal zulässige Paketlänge hat (das Hinzufügen eines Tags verletzt die Vorgaben des MAC - Protokolls und führt dazu, dass die zu langen Pakete als Fehler erkannt und vernichtet werden). Als Ausweg hierfür findet man heute nur herstellerspezifische Techniken, die uns wiederum zur Installation von Komponenten nur eines Herstellers zwingen. Eine Variante des Frame Tagging ist der Ansatz, vorhandene Felder eines Datenpaketes zur Gruppierung von virtuellen LANs zu verwenden. So können die virtuelle LANs nicht nur aufgrund von MAC - Adressen, sondern auch durch weitere Informationen im Datenpaket zusammengestellt werden (z.B. Subnetzadresse oder Protokolltyp). Diese Flexibilität erlaubt beispielsweise die Zusammenfassung nicht routingfähiger Protokolle (NetBIOS,...) zu virtuellen Netzen. Der

Nachteil dieses Verfahrens ist, dass die Switches sehr leistungsfähig sein müssen, um "on-the-fly" alle Paketinformationen auszuwerten und mit entsprechenden Tabellen zu vergleichen.

Zeitmultiplexverfahren
Der dritte Ansatz zur Verständigung der Switches untereinander ist das Zeitmultiplexverfahren. Das die Switches vereinende Backbone wird dazu in Slots fester Bandbreite aufgeteilt. Jedes virtuelle LAN erhält exklusiv einen oder mehrere dieser Slots zur Übertragung der Daten. Jedem Switch muss somit nur noch mitgeteilt werden, welcher Time Slot welchem virtuellen Netz zugeordnet ist. Der Overhead aufgrund von Tags oder zusätzlich zu übertragender Synchronisationsinformation entfällt. Problematisch ist an diesem Verfahren nur, dass ungenutzte Bandbreite in den einzelnen Slots nicht für andere virtuelle Netze zur Verfügung steht und brach liegt. Ein Zeitmultiplexverfahren kann nur dann annähernd sinnvoll genutzt werden, wenn aufgrund stetiger Beobachtung des Netzverhaltens die Time Slots optimal zugeordnet werden können. Oder man verwendet für den Backbone ein dynamisches Verfahren.

Spanning Tree
Auch in virtuellen Netzen wird das bekannte Spanning Tree Protokoll zum Aufbau redundanter Netzstrukturen verwendet. Durch Austausch entsprechender IEEE 802.1d Mitteilungen werden Schleifen in Netz nach altbekannter Weise in Baumstrukturen aufgespalten. Da der Spanning Tree Algorithmus nicht für große LANs optimiert ist, haben einige Switchhersteller auch hier proprietäre Erweiterungen vorgenommen, um den Algorithmus schneller und robuster zu machen. Wichtig ist, dass die Switches mehrere Spanning - Trees parallel unterstützen können, da gegebenenfalls jedes virtuelle LAN getrennt betrachtet werden muss.

Des weiteren ist die Zuordnung von Endgeräten zu VLANs deutlich schwieriger als bei Schicht-1-VLANs, da erst die MAC-Adresse in einer Tabelle gesucht werden muss; die Portnummer am Switch ist ja uninteressant geworden. Verschiedene Schicht-2-VLANs benötigen ebenfalls einen Router, um miteinander kommunizieren zu können; mit den gleichen Nachteilen wie bei Schicht-1-VLANs.

Schicht 3 VLANs

Bisher wurden nur sogenannte Layer 2 Switches betrachtet, die auf Ebene 2 des ISO / OSI - Modells arbeiten. Layer 3 Switches bringen zusätzliche Möglichkeiten, weil sie Basis - Routing - Funktionalitäten wie z.B. ARP in die virtuellen Netze integrieren und den externen Router zur Verbindung der virtuellen LANs überflüssig machen.

Bei Schicht-3-VLANs dienen die Schicht-3-Adressen, also z.B. die IP-Adresse, um die Zugehörigkeit zu einem VLAN zu bestimmen. Hier gehören nicht mehr Endgeräte zu einem VLAN, sondern nur noch Pakete.

Layer 3 Switches können Ebene 3 Informationen auswerten und deshalb virtuelle Netze abhängig vom verwendeten Protokolltyp definieren, so dass man beispielsweise alle Netware- oder alle IP - Stationen unabhängig von Ihrer Platzierung im Netzwerk einem eigenen virtuellen LAN zuordnen kann. Die Zuordnung einzelner Datenpakete zu verschiedenen virtuellen LANs geschieht analog dem klassischen Routing einfach durch Auswertung der Subnetzadressen. Die oben geschilderten Layer 2 Mechanismen zum Informationsabgleich zwischen den Switches treffen hier nicht zu. Trotz Analyse der Ebene 3 Informationen werden alle Verbindungen innerhalb eines virtuellen Netzes so behandelt, als ob eine Brückentopologie vorliegen würde. Die komplette Routingfunktionalität greift nur zwischen den virtuellen Netzen. Innerhalb eines virtuellen Netzes spielen Routingprotokolle wie RIP oder OSPF keine Rolle; unbekannte Datenpakete werden

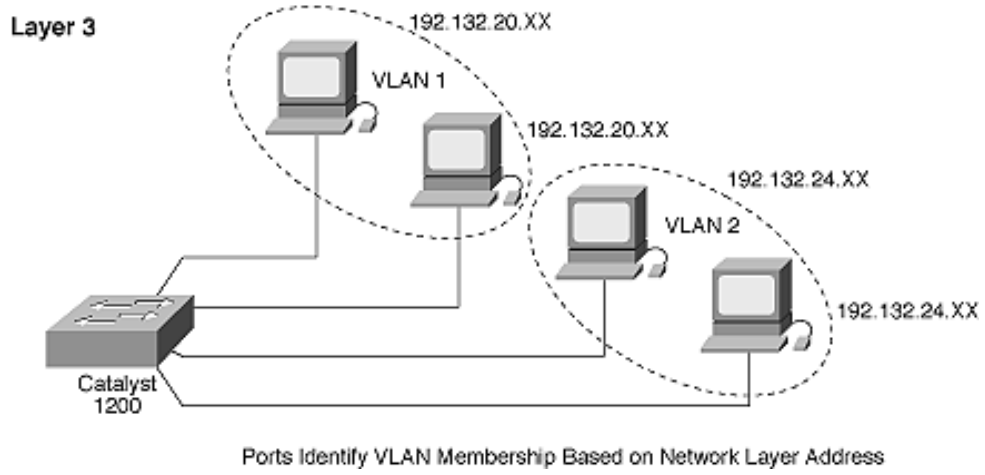


Abbildung 97: VLAN on Layer 3

entgegen der üblichen Vorgehensweise von Routern einfach über das gesamte virtuelle Netz "geflutet".

Der Hauptvorteil von Schicht-3-VLANs ist, dass direkte Kommunikation zwischen verschiedenen Endgeräten verschiedener VLANs unterstützt wird, und dies ohne zusätzliche teure Router. Dies wird natürlich mit erhöhten Verarbeitungskosten in den Switches bezahlt, da ja nun mehr Informationen eines Datenpaketes auszuwerten sind. Die Konfiguration ist einfacher als bei Schicht-2-VLANs, da das umständliche Hantieren mit MAC-Adressen entfällt. Interessant ist die Möglichkeit, pro Schicht-3-Protokoll ein eigenes VLAN zu definieren, also z.B. ein eigenes VLAN für IPX, eins für AppleTalk, eins für IP, etc. Ebenfalls positiv ist der effiziente Multicast-Support, da ja dem Switch klar ist, welche Endgeräte gemeint sind.

Es muss aus den verschiedensten Gründen für ein leistungsstarkes Backbone gesorgt werden. Die virtuellen Netze bringen eine enorme Backbone - Belastung, weil sich der Datenverkehr einzelner Workgroups nun nicht mehr auf ein physikalisches Segment beschränken muss, sondern bei örtlich verteilten Workgroups die Daten über das gesamte Backbone bis hin zu allen Teilnehmern eines virtuellen Netzes zu übertragen sind. Das Backbone muss für Ortstransparenz sorgen, was bedeutet, dass die Kommunikation zwischen zwei beliebigen Teilnehmern eines virtuellen Netzes mit der gleichen Effizienz geschehen muss, egal ob diese über mehrere Switches miteinander kommunizieren oder direkt benachbart sind. Außerdem müssen alle virtuellen Netze gleichzeitig und möglichst mit der vollen Bandbreite der angeschlossenen Endgeräte bedient werden können.

Schicht 4 VLANs

Bei Schicht 4 VLANs besteht die Möglichkeit, die virtuellen LANs nach ihrer Anwendung zu unterschieden, z.B. FTP, WWW, E-Mail. So gibt es für jede Anwendung, die man nach Protokollen oder Portnummern unterscheiden kann ein eigenes Netz. Ein User oder ein Host bekommt dann nur noch Zugriff auf das VLAN, wenn er den entsprechenden Dienst Nutzen darf. Sinnvoll ist die Einteilung dann, wenn man gewissen Diensten besondere Prioritäten zuweisen will. Beispielsweise kann einem VLAN für Videokonferenzen mit wenigen Teilnehmern eine große Bandbreite zugesicherten werden, oder einem VLAN mit vielen Teilnehmern aber wenig Datenaufkommen,

z.B. E-Mail, eine geringe Bandbreite. Eine Art QoS auf Umwegen.

Die technische Realisierung hängt hier sehr stark von der Technologie der verwendeten Switches ab. Die Datenpakete müssen bis auf Anwendungsschicht hinunter aufgelöst und verarbeitet werden. Dies erfordert sehr hohe CPU-Zeiten in den verwendeten Geräten. Für diese Art von VLANs existiert noch kein Standard, so dass, wenn ein Hersteller überhaupt eine Implementierung anbietet nur sehr proprietäre Techniken angewendet werden.

Regelbasierte VLANs

Das Maximum an Flexibilität sind die regelbasierten VLANs. Durch die Erstellung von Regeln lassen sich VLANs ganz einfach anhand von Port-Nummern, MAC-Adressen, Protokollen und Teile von Schicht-3- und Schicht-4-Protokollen definieren. Eine Möglichkeit wäre z.B. ein VLAN zu definieren, in dem alle Stationen enthalten sind, deren Netzwerkkarten von einer speziellen Firma sind, das IP Protokoll benutzen und zu einem speziellen IP-Subnetz gehören. Die Möglichkeiten sind hier unbeschränkt, die Konfiguration erinnert an die Konfiguration von Firewalls.

Natürlich wird dieser "Luxus" durch die Abarbeitung der Regeln in den Switches für jedes Paket bezahlt, was tatsächlich zu Performance-Einbußen führen kann, wenn die Switches nicht leistungsfähig genug sind. Die Konfiguration kann zu einem Geduldsspiel führen, es muss dem Administrator nicht immer klar sein, welches Bit er wo in welche Regel einbeziehen muss, um einen gewünschten Effekt zu erzielen. Die Zuordnung von Endgeräten zu VLANs ist nicht mehr leicht.

7.1.3 Management und Konfiguration

Nun soll der Einfluss von VLANs auf Managementaspekte untersucht werden. Es gibt u.a. folgende Auswirkungen:

Konfigurationsmanagement:
Durch den Einsatz von VLANs ist ein erheblich flexiblere Nutzung der vorhandenen Ressourcen möglich. Die Zugehörigkeit einzelner Endgeräte zu den richtigen LANs ist nun eine Änderung, die über eine Netzwerkmanagementstation vorgenommen werden kann, das physische Umstecken entfällt. Wichtige Aufgabe ist hier dann natürlich, die vorhandenen Ressourcen optimal auf die VLANs zu verteilen.

Sicherheitsmanagement:
Da VLANs voneinander (je nach Realisierungsart) wirklich voneinander getrennt sind, ist es möglich, VLANs nach Sicherheitsbedürfnissen zusammenzustellen. Des weiteren ist es bei Schicht-3-VLANs möglich, Filter einzusetzen, die bestimmte Arten von Verkehr (FTP, Telnet, ...) aus einem VLAN heraushalten.

Abrechnungsmanagement:
Der Netzverkehr kann durch die Einteilung in Benutzergruppen, den VLANs, eindeutig zugeordnet und damit vernünftig abgerechnet werden. Damit können entstandene Kosten eindeutig auf die verschiedenen Benutzergruppen aufgeteilt werden.

Leistungsmanagement:
Die Leistungsfähigkeit von geswitchten LANs ist deutlich höher als die traditioneller LANs; jedem Endgerät steht im Extremfall die volle Bandbreite des verwendeten Übertragungsmediums zu. Teure Router können teilweise vermieden oder ersetzt werden, und durch die Aufteilung eines geswitchten LANs auf VLANs werden die Broadcasts auf die jeweils betreffenden Endgeräte

aufgeteilt. VLANs dienen also der Verkleinerung von Broadcast-Domains. Zu beachten ist, dass VLANs üblicherweise zu einem deutlich höherem Bedarf an Bandbreite im Backbone benötigen, da dieses die Virtualität realisieren muss.

Problematisch beim Einsatz vorhandener Management-Werkzeuge ist die Trennung von physischen und logischen Strukturen, da dieses noch nicht unterstützt wird. Der bekannte Managementspruch *Was man nicht sehen kann, kann man nicht managen* findet hier noch seine Berechtigung. Langfristig sind hier erweiterte MIBs zu standardisieren, und die Managementwerkzeuge entsprechend anzupassen.

7.1.4 Sicherheit

Der Begriff Sicherheit war schon immer ein relativer Begriff. 100%ige Sicherheit gibt es nicht und wird es auch nie geben. Man kann höchstens versuchen sein System mit den verfügbaren Mitteln so sicher wie möglich zu machen. Neben einer vernünftigen Sicherheits-Policy, die natürlich auch eingehalten werden muss, ist auch physische Sicherheit eine wichtige Voraussetzung. Was nützt eine Firewall, die das Firmennetz vom Internet abschottet, wenn jeder beliebige den Zugriff auf Hardware in Büro- oder sogar Server-Räumen hat.

In einem 'einfachen' LAN genügt es, einen Rechner, auf dem der Angreifer root-Rechte (z.B. Laptop mit Linux) hat, an eine freie Netzwerkbuche einzustecken und man kann mit einem Sniffer den gesamten Netzwerkverkehr mitlesen. Um sich in ein Schicht-3-VLAN einzuklinken bedarf es lediglich der Änderung der IP-Adresse in die eines VLAN-Members (IP-Spoofing), und den Original-Host mit einer DoS-Attacke außer Betrieb zu setzen. Bei Schicht-2-VLANs muss der Angreifer für einen MAC-Spoofing-Angriff schon wesentlich mehr Aufwand betreiben, um am Netzverkehr teilnehmen zu können. Möglich ist es aber trotzdem. Bei Schicht-1-VLANs ist es schon etwas schwieriger den Anschluss an eine bestimmte Netzwerkschnittstelle unbemerkt zu erlangen. Da hier die VLANs über ein Patchfeld geschaltet werden ist detailliertes Wissen über die Netz- und Gebäudestruktur von Nöten.

7.1.5 Aktuelle Standards

Der Standard IEEE 802.1Q. [73] ist einer der ersten Versuche die verschiedenen Ansätze unter einen gemeinsmaen Hut zu bringen. Nun liegt es bei den marktführenen Unternehmen dieses Vorhaben auch zu unterstützen.

Ein anderer Quasi-Standard, das Inter-Switch Link Protokoll, kommt von Cisco. Da die Marktmacht von Cisco im Switching-Bereich nicht unwesentlich ist, ist es wahrscheinlich, dass der Cisco-Standard uns die nächsten Jahre noch begleiten wird.

Multi-Protocol Label Switching (MLSP) ist das Pedant dazu, welches von der IETF gerade diskutiert wird. Es ist ein Standard, der Switch- und Routertechnologien in einem Gerät vereinigen soll. Auf dieses Thema wurde in einem vorherigen Vortrag bereits eingegangen, deshalb soll es in diesem Beitrag nur noch einmal erwähnt und darauf verwiesen werden.

Wer heute einen funktionierenden Standard für VLANs einsetzen will, hat tatsächlich dazu die Möglichkeit, und zwar durch den Einsatz von ATM mit der LAN Emulation, der tatsächlich herstellerübergreifenden Einsatz von VLANs ermöglicht.

7.1.6 Zusammenfassung VLANs

Insgesamt kann man sagen, dass der Einsatz von VLANs sehr von den Bedürfnissen und Wünschen abhängt. Auf diese Bedürfnisse muss sowohl die zum Einsatz kommende Technik, als auch der richtige VLAN-Typ gewählt werden. Das Nichtvorhandensein von Standards erschwert im Moment den Einsatz von VLANs über größere Gruppen hinweg, zumindest in einer heterogenen Umgebung. Der zusätzliche Level an Indirektheit ist nicht immer positiv, er erschwert die Fehlersuche und ist auch noch kaum durch gängige Management-Plattformen unterstützt. Hier ist man auf die Unterstützung des Herstellers angewiesen, dessen Switche man benutzt. Interessant wird auch, wie vorhandene Switche und Router entweder nachgerüstet oder anderswie eingebettet werden. Es ist kaum zu erwarten, dass von heute auf morgen nur VLAN-fähige Geräte innerhalb eines Netzes zur Verfügung stehen. Ein anderes Problem ist der Einsatz der üblichen Spanning-Tree-Protokolle. Diese müssen an das Vorhandensein von VLANs angepasst werden; außerdem skalieren sie nicht unbedingt für große, geswitchte Netzwerke. Insgesamt erhöht der Einsatz von VLANs den Bedarf an Bandbreite in den Backbones, da nun die Netzlast, die innerhalb eines traditionellen Segments vorhanden war, oft über das Backbone geswitcht werden müssen, zumindest wenn die Vorteile von VLANs mit Umzügen und wechselnden Zugehörigkeiten zu VLANs ausgenutzt werden. Des weiteren ist zu beachten, dass auch die Größe eines VLANs begrenzt ist, einerseits durch den immer noch vorhandenen Broadcast-Verkehr, andererseits haben auch Switche eine Verzögerungszeit.

Verwendete Quellen: [78] [116] [23] [60] [37] [41] [38] [39] [73] [148] [68] [74] [131] [27]

7.2 VPNs

7.2.1 Einführung

Was sind virtuelle private Netzwerke?

Ein virtuelle private Netzwerk (VPN) ist eine Kommunikations-Umgebung, bei der der Zugang so kontrolliert wird, dass Peer-Verbindungen nur innerhalb einer definierten Interessensgruppe möglich sind. Ein VPN ist also im wesentlichen ein Kommunikationsnetz zwischen einer beschränkten Anzahl von Teilnehmern auf einem öffentlichen Medium. Die Privatheit wird durch einen Tunnel realisiert, der zwei oder mehrere Endpunkte miteinander verbindet. Der Tunnel kann optional die Daten verschlüsseln und/oder komprimieren um die Performanz und die Sicherheit zu erhöhen. "Virtuell" bedeutet in diesem Zusammenhang, dass der Anwender die Illusion hat, seine Daten laufen über ein exklusive, also "private" Verbindung. Tatsächlich wird die vorhanden Netzinfrastruktur jedoch von verschiedenen Anwendern gemeinsam benutzt. Als öffentliches Medium kann beispielsweise das Internet oder ein anderes für mehrere Kunden zugängliches Netzwerk dienen.

Es gibt mehrere Kategorien von VPNs (End-to-End, Site-to-Site und End-to-Site) sowie auch mehrere Methoden und verschiedene Protokolle zur Realisierung, die auf die entsprechenden Bedürfnisse angepasst und kombiniert werden können.

Anwendungsgebiete für VPNs

Für VPNs lassen sich in der heutigen Zeit zahlreiche Anwendungsbeispiele finden:

- Verbund von entfernten Firmen-Intranets.

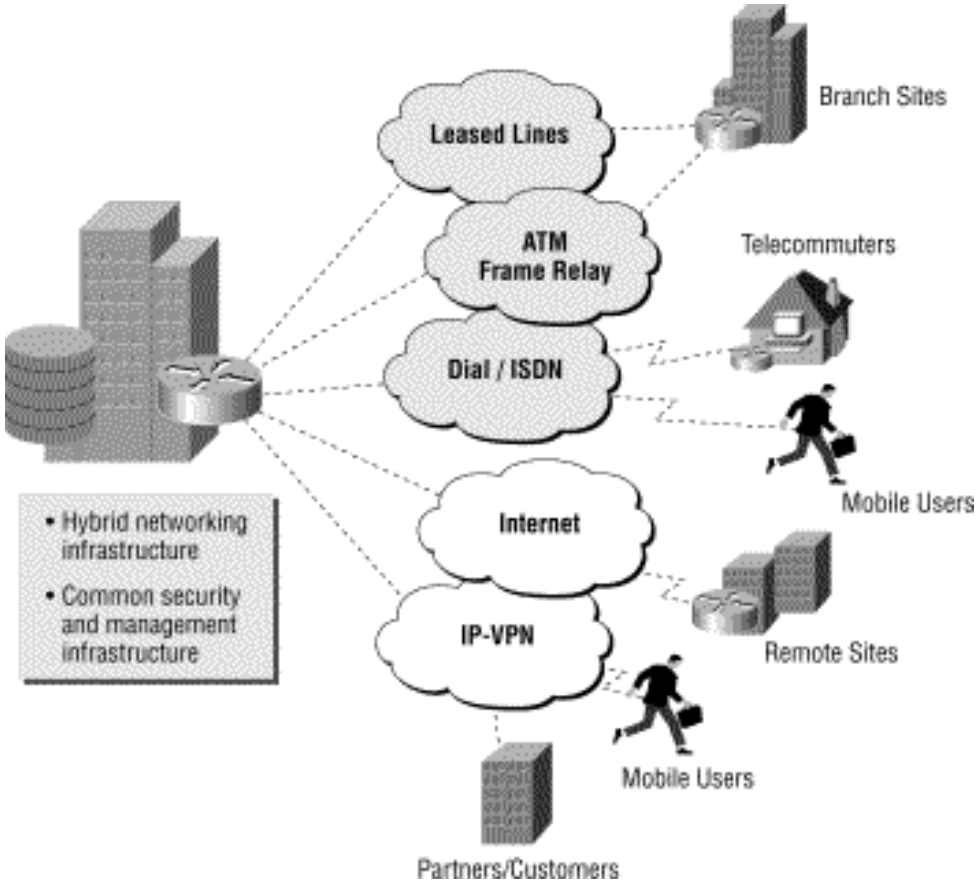


Abbildung 98: Virtual Private Network

- Anbindung eines mobilen Mitarbeiters an das Firmennetz.
- sichere Verbindung eines Online-Banking Kunden im Internet zum Bankenrechner

...um nur einige wenige zu nennen. Jede der, auch später im Abschnitt 3 genauer beschriebenen, Anwendungen hat ihre eigenen Anforderungen, die durch die verschiedenen Realisierungs-Möglichkeiten mehr oder weniger flexibel in Bezug auf Sicherheitsanforderungen und Performanzkriterien verwirklicht werden können.

Vorteile des Einsatzes von VPNs

Die Kommunikationskosten nehmen für immer mehr Firmen einen wichtigen Stellenwert ein. Daher stellt sich oft die Frage, ob die Vorteile eines VPN die relativ hohen Kosten zur Einrichtung und Administration rechtfertigen, und welches diese Vorteile überhaupt sind:

- private Verbindung über öffentliche Netze ermöglichen das einsparen von teuren Standleitungen oder Wählleitungen über große Entfernungen. beim Vorhandensein einer VPN-Infrastruktur fallen lediglich die Gebühren zum nächstgelegenen ISP an.

- mobile Außendienstarbeiter können sich über das öffentliche Netz in das private Firmennetz einwählen. Einsparungen von teuren Modembänken und hohen Verbindungskosten entfallen

- Telearbeitsplätze sind nun einfach zu realisieren. Es bleiben dem Unternehmen hohe Fixkosten, wie Büroflächen, etc. erspart.

Es wird geschätzt, dass der Einsatz von VPNs, gegenüber klassischen Lösungen, eine Kostenersparnis von 20-60% zur Folge hat [138].

Anforderungen

Kompatibilität:
Im Gegensatz zu realen physischen Leitungen, auf welchen x-beliebige Protokolle benutzt werden können, muss bei der Verwendung eines VPN mit Industriestandards verfahren werden. Diese sind meist ATM oder IP. Das VPN muss aber die bestehenden kundenspezifischen Protokolle unterstützen können.

Adressierung:
Ein wichtiger Punkt, der etwas in den Kompatibilitätsaspekt hineingeht ist die Adressierung. So kann es beispielsweise sein, dass in einem bestehenden Intranet, das völlig vom Internet abgeschottet ist, beliebige IP-Adressen verwendet werden. Es gibt zwar für solche private Netze reservierte Adressen, welche im Internet auch nicht weitergeleitet werden. Eine Verpflichtung diese zu verwenden besteht aber nicht. Auf der anderen Seite sollen diese gewählten Adressen aber weiterhin über das VPN benutzt werden können. Für externe Router sind diese Adressen aber von keiner Bedeutung. Eine Adress-Translation muss also in einer geeigneten Form vorgenommen werden.

Sicherheit:
Dieser Punkt ist für gewisse Personen mithin der wichtigste. Vor allem beim Austausch von geschäftsrelevanten und kritischen Informationen über ein öffentliches Netz werden manche Sicherheitsbeauftragte diesem Aspekt größte Bedeutung auferlegen. Hauptaufgabe wird es sein, einerseits keine Information nach außen kommen zu lassen, andererseits aber auch fremde abzuwehren.

Verfügbarkeit/QoS:
VPNs eignen sich in gewissen Konfigurationen hervorragend, alle möglichen Applikationen zu unterstützen. Falls beispielsweise Telefon, Videoconferencing usw. verwendet werden sollen, müssen aber Qualitätsgarantien abgegeben werden können. Im Zusammenhang mit VPNs müssen diese Aspekte ebenfalls betrachtet werden. Als mögliche Lösungsvariante steht sicherlich die Verwendung von ATM, oder dem zukünftigen IPv6 im Vordergrund.

Standardisierung:
Standardisierung ergibt sich als Folge aus den vorigen Punkten. Soll VPN auf dem Markt eine Chance haben, so müssen gewisse Standards geschaffen werden. Ansonsten werden Insellösungen entstehen und ein Wechsel von einem Provider auf einen anderen kann beispielsweise schwierig werden. Dieser Punkt ist aber mehr als Forderung an eine sinnvolle Kooperation der verschiedenen Gremien zu sehen, denn als technisches Problem.

7.2.2 Technische Grundlagen von VPNs

Grundsätzlich gibt es 4 verschiedene Ansatzpunkte für eine Lösung. Diese bestehen in den 4 Schichten des TCP/IP-Stacks.

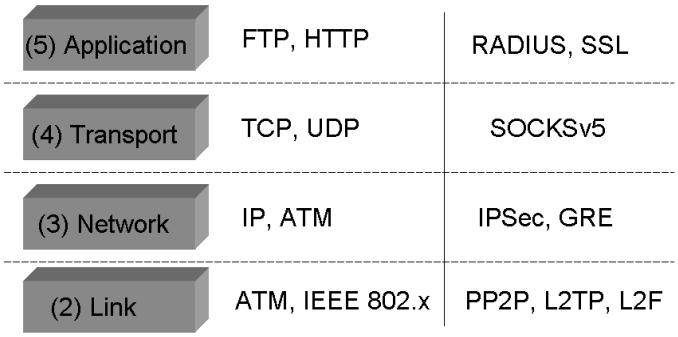


Abbildung 99: Layerübersicht

Die oberste Stufe, der Application-Layer, ist in diesem Zusammenhang aber am wenigsten interessant. Zwar lässt sich mittels Verschlüsselung, wie dies z.B. in den Secure Sockets Layern von Netscape der Fall ist, eine sichere Verbindung aufbauen, die Verlegung der Zuständigkeit in tiefere Schichten bringt aber einige Vorteile bezüglich Wartung, resp. Zentralisierung des Problems.

Auf Stufe Transport Layer gibt es ebenfalls Ansätze von Implementierungen, wie beispielsweise Secure Socket. Die Bearbeitung des VPN-Protokolls findet aber auch hier immer noch in den Endgeräten selbst statt. Somit ließe sich ein Standort-übergreifendes virtuelles Netz nur mit Eingriffen in bestehende Workstations vornehmen. Für größere Netze ist diese Variante ebenfalls nicht zu empfehlen.

Wesentlich eleganter sieht es auf den Stufen Network und Link-Layer aus. Hier gibt es verschiedene Protokolle und Vorschläge. Das bekannteste und wichtigste zugleich ist IPSec (IP Security). Im wesentlichen ist IPSec eine Implementierung des GRE-Protokolls. Es soll im nächsten Release von IP, IPv6 eingebaut werden.

Auf Link-Ebene gibt es einerseits IP-unterstützende Verfahren wie PPTP, dem Point-to-Point-Tunneling-Protokoll, einer Erweiterung von PPP von Microsoft, sowie dem Layer 2 Tunneling Protokoll. Beide stellen eine sichere Verbindung zwischen zwei Routern oder zwischen Endgerät und einem Router zur Verfügung. Andererseits besteht die Möglichkeit ATM selbst zu Verwenden, ev. mit zusätzlicher Verschlüsselung.

Schicht 2 VPNs

Beim Link-Layer handelt es sich um Punkt-zu-Punkt Verbindungen. Es werden direkte Verbindungen mit Hilfe von Tunneln aufgebaut. Dabei wird ein Protokoll in einem anderen (oder auch gleichem) Protokoll eingekapselt. Das neue Paket, welches in einem Tunnel-Server (Gateway) erzeugt wird, hat als Zieladresse den gegenüberliegenden Tunnel-Server, wo die ursprüngliche Information wieder in ein Netz mit gleichem Protokolltyp und gleicher Adressierung (Netz-ID) eingespeist wird. Dabei können die Daten verschlüsselt oder komprimiert werden.

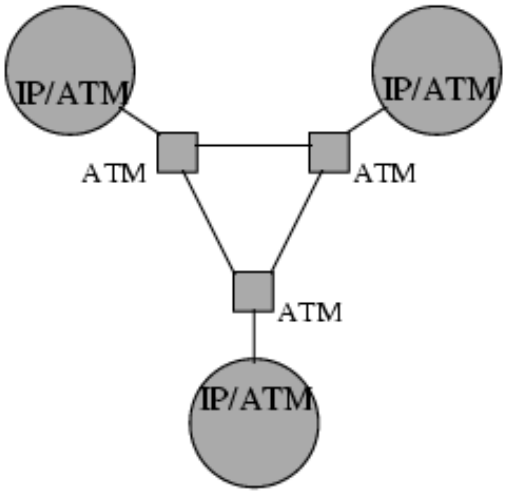


Abbildung 100: Layer 2

Asynchronus Transfer Mode (ATM)

Die Asynchronus Transfer Mode -Technik bringt wegen des Konzeptes schon von Haus aus eigene Möglichkeiten mit, ein VPN aufzubauen. Darauf soll aber hier nicht weiter eingegangen werden, da ATM bereits ein Thema vorheriger Vorträge war. Für den Einsatz von ATM spricht aber, dass ATM-basierte VPN-Technologie die Garantie von Quality-of-Service Parametern unterstützt, wie zum Beispiel minimale Bandbreite oder eine bestimmte, maximale Verzögerung. Weiterhin ist neben der reinen Datenübertragung auch der Transport von Audio- und Videodaten möglich.

Point-to-Point Tunneling Protocol (PPTP)

Das Point-to-Point Tunneling Protocol (PPTP) ist ein von Microsoft entwickeltes Protokoll zur Implementierung eines VPN. Es wurde 1996 der Internet Engineering Task Force (IETF) zur Standardisierung vorgeschlagen. PPTP ist eine Erweiterung des Point-to-Point Protocol (PPP), welches einen Standard zum Transport von Multi-Protocol Datagrammen über eine Punkt-zu-Punkt Verbindung zur Verfügung stellt. Somit können verschiedene Protokolle wie IP, IPX, oder NetBEUI durch ein IP-Netz getunnelt werden.

Das PPTP VPN Protokoll besteht aus zwei Kanälen zwischen Client und Server: einem Kontroll-Kanal, über den Link-Management Information ausgetauscht werden, und einem Daten-Kanal, über den der private Netzwerkverkehr (optional verschlüsselt und/oder komprimiert) geleitet wird. Der Kontroll-Kanal ist eine TCP-Verbindung auf Port 1723 des Servers. Der Daten-Kanal benutzt das GRE-Protokoll [siehe 2.2.2.1]. Die transparente Übermittlung von Daten beruht auf einer gewöhnlichen PPP-Verbindung auf dem Daten-Kanal. Ähnlich, wie wenn eine Wählverbindung zwischen Client und Server bestehen würde. Das PPP kann nun aushandeln, ob die Daten verschlüsselt und/oder komprimiert übertragen werden. PPTP selber verschlüsselt bzw. komprimiert nicht. Für die Zugangskontrolle werden das Password Authentification Protocol (PAP) und Challenge Handshake Protocol (CHAP) verwendet. Als Verschlüsselungsalgorithmen dienen die Rivest´s Cipher 4 (RC4) und der Data Encryption Standard (DES) mit Schlüsseln zwischen 40 und 128 Bit Länge.

Ein PPTP-Paket besteht aus vier Schichten:

- der Zustell-Kopf, der aus dem Netzwerkprotokoll des öffentlichen Netzes besteht
- ein IP-Header
- ein GREv2-Header, eine für das PPTP erweiterte Version des GRE-Protokolls. Er enthält Informationen über die Art der gekapselten Daten und Parameter für die Client/Server Verbindung.
- die Nutzlastdaten in Form eines PPP-Paketes

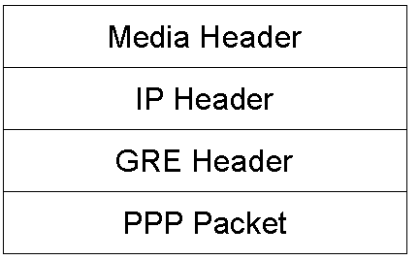


Abbildung 101: PPTP: Point-to-Point Tunneling Protocol

[Point-to-Point Tunneling Protocol (PPTP); RFC2637] [66]

Layer 2 Forwarding (L2F)

Layer 2 Forwarding (L2F) wurde von der Firma Cisco entwickelt. Es unterstützt verschiedene Protokolle und mehrere unabhängige, parallele Tunnel. die Authentifizierung ist allerdings nicht so stark und eine Verschlüsselung der Daten ist gar nicht erst vorgesehen. L2F bildet mit PP2P die Grundlage für das Layer 2 Transport Protocol (L2TF).

L2F erlaubt das Tunneln des Link-Layers (z.B. HDLC, async HDLC, oder SLIP frames) von höheren Protokollen. So ist es möglich, die Seite, die die Dial-Up-Verbindung initiiert, von der Seite, die die Verbindung aufbaut und löst, zu trennen. Es wird keine registrierte Internet-Adresse mehr benötigt, um sich beim ISP einzuwählen, sondern man hat die Möglichkeit, mit privaten Adressräumen aus dem IP, IPX und AppleTalk -Protokoll via SLIPP/PPP eine Verbindung aufzubauen. Ein L2F-Paket besteht aus 3 Teilen:

- dem L2F-Header
- der Nutzlast (SLIP oder PPP -Paket)
- einer optionalen Prüfsumme

[Layer 2 Forwarding (L2F); RFC2341] [140]

Layer 2 Transport Protocol (L2TP)

Layer 2 Transport Protocol (L2TP) ist PPTP sehr ähnlich. es unterstützt wie L2F mehrere parallele Tunnel. Der Unterschied zu PPTP besteht darin, dass die Kontrolle über den Endpunkt nicht beim User liegt, sondern vom ISP vorgegeben wir.

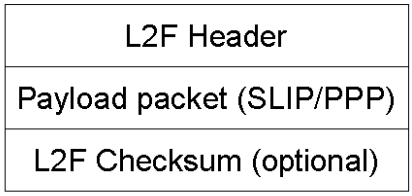


Abbildung 102: L2F: Layer 2 Forwarding

L2TP benutzt zwei Nachrichtentypen: Kontroll-Pakete und Daten-Pakete. Die Kontroll-Pakete werden benötigt, um den Tunnel aufzubauen, zu verwalten und abzubauen. Die Daten-Pakete kapseln, wie bei PPTP, die Nutzlast in PPP-Pakete. Die Kontroll-Nachrichten bauen einen zuverlässigen Kontroll-Kanal auf, der den weniger zuverlässigen Daten-Kanal überwacht. Den schematischen Aufbau von L2TP zeigt folgendes Diagramm.

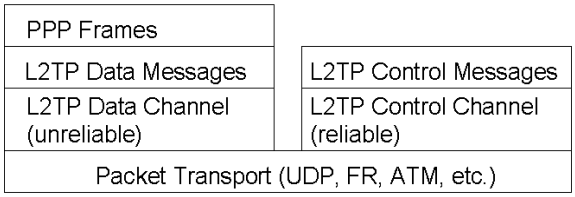


Abbildung 103: L2TP: Layer 2 Transport Protocol

[Layer 2 Transport Protocol (L2TP); RFC2661] [137]

Schicht 3 VPNs

Die Sicht von Netzwerk-Layer, sieht folgendermaßen aus: Einzelne Endrechner oder VPN-Server stellen den Einwählpunkt in das öffentliche Netz dar. Zwischen diesen IP-Routern werden nun vom Provider Tunnels geschaltet, so dass zwischen ihnen jeweils nur ein Hop liegt. So bildet das Firmennetz ein eigenständiges, eigentlich virtuelles Netz ab.

Die Tunnels zwischen den Endrechnern können beliebig implementiert werden. Es stehen die genannten Verfahren IPSec oder auch ähnliche GRE-Algorithmen zur Verfügung.

GRE-Tunneling

Beim Tunneling oder Kapseln werden beliebige Datenpakete aus einem LAN zu einem anderen LAN durch ein unabhängiges drittes Netzwerk transportiert. Dabei kann sowohl im LAN als auch im Trägernetz jedes beliebige Protokoll verwendet werden. Die Kommunikation der Endnetze untereinander ist völlig transparent. Das heißt, die kommunizierenden LANs müssen nicht für den Verbindungsauf- und Abbau sorgen. Dies übernehmen jeweils ein Tunnel-Server (Gateway) in jedem LAN. Die Endstationen arbeiten so, als wären sie alle in einem Netz verbunden.

Ein Standard für das Tunneling-Verfahren in der OSI-Schicht 3 ist Generic Routing Encapsulation (GRE).

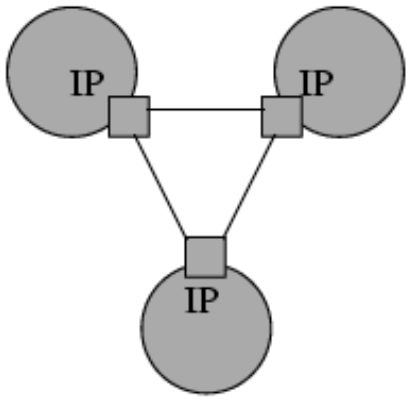


Abbildung 104: Layer 3

Dabei handelt es sich um eine Richtlinie, wie die Tunnel-Pakete aufgebaut sein sollen. Ein GRE-Paket besteht aus 3 Teilen:

- der Tunnel-Kopf, der das Tunnelziel im außerhalb des VPN verwendeten Netzwerkprotokolls enthält
- der GRE-Kopf mit Informationen zum verwendeten Tunnel-Protokoll und Verschlüsselungsinformationen
- die Nutzlast (Payload) die das zu transportierende Datenpaket enthält

Das GRE-Tunneling-Verfahren ist in Schicht 3 des ISO/OSI-Basisreferenzmodells angesiedelt. Dadurch stellt es selber keine Zugriffskontrollmechanismen zur Verfügung. Es bildet aber die Grundlage für einige Schicht-2-Protokolle, die diese Mechanismen implementieren. Beim IP over IP -Tunneling wird beispielsweise einem IP-Paket ein neuer Header vorangestellt. Dies geschieht im Gateway des Quellnetzes. Als Ziel ist im neuen Header das Gateway des Zielnetzes adressiert, wo der Header wieder entfernt und das IP-Paket wieder in das lokale LAN-Segment eingespeist wird. Der Tunnel verhält sich wie eine bidirektionale Direktverbindung zwischen den beiden Tunnel-Servern.

[IP over IP; RFC2004], [Generic Routing Encapsulation (GRE); RFC1701, RFC1702] [IPX over IP; RFC1234], [AX.25 over IP; RFC1226] [67]

IP Security (IPSec)

IP Security (IPSec) ist ein relativ neues Protokoll. Es soll langfristig PPTP ablösen. Es stellt Sicherheitsfunktionen auf dem Internet Protocol (IP)-Niveau zur Verfügung. Es übernimmt die Authentifizierung und/oder Verschlüsselung übertragener Pakete. In IPv6 ist IPSec fester Bestandteil, zu IPv4 kann es optional ergänzt werden.

IPSec unterstützt zwei Kernmechanismen, die alternativ eingesetzt werden können. Der Authentication-Header (AH) ermöglicht die Authentifizierung des Senders. Mit der

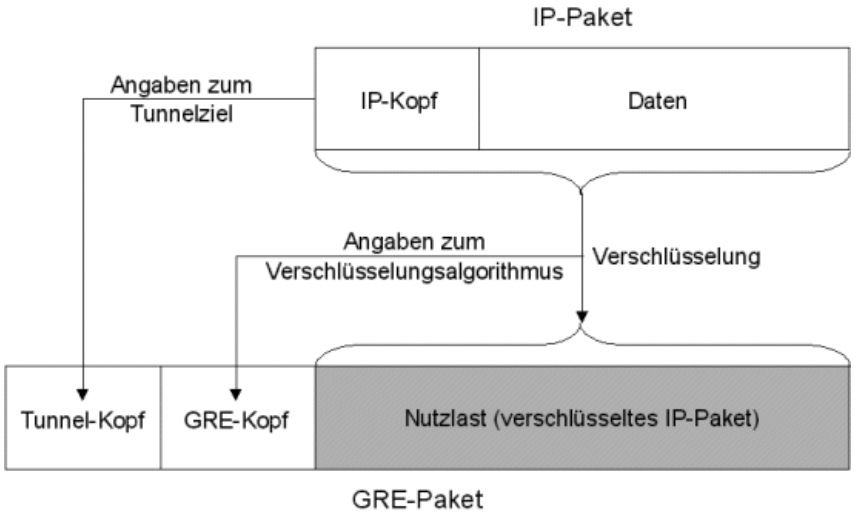


Abbildung 105: GRE-Paket

Encapsulating-Security-Payload (ESP) werden sowohl die Authentifizierung des Senders als auch die Datenverschlüsselung unterstützt. Die Informationen zum AH respektive zur ESP transportiert der IPSec-Header, der dem IP-Header des Datenpaketes nachgestellt ist.

IPSec besitzt zudem zwei verschiedene Modi: den Transportmodus und den Tunnelmodus. Beim Transportmodus werden die Daten des ursprünglichen IP-Paketes verschlüsselt und der Original IP-Header bleibt erhalten. Es wird lediglich noch ein kleiner IPSec-Header eingefügt. Der Vorteil dieses Modus ist, dass ein nur geringer Overhead entsteht. Nachteilig muss jede beteiligte Station IPSec implementiert haben, was eine Neukonfiguration bestehender Netze nach sich zieht. Außerdem kann ein Angreifer aus den nichtverschlüsselten IP-Headern Informationen die Netzstruktur schließen und z.B. feststellen welche Station wie viele Daten sendet oder empfängt.

Im Tunnelmodus wird das ganze IP-Paket verschlüsselt und ein neuer IP-Header und IPSec-Header erzeugt. Dadurch ist das IP-Paket zwar größer, aber die Vorteile dieses Modus überwiegen. Es sind lediglich zwei Gateways von Nöten, die die IP-Pakete verschlüsseln, durch ein öffentliches Netz versenden und am Ziel wieder entschlüsseln. Eine Umstellung des Netzes ist nicht nötig, da nur die Gateways umkonfiguriert werden, somit ist für die Stationen der Datenaustausch völlig transparent.

Auf dieser Basis lassen sich in zwei Bereichen zusätzliche Mechanismen zwischen den Kommunikationspartnern vereinbaren. Dies sind zum einen die Verschlüsselungsalgorithmen und zum anderen die Mechanismen für den Austausch von Schlüsseln zwischen den Kommunikationspartnern. Da IPSec einen erweiterbaren Rahmen für die sichere IP-Kommunikation bildet, können in beiden Bereichen unterschiedlichste Mechanismen eingesetzt werden. Das bedeutet, dass es zu lnkompatibilitäten zwischen den IPSec-Implementierungen kommen kann.

Allerdings hat die IETF einige Basisstandards festgelegt. Diese sind in den RFC1825 bis RFC1829 [16][17][18][104][81] sowie RFC2085 [105] und RFC2104 [90] definiert. Für den AH sind HMAC-MD5 und HMAC-SHA die designierten Mechanismen, die es zu unterstützen gilt, um auch in heterogenen Umgebungen Interoperabilität zu erreichen. HMAC (Hash-Message-Authentication-Code) ist ein Algorithmus, über den die Authentifizierung und Datenintegrität

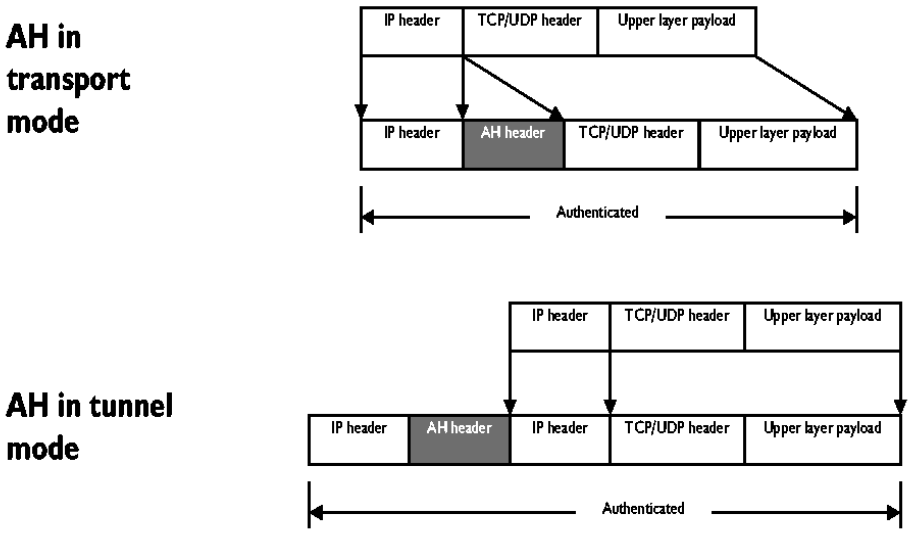


Abbildung 106: IPSec Authentication Header

durch Bildung eines Hash (hier: eine spezielle Form der Verschlüsselung) in Form einer digitalen Signatur für jedes Datenpaket sichergestellt wird. Er lässt sich mit den Hash-Algorithmen MD5 (Message-Digest) beziehungsweise SHA (Secure-Hash-Algorithm) bilden. Bei ESP wird dagegen mit DES-CBC (Data-Encryption-Standard - Cipher-Block-Chaining) als Verschlüsselungsmethode gearbeitet. Daneben können zusätzliche Abläufe programmiert werden, die allerdings nicht standardisiert sind.

Mit den Standards für die Authentifizierung beziehungsweise Verschlüsselung ist es nicht getan. Die zu verwendenden Mechanismen müssen ausgehandelt und Schlüssel ausgetauscht werden. Dazu wird beim Sitzungsaufbau eine Security-Association (SA) vereinbart. Der Standard für diesen Schritt ist das IKMP (Internet-Key-Management-Protocol), das auch als IKP (Internet-Key-Exchange) bezeichnet wird. Dieses Protokoll basiert auf ISAKMP/Oakley. ISAKMP beschreibt das Internet-Security-Association-and-Key-Mangement-Protocol das solche SAs definiert. Oakley ist ein Mechanismus, mit dem der Wechsel von Schlüsseln während Sitzungen in sicherer Weise erfolgen kann. Auch wenn ein Hacker einen Schlüssel knackt, kann er nur auf die mit diesem Key kodierten Informationen zugreifen. Neue Schlüssel errechnen sich nicht auf Basis eines bereits verwendeten Schlüssels. Zusätzlich zu IKMP lassen sich andere Ansätze für das Schlüsselmanagement implementieren. Auch hier gilt, dass IPSec für die Hersteller ein Rahmen zur Reallsation ihrer eigenen Lösungen ist. So soll bei Windows2000 beispielsweise auch Kerberos für den Sitzungsaufbau Anwendung finden. Neben IKMP unterstützen viele Anbieter auch manuelle Mechanismen für den Schlüsselaustausch. Dadurch entsteht aber eine erheblicher Aufwand für die Pflege und regelmäßige Änderung solcher Schlüssel, der für größere, produktive Umgebungen nicht adäquat ist. Bei der Auswahl von IPSec-Lösungen muss der Anwender darauf achten, dass IKMP (ISAKMP/Oakley) auf jeden Fall unterstützt wird.

IPSec ist der Durchbruch zu sicheren Online-Transaktionen über IP. IPSec wird zwar nicht alle Anforderungen abdecken, da es ein Mechanismus für einen Punkt-zu-Punkt-Kanal ist. Es wird

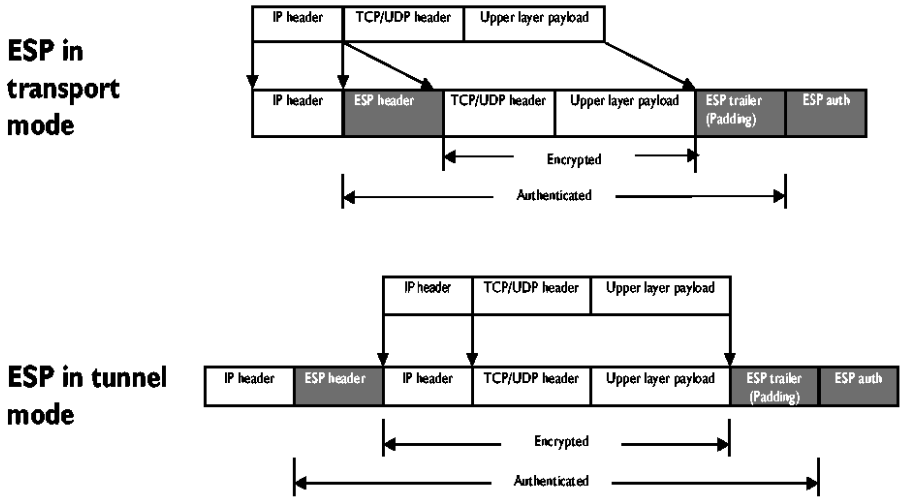


Abbildung 107: IPSec Encapsulating-Security-Payload

aber beispielsweise S/Mime oder PGP nicht ersetzen können. IPSec ist aber mit der breiten Akzeptanz bei Herstellern und durch seine offene Architektur eine ideale Lösung, um sowohl kritische Verbindungen in internen Netzen zu sichern als auch WAN-Verbindungen und virtuelle private Netzwerke zukünftig zu gestalten. Durch die Integration beispielsweise in Windows2000 und transparente Standards für das Schlüsselmanagement wird IPSec einfach nutzbar. Damit ist IPSec ein zentraler Baustein von Sicherheitskonzepten der Zukunft.

[IPSec; RFC1825-1829, RFC2085, RFC2104] [16] [17] [18] [104] [81] [105] [90] [147]

Schicht 4-7 VPNs

Für die verschiedenen Stufen der Implementierung ergeben sich verschiedene Sichten des VPNs. Auf Stufe Application ergibt sich folgendes Bild. Mehrere Endgeräte sind an ein öffentliches Netz angeschlossen. Für die einzelnen Anwendungen sind die Router in dem Netz zwar nicht a priori sichtbar, sie sind jedoch auch nicht explizit versteckt. Auch umgekehrt gilt, dass die Router selbst die Paketinhalte sowie deren Bestimmungsort ablesen könnten. Das daraus entstehende Sicherheitsloch wird mit Verschlüsselung gefüllt.

Es gibt verschiedene existierende Standards, wie das erwähnte SSL, daneben aber auch PGP (Pretty Good Privacy) und PEM (Privacy Enhanced Mail) für Mails und ähnliche.

SOCKS v5

SOCKS ist eigentlich ein Proxy-Protokoll, dass es einem Host ermöglicht Ressourcen hinter einem SOCKS-Server bzw. einer Firewall zu erreichen, ohne direkt eine Verbindung aufbauen zu müssen. Der SOCKS-Server authentifiziert und autorisiert die Anfragen, erstellt eine Proxy-Verbindung, und leitet die Pakete entsprechend weiter.

SOCKS arbeitet auf der Anwendungsschicht (Schicht 5) des ISO/OSI-Referenzmodells. Es hat damit wesentlich mehr Möglichkeiten zur Zugriffskontrolle als Protokolle tieferer Schichten, da

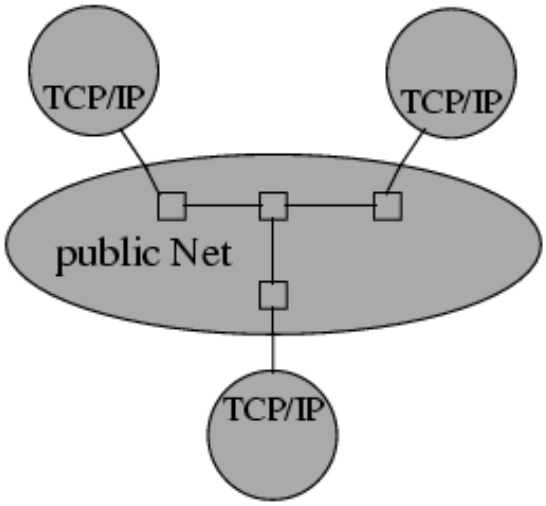


Abbildung 108: Layer 4-7

dem Protokoll auch Informationen zu laufenden Anwendungen zur Verfügung stehen.

SOCKS ist als Firewall weit verbreitet. Gerade in Verbindung mit Secure Socket Layer (SSL) bildet es die Grundlage für hochsichere VPNs. Da SOCKS jeder User einzeln authentifiziert, können so individuelle Zugriffsrecht vergeben werden,

[SOCKSv5; RFC1928, RFC1929, RFC1961] [92] [93] [103]

RADIUS (Remote Authentication Dial-In User Service)

RADIUS (Remote Authentication Dial-In User Service) ist genau genommen kein Protokoll. Es ist ein zusätzlicher Dienst, der die Verwaltung und Sicherung von Wählzugängen bietet, und somit den Aufbau eines VPNs erleichtert und verbessert.

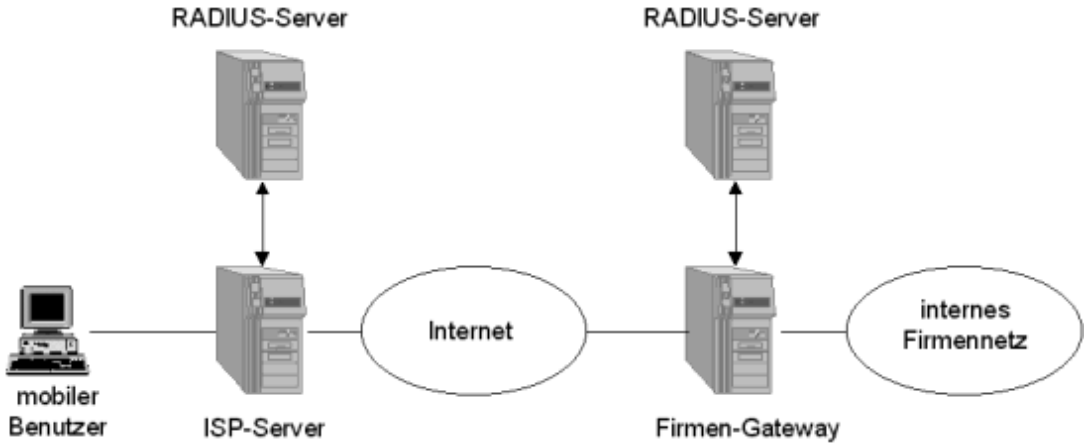


Abbildung 109: RADIUS-Konfiuration

RADIUS arbeitet mit einem Client/Server-Modell. Ein Network Access Server (NAS), z.B. bei

einem ISP oder einer Firma, nimmt als Client die Dienste eines RADIUS-Servers in Anspruch und übergibt diesem die User-Informationen (Login, Passwort). Der RADIUS-Server ist für die Authentifizierung des Users verantwortlich. Nach einer positiven Authentifizierung mittels PAP oder CHAP, übermittelt er dem NAS alle relevanten Informationen, die er braucht, um dem User seine Dienste zur Verfügung zu stellen. Zur Kommunikation zwischen RADIUS-Server und Client wird das User Datagram Protocol (UDP) verwendet.

RADIUS wird oft in Kombination mit anderen Protokollen verwendet, wie zum Beispiel PPP oder PPTP, L2F und L2TP.

[Remote Authentication Dial-In User Service (RADIUS); RFC2058, RFC2059] [113] [114]

Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP),entwickelt 1991 von Philip Zimmermann, benutzt eine Kombination aus public-key und konventionellen Verschlüsselungsverfahren, um sichere Dienste für E-Mail- und Datentransfer gewährleisten zu können. Diese Dienste sind:

- zuverlässige Verschlüsselung
- digitale Signaturen
- Datenkompression
- radix-64, ein Verfahren um binäre Daten in ASCII-Zeichen umzuwandeln

[RFC1505, RFC1847, RFC1991, RFC2015, RFC2440] [47] [61] [13] [52] [32]

Privacy Enhanced Mail (PEM)

Privacy Enhancement for Internet Electronic Mail (PEM) ist ein Standard zum sicheren Übertragen von E-Mail-Verkehr durch heterogene Systeme. Privacy enhancement services, wie Vertraulichkeit und Authentification und Integrität werden durch End-zu-End Verschlüsselung zwischen Sender und Empfänger ermöglicht, und zwar auf oder über dem User Agent Level. Es müssen somit keine Anforderungen an das Message Transfer System gestellt werden, weder an das Endsystem, noch an andere beteiligte Systeme. Damit ist eine Zusammenarbeit in heterogenen Umgebungen auf einer site-by-site oder user-by-user Basis möglich.

[RFC1421-RFC1424] [97] [84] [21] [79]

The TLS Protocol (TLS)

Das Transport Layer Protocol, früher bekannt unter dem Namen Secure Socket Layer (SSL), ist ein Protokoll zur sicheren Übertragung von Anwendungsprotokollen. Das primäre Ziel des TLS Protokolls ist es, zwischen zwei kommunizierenden Anwendungen Privatheit und Datenintegrität zu garantieren. Das Protokoll ist aus zwei Schichten aufgebaut: das TLS Record Protocol und das TLS Handshake Protocol. Auf der untersten Ebene, die auf einem Transportprotokoll aufsetzt (z.B. TCP), arbeitet das TLS Record Protocol. Es emöglicht eine sichere Verbindung mit zwei wesentlichen Eigenschaften:

- Die Verbindung ist privat. Symetrische Algorithmen (z.B. DES, RC4, usw.) werden für die Datenverschlüsselung verwendet. Die Schlüssel für dieses symetrische Verfahren werden durch das TLS Handshake Pprotocol ausgehandelt und sind einmalig. Das Record Protocol kann auch ohne Verschlüsselung verwendet werden.

- Die Verbindung ist zuverlässig. Der Nachrichtentransport beinhaltet einen Integritätscheck der auf einem Message Authentication Code (MAC) beruht. Sichere Hashfunktionen (z.B. SHA, MD5, usw.) werden für eine MAC Berechnung verwendet.

Das TLS Record Protocol wird verwendet, um verschiedene höhere Protokolle einzukapseln. Eines dieser eingekapselten Protokolle ist das TLS Handshake Protocol, welches dem Client und Server ermöglicht sich gegenseitig zu authentifizieren und einen Verschlüsselunsalgorithmus, sowie die entsprechenden Keys auszutauschen, bevor das Anwendnungsprotokoll beginnt, Daten auzutauschen. Das TLS Handshake Protocol hat drei wesentliche Eigenschaften.

- Die Identität der beteiligten Partner kann mittels asymetrischer oder Public Key - Verfahren authentifiziert werden.
- Das Aushandeln der verwendeten Verfahren und Schlüssel ist sicher.
- Das Aushandeln ist zuverlässig.

Ein Vorteil des TLS Protokolls ist, dass es unabhängig von der Anwendungsschicht ist. Höhere Protokolle können transparent auf dem TLS Protokoll aufsetzen.

[The TLS Protocol Version 1.0 (TLS); RFC2246] [49]

7.2.3 Management und Konfigurationen von VPNs

In diesem Abschnitt sollen die verschiedenen Konfigurationsarten von VPNs an Beispielen erläutert werden. Es werden die Netzstrukturen an Hand ihrer Einsatzgebiete erklärt und einige Vor- und Nachteile aufgezeigt.

Grundsätzlich lassen sich zwei Modelle unterscheiden: Peer VPNs und Overlay VPNs. Beim Peer Modell wird die Wegberechnung und Paketweiterleitung Hop by Hop durchgeführt. jeder zwischengeschaltete Switch oder Router ist an der VPN-Technik beteiligt. Ein Beispiel hierfür ist die Routen-Filterung nach dem Prinzip "Privatheit durch Verborgenheit": Die beteiligten Router werden so konfiguriert, dass sie sämtliche Routen eines VPNs nur innerhalb diese VPNs bekannt gegeben und verbinden. Dadurch können unterschiedliche VPNs sich gegenseitig gar nicht wahrnehmen und sich folglich auch nicht gegenseitig ausspionieren. Besteht jedoch der Wunsch nach kontrollierter Kommunikation mit anderen Netzen (etwa von Geschäftspartnern, Kunden, dem Internet), so ist dies nur über spezielle Übergangspunkte mit hochkomplexer Konfiguration möglich. Das Risiko einer Fehlkonfiguration und somit Sicherheitslücken ist erheblich. Außerdem beruht der Backbone-Betrieb auf einem einheitlichen gemeinsamen Routing und setzt dadurch eindeutige Adressen aller beteiligten VPNs voraus.

Beim Overlay-Modell werden sogenannte Cut-Through-Verfahren genutzt, die im Backbone auf der Verbindungs-Ebene arbeiten und nur im Eingangs- bzw. Ausgangspunkt des VPN eine Schicht-3-Kopplung einsetzen. Solche Verfahren werden oft auch als Single-Hop-Verfahren bezeichnet, da aus Sicht der privaten Erdnetze der WAN-Backbone einen einzelnen Hop darstellt. Beispiele sind die Link-Layer-Tunneling verfahren [siehe 2.2.1] oder ATM.

Eine weitere Möglichkeit der Unterscheidung von VPNs bietet die Trennung nach Einsatzgebieten, die in den nächsten Abschnitten näher erläutert werden soll.

End-to-End-VPNs

End-to-End-VPNs verbinden mehrere Hosts direkt miteinander oder mit einem Server. Beispielsweise kann so in einer Bank eine sichere Verbindung der Arbeitsplatz- oder Kundenrechner mit einem Großrechner erreicht werden, oder eine Arbeitsgruppe kann sich über das Internet zu einem Projekt zusammenschließen.

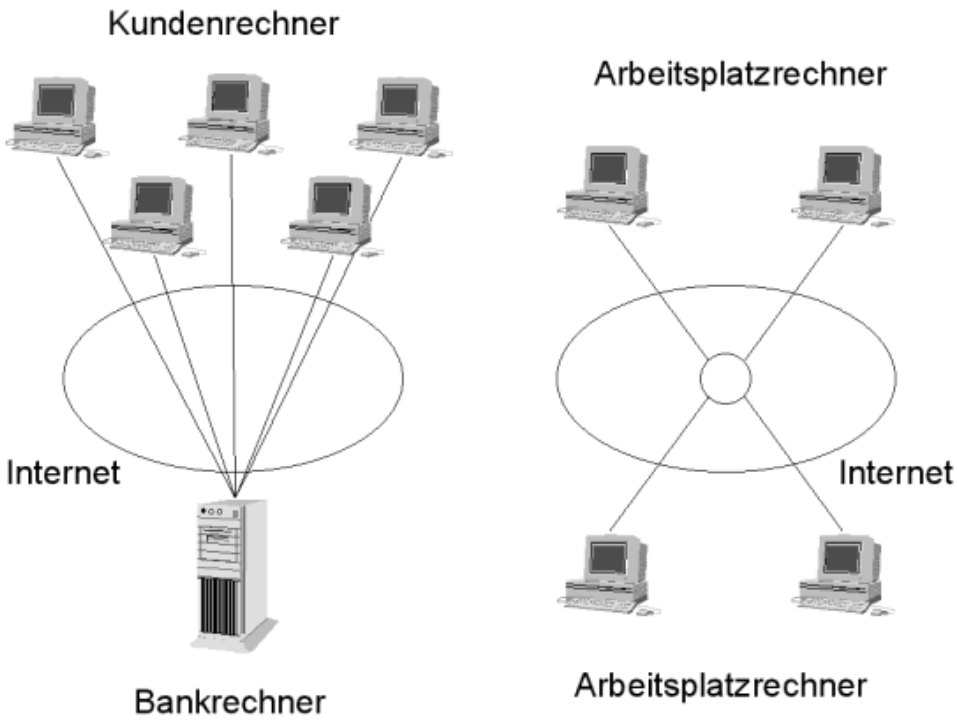


Abbildung 110: End-to-End Scenario

Beachten muss man allerdings, dass jeder an dem VPN angeschlossene Rechner ein entsprechendes VPN-Protokoll unterstützen muss, da die Kommunikation nicht über Gateways, sondern direkt (End-to-End) stattfindet. Außerdem ist zu beachten, dass der Verwaltungsaufwand bei verteilten Gruppen nicht mehr zentral gesteuert werden kann.

Als Implementierungen sind hier besonders die Tunnel-Protokolle wie PPTP, L2TP, L2f und IPSec geeignet.

Site-to-Site-VPNs

Site-to-Site-VPNs sind das klassische Beispiel für VPNs. mehrere LANs an verschiedenen Standorten schließen sich zu einem Gesamtnetz zusammen. Beispielsweise geographisch verteilte Standorte und Filialen einer Firma oder Bank. Es können so teure Langstrecken-Verbindungen eingespart und durch billigere ortsnahe Stand- oder Wählverbindungen zum nächstgelegenen ISP ersetzt werden.

Diese Art des VPN lässt sich noch einmal in zwei Untergruppen einteilen, die sich insbesondere in Sicherheitsanforderungen unterscheiden: Intranet VPN und Extranet VPN:

Intranet VPNs

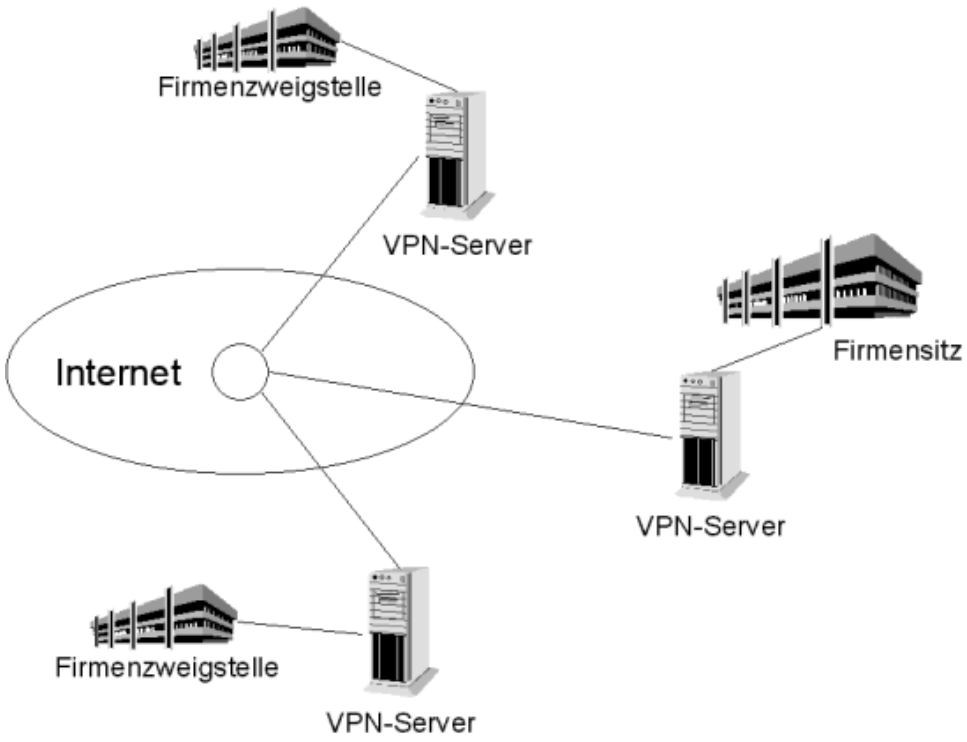


Abbildung 111: Site-to-Site Scenario

Ein Intranet VPN ist ein Netz, das hauptsächlich zur Erweiterung eines LANs dient. Alle angeschlossenen Teilnehmer vertrauen sich gegenseitig. Die Ressourcen sollen allen Parteien zur Verfügung stehen. Der Sicherheitsaspekt spielt eine untergeordnete Rolle, da die Datensicherheit mit Zugriffsbeschränkungen auf Dateiebene realisiert werden kann. Großer Wert wird auf Geschwindigkeit und Verfügbarkeit gelegt. Dieser VPN-Typ ist häufig bei großen Unternehmen anzutreffen, zwischen deren Standorten große Entfernungen liegen, die aber trotzdem auf ein gemeinsames Netzwerk angewiesen sind.

Als sinnvolles Protokoll kann z.B. IPSec im Transportmodus eingesetzt werden. Die Daten werden verschlüsselt übertragen und haben nur einen geringen Overhead, da nur ein paar Byte im IPSec-Header eingefügt werden müssen.

Extranet VPNs

Im Gegensatz zu Intranet VPNs liegt bei Extranet VPNs der Schwerpunkt auf dem Thema Sicherheit. Beispielsweise dient dieses VPN dazu, das interne Netz einer Firma mit Geschäftspartnern oder Zulieferfirmen zu verbinden. Die angeschlossenen Teilnehmer sollen nur beschränkten Zugriff auf bestimmte Ressourcen oder Anwendungen bekommen. Geschwindigkeit hat nur eine untergeordnete Rolle, da auch das Datenvolumen weit geringer ist als bei Intranet VPNs.

Eine Firewall mit SOCKSv5 und SSL wäre eine treffender Einsatzbereich für diese Situation, da mit diesen Programmen neben einer sicheren Verschlüsselung auch eine geeignet Möglichkeit zur Authentifizierung gegeben ist.

End-to-Site-VPNs

End-to-Site VPNs sind geradezu prädestiniert dafür mobile Außendienstmitarbeiter oder Tele-Arbeitsplätze mit dem Firmennetzwerk zu verbinden. Die Anwender können sich dabei bei jedem beliebigen ISP ins Internet einwählen und eine gesicherte Verbindung mit dem LAN des Arbeitgebers aufbauen. Dies spart zum einen teure Fernverbindungen und zum anderen teure Modembänke und Einwählserver bei der Firmenzentrale selbst.

Für den Aufbau eines solchen Netzes sind zum einen die Tunnelingverfahren wie PPTP oder L2TP und L2F gut geeignet, als auch die Möglichkeit über SOCKSv5 und SSL, ähnlich bei Extranet Site-to-Site VPNs, mit Firewalls zu arbeiten. Genaugenommen wird ja bei der Einwahl beim ISP bereits ein VPN mit NAS und RADIUS aufgebaut.

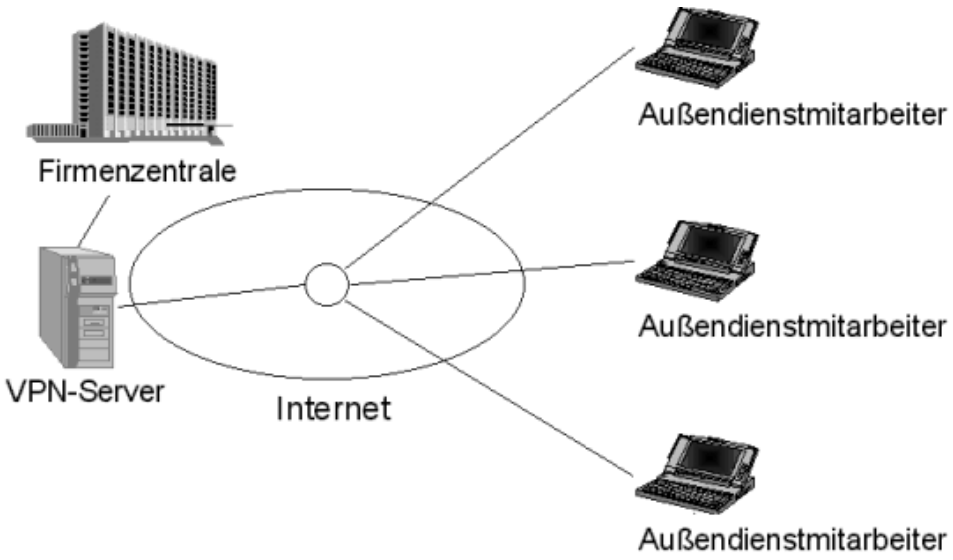


Abbildung 112: End-to-Site Scenario

7.2.4 Sicherheit

Der Grad an Privatheit und Flexibilität in einem VPN hängt entscheidend von der Technologie ab, mit der das VPN realisiert wird: Routen-Filterung bietet den niedrigsten Schutz, Tunneltechnik höherwertigen Schutz und zusätzlich Authentisierung, Paketfilterung a la Firewall bis hin zur Teil- oder Vollverschlüsselung den höchsten Schutz.

7.2.5 Zusammenfassung VPNs

Welche Produkte geeignet sind, und welche Technologien beim Einsatz eines VPN verwendet werden, hängt natürlich vom Einzelfall ab. VPNs werden als kostengünstige Alternative zu teuren Festsverbindungsnetzen und unsicheren Wähldiensten vermarktet. Ausgereifte Angebote der ISPs und Netzbetreiber fehlen noch, ebenso wie erprobte Service-Level-Konzepte mit vereinbarter Dienstgütegarantie. Gleiches gilt für Produktauswahl und -tests, da die aktuell verfügbaren Implementierungen sehr unterschiedlich und in Teilen proprietär sind.

In näherer Zukunft ist vor allem die Entwicklung von IPv6 interessant. Nach längerer Entwicklungszeit scheint hat sich dieses Protokoll so langsam seiner endgültigen Form genähert, nun bedarf es einer Umsetzung in bestehende Systeme.

Die Struktur hat sich dabei gegenüber der Version 4 stark erweitert. Unter anderem befinden sich optional schon Authentication Header- und ESP Header-Teile im Standard IPv6-Header und implementieren eine verschlüsselte Datenübertragung. Des weiteren kommen QoS Elemente hinzu, welche es erlauben sollen, eine bestimmte Ressource zu reservieren und auf der Gegenseite auch zu garantieren.

Dies sind eigentlich die zwei wichtigsten Punkte, um ein VPN aufzubauen. Es ist daher zu erwarten, dass IPv6 als Basis für den Aufbau eines VPNs eine maßgebliche Rolle spielen wird.

8 OSPF & PNNI - Routingtechnologien und Topologieplanung

8.1 Orientierung, Wegewahl, Switching: Grundlagen des Routing

8.1.1 Grundbegriffe

Routing ermöglicht die Sendung von Informationen über ein Netzwerk, von einer Quelle zu einem Ziel. Dabei sind in der Regel ein oder mehrere Zwischenknoten zu überwinden, die die Nachrichten in Richtung des Ziels weiterleiten müssen. Damit dies möglich ist, müssen diese Vermittlungseinheiten („Router“) freilich entweder über die Struktur und den Aufbau des Netzwerks Bescheid wissen oder zumindest die nächste Vermittlungseinheit kennen, die die Daten ihrem Ziel einen Schritt näher bringt.

Im Gegensatz zu Brücken (*Bridges*), die auf dem OSI-Layer 2 (*Link Layer*) operieren, arbeitet Routing auf der dritten Schicht, der Netzwerk-Schicht (*Network Layer*) (vgl. hier und im Folgenden [5]). Hier werden End-zu-End-Verbindungen zwischen Quell- und Zielsystem etabliert. Solche Punkt-zu-Punkt-Verbindungen können zwei Ausprägungen haben:

- virtuelle Verbindung (verbindungsorientierter Dienst) und
- Datagrammdienst (verbindungsloser Dienst).

Ein verbindungsorientierter Dienst benötigt die Zieladresse nur beim Verbindungsaufbau, folglich wird auch die Pfadbestimmung (s. unten) nur hier durchgeführt. Demgegenüber braucht ein Datagrammdienst die Zieladresse in jedem Paket, kann aber auch auf einen expliziten Verbindungsaufbau/-abbau verzichten. Die virtuelle Verbindung bietet dafür (im fehlerfreien Fall) eine dedizierte Verbindung während der gesamten Kommunikationszeit. Für das Routing kann dies jedoch negative Konsequenzen haben: Die bestehende Verbindung kann im Fehlerfall in der Regel nicht umgangen werden, während Datagrammdienste ein dynamisches Rerouting ermöglichen. Andererseits kann diese Dynamik wieder einen weniger ausgewogenen Verkehrsfluss bewirken als er mit festen Verbindungen erzielt werden kann. Außer Frage steht ferner, dass beim verbindungslosen Dienst für die Berechnung der Daten für die jeweilige Weiterleitung in jedem Zwischenknoten die Router mit einer entsprechenden Rechenleistung aufwarten müssen, um alle Daten und Routing-Informationen verarbeiten zu können (man kann von bis zu 20% Routing-Anteil am gesamten Datenverkehr ausgehen), während verbindungsorientierte Dienste i.A. weniger Resourcen benötigen.

Im Grunde lassen sich zwei prinzipielle Aufgaben des Routing festhalten:

- Pfadbestimmung und
- Switching.

Pfadbestimmung
Router müssen den optimalen Pfad zum Zielsystem bestimmen (i.A. ausgehend von sich). Der Terminus „optimal“ kann sich hierbei auf verschiedenste Metriken oder auch eine Kombination von Metriken beziehen (s. unten). Einmal festgelegte optimale Pfade werden in Routingtabellen gespeichert, um wiederholte Weiterleitungen von Informationen zu vereinfachen. Diese Routingtabellen können je nach Implementierung und Routingtechnologie verschiedene Einträge aufweisen; üblicherweise finden sich z.B. die Angaben *destination* und *next hop*: Anhand der Zieladresse eines eingehenden Datenpakets wird versucht, den zugehörigen nächsten Knoten auf

dem Pfad zu bestimmen, und das Paket wird dorthin weitergeleitet. Weitere Einträge in der Routingtabelle können Maßangaben über die mit dem Pfad assoziierten Kosten (Metriken) sein oder andere zusätzliche Daten zu diesem Weg (je nach Routing-Protokoll). Zu Backup-Zwecken oder für die Lastverteilung (z.B. OSPF, s. Kapitel 8.2) können auch mehrere Routen pro Ziel berechnet und eingetragen werden (Redundanz). Um die Aktualität der Routingtabellen gewährleisten zu können, tauschen Router untereinander Pfad-Informationen aus: dies können *routing update messages* sein, die einen Teil oder die ganze Tabelle übermitteln, oder *link-state advertisements*, die den Verbindungsstatus des Senders beschreiben. In allen Fällen ermöglicht der Datenaustausch den Routern, eine einheitliche und konsistente Topologie des Internetwork aufzubauen und so die gewünschten optimalen Pfade zu bestimmen.

Switching
Unter Switching versteht man das sich auf die Vorarbeit der Pfadbestimmung abstützende Weiterleiten der Informationsgruppen bzw. Pakete durch das Netzwerk. Die eigentliche Zieladresse, die vom verwendeten Protokoll bestimmt wurde, wird dabei in ein Routing-Paket mit der physischen MAC-Adresse des *next hop* Routers gekapselt und an diesen weiter geschickt. Lässt sich allerdings in der Routingtabelle keine Zuordnung zum nächsten Router finden, wird das Paket üblicherweise fallen gelassen.
Im Zusammenhang mit diesem Prozess der Weiterleitung schlägt die ISO eine Hierarchisierung der beteiligten Systeme vor:

- ES (*end systems*).
  Endsysteme können keine Pakete zwischen Subnetzwerken weiterleiten.
- IS (*intermediate systems*).
  Zwischensysteme können Pakete zwischen Subnetzwerken weiterleiten. Sie sind wiederum unterteilt in:
  - Intra-Domain IS. Diese kommunizieren innerhalb einer *routing domain*.
  - Inter-Domain IS. Diese kommunizieren sowohl innerhalb aus auch zwischen *routing domains*.

  Unter einer *routing domain* (bzw. einem Autonomen System, im Folgenden AS) versteht man dabei ein zusammenhängendes Netz unter gemeinsamer Administration, das eventuell noch weiter in *routing areas* (s. 8.2) unterteilt werden kann.

Die Algorithmen, die bei der Pfadberechnung angewandt werden (die „Routing-Algorithmen“ und somit letztendlich die Routing-Protokolle als solche), können anhand dreier Gesichtspunkte klassifiziert werden:

- Spezifika des Algorithmus,
- Typ des Algorithmus, und
- verwendete Metriken.

Spezifika des Algorithmus
Verschiedene Routingtechnologien legen auf die zu erzielenden Aufgaben im Netzbetrieb unterschiedlichen Wert. So beeinflusst beispielsweise die Größe des zu betreibenden Netzes die Auswahl der möglichen Routing-Protokolle, bzw. die spezifischen Eigenschaften eines Protokolls

erlauben die Anwendung in einem bestimmten AS, schränken ihn ein oder verbieten ihn sogar. So sind bereits die Spezifika des verwendeten Algorithmus Maß gebend für die Einsatzmöglichkeiten des resultierenden Routing-Protokolls:

- Optimalität.
  Es ist Ausschlaggebend, welche Maßstäbe der Algorithmus bei der Berechnung des „optimalen“ Pfades ansetzt, und wie er die Maße (s. unten) der Teilpfade gewichtet.

- Einfachheit.
  Das Routing soll den Netzwerkverkehr nicht durch hohen Overhead zusätzlich stark belasten, sondern Pfadbestimmung und Switching effizient durchführen.

- Robustheit und Stabilität.
  Im Falle von unvorhergesehenen Fehlern wie Hardware-Ausfällen oder bei hoher Netzlast, d.h. in jeder Situation, soll der Routing-Algorithmus einwandfreie Funktionalität und Ausfallsicherheit gewährleisten können.

- Konvergenz.
  Nach einem Fehler oder bei jeder Neu- oder Umorganisierung der Netzstruktur ist es wichtig, dass sich alle beteiligten Router rasch auf eine neue gemeinsame Topologie und neue optimale Routen einigen, sollen Inkonsistenzen und Schleifen beim Switching vermieden werden. Nur wenn alle Router dasselbe Bild der veränderten Netzwelt haben, ist zuverlässiges Routing gegeben: Besitzen beispielsweise zwei benachbarte Router aufgrund zu langsamer Konvergenz für einen gewissen Zeitraum verschiedene Routingtabellen, kann es zum *Count to Infinity* kommen (s. unten). Die Zeit, die benötigt wird, um den gemeinsamen Zustand über das ganze System hinweg herzustellen, ist daher ein bedeutender Faktor in jedem Routing-Algorithmus.

- Flexibilität.
  Der Routing-Algorithmus muss sich auf verschiedenste Randbedingungen und Ereignisse in einem Netzwerk einstellen und ggf. eine Neuberechnung der Routen anstellen. Das kann beispielsweise bei Veränderungen der Bandbreite, der Router Queue Size oder der Netzverzögerung der Fall sein.

- Update-Strategie.
  In starkem Zusammenhang mit der Flexibilität des Algorithmus steht, auf welche Weise eine veränderte Topologie, Fehler und neue Elemente im Netz erkannt werden. Grundsätzlich müssen dazu Topologiedatenbanken und Routingtabellen in den Routern aktualisiert werden. Wie aber erkennt der Algorithmus ausgefallene Links oder neue Knoten? Muss ein neuer Knoten sich selbst bekannt machen, oder wird er von seinen Nachbarn entdeckt? Gibt es Ereignis-gesteuerte Updates oder periodische, automatisierte? Wie werden die veränderten Daten im Netz bekannt gemacht, so dass neue Ressourcen berücksichtigt oder fehlerhafte Links umgangen werden, und welchen Routern sollen die neuen Informationen zukommen? Wie stark können die Update-Nachrichten komprimiert werden, um unnötigen Overhead zu vermeiden? Dies sind Fragen, die die Update-Strategie des Routing-Algorithmus bestimmen.

- Overhead.
  Wie schon angemerkt, ist vor allem bei verbindungslosen Diensten der Overhead des Routing-Protokolls auf der Leitung nicht zu vernachlässigen. Neben den Updates spielt

auch sein Umfang im normalen Betrieb eine Rolle bei der Beurteilung eines Routing-Algorithmus: Wie groß sind die Pakete mit Routing-Informationen, wie oft werden sie an wie viele Adressaten verschickt?

- Unabhängigkeit von der Netztopologie/Skalierbarkeit.
  Die Routingtechnologie sollte sich nicht auf bestimmte Netzstrukturen beschränken, um eine spätere Erweiterung oder Veränderung des Netzwerkes zu gewährleisten.

Typ des Algorithmus
Routing-Algorithmen und, daraus folgend, Routing-Protokolle können neben den obigen Grundmerkmalen noch nach bestimmten Typen gruppiert werden:

- Statische – dynamische Routing-Protokolle.
  Statisches Routing beschränkt sich eigentlich auf das Switching (und stellt daher gar kein echtes „Routing“ dar), da die Topologiedatenbank und die Routingtabelle vom Netzadministrator vorgegeben und geändert werden. Insofern eignet es sich also nur für einfache, kleine Netzwerke, die selbst keine starken (dynamischen) Veränderungen aufweisen. Vorteile des statischen Routings sind die sich ergebende höhere Sicherheit im Netzwerk (nur ein Ein- bzw. Ausgang) und die bessere Ressourcen-Effizienz, während die manuell vorzunehmenden Änderungen und die Tatsache, dass fehlerhafte Routen nicht automatisch erkannt werden, klar als Hauptnachteile gesehen werden müssen.
  Die heutigen (komplexen, wachsenden und sich stets verändernden) Netze werden deshalb besser durch dynamische Routing-Algorithmen bedient. Auf wechselnde Umweltbedingungen wird eingegangen, die Routingtabellen werden dynamisch aktualisiert und die optimalen Routen ggf. neu berechnet. Die dynamischen Routing-Protokolle lassen sich in Link-State und Distance-Vector Algorithmen (s. unten) sowie in Hybridversionen dieser beider Typen unterteilen.

- Single-Path – Multi-Path Routing.
  Multi-Path Routing-Algorithmen erlauben eine Verteilung des Datenstroms auf mehrere Pfade, um Auslastung und Durchsatz zu optimieren.

- Flache – hierarchische Routingstruktur.
  Routingtechnologien benutzen in der Regel eine bestimmte Topologie der vorhandenen Ressourcen, anhand derer die Routing-Informationen verteilt und das Routing organisiert werden. In einer flachen Hierarchie gibt es keine gliedernden Einheiten, während eine hierarchische Struktur eine Einteilung in Backbone-Router, Areas, AS oder andere Domänen erlauben. So können Routing-Informationen bestimmter Einheiten voneinander abgeschottet werden, was geringeren Datenverkehr und gestaffelte Pfadbestimmung ergibt. (s. unten)
  Es ist klar, dass eine mögliche Gliederung der Routing-Domäne oder Hierarchisierung von der Adressstruktur des darüber liegenden Protokolls abhängt (z.B. IP-/ATM-Adressen).

- Pfadbestimmung durch den Host oder den Router.
  Wenn der Endknoten den Pfad berechnet, spricht man von *Source Routing*; Router vermitteln dann nur weiter. Andernfalls steckt die Routing-Intelligenz ganz in den Routern.

- Link-State – Distance-Vector Routing.
  Diese grundlegenden Routingtypen werden in Kapitel 8.1.2 näher betrachtet.

Metriken
Ein wichtiges Merkmal eines jeden Routing-Algorithmus ist der Maßstab, der für die Beurteilung

von Pfaden und Streckenabschnitten angesetzt wird. Diese Metriken sind oftmals relativ „wirklichkeitsfremd“, da sie keinen direkten Bezug zu den tatsächlichen physischen oder monetären Einheiten haben. Trotzdem unterscheidet man hauptsächlich zwischen den folgenden Metriken, die komplexere Routingtechnologien auch zu Hybrid-Maßen kombinieren können:

- Pfadlänge.
  Die Pfadlänge ist vielleicht die intuitivste Routing-Metrik. Teilstrecken sind fiktive, Einheiten-lose Kosten zugeordnet, deren Summe die Gesamtpfadlänge ergibt.
- Anzahl der Hops.
  Eine andere Möglichkeit neben der Pfadlänge als Metrik ist, die Anzahl der *Hops* zu zählen und zu summieren.
- Zuverlässigkeit.
  Links werden gemäß ihrer Zuverlässigkeit (etwa der *Bit-Error Rate*) bewertet und mit entsprechenden numerischen Werten markiert.
- Delay.
  Je nach möglicherweise auftretenden Verzögerungen auf der Teilstrecke (Bandbreite, Warteschlangen, Stau, tatsächliche (physische) Entfernung) ergibt sich eine Messgröße aus mehreren Variablen, die von der Durchsatz- und Rechenkapazität der Router abhängt.
- Auslastung.
  Der Grad der Auslastung (z.B. CPU, Pakete pro Sekunde) beteiligter Netzwerkkomponenten wird dem Teilpfad zugewiesen.
- Kommunikationskosten.
  Nicht unterzubewerten sind die monetären Kosten, die auf die Benutzung eines Links von etwaigen Betreibern erhoben werden. Diese werden ebenfalls auf die Teilstrecken abgebildet.
- Kobinationen aus verschiedenen, oben genannten Metriken.

Im Zuge der rasanten globalen Vernetzung und immer größer werdenden Netzwerke wird es immer wichtiger, bei der Wegewahl und der Planung und Benutzung der Netzwerktopologien effiziente Modelle und Algorithmen anzuwenden. Skalierbare, hierarchische, ausfallsichere und „smarte“ Routingtechnologien helfen, Netzwerke verwaltbar zu machen und flexibel auf sich ändernde Bedingungen wie Netzlast oder Ausfälle zu reagieren.

8.1.2 Dynamische Routing-Protokolle: Link-State und Distance-Vector Routing

Der Hauptunterschied zwischen Link-State und Distance-Vector Routing (vgl. [3]) liegt darin, dass ein Router bei Link-State (oder auch *Shortest Path First – SPF* Algorithmen nur einen Teil seiner Routingtabelle mit den Angaben über seine Links zu seinen Nachbarn über das ganze Netz flutet, während er bei Distance-Vector (oder *Bellman-Ford*) Algorithmen seine gesamte Tabelle versendet, nun aber nur zu seinen unmittelbaren Nachbarn. Tabelle 23 verdeutlicht dies und zeigt weitere Unterschiede.

Das in der Tabelle angesprochene Problem, das entsteht, wenn ein Routing-Algorithmus nur die Anzahl Hops als Metrik berücksichtigt, ist in Abbildung 113 genauer dargestellt. Wollte im Beispiel der Router in Berlin einen Weg nach Rom wählen, könnte dieser entsprechend der

	Distance-Vector	Link-State
Prinzip	Router sendet größere Updates nur zu Nachbarn	Router sendet kleine Updates überall hin
Arbeitsweise	jeder Empfänger addiert seine Entfernungs-Werte zum Absender zur erhaltenen Topologie-tabelle; ggf. Update auf kürzere Routen; Durchlauf durch das ganze Netzwerk, bis keine besseren Pfade mehr gefunden werden	Routingtabelle aus *Link State Advertisements – (LSAs)* zusammengesetzt; ggf. Update auf kürzere Routen
Orientierung	keine Information über andere Router/Netztopologie Information über „Abstände“ der Router	volle Information über Router, Verbindungen und somit die Topologie
Fehlererken-nung	Ja, aber langsame Konvergenz, u.U. mit Inkonsistenzen oder „flatternden“ Routen	Ja. Event-gesteuerte Updates durch LSA, aber u.U. Gefahr „flatternder“ Routen
Metrik	i.A. nur Anzahl Hops (s. Abbildung 113))	beliebig
Performanz	hoch, außer bei Konvergenz	bei Updates oder Topologieaufbau kritisch durch Flooding; höhere Systemanforderungen durch Pfad-Berechnungen; sonst gut
Einsatz	kleinere Netzwerke, da weniger gut skalierbar	alle Netzwerke; komplexere Konfiguration, aber bessere Skalierbarkeit

Tabelle 23: Vergleich zwischen Distance-Vector und Link-State Routing-Algorithmen

Topologie des Netzes über Frankfurt, München und Wien gehen, oder über New York. Da die Anzahl der Hops über New York zwei beträgt, über die anderen Städte aber vier, würden die Daten über New York geroutet werden!

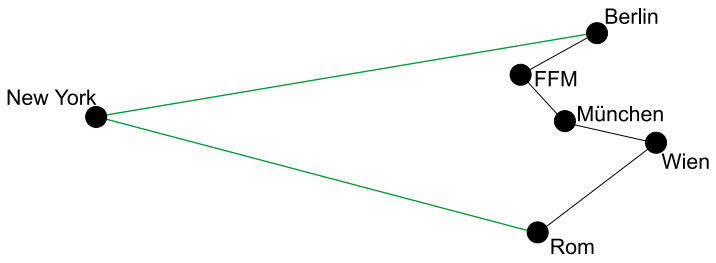


Abbildung 113: Wegewahl bei Anzahl Hops als einzige Metrik

Das Verhalten der beiden Routing-Algorithmen bei der Konvergenz im Fehlerfall verdient noch eine gesonderte Betrachtung: Wie wird erreicht, dass die Router sich unabhängig aus verschiedenen Perspektiven auf eine gemeinsame, neue Topologie einigen? Während die selbständige Funktionsweise der Vermittlungseinheiten im normalen Betrieb nämlich ein großer Vorteil ist, können unterschiedliche Zustände im veränderten Umfeld zu Schleifen und Inkonsistenzen beim Weiterleiten führen.

Dabei muss zuerst die Fehlerquelle genau lokalisiert werden. Dies ist oft nur möglich, wenn zwei Router an beiden Enden eines Links dessen Ausfall bestätigen, oder die Nichterreichbarkeit eines bestimmten Systems durch Vergleich der Meldungen von Zwischenknotens zurückverfolgt werden. Aus globaler Sicht ist das sofort klar; dezentral bereitet es jedoch Schwierigkeiten.

Nachdem beispielsweise ein defekter Link „entfernt“ worden ist, hat sich die Netztopologie verändert und muss bekannt gemacht werden. Werden die Topologie-Informationen nun lediglich zwischen den Nachbarn ausgetauscht (wie bei Link-State Algorithmen), kommt der *Convergence Time* hohe Bedeutung zu. Sie hängt ab von (vgl. [3]):

- dem Abstand des jeweiligen Routers zur Änderung im Netz;

- der Anzahl der Router im Netz;
- der Bandbreite und Auslastung der Links;
- der Auslastung der Router;
- dem Verkehr über die Fehlerquelle;
- der Effizienz des Routing-Protokolls.

Das Protokoll muss die neuen Routen also effizient und schnell berechnen lassen bzw. die entsprechende Information im Netz verbreiten. In instabilen Netzwerken mit redundanten Routen kann es dabei unter Umständen zu „flatternden“ Routen kommen: Jedesmal, wenn ein Router ein Update über eine neue Route erhält, entscheidet er sich für eine alternative Route als neuen besten Pfad. Er sendet ein entsprechendes Update aus, das andere Router allerdings dazu veranlasst, wiederum ihre Routingtabellen zu aktualisieren und neue (alte) Update-Messages zu erzeugen. So ergibt sich ein Hin- und Her„flattern“ zwischen zwei Routen. Alternative Routen können den Konvergenz-Prozess also verlangsamen oder auch behindern.

Distance-Vector Algorithmen haben ein ähnliches Problem: Weil die Distance-Vector Aktualisierungen aus Sicherheitsgründen periodisch verschickt werden, kann es passieren, dass ein Update von Router A einem Router B, der als erster vom Ausfall einer Verbindung von B zu Router C „berichten“ kann und will, zuvorkommt, so dass B die eben erst selbst festgestellte „unendliche“ Entfernung zu C über den fehlerhaften Link „vergisst“ und statt dessen als Route zu C den Eintrag vom Nachbarn A übernimmt, der allerdings den Link von A zu B als next hop in Richtung C anführt. B akzeptiert diesen „neuen“ Weg zu C, weil er kleiner unendlich ist. So verbreitet B nun irrtümlicherweise die Meldung, C sei über den Link von A nach B erreichbar, was dazu führt, dass Pakete an C, die über B gehen, von B an A und wieder zurück usw. geschickt werden. Dies nennt man den **Bouncing Effect** (s. Abbildung 114, vgl. auch [72], S. 72 ff.).

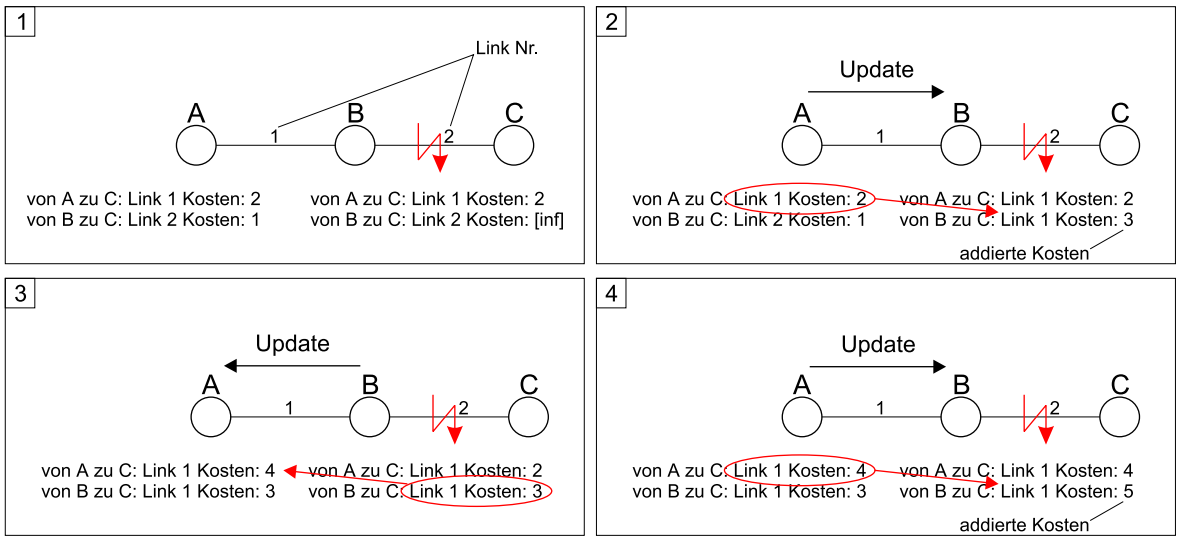


Abbildung 114: Bouncing-Effekt

Ein anderes Problem bewirkt die langsame Konvergenz von Distance-Vector Algorithmen: Plötzlich isolierte Knoten oder Netzteile inkrementieren (durch gegenseitige Distance-Vector Updates) die Entfernung zu den nicht mehr erreichbaren Routern bis zu einer festgelegten Obergrenze

(**Count to Infinity**, vgl. [72], S. 75). Es ist klar, dass daher die maximale Entfernung von Routern in Netzen mit diesen Routing-Algorithmen nicht über die Infinity-Grenze gehen darf.

Diese beiden Probleme können für die meisten Fälle durch die Einführung des **Split Horizon** (vgl. [72], S. 76 ff.) vermieden werden. Die prinzipielle Idee des Split Horizon ist es, den Standard-Distance-Vector nicht automatisch an alle Ausgänge weiterzugeben: So ist es unsinnig, dass ein Router B ein Ziel X durch Router A zu erreichen sucht, wenn A durch B routet (B also hinter A liegt). Damit wird der Bouncing Effect vermieden – dass A an B meldet, X sei nicht weit von A entfernt und B könnte den Routing-Eintrag von A übernehmen. Es existieren zwei Versionen des Split Horizon: In der einfachen Variante (s. Abbildung 115) werden einfach alle Routen über den Link, den auch das Update benutzt, nicht übermittelt. Die zweite Version, „Split Horizon with Poisoneous Reverse“, setzt die Entfernung des Zielknotens auf Unendlich, wenn er über den Link (den die Update-Message nimmt) geroutet wird. In besonderen Ausnahmefällen (verlorengegangene Updates u.ä.) kann aber auch Split Horizon das Count-to-Infinity Problem nicht lösen.

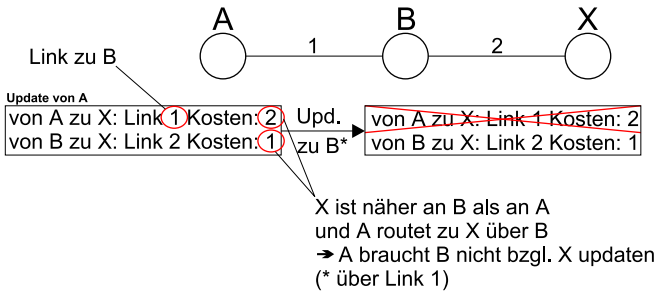


Abbildung 115: Split Horizon (einfache Variante)

Im Folgenden soll nun das Link-State Routing Protokoll OSPF (Open Shortest Path First) als Nachfolger des lange im Internet verwendeten Distance-Vector Protokolls RIP (Routing Information Protocol, heute wird es nur noch in kleineren Netzen eingesetzt) näher untersucht werden; einer Netzwerktechnik der nächsten Generation wie ATM allerdings genügt OSPF wiederum nicht mehr, so dass hier eine weiterentwickelte und verfeinerte Version – PNNI – Verwendung findet, die ebenfalls genauer betrachtet werden soll. Stellen also RIP und OSPF noch zwei prinzipiell verschiedene Routingtechnologien dar, kann der Übergang von OSPF zu PNNI vielleicht eher als Evolution bezeichnet werden.

8.2 OSPF – Open Shortest Path First

OSPF ist ein Link-State Routing-Protokoll und steht für Open Shortest Path First, da es ein **o**ffenes Protokoll ist (Public Domain, Veröffentlichungen in RFC's, Request for Comments). und den für Link-State Routing üblichen **S**hortest **P**ath **F**irst Algorithmus verwendet. Die folgenden Ausführungen basieren vor allem auf [112] und [25] sowie [4], [72] und [135].

8.2.1 Ziele und Einsatz von OSPF

OSPF ist auf die Netzstruktur der TCP/IP- bzw Internet-Welt ausgerichtet und routet IP-Pakete nach der IP-Adresse des IP-Paket-Headers; die IP-Pakete werden dabei nicht in neue Protokollheader eingekapselt. OSPF ist als IGP (*Interior Gateway Protocol*) konzipiert, d.h. es

regelt das Routing innerhalb eines AS (Autonomen Systems) und gehört damit zur Gruppe der Inter-Domain IS (s. oben). OSPF wurde vor allem im Hinblick auf folgende Ziele entwickelt:

- Unterstützung hierarchischer Netzstrukturen
- schnelle Konvergenz bei Topologieänderungen
- Zyklenfreiheit bei und nach der Konvergenz
- geringer Overhead

OSPF-Router besitzen eine Link-State-Datenbank, deren LSA's (Routing-Updates, s. unten) per Flooding verbreitet werden. OSPF unterstützt ferner redundante Routen, um dadurch Lastverteilung realisieren zu können. Jeder Router berechnet so einen Baum mit den kürzesten Entfernungen und sich selbst als Wurzel. Dies ist der prinzipielle SPF-Algorithmus, der freilich für jeden Router einen individuellen Baum mit den jeweilig kürzesten Pfaden ergibt. Bei OSPF können darüber hinaus mehrere Bäume für verschiedene Metriken berechnet und gespeichert werden; dabei sind die Metriken möglich, die durch das drei Bit lange TOS-Feld im IP-Header bestimmt werden können.

Eine wichtige Eigenschaft von OSPF ist, dass Gruppen von Netzwerken innerhalb eines AS zu **Areas** zusammengefasst werden können. Die Topologie einer Area ist von den übrigen Knoten des AS abgeschirmt. Dadurch wird eine Verringerung des Routing-Overheads und -Verkehrs und eine Reduzierung der Daten der Routing- bzw. Topologiedatenbank erreicht. Areas sind wegen der übersichtlicheren lokalen Topologie besser gegen schlechte Routing-Information geschützt. OSPF führt somit ein erstes (zweistufiges) hierarchisches Konzept ein.

Um dieses Modell zu unterstützen, arbeitet OSPF mit *Variable Length Subnetting*, erlaubt also (Zieladresse, Subnetzmaske)-Tupel (VLSM). Weiterhin bietet OSPF die Möglichkeit verschiedener Authentisierung-Schemas für jedes IP-Subnet, so dass beispielsweise nur vertrauenswürdige Router an einem bestimmten Routing teilnehmen dürfen. OSPF ist zwar nur ein IGP, kann aber Routing-Informationen von EGP's (Exterior Gateway Protocols) im AS verteilen. Diese externen Daten nehmen in den Routingdatenbanken einen Sonderstatus ein.

8.2.2 Das OSPF-Topologiemodell und seine Elemente

OSPF unterstützt folgende Netzwerke und Verbindungen:

- Punkt-zu-Punkt-Verbindungen/Netze. Ein Netz, das zu einem einzelnen Router-Paar gehört; die Verbindung zwischen diesen ist eine Punkt-zu-Punkt-Verbindung. Auch Direktverbindungen von Endsystemen (Hosts) an Router werden als Punkt-zu-Punkt-Verbindungen behandelt.
- Broadcast-Netze. Diese Netze unterstützen mehr als einen Router; alle Router können allerdings mit einer einzigen physikalischen Nachricht erreicht werden (oder auch jeder einzelne Router). Nachbar-Router werden über das **Hello-Protokoll** (s. unten) erkannt, welches auf der Broadcast-Eigenschaft aufbaut.
- Non-Broadcast-Netze. Dies sind Netze mit mehr als zwei Routern, aber ohne Broadcast-Fähigkeit. Das Hello-Protokoll funktioniert auch in Non-Broadcast-Netzen, muss die fehlende Broadcast-Funktionalität aber kompensieren, indem es die Nachbar-Router einzeln

anspricht. OSPF kennt hier zwei Alternativen: zum einen *Non-Broadcast Multi-Access (NBMA)*, das ein Broadcast-Netz simuliert, zum anderen *Point-to-Multipoint*, das das Netz als eine Kollektion von Punkt-zu-Punkt-Verbindungen sieht.

OSPF arbeitet daneben auf virtuellen Links, die im Fehlerfall eine Verbindung zum Backbone (s. unten) aufrecht erhalten.

Netzwerke an sich können dann transient sein oder **Stub** Netzwerke. Stubs sind Netze, die nur einen Ein-/Ausgang haben, also sozusagen „Sackgassen“ im AS. Hosts, die direkt an einen Router angeschlossen sind, werden ebenfalls als Stub Netzwerke gesehen. Im Beispiel-AS von Abbildung 116 ist etwa N7 ein Stub.

Die Topologie in OSPF kennt dann an sich drei Einheiten: Netze, Areas (als Gruppierung mehrerer Netze), und AS (das in Areas aufgeteilt sein kann).

Area
Die Area als „untere“ Routing-Ebene besteht, wie schon angedeutet, aus (logisch und physikalisch) zusammenhängenden Netzwerken und Hosts und den Routern, die Interfaces zu diesen Systemen haben. Jede Area kann innerhalb ihrer Grenzen ihre eigene Version des Link-State-Algorithmus besitzen. Folglich existieren pro Area eigene Topologiedatenbanken und Graphen. Diese feine Topologie ist wiederum im AS außerhalb der Area nicht sichtbar, während die Area-Router kein detailliertes Wissen über die Welt des restlichen AS haben. Die Kosten der Wege zu allen Netzwerken außerhalb der Area werden innerhalb einer Area summiert bekannt gegeben (s. Kapitel 8.2.3).

Die Router, die an der Grenze der Area (und somit zugleich in einer andere Area des AS) sitzen, heißen **Area Border Router**. Durch ihre Zugehörigkeit zu mehreren Areas besitzen auch sie mehrere Link-State-Datenbanken, eine pro Area, mit der sie verbunden sind. Innerhalb einer Area unterscheidet man dann zwischen *Inter-Area Routing* (aus der Area heraus oder darüber hinweg, s. unten) und *Intra-Area Routing* (nur innerhalb der Area).

Backbone
Die spezielle Area 0 in OSPF ist der Backbone. Der Backbone enthält alle Area Border Router und Router, die keiner Area zugeordnet sind (also zu keinem Netz oder Host in der Area ein Interface besitzen). Der Backbone muss zusammenhängend sein – allerdings kann dies auch durch eine logische Verbindung über Virtuelle Links erreicht werden, falls es physikalisch nicht möglich ist. Diese Virtuelle Links können dann freilich durch Areas laufen (mit Intra-Area Routing) und werden als Punkt-zu-Punkt-Verbindungen gehandhabt. Inter-Area Routing geht nach diesen Festlegungen also stets über den Backbone; dem Intra-Area Routing aus der ersten Area heraus folgt ein Pfad durch das Backbone (an sich wieder Intra-Area), und ein Intra-Area-Endstück in der Ziel-Area. Insofern kann man dies als erzwungene Sterntopologie betrachten, mit dem Backbone als Hub.

AS
Zusammenfassend besteht ein AS also aus mehreren Areas, wovon der Backbone eine besonders ausgezeichnete Area darstellt. Die dazugehörigen Router-Klassen sollen ebenfalls noch einmal aufgeführt werden:

- (Area-)Interne Router: Router, deren direkt verbundene Netzwerke in einer Area liegen.
- Area Border Router: Router, die zu mehreren Areas (z.B. auch zum Backbone) gehören. Sie lassen mehrere Kopien des Routing-Algorithmus laufen und kondensieren die Topologie-Informationen jeder Area für die Weitergabe nach „außen“ (also z.B. zum Backbone).

- Backbone Router: Interne und Area Border Router der Backbone-Area.
- AS Boundary Router: Router, die Informationen mit Routern anderer AS austauschen und diese Wegeinformationen dem eigenen AS verfügbar machen. Die Pfade zu den AS Boundary Routern sind allen (!) Routern des AS bekannt: Die externen Routingdaten werden gesondert bekannt gemacht; analog ist die Klasse der AS Boundary Router auch völlig unabhängig von den vorher Genannten.

Ein Router kann in OSPF auch noch zum **Designated Router** ernannt werden; diese Klassifizierung geschieht im Zusammenhang mit den dynamischen Routing-Vorgängen, die im folgenden Kapitel näher betrachtet werden sollen.

Analog zu Stub Netzwerken gibt es in OSPF (seit Version 2) noch **Stub Areas**. Diese besonderen Areas besitzen zwar vielleicht mehrere Area Boundary Routers als Verbindung zur „Außenwelt". Um nun aber nicht alle möglichen externen Ziele in die Area propagieren zu müssen, wird innerhalb der Stub Area nur ein bestimmter Area Boundary Router als Adressat für die externen Ziele bekannt gemacht, über eventuelle weitere Boundary Router kann nicht „extern" geroutet werden. So wird vermieden, dass innerhalb der Area große Datenmengen an Informationen über externe Zielpunkte gehalten werden müssen. Durch Stub Areas können andererseits keine Virtuellen Links gelegt werden (diese bräuchten ja zwei offizielle Area Border Router als Ein-/Ausgang), und es ist auch nicht möglich, dass ein AS Boundary Router Mitglied einer Stub Area ist (dieser würde ja die externen Informationen wieder importieren) – der Area Border Router der Stub Area kann er allerdings durchaus sein. Dieses Konzept erwies sich allerdings in manchen Fällen als zu restriktiv, weshalb man **Not So Stubby Areas (NSSA)** erfand: Hier ist es manchen Routern innerhalb einer Stub Area erlaubt, auch AS Boundary Router zu sein und externe Informationen zu erhalten, die jedoch nicht im gesamten AS (wie für externe Routing-Informationen üblich, s. oben) verteilt werden, sondern nur in der NSSA.

8.2.3 OSPF-Routing

Anhand eines Beispiels sollen nun die Prinzipien des OSPF-Routing-Algorithmus eingehend betrachtet werden: ausgehend von der Initialisierung der Routing-Umgebung, über den Betrieb des System bis hin zum Fehlerfall und zur Recovery. Dabei werden noch einige neue Elemente von OSPF eingeführt werden, die die im vorhergehenden Kapitel gezeigte Übersicht über OSPF vervollständigen werden.

Abbildung 116 zeigt ein AS, wie es auch in der Spezifikation von OSPF [112] (und auch in weiten Teilen der Sekundärliteratur wie [25]) zur Demonstration der Eigenschaften des Routingverfahrens verwendet wird, da es alle Konzepte von OSPF anschaulich zeigt. Kreise symbolisieren Netzwerke, Rechtecke Router. Das Rechteck mit der Markierung H repräsentiert einen Host mit SLIP-Verbindung zum Router R12. Linien zwischen Routern symbolisieren physikalische Punkt-zu-Punkt-Netzwerke, der Router-Interfaces keine eigenen Adressen benötigen. Andererseits kann eine solche aber trotzdem zugewiesen werden: Bei den Netzwerken an Router R6 und R10 ist das der Fall (Ia und Ib). RT5 und RT7 haben BGP (Border Gateway Protocol) Verbindungen, also Verbindungen zu externen AS.

Mit der Ausgangsseite der Router ist jeweils ein (aufsteigend wertiges) Kostenmaß assoziiert, das die gesamten Kosten bis zum nächsten Router beschreibt. Auch von extern erhaltene Routen erhalten diese Kosten. Ein Weg von einem Netzwerk (bzw. Host) zum Router hat keine Kosten. Das AS ist nun ein in 3(+1, der Backbone) Areas aufgeteilt. Es ist leicht zu sehen, welche Router interne Router sind (R1, R2, R5, R6, R8, R9, R12), welche Area Border Router (R3, R4, R7,

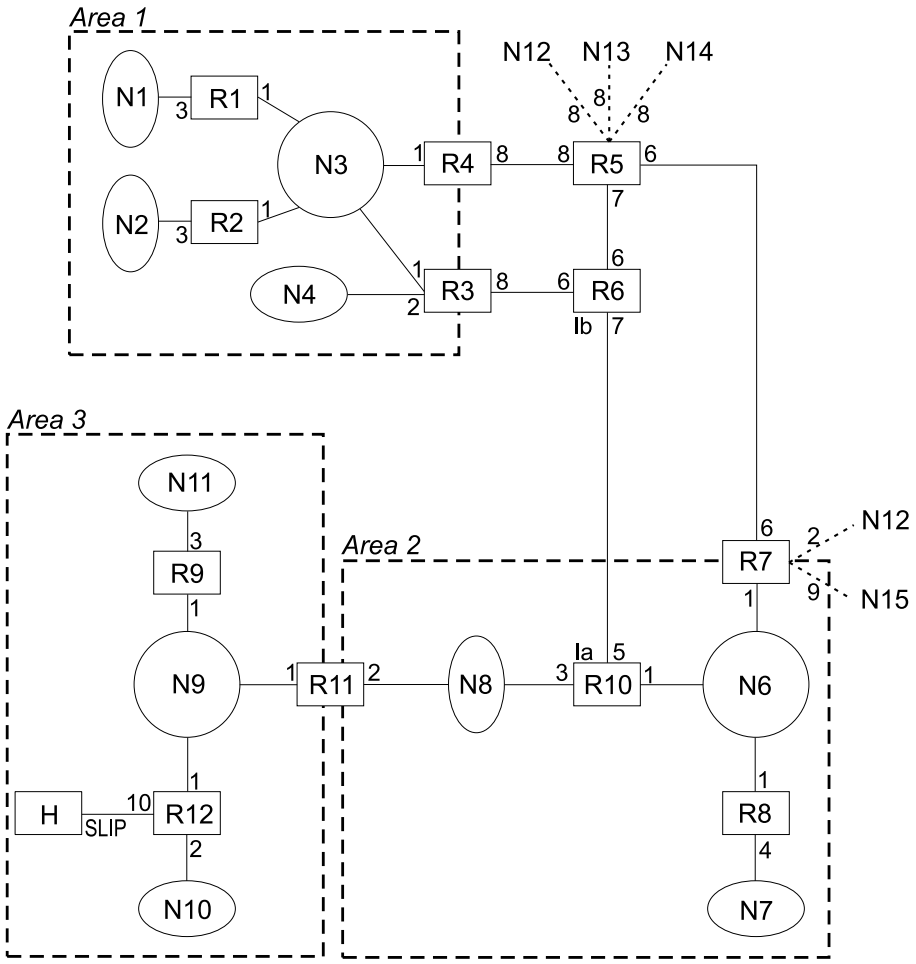


Abbildung 116: OSPF-AS mit Areas (aus [112] bzw. [25])

R10, R11), welche Backbone Router (R3, R4, R5, R6, R7, R10, R11) und welche AS Boundary Router (R5 und R7). R11 gehört sowohl zu Area2 wie auch zu Area3 und zum Backbone, zu dem er keine physikalische Verbindung hat – so wird ein Virtueller Link zwischen R10 und R11 konfiguriert.

Doch nun zum Routing selbst. Zuerst (wir nehmen an, das AS wird „frisch“ in Betrieb genommen) müssen sich die Router gegenseitig kennenlernen, einen Topologieplan ihrer Area erstellen (ihn dann an den Grenzen zusammenfassen, für außerhalb bereitstellen) und ihn mit den summarischen Angaben über das restliche AS vervollständigen.

Area-Topologie
Wie können die an ein bestimmtes Netzwerk angeschlossenen Router miteinander kommunizieren, ohne dass jeder Router zu jedem anderen eine Adjazenz aufbauen muss und es so (bei n Routern) zu $\frac{n \cdot (n-1)}{2}$ Verbindungen kommt?

OSPF unterscheidet hier zwischen Point-to-Multipoint Netzwerken auf der einen Seite und Broadcast und NBMA Netzwerken auf der anderen. Bei ersteren existieren für OSPF ja nur Punkt-zu-Punkt-Verbindungen, und so werden zwischen jedem benachbarten Paar von Rou-

tern, die direkt miteinander kommunizieren können, Adjazenzen erstellt. Ansonsten kann ein **Designated Router** bestimmt werden, der sozusagen die Leitung für das Netzwerk und seine Router übernimmt und den Kommunikationsverkehr wie gewünscht vermindert. Der Designated Router wird durch das **Hello-Protokoll** ernannt.

Hello-Pakete werden periodisch mittels ICMP-Massages an alle Router-Interfaces verschickt (dazu existiert eine Multicast-Adresse *AllSPFRouters*; die Hello-Nachrichten sind dabei ICMP-Messages). Das Hello-Protokoll knüpft somit Beziehungen zwischen Nachbarn und hält sie auch aufrecht. Dabei muss sichergestellt sein, dass die Kommunikation zwischen den Routern auch bidirektional ist, weil andernfalls Verbindungen einseitig ins Leere gehen könnten. Die Bidirektionalität ist dann gegeben, wenn der Nachbar-Router in seiner Liste der Nachbarn den ersten Router bereits aufgeführt hat. Diese Liste macht i.A. den größten Teil eines Hello-Pakets aus und besteht an sich aus den ID's aller Router, die dem Nachbar-Router innerhalb des letzten *Dead Intervals* (ebenfalls ein 32-Bit-Feld, in Sekunden) ein Hello-Paket geschickt haben.

Im Hello-Paket existiert weiterhin ein 8-Bit-Feld mit der Priorität (einem Wert zwischen 0 und 255) des versendenden Routers für die Rolle des Designated Routers, sowie ein Feld mit der Adresse des gewünschten/als gültig erkannten Designated Routers (und Backup Designated Routers, s. unten). Anfangs sind beide Felder üblicherweise leer, so dass nach dem gegenseitigen Austausch der Hello-Pakete der Router mit der höchsten Priorität (und im Falle einer doppelt vorkommenden Priorität der mit der höheren ID) zum Designated Router bestimmt wird. Ein neu zum Netz hinzukommender Router akzeptiert den bestehenden Designated Router, auch wenn er selbst eine höhere Priorität hätte.

Adjazenzen werden nun in einem Netz nur mit dem Designated Router aufgebaut. Das ist deswegen von Bedeutung, weil auch nur zwischen adjazenten Routern die (aufwändige) Synchronisation der Link-State-Datenbanken (s. unten) stattfindet. Der Designated Router generiert andererseits auch ein Link-State Advertisement (Informationen über die ihm bekannte Topologie eines Netzabschnittes oder Netzwerks, s. unten) für das betrachtete Netz. Damit ist ein Ausfall des Designated Routers besonders kritisch: Das Netz erscheint dann von außen als komplett anderer Knoten, und sämtliche Topologiedatenbanken müssten geändert werden. Aus diesem Grund bestimmt OSPF noch den so genannten Backup Designated Router, der ebenfalls durch das Hello-Protokoll bestimmt wird (in einem weiterem 32-Bit-Feld) und praktisch „unsichtbar“ parallel zum Designated Router arbeitet (Mithören der Nachrichten zum/vom Designated Router, gleiche Link-State-Datenbank usw.). Im Ernstfall wird der Backup Router so schnell zum Designated Router, und das Hello-Protokoll bestimmt einen neuen Backup Designated Router.

In der Area 1 des Beispiel-AS von Abbildung 116 könnte etwa R4 als Designated Router für N3 bestimmt worden sein, und R1 als Backup Designated Router. Obwohl das natürlich nur ein sehr eingeschränktes Beispiel ist, wird anhand Abbildung 117 klar, dass Kommunikationsverbindungen eingespart wurden: in diesem Fall zwischen R1 und R2.

Stehen also endlich die Adjazenz-Nachbarn fest, müssen, wie schon angedeutet, die Topologiedatenbanken (Routing-Datenbanken/-Tabellen, Link-State-Datenbanken) erstellt werden. Da ja eine einheitliche Fassung dieser Datenbank angestrebt wird, werden die Daten der einzelnen Nachbarn synchronisiert und gegenseitig aktualisiert. Diese initiale Synchronisation wird durch das **Exchange-Protokoll** erledigt. Drei Bits des zugehörigen **Database Description (DD)** Pakets steuern diese Prozedur: Initialize (I), More (M) und Master-Slave (MS). Der initialisierender Router setzt alle Bits auf 1 und erklärt sich somit zum Master (MS=1). Der Partner ist im Normalfall mit dem Slave-Status zufrieden und antwortet mit MS=0. (Sonder- und Fehlerfälle wie verlorene Pakete seien hier vernachlässigt). Es folgt der asynchrone Datenaustausch: Der Master sendet DD's mit DD-Sequenznummer und der Beschreibung jeweils eines Link-State-

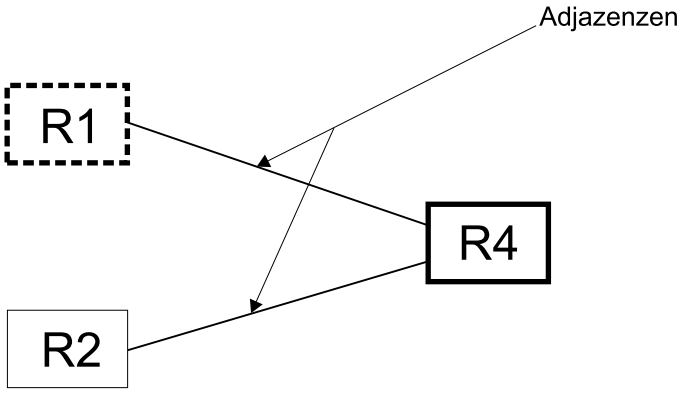


Abbildung 117: Adjazenzen für N3 im Beispiel-OSPF-AS

Records. Die wichtigsten Bestandteile dieser Beschreibung sind Router-ID, Link-State Typ und Link-State ID. Der Slave reagiert mit Acknowledgments, die seinen Eintrag für den Link enthalten. Jeder behält sich eine Liste mit Records, die ein Update benötigen. Diese erste Phase des Exchange-Prozesses arbeitet, bis beide Router das M-Bit auf 0 gesetzt haben, also keine Records mehr bekannt zu geben sind. Die benötigten Updates werden dann in **Link State Request** Paketen angefordert. Als Antwort erhält der Router die benötigten Link-State Angaben, verpackt in **Link State Updates**, wie sie auch beim Flooding im laufenden Betrieb verwendet werden.

Diese Link State Update Pakete werden durch das Tripel sendender Router/Link State ID/Link State Typ 4 (OSPF-interne Typnummer) identifiziert. Auf diesen Header folgen zuerst Angaben über die Anzahl der enthaltenen Link State Records und dann diese selbst. Man spricht in diesem Zusammenhang von **Link State Advertisements (LSA)**: Informationseinheiten, die den Status bestimmter Verbindungen eines Routers beschreiben. Diese LSA's besitzen auch eine Sequenznummer (in einem Modulo-Zahlenraum), die für die Anwendung und die Weitergabe des Updates gebraucht wird. Ist die Nummer des empfangenen LSA's nämlich größer als die des entsprechenden Eintrags in der Datenbank, wird der Record ersetzt; ist sie andererseits kleiner, wird der bestehende Eintrag, der aktueller ist, als LSA geflutet. Wenn die Sequenznummern gleich sind, bleibt der Router aktionslos; dies ist auch das Ende einer Update-Welle, und der Flooding-Algorithmus stoppt. Jedem empfangenen LSA muss ein Acknowledgment folgen, weil sonst der Absender Retransmits durchführt.

Diese zwischen den Routern versandten LSA's heißen in OSPF **Router-LSA's**. In Broadcast- und NBMA-Netzwerken versenden ja die Designated Router die Updates an die angeschlossenen Router; diese LSA's nennt OSPF **Network-LSA's**.

Betrachten wir nun Area 1 in Abbildung 116. Nach den obigen Schritten ist die gesamte Topologie der Area den Routern R1 bis R4 bekannt. Tabelle 24 zeigt die entsprechenden Einträge in der Topologiedatenbank.

An dieser Stelle sollte erwähnt werden, dass diese Topologiedatenbank natürlich noch nicht den Weg zum Ziel weist. Die tatsächliche „Routingtabelle" erstellt jeder Router mit Hilfe der Datenbank – bei OSPF einen Baum der kürzesten Wege, einen **Shortest-Path Tree**. Der dafür zu verwendende Algorithmus ist durch die OSPF-Spezifikation nicht festgelegt, doch meistens handelt es sich um den wohlbekannten Dijkstra-Algorithmus, der hier wohl nicht mehr weiter

VON NACH	R1	R2	R3	R4
R1				
R2				
R3				
R4				
N1	3			
N2		3		
N3	1	1	1	1
N4			2	

Tabelle 24: Link-State-Datenbank Area 1 (nur intern)

erläutert werden muss. Gemäß der RFC 1349 Spezifikation, die IP-TOS (Type of Service) Werte festlegt, kennt OSPF 5 verschiedene Codes für Metriken. Router, die *TOS Routing* unterstützen, erstellen einen Shortest Path Tree für jede Metrik; um die dazu benötigten Informationen zu erhalten, können die LSA's auch mehrere Routen für unterschiedliche TOS Werte beinhalten. Das Switching nimmt jeder Router dann entsprechend des TOS-Wertes im IP-Header vor, wobei der passende Baum zu Hilfe genommen wird.

Den Area Border Routern (R3 und R4) fällt die Aufgabe zu, die Entfernungen der Knoten in Area 1 zusammenzufassen (nicht die gesamte Topologie, sondern nur die summierten Kosten von ihnen aus). So berechnet z.B. R3 einen Abstand von 4 Einheiten zu N1 (R3 $\rightarrow$ N3 $\rightarrow$ R1 $\rightarrow$ N1), und R4 zählt 3 bis N4. Beide Router verpacken diese Informationen in **Summary-LSA's**. Als Mitglieder des Backbones (Area 0) haben sie bereits die Backbone-Router kennen gelernt. Neben den „normalen" LSA's fluten R3 und R4 nun auch ihre Summary-LSA's der Area 1 über den Backbone. Da dies aber auch die übrigen Area Border Router tun, kommen R3 und R4 auch in den Besitz der Summary-LSA's aller übrigen Areas und können sie in Area 1 bekannt machen (s. Tabelle 25 für die aktualisierte Datenbank). Die Entfernungen zu den anderen Areas (ermittelt durch einen Shortest Path Tree) werden nur für die Area Border Router eingetragen: So erhält beispielsweise R1 keinen neuen Eintrag zu N6.

VON NACH	R1	R2	R3	R4
R1				
R2				
R3				
R4				
N1	3			
N2		3		
N3	1	1	1	1
N4			2	
Ia, Ib			20	27
N6			16	15
N7			20	19
N8			18	18
N9-11,H			29	36

Tabelle 25: Link-State-Datenbank Area 1 (intern und über Backbone erhalten)

Wie aus Tabelle 25 ersichtlich ist, wurden die Netze N9 bis N11 und der Host H zusammengefasst und mit einheitlicher Entfernung (als ein Ziel) bekannt gemacht; die ist ebenfalls möglich.

Weiter oben wurde bereits erwähnt, dass die Propagierung der AS-externen Routen die Hierarchie im AS durchbricht – die Entfernungen zu den Router mit externen Verbindungen (im

Beispiel R5 und R7) werden direkt an alle Router weitergegeben. Auch die AS Boundary Router werden mit ihren Verbindungen in den Topologiedatenbanken eingetragen. Die erweiterte Datenbank für Area 1 ist in Tabelle 26 dargestellt.

VON NACH	R1	R2	R3	R4	R5	R7
R1						
R2						
R3						
R4						
R5			14	8		
R7			20	14		
N1	3					
N2		3				
N3	1	1	1	1		
N4			2			
Ia, Ib			20	27		
N6			16	15		
N7			20	19		
N8			18	18		
N9-11,H			29	36		
N12					8	2
N13					8	
N14					8	
N15						9

Tabelle 26: Link-State-Datenbank Area 1 (intern, Backbone und AS-extern)

Betrachtet man Tabelle 26, so ist ersichtlich, dass die Router in Area 1 nun die Topologie der Area und (über die Area Border Router) die Entfernungen zu allen Netzwerken innerhalb und außerhalb des AS kennen. Jeder Router in Area 1 kann also einen Shortest Path Tree zu allen Zielnetzwerken erstellen. Geroutet (switching) wird dann allerdings *hop by hop*, d.h. nur der jeweils nächste Knoten wird für die Weiterleitung benutzt. Dies erscheint auch klar, denn die Informationen über die Wegstrecke liegen immer nur innerhalb einer Area genau vor, außerhalb nur in summarischer Form.

Fehler und Konvergenz

Wie reagiert OSPF, wenn der klassische Fehler eintritt: der Ausfall eines Links, einer Teilstrecke? OSPF setzt hier ganz auf die rasche selbständige Erkennung des Fehlers durch die benachbarten Router und die Weiterverbreitung der Link-State Updates im ganzen AS. Diese Konvergenz muss sehr schnell ablaufen, denn zwischenzeitliche Routings laufen unweigerlich ins Leere. Anders als PNNI diese Situation zu meistern versucht (s. Kapitel 8.3.3), lässt also OSPF nicht jeden Sender in die Sackgasse laufen und eine Alternativroute berechnen, sondern setzt auf Prävention. OSPF erwähnt den Fehlerfall dann auch nicht explizit in der Spezifikation, sondern kennt nur die üblichen Flooding- und Exchange-Algorithmen, die auf Grund des Ereignisses eines ablaufenden Timers aktiviert werden.

Im Hello-Protokoll wird für jedes Netzwerk ein *RouterDeadInterval* festgelegt, das für einen Router angibt, wie lange er „stumm“ bleiben darf, bevor der Nachbar die Verbindung für unterbrochen erklärt (nach Ablauf eines entsprechenden *Inactivity Timers* und mit Auslösung eines entsprechenden Events). Um ihren aktiven Zustand zu bestätigen, versenden die Router ihre LSA's periodisch. Im Fehlerfall kommt nun also ein erwartetes LSA nicht mehr beim Nachbarn an, was dort ein Update der Routing-Informationen bewirkt, eine Neuberechnung des Shortest Path Tree zur Folge hat und das augenblickliche Flooding der LSA's mit den aktualisierten Link States einleitet.

Nehmen wir an, im obigen Beispiel-AS sei die Verbindung zwischen R4 und R5 ausgefallen. Dies

ist ein besonders kritischer Ausfall, da er den Backbone betrifft. Das RouterDeadInterval für die LSA's von R4 ist bei R5 verstrichen, und so ändert R5 den Zustand des Links auf DOWN. R5 trägt für die Route zu R4 eine unendliche Metrik ein und für seine summarischen Streckenangaben zu den Netzen in Area 1 über R4 ebenfalls. R5 besitzt aber zwei Einträge für den Weg zu Area 1; da der Shortest Path Tree nach jeder Änderung der Link States neu berechnet wird, kann R5 seine Routing-Tabelle einfach anpassen. LSA's mit den neuen Informationen werden verschickt (mit dem Flooding-Protokoll), und die übrigen Router passen ihre Link States an, wie anfangs mit dem Exchange-Protokoll. R4 hat den Fehler ebenfalls bemerkt und meldet innerhalb von Area 1 die Unerreichbarkeit der Netzwerke der anderen Areas. Weil die einzelnen Routing-Einträge auch hier jeweils mittels des nächsten Routers identifiziert werden, fallen „rückwärts wirkend" schließlich die Wege über R4 aus, und die Router in Area 1 wissen, dass sie für Area-externes Routing über R3 gehen müssen, und passen ihren Shortest Path Tree an.

Haben redundante Wege und deren Unterstützung durch OSPF in diesem Fall einen Zusammenbruch des AS vermieden, kann es bei Stichverbindungen natürlich auch zu irreparablen Schäden kommen. Wichtig ist aber, dass durch die kleinen LSA's, die mit höchster Priorität schnell durch das Netz laufen, eine rasche Konvergenz erreicht wird, wozu auch die Hierarchiebildung mit der abgestuften Bekanntmachung der Veränderungen im AS beiträgt.

8.3 PNNI – Private Network to Network/Node Interface

PNNI ist sozusagen eine Verfeinerung von OSPF und ähnlichen Link-State Routing-Protokollen. Die Abkürzung steht für **P**rivate **N**etwork to **N**etwork (oder **N**ode) **I**nterface: eine Technologie für das Routing zwischen ATM Switches in privaten ATM Netzwerke (→ „Node") und für das Routing zwischen privaten ATM Netzwerken (→ „Network"). Die PNNI-Spezifikation wurde vom ATM-Forum herausgegeben, aktuell in der Version PNNI-1 vom März 1996, und zum Standard-Routingverfahren für ATM-Netze erklärt. PNNI ist ein Link-State Protokoll, das dynamisch und automatisch Routing-Informationen verteilt, und dabei Switches verschiedenster Hersteller bedienen kann. Obwohl man es als eine Evolution gegenüber OSPF bezeichnen könnte, bietet es viele neue Elemente. Die Daten und Beispiele der folgenden Kapitel gehen vor allem auf die PNNI-Spezifikation ([108]) und [1] zurück; daneben wurden noch [99] und [130] herangezogen.

8.3.1 Ziele und Einsatz von PNNI

PNNI wurde für das ATM-Modell konzipiert und lässt sich daher nicht in einen Layer wie im ISO/OSI Schichtenmodell einordnen. Da ATM verbindungsorientiert arbeitet und Datenpakete auf logischen Pfaden (VC's) weiterleitet, ist auch das Routing verbindungsorientiert, mit allen Vor- und Nachteilen (s. Kapitel 8.1.1). Routen müssen mit PNNI also nur einmal, vor dem Verbindungsaufbau, erstellt werden; fällt diese Route aus, wird der Routing-Prozess erneut initiiert und ein neuer Weg ermittelt. In jedem Fall beschränkt sich das Routing in den Zwischenknoten eines Pfades nach dem Verbindungsaufbau auf das Switching, weshalb man auch den Begriff Router vermeidet.

Das Routing selbst geschieht quellenbasiert (Source Routing), d.h. der erste Switch, der den Setup-Request für den Aufbau einer Verbindung erhält, berechnet den Pfad zum Zielknoten. Das würde aber auf den ersten Blick bedeuten, dass dieser Ausgangs-Switch die gesamte (globale) Topologie des ATM-Netzwerks kennen müsste, um aus diesem Pool an Pfaden einen möglichst optimalen auszuwählen, der auch noch den differenzierten QoS-Anforderungen von ATM genüge tut oder eine Ressourcen schonende und intelligente Lastverteilung ermöglicht. In den großen

Netzen, die ATM erlaubt, würde der Umfang der benötigten Topologiedatenbanken schnell zu erheblichen Zeit- und Speicherplatz-Problemen führen. PNNI erweitert deshalb das Source Routing zu einer hierarchischen Wegewahl und erlaubt dabei eine große Anzahl frei konfigurierbarer Hierarchieebenen. So wird eine enorme Skalierbarkeit erreicht.

Die PNNI Routingtechnologie sieht zwei prinzipielle Protokolle vor:

- Routing-Protokoll. Das Routing-Protokoll verteilt die Topologie-Informationen und hilft so, die Topologiedatenbanken zu erstellen. Außerdem werden somit die Hierarchieebenen definiert. Die Bestimmung eines genauen Pfades wird allerdings noch nicht durch das Routing-Protokoll eingeleitet; vielmehr zielt es darauf ab, die komplexe Topologie, zugeschnitten auf den jeweiligen Switch, bekannt zu machen. Der Switch kann mittels dieser Informationen freilich sofort „seinen“ Teil des Pfades zum Zielknoten berechnen (s. Kapitel 8.3.2 und 8.3.3).
- Signalling-Protokoll. Dieses zweite Protokoll dient dazu, Punkt-zu-Punkt- oder Punkt-zu-Multipunkt-Verbindungen im ATM-Netzwerk aufzubauen. Die tatsächliche Pfadbestimmung geschieht also erst hier. Das Protokoll basiert auf dem UNI Signalling des ATM-Forums und ermöglicht das eigentliche Source Routing, Crankback und alternative Wegewahl im Fehlerfall beim Setup. S. Kapitel 8.3.4.

PNNI ist darauf ausgerichtet, große Netze bedienen und flexibel auf die Netztopologie eingehen zu können. Dabei kann es fehlerhafte Links beim Verbindungsaufbau automatisch umgehen und die Wegewahl auf komplexe QoS-Anforderungen ausrichten.

8.3.2 Das PNNI-Topologiemodell und seine Elemente

PNNI routet zwischen Knoten der untersten Schicht in einem Netzwerk. Im ATM-Modell sind dies die Vermittlungseinheiten: Switches. Auch Endgeräte kommen im Topologiemodell von PNNI vor, werden aber i.A. nicht in entsprechende Diagramme eingetragen (s. unten). Endsysteme werden durch die ersten 19 Bytes der 20-Byte-ATM-Adresse identifiziert; das letzte Byte der Adresse wird für PNNI-Routing nicht berücksichtigt. Die Verbindungen zwischen den Switches sind entweder physikalische Links oder ATM *Virtual Path Connections (VPC)*.

PNNI muss in weitaus größeren Netzwerken als OSPF einsetzbar sein. Ein Netz-weites Fluten der LSA's oder sonstiger Routing-Informationen wäre unökonomisch, und die Topologiedatenbanken würden stark anwachsen, müsste der Quellknoten beim Routing alle Zwischenknoten bis zum weit entfernten Endsystem kennen. Dazu kommt, dass PNNI jeden physikalischen Link mit einem Set aus zwei Parametern kennzeichnen muss, einen pro Richtung, bestehend aus Port-ID und Knoten-ID; daneben müssen auch die geforderten QoS-Parameter gespeichert werden. Aus diesen Gründen setzt PNNI auf ein noch ausgeprägteres logisches Hierarchiesystem als OSPF.

Es sind folgende hierarchische Einheiten vorgesehen:

- Switches
- Peer Groups
- Peer Group Leaders (PGL's)
- Logical Group Nodes (LGN's)

Peer Group
Mehrere (durch Links physikalisch miteinander verbundene und somit „benachbarte“) Switches können durch entsprechende Konfiguration zu Peer Groups zusammengefasst werden. Analog zu den Areas in OSPF sind Peer Groups logische Einheiten, innerhalb derer alle Topologie-Informationen untereinander ausgetauscht werden und somit allen Knoten in gleicher Weise vorliegen. Die Switches werden dabei durch *Logical Node ID's* unterschieden und adressiert.

Im Beispiel-ATM-Netzwerk in Abbildung 118 gibt es sieben Peer Groups, die mit PG(A.1) bis PG(A.4), PG(B.1), PG(B.2) und PG(C) markiert sind. Diese abstrakten Bezeichner dienen der Anschaulichkeit, korrelieren aber mit der hierarchischen Adressstruktur, die PNNI verwendet. So ist auch zu interpretieren, dass ein Knoten mit Namen A.4.6 in Peer Group A.4 (PG(A.4)) ist und zu einer größeren Einheit von Knoten der Gruppe „A“ gehört. Die tatsächlichen *Peer Group Identifiers* können konfiguriert werden, und stimmen dann mit den 13 höherwertigen Bytes der ATM-Adresse der zugehörigen Endsysteme überein (aber nicht notwendigerweise).

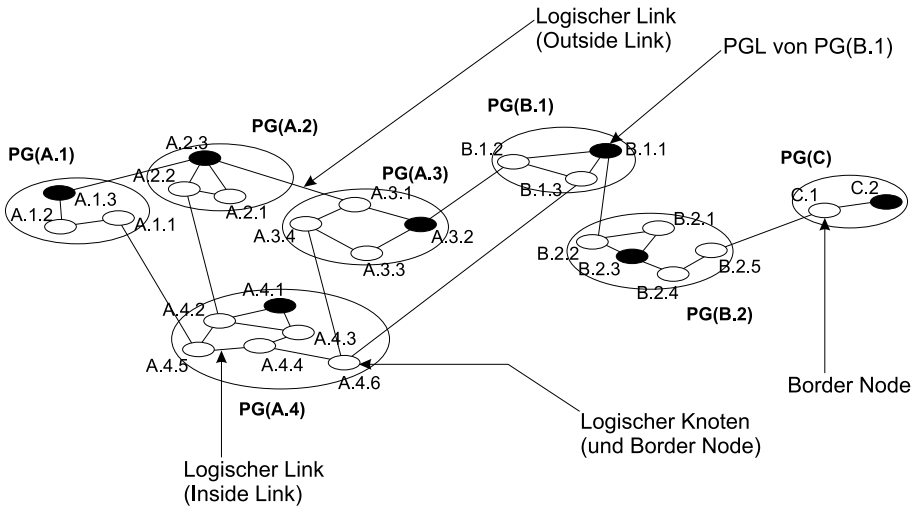


Abbildung 118: Ausschnitt aus der PNNI-Hierarchie (unterste Ebene)

Gab es bei OSPF die Klasse der Area Border Router, so findet sich bei PNNI wieder ein (zumindest auf den ersten Blick) ähnliches Element: die **Border Nodes**. Ein Border Node liegt an der Grenze einer Peer Group, so dass mindestens einer seiner Links deren Grenze überschreitet. Weil es bei PNNI kein Konstrukt wie den OSPF-Backbone gibt (der auch Knoten außerhalb der Areas enthalten konnte), sondern eben nur Peer Groups, folgt, dass ein Border Node eine Verbindung zu einem Border Node einer anderen Peer Group besitzt. Ein solcher Link heißt dann **Outside Link**, im Gegensatz zu **Inside Links** innerhalb einer Peer Group.

Peer Group Leader
Die hierarchische Einheit der Peer Groups muss sich nach außen bzw. den anderen Hierarchieebenen gegenüber repräsentieren. Wie bei OSPF sollen auch die dichten Topologie-Informationen der Peer Groups zusammengefasst weitergegeben werden können; außerdem soll es, um es bildlich auszudrücken, auch in PNNI einen genau bestimmten „Ansprechpartner“ geben, der ankommende Nachrichten am Eingang der Peer Group entgegennimmt und entsprechend seines größeren Wissens über die interne Struktur der Peer Group verteilt. Diese Aufgaben kamen bei OSPF dem Designated Router und den Area Border Routers zu. PNNI hingegen zeichnet einen (beliebigen) Switch der Peer Group als Peer Group Leader aus, der die Gruppe nach außen vertritt. Der PGL ist in einem separaten Prozess (neben seinem Dasein als normales Peer Group Mit-

glied) dafür zuständig, Informationen zur Aufrechterhaltung der Hierarchie zu sammeln und zu verteilen. Für die Existenz einer Peer Group selbst ist er allerdings nicht ausschlaggebend.

Logical Group Node
Mit dem Konzept des Logical Group Nodes schließt sich der Kreis der Elemente der flexiblen PNNI-Hierarchie. Ein LGN ist nämlich nichts anderes als die Abstraktion einer Peer Group in der nächst höheren Routing-Hierarchieebene. Die Darstellung eines LGN ist wieder ein Knoten im Sinne von PNNI, in diesem Fall ein logischer Knoten. Der Unterschied zwischen LGN und PGL der zugehörigen Peer Group ist sehr klein; es gibt zwar ein Interface zwischen diesen beiden logischen Einheiten, aber die Spezifikation sieht vor, dass beide Aufgaben von einem physikalischen System ausgeführt werden. Das weitere Vorgehen ist sofort einleuchtend: die LGN's können ihrerseits wieder gruppiert werden und eine Peer Group bilden, auf einer höheren (logischen) Ebene. Diese Peer Group kann nun ebenfalls einen PGL bestimmen, der ihre Topologie zusammenfasst und nach oben weiterreicht, wo sie auch wieder einen LGN besitzt. Das einfache Prinzip der Peer Groups mit PGL und LGN wird also rekursiv bis zur Spitze der gewünschten oder vorhandenen Hierarchie angewandt.

Nun ist auch klar, dass man im Vergleich zur doch recht beschränkten Hierarchie von OSPF bei PNNI mit einem dreidimensionalen Modell aus Hierarchieebenen arbeitet. Abbildung 119 zeigt die untersten beiden Ebenen des Beispiel-ATM-Netzwerks. Die LGN's der Peer Groups A.x wurden zu einer PG(A) zusammengefasst (dies erklärt nun auch den Präfix „A"). Diese PG(A) wird als **Parent Peer Group** der PG(A.1) bis PG(A.4) bezeichnet; analog sind PG(B.1) und PG(B.2) **Child Peer Groups** von PG(B). PGL der PG(A) ist im Beispiel A.2, der LGN der PG(A.2). Die PGL-Funktionalität von A.2 wird tatsächlich vom Switch A.2.3 übernommen. Innerhalb eines Switches können sich so je nach Anzahl der Hierarchieebenen, in denen er noch eine Rolle spielt, mehrere logische Maschinen ergeben.

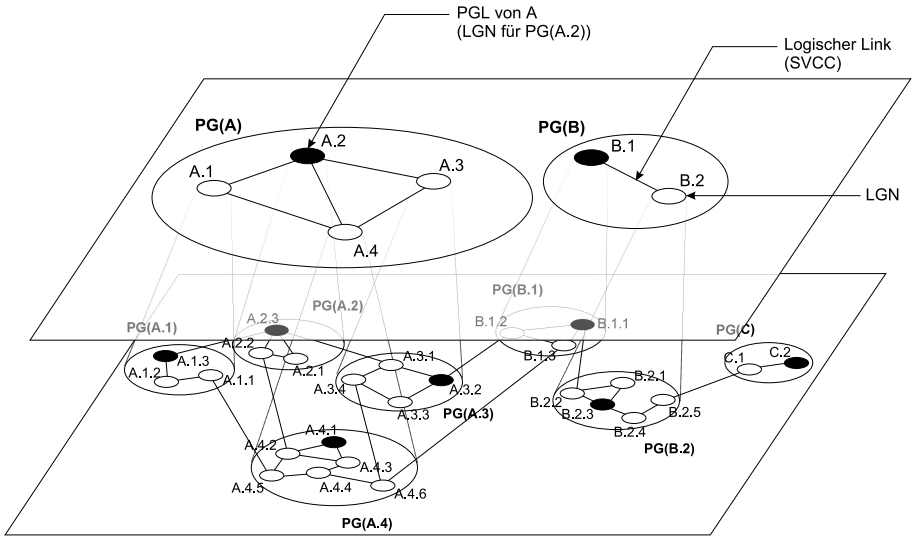


Abbildung 119: Ausschnitt aus der PNNI-Hierarchie (untere beiden Ebenen)

LGN's können über entsprechend konfigurierte ATM Endsystem-Adressen angesprochen werden. Daneben besitzt jede Peer Group ja noch eine ID. Die Länge dieser ID zeigt die Lage der Peer Group im Ebenen-„Stapel" an: je kürzer, desto höher (daher auch im Beispiel die Abstraktionen PG(A), PG(A.3)). Man spricht vom **Level Indicator**. Da PNNI 13 Bytes für diese unterschiedlichen Peer Group ID Längen vorgesehen hat, folgt, dass es maximal 104 ($= 8 \cdot 13$)

verschiedene Level Indicators, also ID's verschiedener Länge, und somit Ebenen geben kann.

Wenn man das rekursive Prinzip nun fortführt, gelangt man zu einer obersten Ebene aus LGN's. Die Peer Group aus diesen LGN's benötigt keinen PGL mehr, da ihre Topologie nicht verdichtet weitergegeben werden muss. Abbildung 120 zeigt das für das Beispiel vollständige Hierarchiemodell. Die Switches C.1 und C.2 bilden dabei eine Peer Group, die sofort in der höchsten Ebene vertreten ist; die zweite Ebene wird also übersprungen. Konsequenterweise kann die Peer Group der Switches dann auch PG(C) heißen, da keine Zwischengruppen identifiziert werden müssen. An diesem Beispiel wird klar, dass die Ebenen in PNNI nicht vollständig ausgefüllt sein müssen; das modulare Konzept erlaubt es, dass einzelne Stufen übergangen werden. Ein anderes Extrem ist ein Netzwerk mit nur einer Ebene, d.h. einer Peer Group, und dadurch flachem Adressraum.

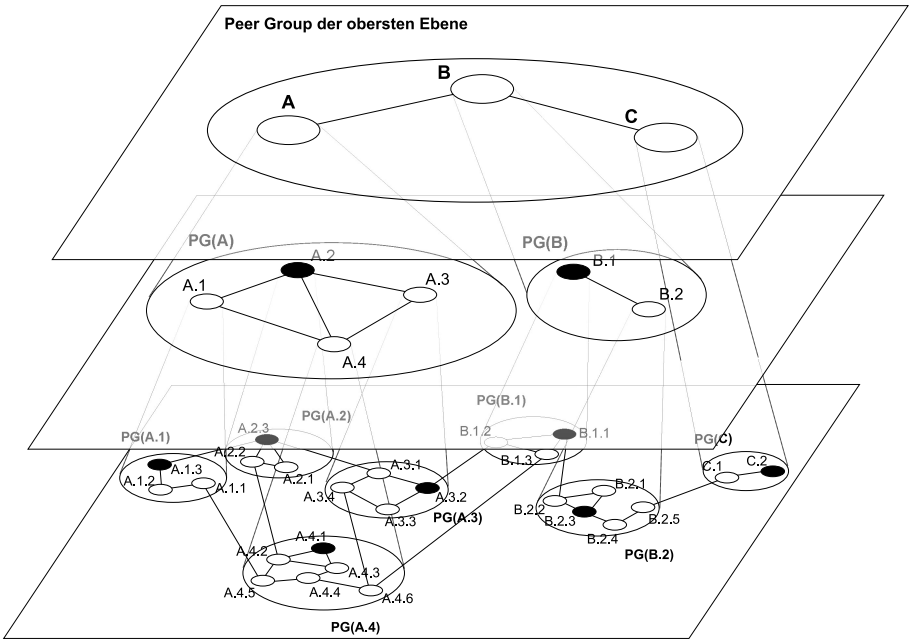


Abbildung 120: Vollständige PNNI-Hierarchie

8.3.3 PNNI-Routing

Nun geht es wieder darum, das Topologiemodell in geeigneter Weise den Switches bekannt zu machen, denn – wie schon gesagt – jedes Quellsystem soll eine Route zum Zielsystem erstellen können. Wie werden also die Informationen dem hierarchischen System entsprechend verteilt, so dass jeder Knoten die für ihn relevanten Routingdaten aufbauen kann?

Die Topologie einer Peer Group soll allen Mitgliedern in gleichem Maße bekannt sein (dies scheint vernünftig und (ökonomisch) vertretbar und entspricht so auch dem Modell der Area in OSPF). Dazu müssen sich die Switches (oder besser: Knoten, da Peer Groups ja auch auf höheren Ebenen vorkommen und sich dann LGN's verständigen müssen) gegenseitig kennen lernen. PNNI bietet für dieses Prozess eine festgelegte VCC (Virtual Channel Connection) an, die als **RCC** (PNNI Routing Control Channel) benutzt wird. Über den RCC läuft periodisch das PNNI **Hello-Protokoll**.

Die Hello-Pakete geben die ATM Endsystem-Adresse, die Knoten- und Port-ID des Senders an. Außerdem wird die Peer Group ID über das Hello-Protokoll ausgetauscht, so dass miteinander

verbundenen Knoten sofort erkennen können, ob sie sich in derselben Peer Group befinden und deshalb genaue Topologie-Informationen austauschen sollen, oder ob sie zwei verschiedenen Peer Groups angehören. Wir betrachten nun zuerst Knoten einer einzelnen Peer Group. Diese Knoten verbreiten in einem zweiten Schritt nach dem Kennenlernen der Nachbarn ihre lokalen Zustandsinformationen mittels Flooding in der Peer Group.

PTSE
Die Statusangaben eines Knoten werden in **PTSE's** (PNNI Topology State Elements) verpackt und weitergegeben. Die Topologiedatenbank der Peer Group besteht dann aus allen aktuellen PTSE's der Mitgliedsknoten. Die Synchronisation der einzelnen Datenbanken der Knoten funktioniert nach einem Prinzip, das dem in OSPF sehr ähnlich ist. Die Nachbarn senden sich Database Summary Pakete (in PNNI „PTSE Header Information") mit Informationen, die die PTSE's beschreiben. Schon vorhandenen PTSE's werden auf ihre Aktualität überprüft und ggf. für eine Ersetzung markiert; nicht vorhandene PTSE's werden sofort angefordert. Maximal ein PTSE darf bei der Synchronisation wechselseitig ausstehen. Das gegenseitige Update wird fortgeführt, bis keine Aktualisierungen oder Neueinträge mehr notwendig sind.

PTSE's enthalten neben Angaben über Switch-ID und -Spezifika, PGL und Position in der Hierarchie **Topology State Parameters**, die die angeschlossenen Links und Knoten beschreiben. Mittels der Topology State Parameters können Attribute oder Metriken an den jeweiligen nächsten Hop vergeben werden. Metriken sind im Gegensatz zu Attributen kumulativ. PNNI unterscheidet zwischen statischen (z.B. Bandbreite) und dynamischen (z.B. Administrationsaufwand) Topology State Parameters.

Sobald die Synchronisation der Datenbanken abgeschlossen ist, werden die PTSE's durch die Domäne (die Peer Group) geflutet, verpackt in **PTSP's** (PNNI Topology State Packets). PTSP's werden sowohl periodisch als auch Ereignis-gesteuert verschickt und müssen immer bestätigt werden.

PGL
Die **PGLE** (Peer Group Leader Election) in PNNI ist der Bestimmung des Designated Routers in OSPF sehr ähnlich. Ausschlaggebend für die Rolle des PGL ist die „Leadership Priority", bzw. bei zwei Switches mit derselben Priorität die Knoten-ID. Die Wahl des PGL ist ein kontinuierlicher Prozess, und ein neuer Switch mit höchster Priorität verdrängt (anders als in OSPF) den bisherigen PGL. Der PGL sammelt die Topologie-Informationen seiner Gruppe und fasst sie zusammen, um sie außerhalb der Peer Group weitergeben zu können. Wie schon angedeutet, geht die PNNI-Spezifikation davon aus, dass PGL und LGN vom selben System realisiert werden, so dass durch die Wahl des PGL auch der LGN der Peer Group feststeht.

LGN
Der LGN arbeitet auf einer logisch höheren Ebene als die Mitglieder seiner Peer Group einschließlich des PGL. Daher kann man sagen, dass der PGL eine Summierung der unter ihm erreichbaren Zieladressen und die zusammengefassten Topologie-Informationen zum LGN „hinaufspielt". Andererseits gibt jeder LGN alle PTSE's seiner Peer Group unverkürzt und unkomprimiert an den PGL seiner Child Peer Group hinunter, der sie dann durch Flooding in der gesamten Peer Group verteilt. Alle Mitglieder aller Child Peer Groups (rekursiv!) unter einem LGN erhalten so detaillierte Informationen über die LGN's und Peer Groups oberhalb von ihm.

In unserem Beispiel kennt nun Knoten A.4.5 durch das Hello-Protokoll alle Mitglieder seiner Peer Group PG(A.4) einschließlich deren Outlinks, z.B. auch zu A.3.4. Knoten A.4.1 ist PGL der PG(A.4) und repräsentiert die Peer Group auch auf der nächsten Ebene, als LGN A.4. Die Topologie-Informationen über seine PG(A) – LGN A.1 bis A.4 samt ihrer Verbindungen – gibt A.4 an den PGL von PG(A.4) hinab, der sie durch PG(A.4) flutet. Folglich kennt A.4.5 auch

den Aufbau der PG(A).

Die LGN's der höheren Ebenen bilden nun, ihrem Adressprefix entsprechend, wiederum Peer Groups auf ihrem hierarchischen Level. Existierten mehrere Verbindungen zwischen zwei Peer Groups in der direkt darunter liegenden Ebene, werden diese Links auf der höheren Ebene zu *einer* Verbindung zusammengefasst. Diese Verbindungen zwischen LGN's sind **SVCC** (Switched Virtual Channel Connections). Allgemein nennt PNNI Verbindungen innerhalb einer Hierarchieebene (auch auf der untersten) **Horizontal Links**. LGN's können Horizontal Links etablieren, wenn sie den Weg zum Knoten kennen, der den Nachbars-LGN darstellt. Es ist klar, dass dazu auf der unteren Ebene eine oder mehrere Grenzen zwischen Peer Groups übersprungen werden müssen.

Uplinks
Diese grenzüberschreitenden Verbindungen (Outside Links, s. Kapitel 8.3.2 (Peer Group)), die notwendig sind, um einen physikalischen Pfad von LGN zu LGN zu schalten, öffnen nun sozusagen das Tor zu einer Peer Group, die nur als LGN auf einer höheren Ebene bekannt ist. Die Border Nodes tauschen nämlich im Hello-Protokoll zwar keine Topologie-Informationen aus, erweitern aber die Hierarchieangaben in den Topology State Parameters um eine Liste von Parent Peer Groups und deren LGN's. So können die Border Nodes die unterste Ebene mit gemeinsamer Peer Group feststellen und den LGN der jeweils anderen Peer Group bestimmen. Im Beispielnetz (s. Abbildung 120) erkennen etwa A.1.3 und A.2.3, dass sie PG(A) gemeinsam haben, und dass A.2 PG(A.2) repräsentiert und A.1 PG(A.1).

Letztendlich entsteht pro Verbindung zu einer Nachbars-Peer Group praktisch ein Link vom Grenz-Knoten zum bekannten LGN der ersten gemeinsamen Peer Group einer höheren Ebene. Wie in Abbildung 121 (einem Ausschnitt der Abbildung 119) zu sehen ist, ergibt sich dadurch ein so genannter **Uplink**, der *zwischen* Ebenen verläuft. Da die Verbindung zwischen den Peer Groups i.A. auch in die andere Richtung gegeben ist, entsteht noch ein zweiter Uplink von der Nachbars-Peer Group zum LGN der anderen Peer Group. Im Beispiel ergeben sich die Uplinks (A.1.3–A.2) und (A.2.3–A.1). Die Uplinks werden in den jeweiligen Peer Groups allen Knoten bekannt gemacht.

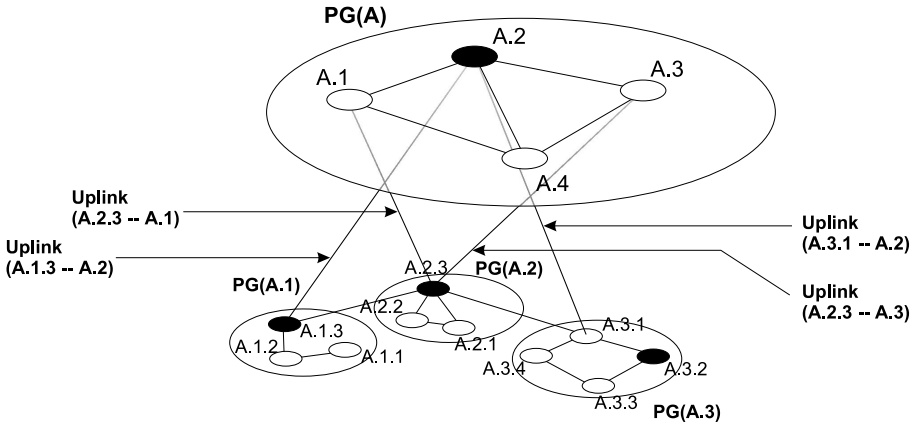


Abbildung 121: Uplinks Ebene 1 – Ebene 2

Neben den direkt ersichtlichen Uplinks kennt PNNI noch **induzierte Uplinks**. Diese entstehen, wenn der Knoten mit dem Outside Link den LGN seiner Nachbars-Peer Group erst mehr als eine Ebene höher in einer gemeinsamen Peer Group wiederfindet – dann haben auch Knoten der Zwischenebenen Uplinks zu diesem LGN. Beispielsweise existiert in Abbildung 122 (Ausschnitt

aus 120) ein Uplink (B.2.5–C). Der passende LGN C befindet sich aber erst zwei Stufen höher. Deshalb entsteht auch für den LGN B.2, der über B.2.5 vom Uplink erfährt, ein Uplink, nämlich (B.2–C).

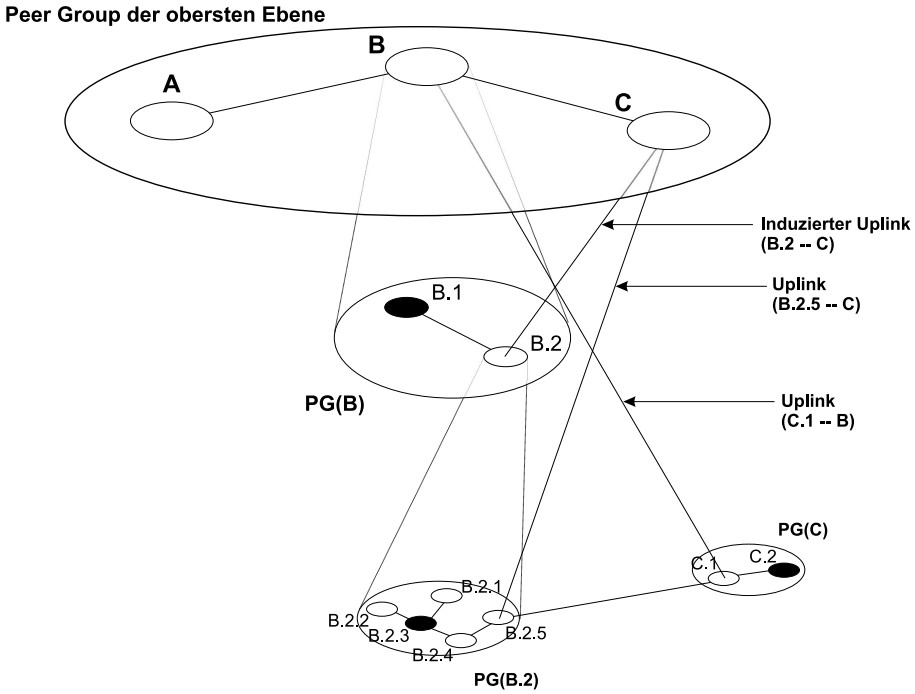


Abbildung 122: Uplinks Ebene 1 – Ebene 3

Zurück zum rekursiven Aufbau der Topologie und zur Verteilung der entsprechenden Informationen. Die SVCC's zwischen LGN's höherer Ebenen können also mit Hilfe der Uplinks realisiert werden. Somit kann auch ein logischer Pfad bzw. ein Horizontal Link sowie ein RCC zwischen den LGN's eingerichtet werden. Letztendlich ist also wieder eine Peer Group mit Knoten (LGN's) und Verbindungen (SVCC's) zwischen ihnen entstanden. In dieser Peer Group kann nun ein **LGN Hello-Protokoll** laufen, das aus einem **SVCC-basierten RCC Hello-Protokoll** und einem **LGN Horizontal Link Hello-Protokoll** besteht. Auf die Details soll hier nicht näher eingegangen werden; das LGN Hello-Protokoll erweitert das einfache Hello-Protokoll unter anderem um Mechanismen wie beispielsweise zur Kontrolle des Zustands der virtuellen Verbindungen oder um zusätzliche Attribute der Links (wie etwa die summierte Bandbreite).

Auf die oben beschriebene Weise können nun rekursiv immer höhere Ebenen von Peer Groups aus LGN's erstellt werden. Sobald PTSE's aus diesen Gruppen auf höheren Ebenen vorhanden sind, werden sie durch die LGN's bzw. PGL's in den Child Peer Groups verteilt. Im Beispiel von Abbildung 120 bilden neben PG(A) auch die „B"-Knoten eine Peer Group auf der nächsthöheren Ebene. PG(A) und PG(B) sowie PG(C) bestimmen ihrerseits PGL's und somit LGN's auf einer nochmals höheren Ebene. Die Peer Group an der Spitze der Hierachie bestimmt keinen PGL, sondern sammelt nur ihre PTSE's, die die LGN's nach unten weitergeben. Der anfänglich betrachtete Knoten A.4.5 kennt nun neben der Topologie seiner Peer Group und den Mitgliedern der PG(A) auch die Knoten der obersten logischen Ebene. Wegen der hierarchischen Adressbildung (s. auch unten) weiß er nun ebenfalls, dass z.B. C.2 über PG(A.4), PG(A) und C in der obersten Ebene erreicht werden kann (s. Abbildungen 120 bzw. 124). Die Information über Pfade zu Zielknoten wird zwar mit zunehmender Entfernung unschärfer, ein Repräsentant der

Zielgegend ist aber immer erreichbar; die Menge der bekannten Daten spitzt sich sozusagen mit zunehmender Entfernung zum Ziel und Höhe in der Hierarchie zu (s. Abbildung 123).

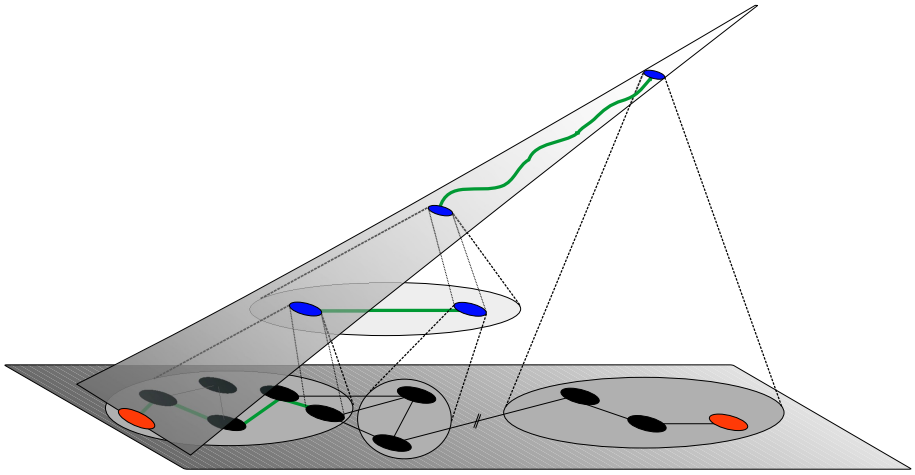


Abbildung 123: Bild eines Knotens vom Aufbau des Netzes

Wie schon angedeutet, erlauben die 13 Bytes Präfix des ATM-Adress-Schemas bis zu 104 Hierarchieebenen.Ähnlich einer Telefonvorwahl haben im Allgemeinen die Mitglieder einer Peer Group denselben Adress-Präfix, durch den eben ihre Peer Group eine oder mehrere Ebenen höher bestimmt ist. Ein Knoten erhält eine voreingestellte oder explizit vergebene **Summary Address**, die die durch ihn erreichbaren Unterknoten (mit **Native Addresses**) angibt. Summary Addresses sind die kürzesten Präfixe, die die Knoten noch unterscheidbar machen. Jeder LGN versucht, die Adress-Präfixe, die in seiner Child Peer Group durch das Hello-Protokoll und PTSE-Austausch ermittelt wurden, zu filtern, indem er sie durch das kleinstmögliche Präfix zusammenfasst (z.B. Präfixe $\langle A.2.1\rangle, \langle A.2.2\rangle$ und $\langle A.2.3\rangle$ durch $\langle A.2\rangle$) und in seiner Peer Group bekannt macht.

Neben den Summary Addresses kennt PNNI auch Knoten mit **Foreign Addresses**, die nicht durch die Präfix-Maske fallen. Diese Adressen müssen immer einzeln und explizit nach oben weitergegeben werden, bis sie auf einem Level mit allgemeinerem Präfix von einer Summary Address überdeckt werden. Hier zeigt sich ein Nachteil dieses Adressierungsprinzips: Da Foreign Addresses ja ungefiltert nach oben weitergereicht werden und andererseits Informationen aus höheren Peer Groups unverändert nach unten gelangen, wissen schließlich alle Switches von diesen Foreign Addresses. Dieser Effekt ist umso ausgeprägter, je weiter entfernt der Knoten mit der Foreign Address ist. Das Mittel, mit dem ATM und PNNI große Netze und Adressbereiche in den Griff zu bekommen versuchen, liegt eben in der hierarchischen Adressstruktur, die mit der Routing-Hierarchie übereinstimmt und so implizit Topologie-Informationen angibt; und eben dieses Prinzip wird durch Foreign Addresses umgangen.

8.3.4 PNNI-Signalling

Wie schon gesagt, ist ATM ein verbindungsorientierter Dienst. PNNI etabliert eine virtuelle Verbindung oder einen virtuellen Pfad für den gesamten Zeitraum der Kommunikation der betroffenen Endgeräte. Aus diesem Grund muss die Wegewahl „vorausschauend“ arbeiten, denn eine schlechte Route, die vielleicht zu Überlastungen im Netz führt oder den QoS-Anforderungen nicht ausreichend nachkommen kann, bleibt für die gesamte Verbindungszeit bestehen, und ein

eventuelles „Rerouting“ benötigt eine komplette Neuberechnung des Pfades. Der gesamte Verbindungsaufbau (*Call Establishment*) in PNNI wird durch das Signalling-Protokoll durchgeführt und besteht aus

- Pfadselektion und
- Verbindungsaufbau in den einzelnen Knoten entlang des Pfades.

Man entschied sich für ein quellenbasiertes Routing, da die Alternative – *Hop-by-Hop-Routing* – mehrere Nachteile mitbringen würde: Zum einen Routing-Schleifen z.B. wegen unterschiedlich schneller Verbreitung von Topologie-Updates (wie bereits in Kapitel 8.1.2 angedeutet), zum anderen die Gefahr suboptimaler Pfade wegen inkonsistenter Topologiedatenbanken. Beide Probleme werden durch quellenbasiertes Routing vermieden, weil nur eine Datenbank (die des Ausgangsknotens) in die Routenberechnung involviert ist.

Das PNNI Signalling basiert im Grunde auf UNI 4.0 (*User Network Interface*); es unterstützt zwar einige dessen Funktionen nicht, erweitert es aber (u.a.) um folgende Eigenschaften:

- DTL (Designated Transit List)
- Crankback

DTL
Am Anfang eines Verbindungsaufbaus steht ein Setup-Request eines Endsystems an einen Switch (über ein UNI). Angegeben sind darin Zieladresse und QoS-Anforderungen für die Verbindung. Anhand seiner Topologie-Informationen und seiner Sicht vom Netz (vgl. Abbildung 124 für A.1.2's Sicht vom Beispielnetz, wie in Kapitel 8.3.2 hergeleitet) berechnet der Switch einen Pfad zum Zielknoten bzw. desses Vertreter auf höherer Ebene.

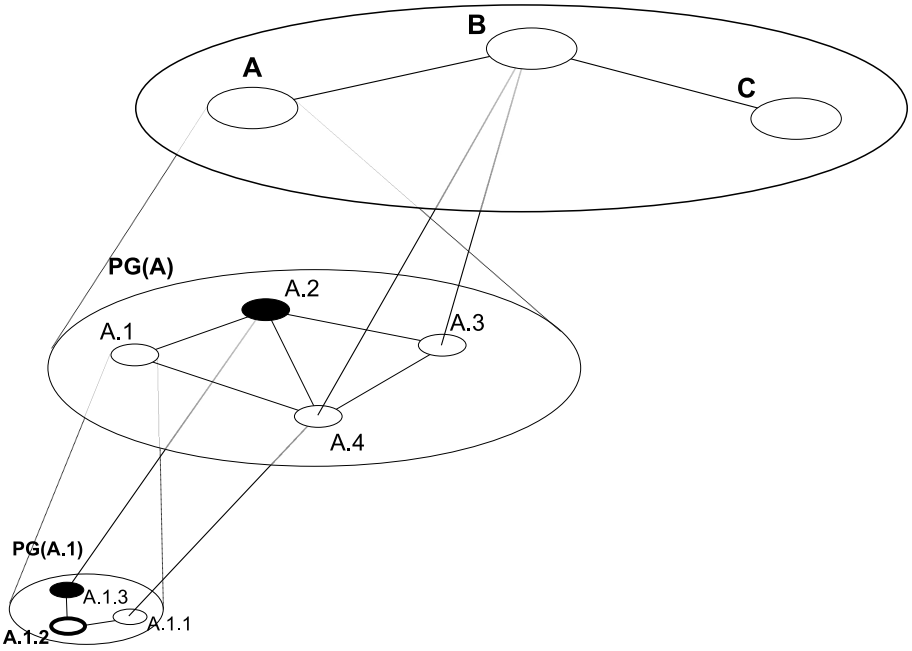


Abbildung 124: Sicht des Netzes von A.1.2 aus

Auch die PNNI-Spezifikation schreibt nicht vor, welcher Algorithmus zur Bestimmung des optimalen Pfades angewandt werden sollte. Vielmehr erlaubt das hierarchische Routingmodell, dass verschiedenen Hierachieebenen oder Peer Groups unterschiedliche Algorithmen verwenden; PNNI gibt nur das Rahmenwerk vor. Allerdings ist ein Routing, das komplexen QoS-Forderungen gerecht wird, immer noch Gegenstand der Forschung. PNNI schlägt als einfachste Lösung nur den Dijkstra-Algorithmus für minimale Wege vor, der ja nur Gewichtsparameter von Teilpfaden berücksichtigt.

Wie auch immer der Pfad nun in einer spezifischen Implementierung von PNNI berechnet wird, er wird durch **DTL's** beschrieben: Entsprechend der PNNI-Hierarchie werden übereinander, in umgekehrter Reihenfolge der Abarbeitung (also als Stack, gemäß dem LIFO-Prinzip), die Teilstrecken der Route mit der Angabe aller beteiligten Knoten sequentiell aufgelistet. D.h. für jede Hierarchiestufe, von der Peer Group des ausgehenden Switch's mit genauen Wegbeschreibungen, bis zur untersten Peer Group, die der Quell- und der Zielknoten gemeinsam haben, existiert eine DTL mit den Knoten und LGN's des Pfades. Nacheinander werden nun die DTL's bearbeitet und, sobald erledigt, vom Stack genommen; ist keine DTL mehr vorhanden, wurde das Ziel erreicht.

Ein Beispiel
Nehmen wir nun an, A.1.2 habe von einem seiner Endgeräte eine Setup-Request erhalten, um eine Verbindung zu C.2 aufzubauen (vgl. Abbildung 120). A.1.2 besitzt das in der Abbildung 124 dargestellte Bild vom Aufbau des ATM-Netzes.

Um der Service-Kategorie der zu errichtenen Verbindung und den QoS-Parametern genüge zu tun und das Netzwerk effizient nutzen zu können, entscheidet sich A.1.2 – entsprechend vorkonfigurierter Parameter und seiner aktuellen Topologiedatenbank – für den Weg
A.1.2 $\rightarrow$ A.1.3 $\nearrow$ A.2 $\rightarrow$ A.3 $\nearrow$ B $\rightarrow$ C.
C ist für A.1.2 der Endpunkt der Route, da er der auf der niedrigsten Ebene erreichbare Vertreter von C.2 ist, der Knoten mit dem längsten noch passenden Präfix. A.1.2 generiert den zu diesem Pfad gehörigen DTL-Stack:

DTL	[A.1.2, A.1.3]	pointer-2
DTL	[A.1, A.2, A.3]	pointer-1
DTL	[A, B, C]	pointer-1

Jede DTL beschreibt also den Weg durch ein hierarchisches Level. Pointer zeigen je DTL auf den Knoten, der auf der jeweiligen Ebene gegenwärtig besucht wird; Ausnahme ist die oberste DTL (die aktuell bearbeitete DTL), deren Pointer auf den nächsten Knoten zeigt. Für den Fall, dass der Verbindungsaufbau scheitern sollte (s. unten), speichert A.1.2 den Inhalt seiner Setup-Nachricht und den DTL-Stack. Dann wird der Request um Verbindungsaufbau an A.1.3 weitergeleitet.

CAC
Jeder Switch prüft unmittelbar vor der Weiterleitung eines Setup-Requests, ob die neue Verbindung (bzgl. Verkehrsaufkommen, QoS-Anforderungen usw.) akzeptiert werden kann, ohne dass bestehende Verbindungen mit ihren QoS-Parametern benachteiligt werden. Dies ist die **CAC** (Connection Admission Control). Das genaue Vorgehen bei der Prüfung eines Links auf Akzeptanz der Verbindung wird durch die PNNI-Spezifikation nicht festgelegt. Falls also, aufgrund welcher Indikatoren auch immer, die neue Verbindung angenommen wird, läuft der Setup-Request weiter. Eine akzeptierte Verbindung kann freilich zur Versendung neuer PTSE's führen, wenn sich die Parameter des Knotens signifikant verändert haben. Allgemein werden über die PTSE's

GCAC's (Generic CAC's) verschickt, die den Switches für die Routenplanung typischerweise zu erwartende CAC's vorgeben sollen.

Wir nehmen an, der Request sei erfolgreich an A.1.3 weitergeleitet worden. A.1.3 sieht den Pointer des obersten Stack-Elements auf seine eigene ID zeigen; somit erkennt er sich für den nächsten Streckenabschnitt zuständig. Die oberste DTL ist nun allerdings abgearbeitet, und so wird sie vom Stack genommen. Die DTL [A.1, A.2, A.3] liegt nun oben auf dem Stack, weshalb ihr Pointer auf A.2 gesetzt wird:

DTL [A.1, A.2, A.3] pointer-2
DTL [A, B, C] pointer-1

A.1.3 muss nun also A.2 erreichen, erkennt aber, dass er nicht zur Peer Group gehört, die durch A.2 vertreten wird. A.1.3 weiß allerdings, dass er einen unmittelbaren Nachbarn in A.2 durch einen Outside Link bzw. Uplink erreichen kann. Der Nachbar ist A.2.3, und an ihn schickt A.1.3 den Setup-Request mit den DTL's weiter.

A.1.3 hat – im Gegensatz zu A.1.2 – dem DTL-Stack keinen neuen Eintrag hinzugefügt und auch keine neuen Routing-Entscheidungen getroffen. In diesem Fall muss der Knoten *kein* Backup der Setup-Nachricht anlegen.

Im nächsten Schritt erkennt nun A.2.3, dass der Request an A.3 (den nächsten Eintrag in der aktuellen DTL) weitergereicht werden muss, zu dessen Peer Group er nicht gehört. Mit Hilfe seiner Topologiedatenbank findet A.2.3 heraus, dass der Uplink zu A.3 über A.3.1 weiterführt. Da keine neue DTL auf den Stack gelegt wurde, und A.2 verlassen wird, inkrementiert A.2.3 den Pointer und gibt den Setup ohne Sicherungskopie an A.3.1 weiter:

DTL [A.1, A.2, A.3] pointer-3
DTL [A, B, C] pointer-1

A.3.1 sieht die oberste DTL abgearbeitet und erkennt in der darunterliegenden, dass er B erreichen muss. Das ist wegen der Berechnungen von A.1.2 auch tatsächlich möglich: A.3.1 muss zu A.3.2 routen, der einen Uplink zu B besitzt; daher legt er eine neue DTL auf den Stack:

DTL [A.3.1, A.3.2] pointer-2
DTL [A.1, A.2, A.3] pointer-3
DTL [A, B, C] pointer-1

Da er den Stack um einen neuen Eintrag erweitert hat, speichert A.3.1 den Inhalt der Setup-Nachricht, bevor er den Aufruf an A.3.2 weitergibt. Dieser sieht zuerst die oberste DTL vollendet, dann die zweite, und nimmt beide vom Stapel. Durch seinen Uplink zu B bzw. B.1.2 wird A verlassen, so dass der weitergegebene Stack folgendermaßen aussieht:

DTL [A, B, C] pointer-2

Die Verbindung wurde in allen bisherigen Knoten durch CAC's akzeptiert. Nehmen wir nun an, der Link A.3.2 – B.1.2 kann den QoS-Anforderungen nicht genüge tun.

Crankback
Ist eine GCAC, die ja bei der Routenplanung herangezogen wurde, nicht mehr aktuell, weil sich

zwischen Routenplanung und Setup-Request Topologieänderungen ergeben haben oder Dienstparameter variieren, weil sich Aktualisierungen der Topologie-Informationen verzögern, schlägt die betreffende CAC fehl. Ein anderer Fehler beim Verbindungsaufbau ist, dass der gewählte Link unterbrochen ist oder auch sonst kein Kontakt zum Zielknoten hergestellt werden kann, was eine RELEASE-Nachricht zurück zum aufrufenden Knoten zur Folge hat.

In beiden Fällen ergibt sich ein **Crankback**. Eine RELEASE-Nachricht mit einem Crankback-IE (Information Element) läuft den bisher aufgebauten Weg der Verbindung (mit Hilfe der VCI, s. Kapitel ATM) zurück bis zur letzten Routing-Instanz, die eine Veränderung der DTL's bezüglich des unbrauchbaren Links vorgenommen hat; diese Knoten mussten ja ihren DTL-Stack speichern – nun kann von ihrem Punkt aus eine Alternativroute berechnet werden. Der Crankback geht stufenweise über die „entscheidenden" Switches zurück, notfalls bis zum ersten Knoten.

Fahren wir im Beispiel fort: Die CAC auf den Link A.3.2 – B.1.2 liefere ungenügende QoS-Leistung. A.3.2 hat keinen zweiten Uplink zu B, daher wird ein Crankback generiert, der zurück zu dem Knoten läuft, der die letzte relevante Instanz mit gespeichertem DTL-Stack darstellt. In unserem Fall ist das A.1.2, der Ausgangsknoten. Es bestünde zwar die Möglichkeit, aus PG(A.3) oder PG(A.2) auf A.4 zu kommen, doch diese Alternativen wurden anfnags von A.1.2 (durch die unteren DTL's) nicht vorgegeben.

Der Crankback stoppt nicht bereits bei A.3.1, der der letzte Knoten mit gespeichertem Stack war, weil die DTL, die er auf den Stack gelegt hatte, völlig irrelevant für den defekten Link A.3.2 – B.1.2 ist. Die Entscheidung für diesen Weg wurde von A.1.2 getroffen.[37]

A.1.2 muss nun also eine Route zu C.2 finden, die den Uplink A.3 $\nearrow$ B nicht verwendet. A.1.2 wählt den Pfad A.1.2 $\rightarrow$ A.1.1 $\nearrow$ A.4 $\nearrow$ B $\rightarrow$ C. Er hätte freilich auch über PG(A.2) und den Uplink A.2.2 $\nearrow$ A.4 oder über PG(A.3) und den Uplink A.3.4 $\nearrow$ A.4 routen können, aber durch GCAC's seien diese Pfade im Beispiel ausgeschlossen, weil sie eventuell die geforderte Peak Cell Rate nicht unterstützen.

Der neue DTL-Stack sieht nun folgendermaßen aus:

DTL	[A.1.2, A.1.1]	pointer-2
DTL	[A.1, A.4]	pointer-1
DTL	[A, B, C]	pointer-1

A.1.1 nimmt die oberste DTL vom Stack, setzt den Pointer der folgenden DTL neu und sendet den Request an A.4.5, seinen direkten Nachbarn in PG(A.4). Dieser erkennt, dass er zu B routen muss, wozu PG(A.4) durchquert werden muss. Er findet eine den QoS-Forderungen entprechende Route, legt deren DTL auf den Stack und speichert diesen:

DTL	[A.4.5, A.4.2, A.4.3, A.4.4, A.4.6]	pointer-2
DTL	[A.1, A.4]	pointer-2
DTL	[A, B, C]	pointer-1

Der Request wird an A.4.2 weitergeleitet, der lediglich den Pointer fortschaltet und den Aufruf weitergibt, so dass dieser über A.4.5 und A.4.4 an A.4.6 gelangt. A.4.6 erkennt die oberste DTL

[37] Der interessierte Leser sei hier an die PNNI-Spezifikation verwiesen. PNNI unterscheidet die Endpunkte eines Crankbacks nämlich anhand des Scoping Levels des Knotens, der eine neue DTL erzeugt hat. Auf das Prinzip des Soping soll hier aber nicht weiter eingegangen werden.

als abgearbeitet, ebenso die zweite. Durch die dritte sieht er, dass er zu B routen muss, wozu er den Uplink zu B.1.3 benutzen kann. Also nimmt er die beiden oberen DTL's vom Stack und setzt den Pointer auf B:

DTL [A, B, C] pointer-2

Dieser Uplink zu B sei nun brauchbar. Logisch ist der Setup-Request nun also bereits in der höchsten Hierarchieebene angelangt, physikalisch zwei Schichten tiefer in PG(B.1) bei B.1.3. Der ursprüngliche Switch hatte keine einzige Information über Switches und Links unterhalb von B; das hierachische Fortschalten und die stufenweise Detaillierung der Pfadbestimmung blendet aber immer wieder von höheren Stufen bis auf die physikalischen Elemente hinab. Die für den gewünschten Pfad benötigten Peer Groups werden also nach und nach sichtbar, rekursiv fällt Licht von oben herab auf die tieferen Stufen. Abbildung 125 mag dies verdeutlichen (abgebildet ist der Stand des bis jetzt besprochenen Verbindungsaufbaus).

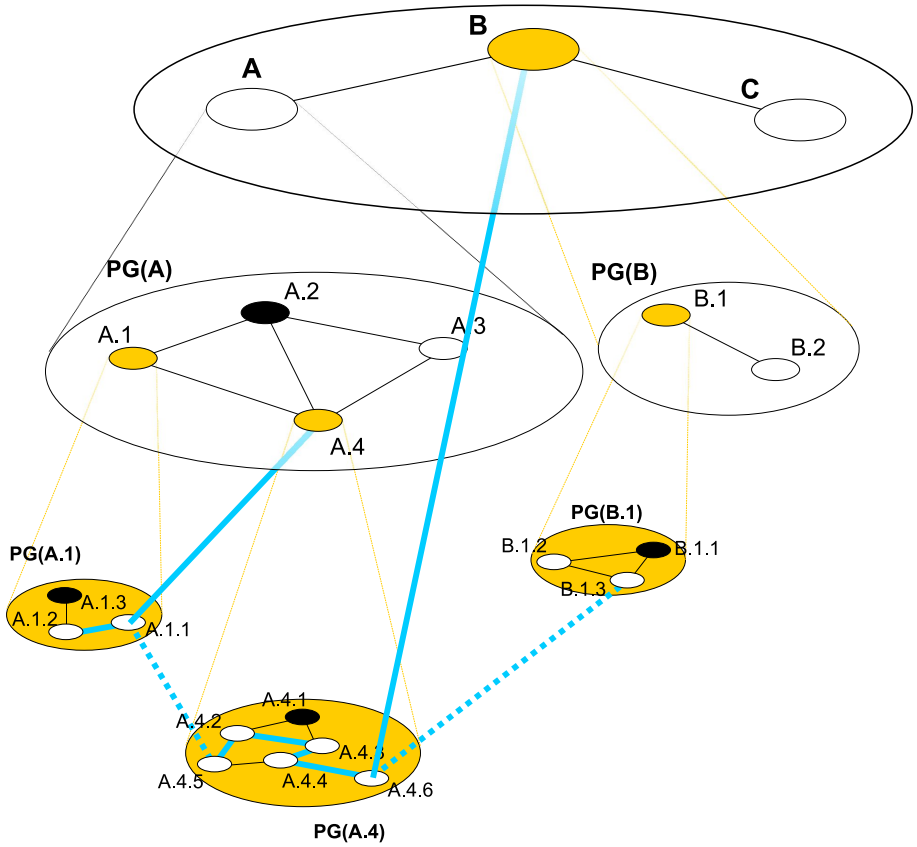


Abbildung 125: Einblendung tieferer PNNI-Hierachieebenen beim Verbindungsaufbau

B.1.3 erkennt, dass irgendwie zu C geroutet werden muss. Aus seiner Topologiedatenbank ist ersichtlich, dass es einen Uplink B.2 ↗ C gibt. Folglich muss PG(B.2) erreicht und durchquert werden (s. Abbildung 120). B.1.3 kreiert zwei neue DTL's auf dem Stack, speichert diesen, und gibt den Request an B.1.1 weiter, da dieser einen Uplink zu B.2 hat:

DTL [B.1.3, B.1.1] pointer-2
DTL [B.1, B.2] pointer-1
DTL [A, B, C] pointer-2

B.1.1 nimmt die oberste DTL vom Stack, setzt den Pointer auf B.2 und übergibt an B.2.2. Dieser muss durch PG(B.2) routen, um (wie er aus der untersten DTL sieht) an C zu kommen. Der bei ihm neu gespeicherte Stack ist der folgende:

DTL	[B.2.2, B.2.3, B.2.4, B.2.5]	pointer-2
DTL	[B.1, B.2]	pointer-2
DTL	[A, B, C]	pointer-2

Schließlich kommt der Request bei B.2.5 an. Dieser erkennt, dass die obersten beiden DTL's abegarbeitet sind und nimmt sie vom Stack. Außerdem existiert ein Uplink zu C bzw. C.1, also setzt B.2.5 den letzten Pointer auf C. PG(C) wird endlich eingeblendet. C.1 liest aus dem Setup-Request, dass C.2 der Switch des Zielsystems ist, und so generiert er eine letzte neue DTL:

DTL	[C.1, C.2]	pointer-2
DTL	[A, B, C]	pointer-3

C.2 schließlich erkennt, dass ein an ihn angeschlossener Host das Endsystem der gewünschten Verbindung ist, denn alle DTL's sind durchlaufen, C.2 ist auf der untersten Ebene und das Endsystem ist physikalisch erreichbar. Der Stack wird geleert, die Verbindung ist etabliert.

9 GSM, DECT, UMTS & IMT-2000 - Mobilkommunikation

9.1 Einführung

Durch die rasanten Fortschritte in den Bereichen der Telekommunikation, Mikroelektronik, Computer- und Softwaretechnik, um nur einige zu nennen, ist man dem Ziel überall, mit jedem, zu jeder Zeit und zu einem erschwinglichen Preis zu kommunizieren einen großen Schritt näher gekommen. Die größten Schwierigkeiten bei der Realisierung dieses Ziels liegen dabei in der Mobilität der Teilnehmer. Vorweg lassen sich hierbei zwei Arten der Mobilität unterscheiden, die Terminalmobilität und die persönliche Mobilität. Beide Arten lassen sich dabei nicht exakt voneinander trennen, sondern gehen nahtlos ineinander über. Bei der Terminalmobilität ist der Teilnehmer drahtlos über Funk oder Licht im näheren Umkreis am Netz angeschlossen, wie zum Beispiel bei einem schnurlosen Telefon. Durch Erweiterungen vermittlungstechnischer und administrativer Funktionen kann diese Mobilität über Netzgrenzen oder sogar Landesgrenzen hinweg ausgedehnt werden. Diese Erweiterungen können zu einer universellen Erreichbarkeit und somit zur Realisierung der persönlichen Mobilität führen. In diesem Seminar sollen nun Mobilkommunikationssysteme aus beiden Bereichen angesprochen werden. Zum einen im Bereich der Terminalmobilität GSM (Global System for Mobile Communication) und DECT (Digital Enhanced Cordless Telecommunication) und im Bereich der persönlichen Mobilität, in einem Ausblick auf künftige Entwicklungen, UMTS (Universal Mobile Telecommunications System) bzw. IMT-2000 (Integrated Mobile Telecommunications at 2000 MHz). Dabei wird das Hauptaugenmerk auf dem GSM-System liegen, da dieses sozusagen die Grundlagen und Hauptideen für die beiden anderen Systeme zur Verfügung stellt. Von diesen wird aus Komplexitätsgründen lediglich ein kurzer Abriß mit eingebracht.

9.2 GSM - Global System for Mobile Communication

In den folgenden Kapiteln wird ein kurzer Überblick über die Entstehung, die Architektur, die Funkschnittstelle, die Dienste und das Feature des Handovers innerhalb des GSM-Netzes gegeben. Es soll ein Einblick in den Aufbau und die Funktionsweise des Mobilfunksystems gewährt und dies zum Abschluß an Hand der aufgeführten Beispiele des Rufaufbaus noch einmal veranschaulicht werden. Die Grundlage hierfür bildeten [51], [91], [141].

9.2.1 Entstehung

Die Arbeit an der Entwicklung eines paneuropäischen, zellularen Mobilfunknetzes begann bereits 1982 durch eine Arbeitsgruppe Groupe Speciale Mobile (GSM), die von der CEPT (Conference of European Posts and Telegraphs) ins Leben gerufen wurde. Von dieser stammt auch der eigentliche Name des Mobilfunknetzes. Dieser wurde dann im Jahre 1991, als die Arbeitsgruppe von dem ETSI (European Telecommunications Standardisation Institute) übernommen wurde, in Global System of Mobile Communication umbenannt. Nachdem im Februar 1987 die Angebotsanforderungen festgelegt wurden, konnten die ersten Basisstationen Mitte 1991 in Betrieb genommen werden. Der endgültige flächendeckende Betrieb ist seit 1995 erreicht. Das GSM-Netz stellt das bisher einzige von Europäern entwickelte Mobilfunksystem dar.

9.2.2 Architektur

Das GSM-System spaltet sich in folgende Teilsysteme auf (Abbildung 1):

- Funkteilsystem (Radio Subsystem (RSS))
- Vermittlungsteilsystem (Network and Switching Subsystem (NSS))
- Betreiberteilsystem (Operation Subsystem (OSS))

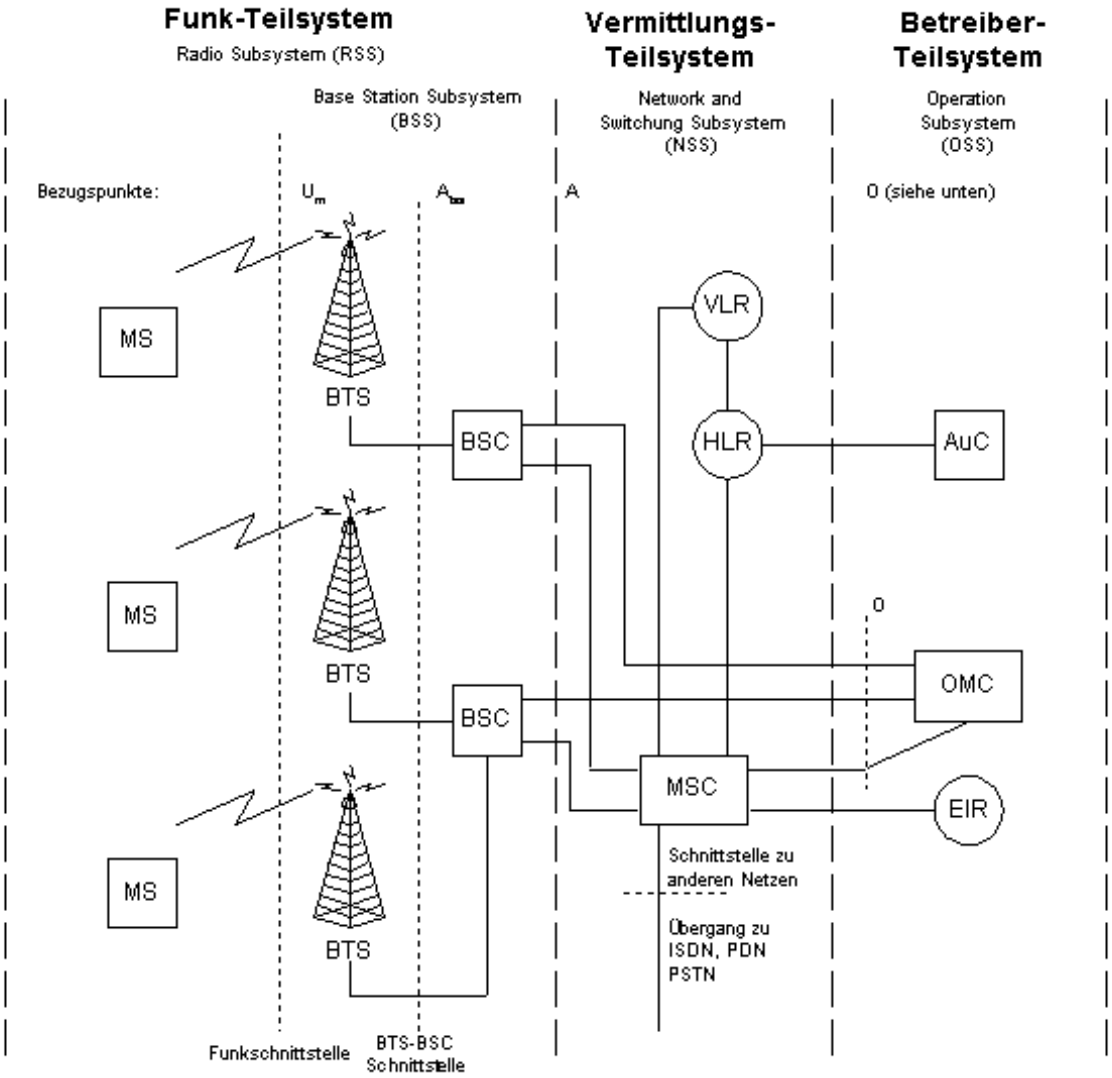


Abbildung 126: Architektur des GSM-Mobilfunknetzes

Funkteilsystem (Radio Subsystem):

Das Funkteilsystem setzt sich aus zwei Komponeneten, der mobilen Station (Mobile Station, MS) und dem Feststationsteilsystem (Base Station Subsystem, BSS) zusammen.

Mobile Station (Mobile Station, MS): Die MS besteht aus dem Funkgerät und der Benutzerschnittstelle. Die Benutzerschnittstelle besteht meist aus folgenden Komponenten:

- Mikrophon
- Lautsprecher

- LCD-Anzeige
- Alphanumerisches Tastenfeld
- Softkeys: Tasten mit keiner festen Funktionszuordnung

Dabei spaltet sich die MS in zwei Teile auf. Der Erste enthält die für die Funkschnittstelle spezifischen Hard- und Softwarekomponenten. Der zweite Teil ist das Subscriber Identity Module (SIM), auf dem alle teilnehmerspezifischen Informationen enthalten sind. Das SIM ist, heutzutage fast nur noch als kleines Plug-in-Modul realisiert, in die MS einsetzbar. Dabei ist diese ohne das SIM, je nach Mobilfunknetz, nur noch zu Notrufen in der Lage. Die MS wird durch das SIM personalisiert. Dadurch ist es einem Teilnehmer möglich sich durch sein SIM über jede beliebige Mobilstation im Netz zu identifizieren. Im SIM sind sowohl unveränderliche als auch temporär veränderliche Daten im Speicher abgelegt. Unveränderliche, teilnehmerbezogene Elemente des Speichers sind:

- SIM-Kartentyp
- IC-Kartenidentifikator: Seriennummer des SIM
- SIM Service Table: Liste der zusätzlich abonnierten Dienste
- IMSI, International Mobile Subscriber Identity
- PIN, Personal Identity Number
- PUK, PIN Unblocking key
- Authentifikationsschlüssel K(i)

Hierbei sind zuerst vor allem die PIN und die PUK hervorzuheben. Beide Nummern werden dem Benutzer mit der SIM-Karte übergeben. Dabei dient die 4- bis 8-stellige PIN-Nummer als Paßwort, um die eingelegte SIM-Karte zu aktivieren und somit in das Netz zu gelangen. Diese Nummer kann vom eingeloggten Benutzer beliebig oft verändert werden. Wird die PIN jedoch dreimal beim Einloggvorgang falsch angegeben, dann wird die SIM- Karte gesperrt. In diesem Fall muß der Benutzer den 8-stelligen Entsperrschlüssel PUK eingeben, um die Karte zu reaktivieren. Hierfür bleiben ihm 10 Versuche. Sollten diese auch fehlschlagen, muß die Karte vom Dienstanbieter entsperrt werden. Im Gegensatz dazu stehen die folgenden, permanent aktualisierten Daten. Diese dienen zur Beschleunigung des Einbuchungsvorganges. Sie beinhalten:

- Aufenthaltsinformationen: bestehend aus TMSI, LAI ein periodisch veränderlicher Location Updating-Zeitgeber und Aktualisierungsstatus
- Übertragungsschlüssel K(c) zur Chiffrierung und seine Sequenznummer
- BCCH-Informationen: Liste der Trägerfrequenzen für Zellenwahl bei Handovern und Verbindungseinrichtungen
- Liste gesperrter PLMNs
- HPLMN-Suchphase: Zeitdauer, die die MS bei der Gesprächssuche (Roaming) im Heimatnetz abwartet, bevor sie sich in ein anderes Netz einzubuchen versucht.

Sowohl die permanent aktualsierten, als auch die unveränderlichen Daten des SIM werden nur für den Zeitraum des aktiven Betriebszustandes in den Speicher der mobilen Station übernommen und danach wieder entfernt. Ausnahmen können für den Betrieb irrelevante Daten, wie zum Beispiel Kurzmitteilungen, sein. Diese können zwischengespeichert werden. Sie können jedoch nur vom Benutzer mit der gleichen SIM-Karte wieder aufgerufen werden.

Feststationsteilsystem (Base Station Subsystem, BSS): Das BSS enthält den gesamten funkbezogenen Teil des GSM-Netzes. Dabei besteht es aus der Funkfeststation (Base Transceiver Station, BTS) und der Feststationssteuerung (Base Station Controller, BSC)

- Funkfeststation (Base Transceiver Station, BTS): Die BTS beinhaltet die Sende- und Empfangsanlagen einschließlich der Antennen und der gesamten für die Funkschnittstelle spezifischen Signalverarbeitung. Eine Antenne kann hierbei je nach Positionierung eine oder mehrere Zellen versorgen (z.B. sektorisierte Antennen können drei in 120 Grad zueinander angeordnete Zellen bedienen). Im GSM Netz versorgt eine Antenne jeweils eine hexagonale Zelle. Die Größe der einzelnen Zellen und somit die Anzahl der Antennen zur flächendeckenden Kommunikation hängt dabei von einer Reihe von Faktoren wie Sendeleistung, charakteristische Wellenausbreitung, örtliche Morphologie und Teilnehmerdichte ab.

- Feststationssteuerung (Base Station Controller, BSC): Der BSC verwaltet die Funkschnittstelle mit Hilfe der BTS. Dabei übernimmt er die Reservierung und Freigabe von Funkkanälen, das Handover Management, die Steuerung von Funkrufen (Paging) und die Übetragung von verbindungsbezogenen Daten über eine Mobilvermittlungsstelle (Mobile Service Switching Center, MSC) zum Vermittlungsteilsystem (Network & Switching Subsystem, NSS). Ein BSC verwaltet meist mehrere BTS.

Um einen Teilnehmer des Mobilfunknetzes mit einem Gesprächspartner z.B. im Festnetz verbinden zu können, verfügt das BSS über zusätzliche Hard- und Softwareeinrichtungen:

- Signalisierungsprotokolle für die Verbindungssteuerung
- Sprachcodecs (Codierer/Dekodierer)
- Datenratenadaption für den Übergang zum Festnetz (Transcoder/Rate Adaptor Unit, TRAU)
- Digitale Signalverarbeitung zur Codierung von Daten etc.

Mit Hilfe dieser Funktionen wird ein Informationsaustausch zwischen dem Benutzer und dem GSM-Netz oder anderen Netzen und zwischen dem BSS und dem NSS über verschiedene Schnittstellen ermöglicht:

- U(m)-Schnittstelle: Funkschnittstelle zum mobilen Teilnehmer
- A-Schnittstelle: Schnittstelle zum Festnetz des GSM-Netzes zur Kommunikation mit externen Netzen
- O-Schnittstelle: Schnittstelle zum Betriebs- und Wartungszentrum (OMC) zur Ermittlung der Netzverfügbarkeit und -qualität

Vermittlungsteilsystem (Network & Switching Subsystem, NSS):

Das NSS verbindet das Funknetz mit den öffentlichen Partnernetzen (z.B. Telefonnetz, ISDN, Datennetz). Es besteht aus der Mobilvermittlungsstelle (Mobile Service Switching Center, MSC), der Heimatdatei (Home Location Register, HLR) und der Besucherdatei (Visitor Location Register, VLR). Darüber hinaus stellt es eine Reihe von Funktionen für den Hersteller und Netzbetreiber zur Verfügung, deren Aufgabe es ist, diese geeignet zu realisieren und implementieren.

- Mobilvermittlungsstelle (Mobile Service Switching Center, MSC): Das MSC ist eine digitale ISDN-Vermittlungsstelle, die um die notwendigen Mobilvermittlungsfunktionen erweitert ist. Jedem MSC sind meist mehrere BSC's zugeordnet. Es verbindet die mobilen Teilnehmer in dem ihm zugeordneten Bereich untereinander oder stellt eine geforderte Verbindung zum Festnetz her. Hierbei erledigt es sämtliche Signalisierungsvorgänge, die zum Aufbau, Abbau und zum Verwalten dieser Verbindungen benötigt werden. Zusätzlich erfüllt es einerseits noch mobilfunkspezifische Funktionen wie z.B. einen Zellwechsel (Handover), Zuteilung und Aufhebung von Funkkanälen oder die Verbindungsumschaltung bei zu starken Störungen, und andererseits die vom ISDN bekannten Zusatzdienste wie z.B. Konferenzschaltung oder Rufumleitung. Die zur Übertragung von Datendiensten notwendigen Funktionen werden durch spezifische Funktionseinheiten, den Interworking Functions, zur Verfügung gestellt.

- Heimatdatei (Home Location Register, HLR): Das HLR ist eine Datenbank, in der jeder Teilnehmer mit seinen Daten gespeichert ist. Jeder Teilnehmer ist in genau einem HLR registriert. Es enthält sowohl die unveränderlichen Daten wie z.B. Rufnummer, Zusatzdienste, Authentifikationsschlüssel, als auch die temporär veränderlichen Daten wie den momentanen Aufenthaltsort (Location Area, LA) oder die Mobile Station Roaming Number (MSRN), die für einen Verbindungsaufbau notwendig sind. Diese werden bei einem etwaigem Ortswechsel des Teilnehmers sofort aktualisiert. Das HLR ist meist einer MSC zugeordnet.

- Besucherdatei (Visitor Location Register, VLR): Das VLR ist wiederum eine Datenbank, die vom zuständigen HLR übertragene Informationen über jeden Teilnehmer in ihrem Zuständigkeitsbereich enthält. Der Zuständigkeitsbereich wird durch das ihr zugeordnete MSC bestimmt. Das VLR stellt somit dem MSC die für den Verbindungsaufbau notwendigen Daten zur Verfügung. Es wird ebenfalls bei einem Aufenthaltswechsel des Teilnehmers innerhalb eines MSC aktualisiert. Das VLR dient im allgemeinen dazu ein häufiges Abfragen des HLR zu vermeiden.

Der exakte Ablauf des Verbindungsaufbaus wird in Kapitel 1.2.6 beschrieben.

Betreiberteilsystem (Operation Subsystem OSS):

Das OSS beinhaltet alle für den Betrieb und die Wartung wichtigen Funktionen. Es besteht aus dem Betriebs- und Wartungszentrum (Operation & Maintenance Centre, OMC), dem Authentisierungszentrum (Authentication Centre, AuC) und dem Geräteidentifikationsregister (Equipment Identity Register, EIR).

- Betriebs- und Wartungszentrum (Operation & Maintenance Centre, OMC): Das OMC ist über die standardisierte O-Schnittstelle mit allen Netzelementen verbunden und überwacht diese zentral. Es bedient sich dabei der Dienste der den einzelnen Netzelementen zugewiesenen Netzverwaltungs- und Steuerfunktionen. Diese werden vom hierarchischen

Netzverwaltungssytem (TMN) zur Verfügung gestellt. Dadurch besteht für das OMC die Möglichkeit, durch Operatorkommandos Eingriffe in Netzelementen vorzunehmen, und durch einen Alarm über unvorhergesehene Aktionen benachrichtigt zu werden. Konkrete Aufgaben für das OMC sind die Verwaltung von Teilnehmern und Endgeräten, die Gebührenberechnung und die Statistik über Zustand und Auslastung der einzelnen Netzelemente.

- Authentisierungszentrum (Authentication Centre, AuC): Das AuC umfaßt alle für den Schutz der Identität des Teilnehmers, den Schutz gegen Abhören dessen Gespräche und dessen Nutzung seiner Berechtigung über die Funkschnittstelle erforderlichen Funktionen. So werden z.B. der Authentifikationsalgorithmus und der Verschlüsselungscode im AuC gespeichert und nur nach festen Regeln zugänglich gemacht.
- Geräteidentifikationsregister (Equipment Identity Register, EIR): Beim EIR handelt es sich um eine zentrale Datenbank, in der alle Teilnehmer- und Gerätekennungsnummern (International Mobile Equipment Identity, IMEI) gespeichert sind. Die Datenbank setzt sich aus einer weißen, schwarzen und grauen Liste zusammen. Die weiße Liste besteht aus den IMEI aller gültigen Mobilfunkgeräte, die schwarze Liste aus der aller gestohlenen oder gesperrten Geräte. Die graue Liste enthält die IMEI aller Geräte mit Funktionsstörungen, die daher keine Dienste bereitgestellt bekommen.

Die Funktionen des OSS, die mit Hilfe dieser Komponenten realisiert werden sind:

- Teilnehmerverwaltung: Innerhalb der Teilnehmerverwaltung wird der Benutzer mit Hilfe der im HLR gespeicherten persönlichen Daten und der im AuC gespeicherten datensicherheitsspezifischen Informationen authentifiziert und ihm die vereinbarten Dienste zur Verfügung gestellt (Subscriber Data Management). Dadurch wird es den Netzanbietern und Dienstanbietern ermöglicht, über sogenannte Verbindungstelegramme genommene Dienste in Rechnung zu stellen (Call Charging). Dabei können die Telegramme ortsunabhängig von den zuständigen MSC's ausgestellt werden.
- Netzbetrieb und Wartung: Wie bereits beim OMC angesprochen, wird bei der Steuerung des Netzbetriebes und von Wartungsaufgaben ein getrenntes Vermittlungsnetz zwischen OMC und den Netzelementen benutzt. Dieses integrierte, auf dem TMN (Telecommunication Management Network) basierende, Netzwerk enthält eigene Datenbanken und stellt dem Betreiber Überwachungs- und Eingriffsmöglichkeiten zur Verfügung. Die Funktionen des TMN-Netzes sind ähnlich derer des OSI-Referenzmodells in Schichten unterteilt:
  - Business Management: kontrolliert die Interaktionen zwischen dem Netz und den Diensten und stellt darüber hinaus Informationen zur weiteren Dienst- und Netzentwicklung zur Verfügung;
  - Service Management: dient zur Abwicklung sämtlicher vertraglicher Aspekte eines Dienstes zwischen Anbieter und Kunde;
  - Network Management: unterstützt sämtliche Netzelemente und ermöglicht das Aktivieren von Funktionen gleichartiger Elemente;
  - Network Element Management: ermöglicht den Zugriff auf einzelne Elemente im Netz
- Mobil-Endgeräteverwaltung: Im Gegensatz zum NSS betrifft die Verwaltung der Endgeräte im OSS nur die Benutzer- und Endgeräteidentität. Diese sind in der eigenen Datenbank, dem vorher beschriebenen EIR, gespeichert. Damit können zum Beispiel gestohlene oder fehlerhafte Geräte ausfindig gemacht werden.

9.2.3 Funkschnittstelle

Die Funkschnittstelle befindet sich, wie bereits erwähnt, zwischen MS und BTS. Die Übertragungsrate beträgt 270,833 kbit/s. Hierbei wird eine Kombination des FDMA- (Frequency Division Multiple Access) und des TDMA-Verfahrens (Time Division Multiple Access) angewandt. Sowohl diese Verfahren, als auch die dadurch mögliche Rahmenstruktur des Übertragungsmediums und die darin einfließenden logischen Kanäle werden in diesem Kapitel betrachtet.

Frequenzmultiplex-Struktur:

Zur Funkverbindung der MS mit der BTS wird im GSM-Netz ein Frequenzbereich von 890 bis 915 MHz in Richtung Basisstation (Uplink) und 935 bis 960 MHz in Richtung Mobilstation (Downlink) verwendet. Dabei haben die Up- und Downlinkfrequenz stets einen Abstand von 45 MHz, den man als Duplexabstand bezeichnet. Beide Frequenzbereiche mit der Bandbreite 25 MHz spalten sich wiederum in Trägerfrequenzen mit einem Kanalabstand von 200 kHz auf. Dies bedeutet, man erhält 124 Trägerfrequenzen pro Frequenzbereich (siehe Abbildung 2), wobei die Kanäle 1 und 124 als Schutzbänder zu benachbarten Frequenzbändern freigehalten werden sollten. Innerhalb des GSM-Netzes werden die zur Verfügung stehenden Frequenzen mehrfach benutzt. Dies ist durch die bereits angesprochene Struktur des GSM-Netzes möglich. Mehrere der hexagonalen Zellen werden zu einer Gruppe (Cluster) zusammengefasst, welche bestimmte FDM-Kanäle exklusiv benutzt. Gleiche Frequenzen können nun in weiter voneinander entfernten Gruppen parallel benutzt werden.

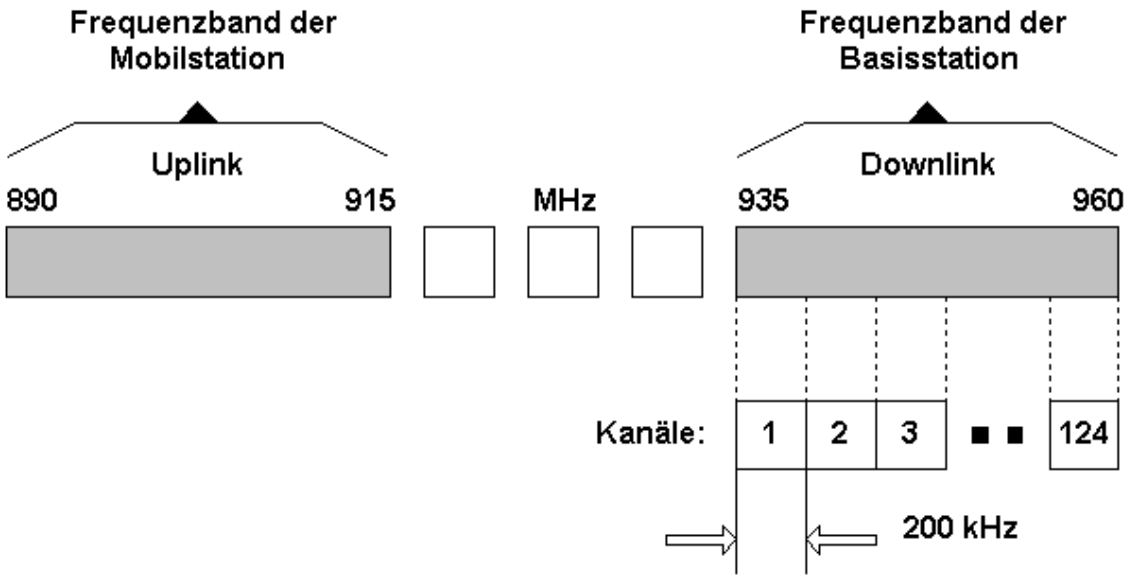


Abbildung 127: GSM-Frequenzbänder

Zeitmultiplex-Struktur:

Um nun mehr als einen Teilnehmer pro Kanal telefonieren lassen zu können, wird das TDM-Verfahren (Time Division Multiplex) eingesetzt. Hierbei werden auf einer Trägerfrequenz 8 physikalische TDM-Kanäle realisiert (siehe Abbildung 3), wobei die Zeitachse in 8 periodisch angeordnete Zeitschlitze (Time Slots) der Dauer von 0,577 ms aufgeteilt wird. Acht Zeitschlitze bilden wiederum einen TDM-Rahmen (Frame), der von der Dauer 8x0,577 ms = 4,615 ms ist. Da diese Kanäle im Vielfachzugriff genutzt werden, wird im GSM-Netz vom TDMA-Verfahren

(Time Division Multiple Access) gesprochen. Ein physikalischer Kanal ist nun durch seinen Zeitschlitz, der alle 4,615 ms wieder auftritt, und seine Trägerfrequenz gekennzeichnet. Wie schon angesprochen entspricht ein Zeitschlitz der Dauer von 0,577 ms, was umgerechnet 156,25 bit entspricht. Dieser Wert entsteht aus der Übertragungsrate des Modulationsverfahrens und der Anzahl der Bits, die in einem Slot übertragen werden sollen. Die Übertragung an sich erfolgt über sogenannte Bursts. Ein Burst von der Länge 148 bit wird genau einem Slot zugeteilt. Die restlichen 8,25 bit des Slots dienen als zeitliche Toleranzgrenze bei der Übertragung. Nachrichten, die jene 148 bit-Grenze der Bursts überschreiten, werden in mehrere Bursts aufgeteilt. Man kann 5 Arten von Bursts nach Funktion und Inhalt unterscheiden.

- Normal Burst: dient der Nachrichtenübertragung in Verkehrs- und Steuerkanälen
- Access Burst: dient dem Verbindungsaufbau
- Synchronisation Burst: dient zur Synchronisation
- Frequency Correction Burst: dient zur Frequenzkorrektur bei der Mobilstation
- Dummy Burst: dient zum Auffüllen freier Slots

Der in Abbildung 3 zu sehende Beispielburst ist ein Normal Burst der Tail Bits enthält, welche lediglich zur Modulation innerhalb des Bursts dienen. Damit nun ein gleichzeitiges Senden und Empfangen an der MS vermieden werden kann, sendet man die TDMA-Rahmen mit einer Verzögerung von 3 Zeitschlitzen vom Up- zum Downlink.

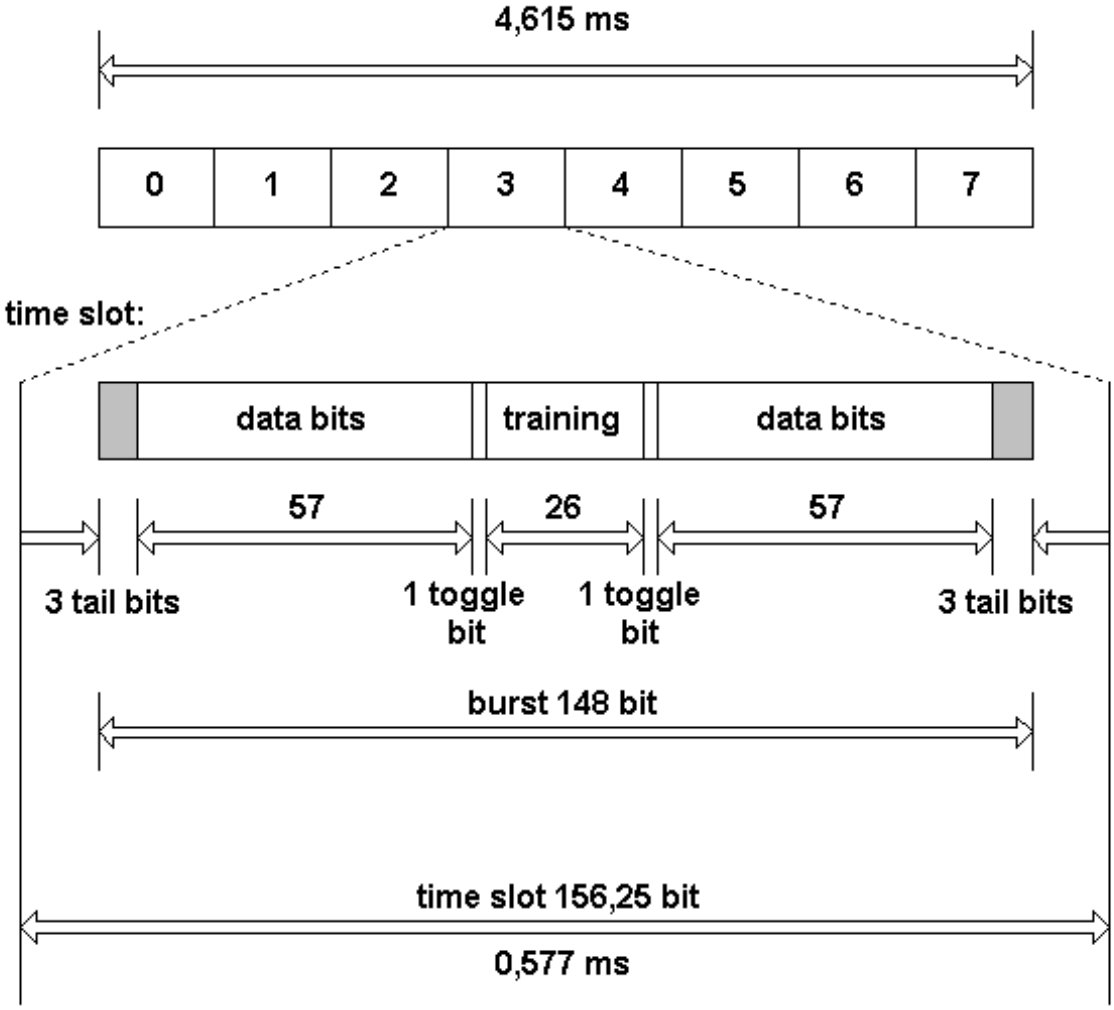


Abbildung 128: Aufbau eines TDMA-Rahmens

Logische Kanäle:

Logische Kanäle werden durch die Zuordnung von Zeitschlitzen physikalischer Kanäle gebildet (siehe Abbildung 4). Dabei kann ein logischer Kanal genau einem physikalischen Kanal entsprechen oder es können sich mehrere logische Kanäle einen physikalischen Kanal teilen, wie in Abbildung 4, worin ersichtlich ist, daß der physikalische Kanal mit einer Übertragungsrate von 4a sich in die logischen Kanäle K1 mit 3a und K2 mit Übertragungsrate a aufspaltet.

Die logischen Kanäle lassen sich auf Grund ihres Informationsgehaltes in Verkehrs- und Steuerkanäle unterteilen.

- Verkehrskanäle (Traffic Channel, TCH): Über Verkehrskanäle lassen sich Nutzinformationen während einer Verbindung von einem zum anderen Teilnehmer übertragen. Auf Grund des Angebotes an verschiedenen Diensten im GSM-Netz (siehe Kapitel 1.2.4), werden unterschiedliche Übertragungskapazitäten benötigt, nach denen sich die Verkehrskanäle nochmals in B(m)- und L(m)-Kanäle aufspalten lassen. Der B(m)-Kanal wird auch als Vollratenkanal (Full Rate TCH) mit 22,8 kbit/s und der L(m)-Kanal als Halbratenkanal (Half Rate TCH) mit 11,4 kbit/s bezeichnet.

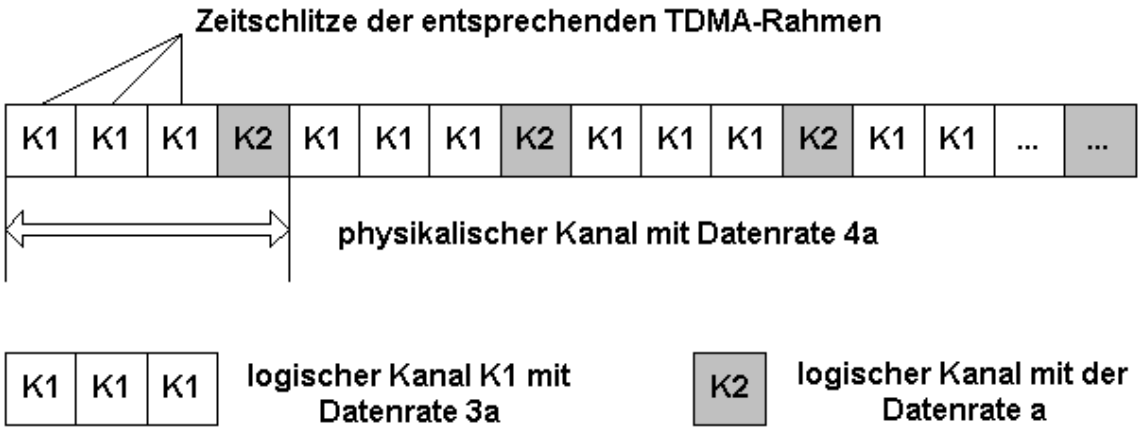


Abbildung 129: Zusammenhang zwischen logischen und physikalischen Kanälen

- Steuerkanäle (Control Channel, CCH): Steuerkanäle beinhalten Steuerinformationen, die zur Signalisierung und Steuerung des Systems dienen (z.B.: Vermittlung von Verkehrskanälen). Man unterscheidet:
  - Broadcast Control Channel (BCCH): Dient zur Übertragung von Informationen von der Feststation zu den Mobilstationen. Enthält den Frequency Correction Channel (FCCH) und den Synchronisation Channel (SCH).
  - Common Control Channel (CCCH): Dient zur Verbindungsaufnahme von der Feststation zu den Mobilstationen. Enthält den Paging Channel (PCH), den Random Access Channel (RACH) und den Access Grant Channel (AGCH).
  - Dedicated Control Channel (DCCH): Dient zur Verbindungssteuerung zwischen Netz und Mobilstation. Enthält den Stand-Alone DCCH (SDCCH), den Slow Associated DCCH (SACCH) und den Fast Associated DCCH (FACCH).

Die Erläuterung der Bedeutung der einzelnen Unterkanäle würde an dieser Stelle zu weit führen. Es ist für die weiteren Kapitel nur das Wissen über deren Existenz erforderlich.

Hierarchie der Rahmenstruktur:

Im GSM-Netz existieren, wie in der Zeitmultiplex-Struktur angesprochen, TDMA-Rahmen aus jeweils 8 Zeitschlitzen. Diese stellen die kleinsten Bausteine in der Rahmenstrukturierung des Übertragungsmediums dar (siehe Abbildung 5). Die Rahmen lassen sich abhängig vom Inhalt zu 26er- oder 51er-Mehrfachrahmen (Multiframes) zusammenfassen. Wobei die 26er-Mehrfachrahmen für die Übertragung der Sprache und der Daten (außer SACCH/T, FACCH) und die 51er-Mehrfachrahmen für die Übertragung von Signalisierungsdaten zuständig sind. 26 der 51er- und 51 der 26er-Mehrfachrahmen bilden einen Superrahmen (Superframe). 2048 Superrahmen ergeben wiederum einen Hyperrahmen (Hyperframe), für dessen Übertragung knappe 3,5 Stunden benötigt werden.

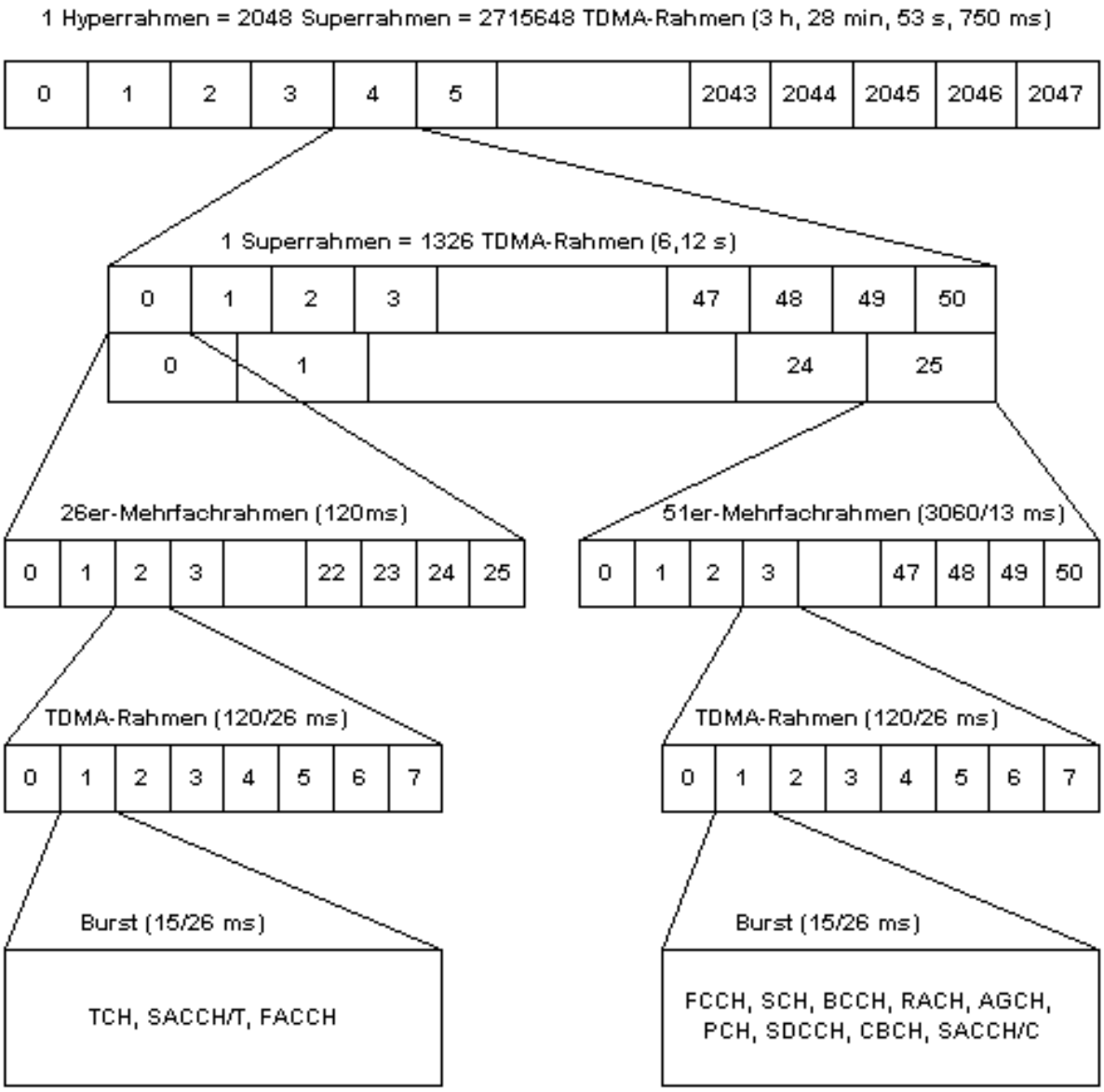


Abbildung 130: Rahmenstruktur des Übertragungsmediums

9.2.4 Dienste

Im GSM-Netz werden die angebotenen Telekommunikationsdienste nach zwei Gesichtspunkten unterteilt. Erstens nach der Wichtigkeit der Einführung, in wesentliche (Essential, E) oder zusätzliche (Additional, A) Dienste. Als E-Dienste werden Dienste bezeichnet, die vom Mobilnetz angeboten werden müssen, A-Dienste hingegen können angeboten werden. Die Kennzeichnung der Dienste erfolgt im Anschluß durch die Angabe eines E oder A für den jeweils vorliegenden Dienst. Die zweite Unterteilung erfolgt nach der Funktion der Dienste. Hierfür existieren drei Hauptkategorien:

- Trägerdienste (Bearer Service): Trägerdienste sind reine Transportdienste, die zwischen einem Mobilfunkteilnehmer und einem Teilnehmer eines beliebigen anderen Netzes Signale

bittransparent übertragen. Hierbei handelt es sich um verbindungsorientierte Kanal- und paketvermittelte Datenübertragung, wie sie in den unteren drei Schichten des ISO/OSI Modells definiert ist.

- Teledienste (Tele Service): Teledienste ermöglichen eine anwendungsbezogene Kommunikation zwischen dem Mobilfunk- und einem Teilnehmer eines beliebigen anderen Netzes. Hierfür werden Protokolle aller 7 ISO/OSI Schichten verwendet. Ein Teledienst nimmt meist nur einen oder eine geringe Anzahl von Trägerdiensten in Anspruch. Teledienste sind:
  - Telefondienste(E)
  - Notrufdienste(E)
  - Kurznachrichtendienste(A,E)
  - Videotextzugangsdienste(A)
  - Telefaxdienste(E)
  - Elektronische Post(A)
- Zusatzdienste (Supplementary Services): Zusatzdienste sind keine selbständigen Dienste, sondern weitergehende Leistungsmerkmale die in Verbindung mit Tele- und Trägerdiensten angeboten werden. Zusatzdienste sind:
  - Teilnehmeridentifikation
  - Rufumleitung
  - Rufweiterleitung
  - Halten eines Rufes
  - Konferenzschaltung
  - Geschlossene Benutzergruppe
  - Sperren von Verbindungen

9.2.5 Handover

Ein typisches Feature für Mobilfunksysteme, und deshalb hier als einziges herausgegriffen, ist der Handover. Als dieser wird die Übergabe der Verbindung zu einer anderen BTS, BSC oder MSC bezeichnet, die durch das Verlassen des Sende- bzw. Empfangsbereiches einer BTS, einer BSC oder sogar einer MSC durch den Teilnehmer veranlaßt wird (siehe Abbildung 6). Weitere Gründe außer einem Ortswechsel der MS können ein gestörter Empfang (z.B. durch Gleichkanalstörungen) oder das Ziel der gleichmäßigen Verteilung auf Zellen äquivalenten Empfangs sein. Je nachdem, zwischen welchen Teilen des GSM-Netzes der Handover stattfindet, wird er entweder vom BSC alleine (1,2) oder vom MSC (3) bzw. den beteiligten MSC's (4) durchgeführt. Die Initiative zu einem Handover kann dabei sowohl vom MSC ausgehen (Lastverteilung auf verschiedene BSC's), als auch vom BSC, in dessen Zelle sich die MS befindet. Das MS mißt laufend die Qualität der Verbindung zur aktuellen Basisstation und die Empfangsstärke der umliegenden Zellen. Diese Daten meldet sie an ihre momentane Basisstation, die somit über einen Handover zu einer besseren Verbindung innerhalb der gleichen Zelle durch Wechsel des Zeit- und/oder Frequenzkanals oder zu einer anderen Basisstation entscheidet.

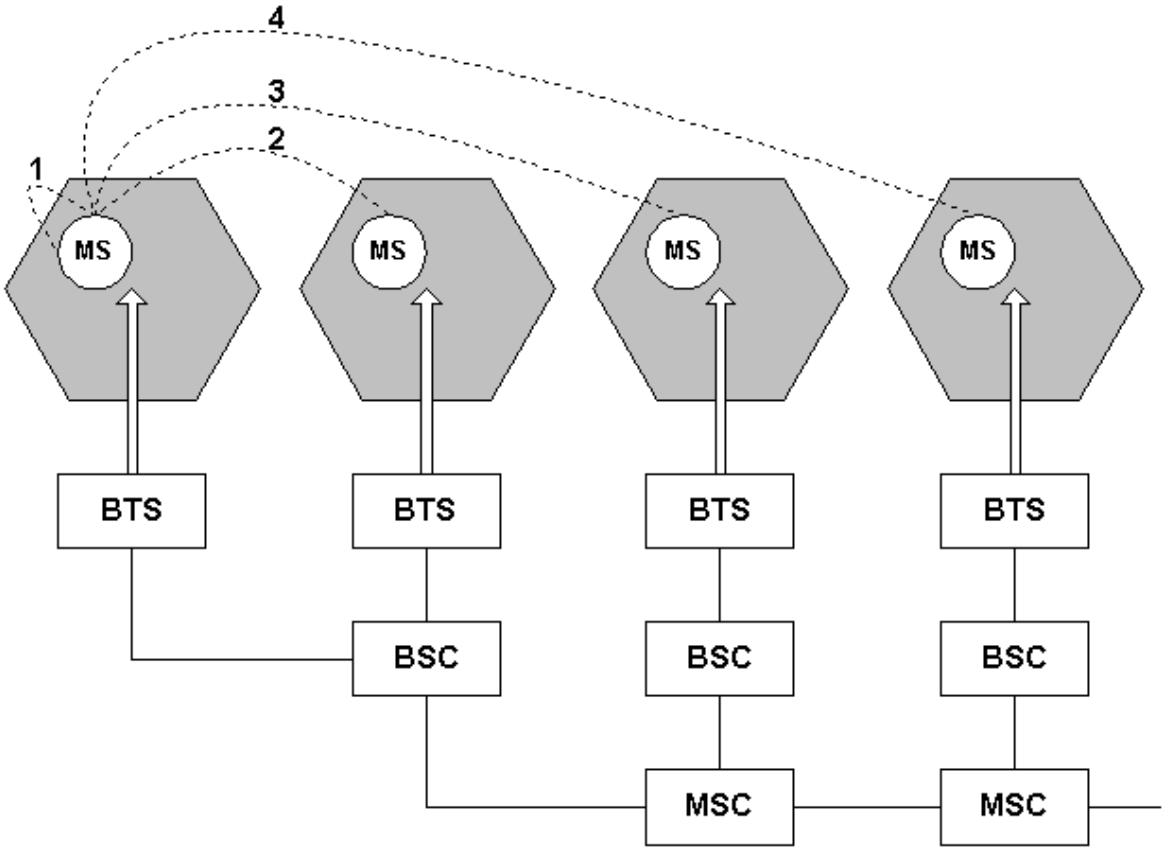


Abbildung 131: Arten des Handover

9.2.6 Beispiele für den Verbindungsaufbau

Abschließend noch je ein Beispiel zum Rufaufbau in beiden Richtungen. Diese sollen zum besseren Verständnis der bisher angesprochenen Themen beitragen.

Kommender Ruf:

Möchte ein Anrufer aus dem Festnetz eine Verbindung zu einem Mobilfunkteilnehmer des GSM-Netzes aufbauen (siehe Abbildung 7), wählt er dessen ISDN-Nummer. Die Vermittlungsstelle des Festnetzes erkennt, daß die gewünschte Nummer zu einem Teilnehmer eines PLMN gehört und leitet den Anruf mit der Initialisierungsnachricht IAM (Initial Address Message) an die nächste Übergangsvermittlung GMSC (Gateway-MSC) weiter (1). Über die in der IAM-Nachricht enthaltenen Rufnummer bestimmt die GMSC die zuständige Heimatdatei des gewünschten Anrufempfängers (2). Zusätzlich wird noch die Autorisierung für die ebenfalls in der IAM-Nachricht mitgeteilten Dienstwünsche vom HLR überprüft. Danach wird das zuständige VLR in dessen Bereich sich der gewünschte Gesprächsteilnehmer aufhält aufgefordert eine Aufenthaltsnummer MSRN bereitzustellen (3). Anhand dieser Nummer (4) ist das HLR in der Lage die zuständige MSC zu bestimmen und teilt diese der GMSC mit (5), die zu dieser eine Verbindung herstellt (6). Desweiteren überprüft das VLR auf Veranlassung der MSC (7) die Erreichbarkeit der Mobilstation. Ist eine Verbindung möglich, sendet die vom VLR benachrichtigte (8) MSC einen Funkruf an alle ihr zugeordneten Funkzellen (9). Meldet sich der gesuchte Teilnehmer (10), wird das

MSC nach Ablauf aller Sicherheitsprozeduren (11) vom VLR aufgefordert (12) die Verbindung im Funknetz einzurichten (13).

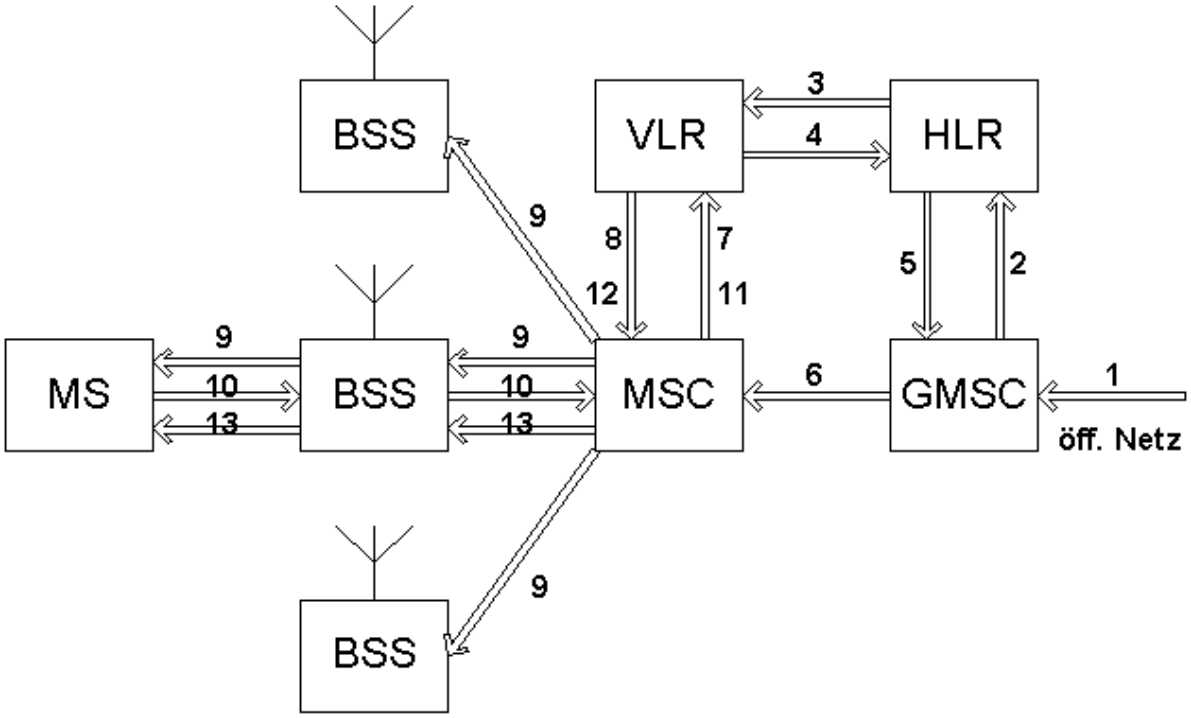


Abbildung 132: Kommender Ruf

Gehender Ruf:

Wenn ein Teilnehmer des GSM-Netzes einen Anruf tätigen möchte (siehe Abbildung 8), geht nach Abwicklung der entsprechenden Sicherheitsprozeduren der Rufwunsch über das BSS (1) an das zuständige MSC (2) weiter. Diesem wird sowohl die gewünschte Rufnummer als auch die Forderungen bezüglich der Dienstgüte des Netzweges und der Kompatibilität des Empfangsgerätes mitgeteilt. Danach überprüft das MSC die Berechtigung des Teilnehmers im VLR (3) und die im Moment zur Verfügung stehenden Betriebsmittel (5) (z.B.: freie Leitung zum Festnetz). Ist die Teilnehmerberechtigung in Ordnung (4) und stehen die erforderlichen Betriebsmittel zur Verfügung, so werden diese dem Teilnehmer von der MSC zugewiesen und die entsprechenden Umsetzfunktionen gewählt. Ist der Verbindungsaufbau erfolgreich wird dem Teilnehmer eine Nachricht zugesandt, die sich in der Mobilstation als Rufton bemerkbar macht (6+7).

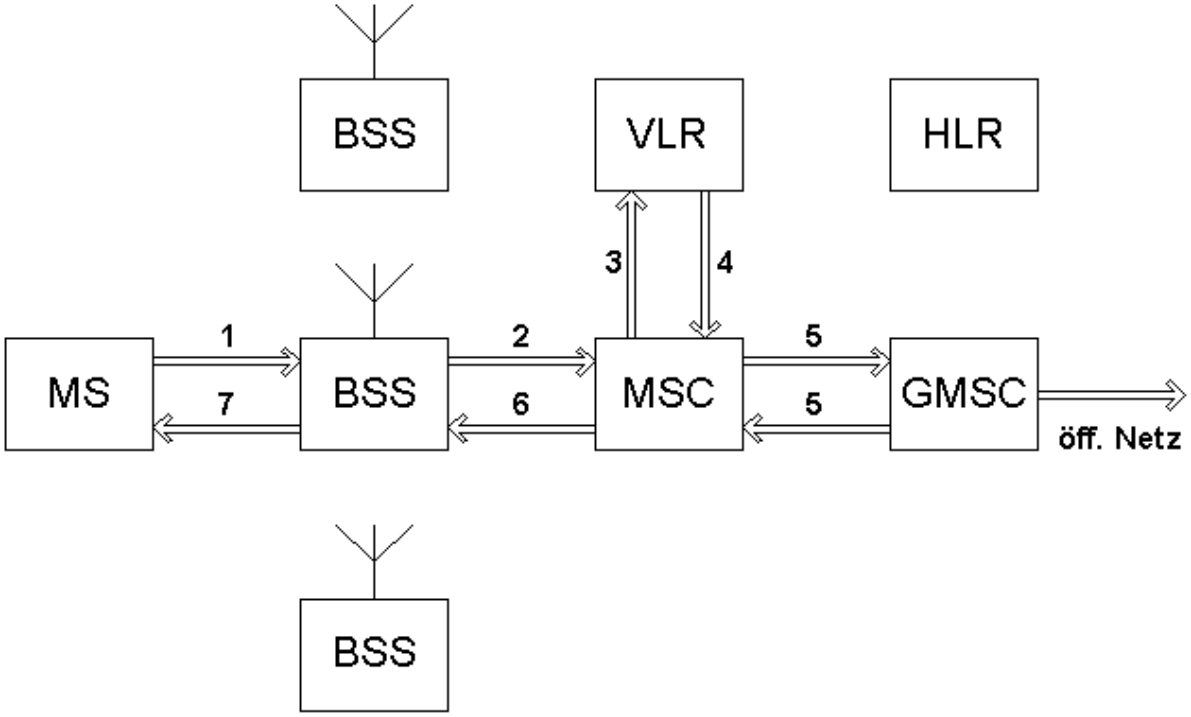


Abbildung 133: Gehender Ruf

9.3 DECT - Digital Enhanced Cordless Telecommunication

Das DECT-System ist ein Mobilkommunikationssystem für die sogenannte letzte Meile und soll daher in geraumer Zeit mit fortschrittlicherer Technik und somit Komfort die analogen Festanschlüsse ersetzen. In den folgenden Kapiteln wird im Rahmen dieses Seminars nur ein kleiner Blick auf die Entstehung, die Architektur und die Verbindungsmöglichkeit zum bereits besprochenen GSM-System gegeben. Die Grundlage hierfür bildeten [51], [91], [142].

9.3.1 Einführung

DECT bedeutete früher Digital European Cordless Telecommunication, wurde dann aber wegen der geplanten globalen Ausdehnung umbenannt. 1992 wurde der Standard von dem ETSI (European Telecommunications Standardisation Institute) festgelegt und 1993 die ersten Systeme der Öffentlichkeit präsentiert. DECT ist ein Mobilfunknetz, das im Gegensatz zu GSM nicht für den Einsatz in großflächigen Gebieten geeignet ist. Es dient vielmehr zur Kommunikation innerhalb von Gebäuden und wird dort auf Grund der Vorzüge wie besserer Sprachqualität oder höherer Abhörsicherheit, gegenüber den analogen, schnurlosen Telefonen in naher Zukunft eingestzt werden. Es besitzt eine Reichweite von ca. 50 m in Gebäuden und ca. 300 m im Freien von der Mobil- zur Basisstation. Diese Entfernung kann aber durch bestimmte Relaiskonzepte vergrößert werden. Das Netz setzt sich, wie die großflächigen Zellularfunknetze (GSM), aus einzelnen Zellen zusammen und hat gleichermaßen die Fähigkeit den Benutzer untereinander weiterzureichen, wenn er den Bereich einer Zelle verläßt (handover). Das DECT-System ermöglicht sowohl die Übertragung von Sprache, als auch von Daten. Es können ebenfalls, wie im GSM-Netz, ISDN-Dienste genutzt werden.

9.3.2 Architektur und Beispiele von DECT-Festnetzen

Das DECT-System besteht immer aus zwei Komponenten. Erstens der Mobilstation und zweitens der Heim-Feststation (Abbildung 9). Die Mobilstation oder auch Portable Part (PP) genannt ist mit dem MS aus dem GSM-Netz zu vergleichen. Sie enthält ebenfalls eine Berechtigungskarte DAM (DECT Authentification Module), die Informationen zur Identifizierung und Authentifizierung des Teilnehmers beinhaltet. Durch den PP wird über die Funkschnittstelle, die sich einer andersartigen Kombination des TDMA- und FDMA-Verfahrens wie GSM bedient, eine Verbindung zur Heim-Feststation hergestellt. Diese setzt sich aus dem mit dem PP kommunizierenden Teil der Feststation (Fixed Part, FP), der Interworking Unit (IWU), dem DECT Fixed System (DFS) und der Database (DB) zusammen. Die IWU dient zur Verbindung zum Festnetz, das DFS zur Steuerung des Systems. Dieses kann je nach Komplexität des Systems noch eine zusätzliche Steuereinheit (Subsystem Control Unit, SCU) enthalten (Abbildung 10), die auch als Ersatz für das DFS in Untersystemen dienen kann. Die DB erfüllt die Aufgabe der Mitgliederverwaltung. Hierbei kann sie je nach Komplexität des zu verwaltenden Systems auch aus einer Home Data Base (HDB) und einer Visitor Data Base (VDB) zusammengesetzt sein, die bei möglichen Handovern oder Roaming unverzichtbar für die Übergabe der teilnehmerspezifischen Daten, wie aus dem GSM-Netz bekannt, sind (Abbildung 10).

In Abbildung 9 und Abbildung 10 sieht man zwei Beispiele für DECT-Festnetze. Abbildung 9 zeigt den einfachsten Fall, den einer privaten Heim-Feststation. Diese versorgt eine oder mehrere Mobilstationen innerhalb des Hauses, deren Daten in einer einfachen Datenbank gespeichert sind.

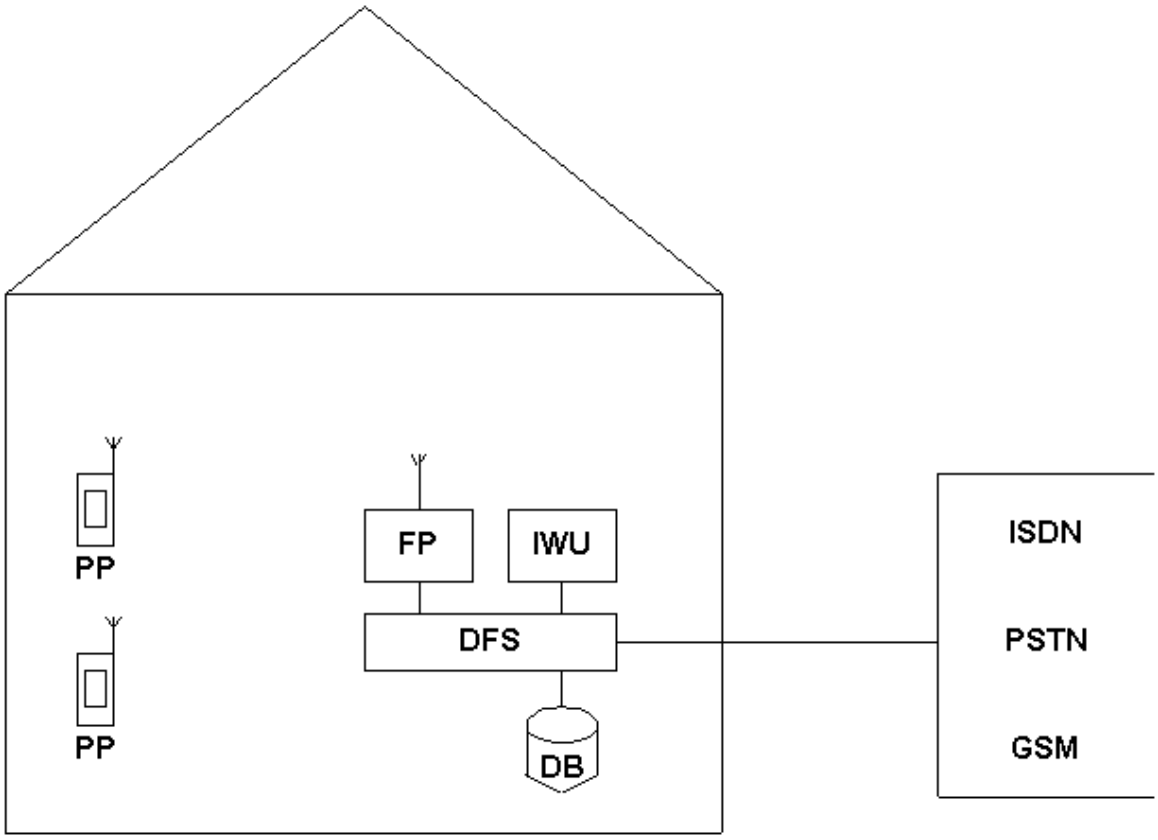


Abbildung 134: Private Heim-Festnetze

Abbildung 10 zeigt einen komplexeren Fall einer Nebenstellenanlage mit Ring, einem dezentralen DFS und direktem Anschluß der FP. Hierbei sind mehrere SCU's über einen Backbone Ring miteinander verbunden, um Daten und Signale untereinander austauschen zu können. Jedes DFS ist über eine IWU mit dem Festnetz verbunden. Zur Teilnehmerverwaltung stehen jedem DFS ein HDB für in diesem Teilsystem beheimatete Teilnehmer und ein VDB für gastierende Teilnehmer zur Verfügung. Diese dienen zur Verkehrsminimierung auf dem Backbone Ring, da die Daten der gastierenden Teilnehmer nicht ständig über den Backbone Ring von der entsprechenden HDB angefordert werden müssen.

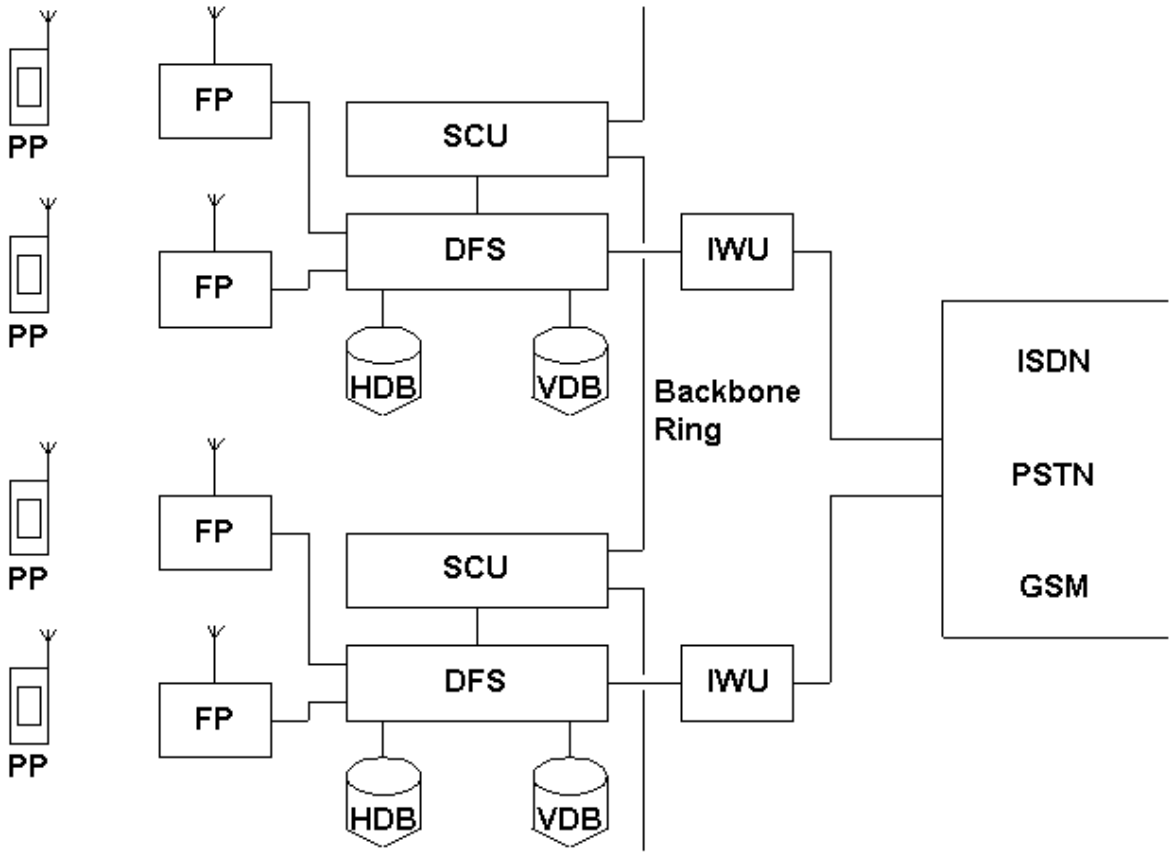


Abbildung 135: Nebenstellenanlage

Es gibt natürlich noch einige andere Möglichkeiten der Strukturierung. Die in ihrem Umfang jedoch den Rahmen dieses Seminars sprengen würden.

9.3.3 Integration des DECT-Systems in GSM

Die Festnetzseite des DECT-Systems ist im Standard nicht festgelegt und daher herstellerspezifisch. Es kann sich somit auch um einen Anschluß an ein Mobilkommunikationssystem wie GSM handeln (Abbildung 11). Das Problem bei der Verknüpfung beider Systeme liegt in der Schnittstelle, die zur Kommunikation dienen soll. Die Funkschnittstelle der jeweiligen Systeme steht auf Grund von differierender Trägerfrequenz, Kanalstruktur, Sprachcodierung und Protokollstruktur als Verbindungsstelle ebenso wenig zur Verfügung, wie auch die Schnittstelle zwischen BTS und BSC im GSM-System, da auch hier die unterschiedlichen Kanalzugriffsverfahren und

Kanalstrukturen eine Kommunikation verhindern. Somit eignet sich als einzige Schnittstelle, die zwischen BSC und MSC im GSM-System. Über diese Schnittstelle werden keine Steuerinformationen für die Funkschnittstelle übertragen, sondern lediglich Daten, die zum Verbindungsaufbau und zum Routen dienen. Diese Daten werden mit Hilfe von Protokollen übertragen, die in beiden Systemen von den Aufgaben und Funktionen vergleichbar sind. Die anstehende Umsetzung von einem System zum anderen wird durch eine Interworking Unit (IWU) durchgeführt, die ebenfalls die zu übertragenden Daten und die Sprache vom Teilnehmer in den ISDN-Standard von 64 kbit/s umsetzt.

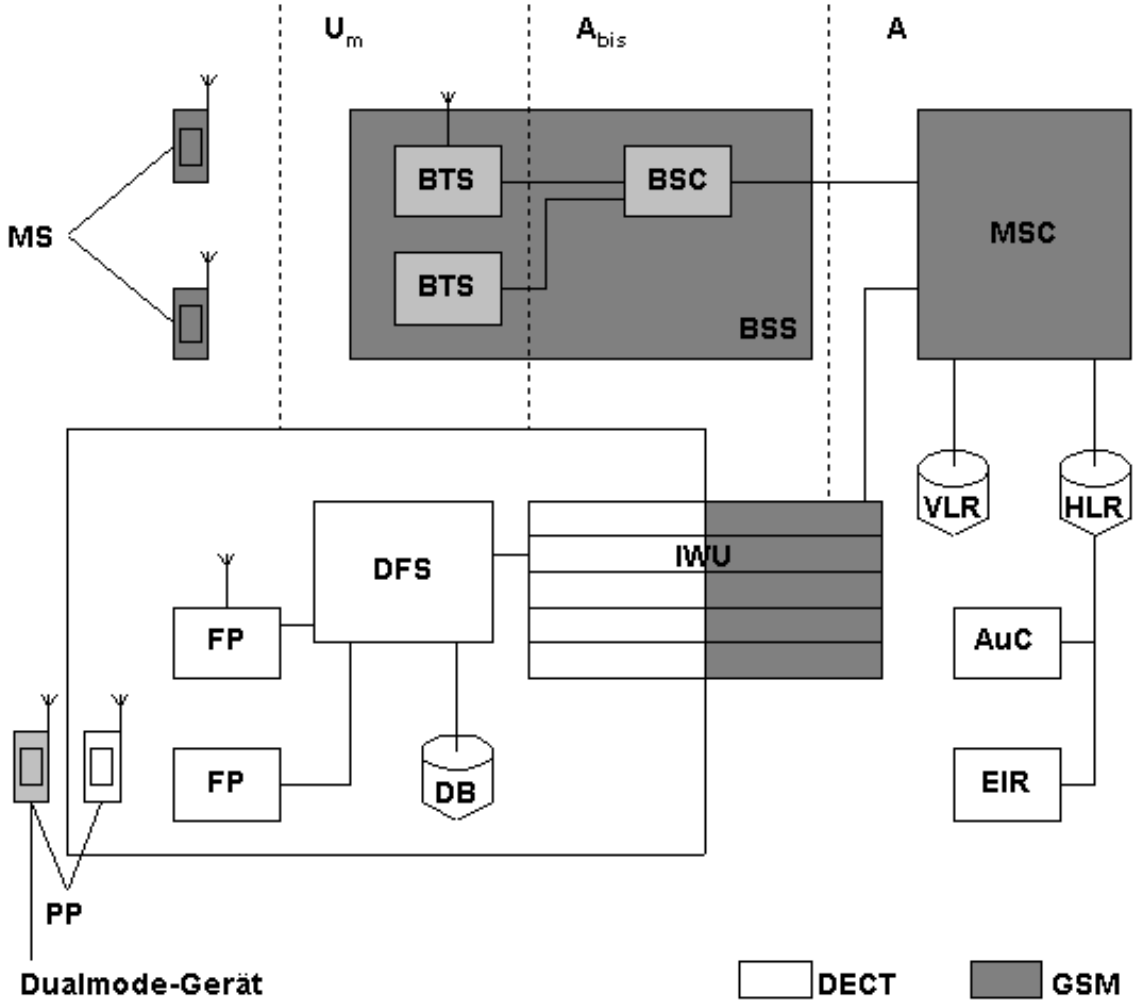


Abbildung 136: DECT-Anbindung an die GSM-A-Schnittstelle

9.4 UMTS & IMT-2000

UMTS und IMT-2000 gehören im Gegensatz zu den beiden bereits besprochenen Mobilfunksystemen zur dritten Generation. Diese sollen nach jetzigem Stand der Dinge im Laufe der nächsten Jahre in Betrieb genommen werden und die bereits bestehenden Systeme der zweiten Generation, wie eben GSM und DECT, ersetzen bzw. miteinander vereinigen. In den folgenden Kapiteln wird ein Abriß der bisher geplanten Erweiterungen und Änderungen im Vergleich zu

den Systemen der zweiten Generation gegeben. Der Großteil der Ausführungen bezieht sich dabei auf UMTS, da UMTS den europäischen Teil des globalen IMT-2000 - Systems bildet und sich die entwickelten Standards einander entsprechen. Außerdem wird somit ein Vergleich der beiden europäischen Entwicklungen GSM und UMTS ermöglicht. Die Grundlage hierfür bildeten [51], [91], [142].

9.4.1 Einführung in UMTS & IMT-2000

UMTS (Universal Mobile Telecommunications System):

Seit 1989 werden die Standards für UMTS in der Zusammenarbeit von mehreren EU-Programmen mit dem ETSI entwickelt. Unterstützt wird diese Entwicklung ebenfalls durch ein UMTS-Forum, das einen Zusammenschluß der europäischen Partner darstellt. Seit 1998 ist die Entwicklung abgeschlossen und ein Start des Betriebs des europaweiten Systems im Jahr 2005 geplant. Das bisherige Konzept, das UMTS verfolgt, sieht folgendermaßen aus: Es wird jedem Benutzer, egal an welchem Ort er sich befindet, eine Kommunikation durch die weltweite Integration aller bestehender Systeme (z.B.: Mobilfunk-, Satellitensysteme) ermöglicht. Hierbei werden intelligente Netze verwendet, die dem Benutzer sogar einen Wechsel des Betreibers bei bestehenbleibender Verbindung gewährleisten. Der Frequenzbereich liegt zwischen 1,885-2,2 GHz. Die Übertragungsrate entspricht für Dienste (z.B.: Bildtelefon) der von ISDN. Außerdem ist eine parallele Übertragung von Sprache, Text, Daten und Bildern über eine Verbindung möglich. Jeder Benutzer ist durch eine persönliche Telefonnummer weltweit erreichbar.

IMT-2000 (International Mobile Telecommunications at 2000 MHz):

IMT-2000 entspricht dem sich seit 1985 durch die CCIR (Centre for Communication Interface Research) in Planung befindlichen FPLMTS (Future Public Land Mobile Telephone System). Der Name wurde 1995 in IMT-2000 geändert. Das Inbetriebnahmedatum 2005 entspricht ebenfalls, wie die Anforderungen, denen von UMTS. Der einzige Unterschied ist, daß IMT-2000 global ausgerichtet ist und UMTS nur die Europakomponente mit der Verbindung zu anderen, nichteuropäischen Systemen, darstellt. Daher enthält IMT-2000 im Gegensatz zu UMTS mehrere Luftschnittstellen, die je nach der Besiedelung eines Gebietes Verwendung finden (z.B.: Unterschied: Entwicklungsländer - Industrieländer).

9.4.2 Architektur von UMTS

Das UMTS-Netz besteht aus vier Systemkomponenten (siehe Abbildung 12), dem Mobile Terminal (MT), dem Access Network, dem Fixed (Core) Network und dem Intelligent Network. Das Mobile Terminal ist, wie aus dem GSM-System bekannt, über die Funkschnittstelle mit dem BTS (Base Transceiver System) verbunden. Für das Zugriffsverfahren wird jedoch ATDMA (Advanced Time Division Multiple Access) verwendet. Dies soll nach den bisher bekannten Entwürfen eine Kombination aus TDMA und CDMA (Code Division Multiple Access) sein. Das BTS bildet mit dem CSS (Cell Site Switch) das Access Network. Sie sind ebenfalls Bestandteile des RAS (Radio Access Systems). Das CSS ermöglicht es, die Informationen vom BTS zum Festnetz zu übertragen. Das Festnetz wird als Fixed (Core) Network bezeichnet. Die entsprechenden Elemente, die mit dem CSS kommunizieren, sind LE (Local Exchange) und TX (Transit Exchnage). Beide Teilnetze das Access Network und das Fixed (Core) Network beinhalten Teile des Intelligent Network, um Signalisierungsnachrichten untereinander auszutauschen. Diese sind der Mobile Service Control Point (MSCP)und der Mobile Service Data Point (MSDP). Die Signalisierungsinformationen laufen über ein ATM-basiertes Signalisierungsnetz. Ebenso soll das

Festnetz, das ein B-ISDN-Netz sein soll, virtuelle ATM-Verbindungen verwenden. Dies ist der derzeitig vorliegende, grobe Entwurf ohne genauere Definitionen der einzelnen Bestandteile, was an dieser Stelle zur Vorstellung ausreichen sollte.

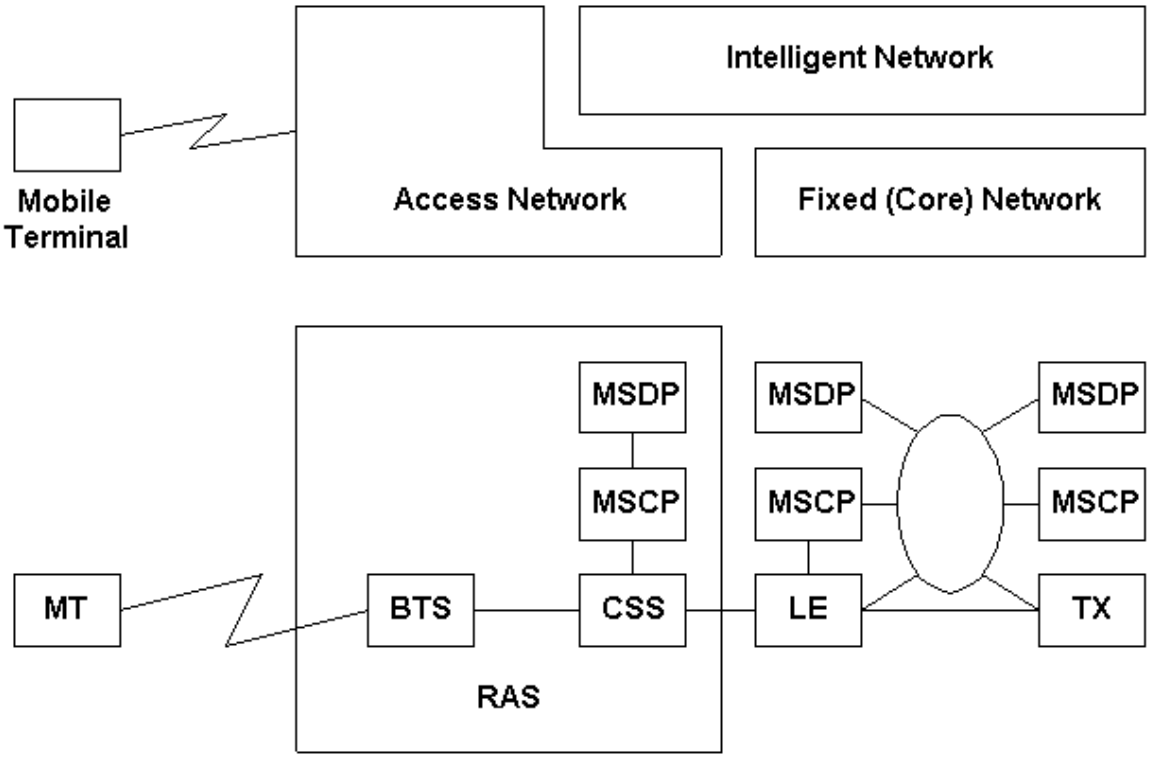


Abbildung 137: UMTS-System

9.4.3 Dienste für UMTS und IMT-2000

Auf Grund der neu gestellten Aufgaben und Anforderungen müssen die von den bisherigen Systemen bekannten Dienste erweitert werden. Da die Dienste des IMT-2000 als Vorlage für die des UMTS-Netzes dienten, werden hier nur die Dienste von UMTS beschrieben. Sie teilen sich im Gegensatz zum GSM-Netz nicht in drei, sondern vier Sparten auf:

- Trägerdienste: Die Trägerdienste im UMTS-Netz entsprechen denen von ISDN und Breitband-ISDN. Dies bedeutet eine Erweiterung der Übertragungsrate dem GSM-Netz gegenüber auf bis zu 2 Mbit/s für mobile Benutzer. Es werden 2 Arten von Trägerdiensten unterschieden, interaktive und Verteildienste. Verteildienste ermöglichen es, daß beliebig vielen Benutzern kontinuierlich Informationen von einer zentralen Stelle aus geschickt werden. Interaktive Dienste sind entweder Konversations-, Nachrichten- oder Abfragedienste, die je nach Funktion entsprechende Verbindungen zum Benutzer haben.

- Teledienste: Die Teledienste teilen sich in 3 Kategorien auf. Die Erste bilden die Teledienste, die bereits im Festnetz und somit auch im GSM-Netz vorhanden waren. Dies ist die Telefonie und die Telekonferenz. Die zweite Kategorie sind Dienste und Anwendungen, die

zum einem aus dem GSM-Netz schon bekannt sind und zum anderen speziell für UMTS entwickelt wurden:

- Audio- und Videoübertragung
- Paging
- Rundsendedienste
- Datenbankabfragen
- Datenübertragung
- Verzeichnisdienste (z.B.: Telefonbuch)
- Mobilitätsdienste (z.B.: Navigation)
- Elektronische Zeitung
- Notruf
- Notruf-Rundsendung
- Kurznachrichtendienste
- Teleaktions-Dienste (z.B.: Fernsteuern)
- Teleshopping
- Videoüberwachung
- Sprachnachrichten

Die letzte Kategorie bilden Multimedia (MM) und interaktives Multimedia(IMM).

- Zusatzdienste: Die Zusatzdienste wurden in Anlehnung an die GSM- und ISDN-Standards vorgeschlagen und lauten:
  - Nummernidentifikation, z.B.: Identifikation des Anrufers
  - Rufanbietung, z.B.: Rufweiterleitung
  - Rufbeendung, z.B.: Ruf halten
  - Mehrparteienkommunikation, z.B.: Konferenzgespräche
  - Gruppenkommunikation, z.B.: Benutzergruppen
  - Abrechnung, z.B.: Anzeige des Guthabens
  - Zusatzinformationen, z.B.: Benutzer-zu-Benutzer-Signalisierung
  - Rufzurückweisung, z.B.: Sperren aller kommenden Anrufe
- Mehrwertdienste: Es wird drei neue Dienste, die als Mehrwertdienste bezeichnet werden, im UMTS-Netz geben, von denen lediglich die Personal Mobility von der Idee her aus dem GSM-Netz bekannt ist. Bei dieser kann ein Benutzer durch eine Smart Card (SIM-Card bei GSM) seine Telefonnummer auf jedes Endgerät übertragen. Völlig neu hingegen sind die beiden anderen Dienste. Zuerst das Virtual Home Enviroment (VHE) und Dienst-Portabilität, das einen Emulator für die vom Benutzer ausgewählten Dienste darstellt, welcher ihm ermöglicht in fremden Netzen seine gewohnte Benutzerumgebung vorzufinden. Und zweitens das Bandwidth on demand, das es dem Benutzer erlaubt die Übertragungsbandbreite dem zu nutzen wollenden Dienst anzupassen.

Alle aufgezählten Dienste werden im UMTS-Netz durch Dienstparameter gekennzeichnet. Diese sind:

- Nettobitrate
- Symmetrie des Dienstes
- max. erlaubte Bitfehlerwarscheinlichkeit nach Kanalkodierung
- max. erlaubte Verzögerung bei der Datenübertragung
- Nutzungsgrad
- Codierfaktor

Mit Hilfe dieser Parameter läßt sich die erforderliche Dienstbandbreite, die z.B. für Bandwidth on demand benötigt wird, berechnen, die mit Inbezugnahme der erwarteten Dauer und Häufigkeit der Nutzung der Dienste die anfallende Verkehrsdichte ergibt. Die so entstehende Verkehrsdichte läßt einen Schluß auf die für das UMTS-Netz erforderliche Bandbreite zu, welche laut diesen Berechnungen bei vollem Ausbau des Netzes bei 554 MHz Verkehrs- und 28 MHz Schutzbändern liegen sollte. Auf Grund dieser Abschätzung (oder besser Berechnung) ist bis 2008, wenn die Entwicklung wie erwartet verläuft, eine Bandbreite zwischen 300-500 MHz geplant.

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

[1] *„ATM Routing with IISP and PNNI“, in: Guide to ATM Technology for the Catalyst 8540 MSR, Catalyst 8510 MSR, and LightStream 101.* http://www.cisco.com.

[2] Synchrounous Digital Hierarchy (SDH). http:www.iec.org.

[3] The Mechanics of Routing Protocols. Cisco Press, http://www.cisco.com.

[4] *„Open Shortest Path First (OSPF)“, in: Internetworking Technology Overview.* June 1999. http://www.cisco.com.

[5] *„Routing Basics“, in: Internetworking Technology Overview.* June 1999. http://www.cisco.com.

[6] Virtuelle Netze müssen wohlüberlegt sein. Computer Zeitung Nr.34, Seite 9, August 1999.

[7] Aber, R. xDSL Local Loop Access. Tech. rep., 3COM, 1998.

[8] Aboba, B. RFC2716: PPP EAP TLS Authentication Protocol. Tech. rep., Network Working Group, 1999.

[9] ADSL Forum. ADSL Tutorial. `http://www.adsl.com`.

[10] ADSL Forum. General Introduction to Copper Access Technologies. `http://www.adsl.com`.

[11] ADSL Forum. VDSL Tutorial. `http://www.adsl.com`.

[12] Anatol Badach, Erwin Hoffmann, O. K. *High Speed Internetworking.* Addison-Wesley, 1994.

[13] Atkins, D. RFC1991: PGP Message Exchange Formats. Tech. rep., Network Working Group, 1996.

[14] Atkinson, R. IP Athentication Header. Tech. rep., Network Working Group, 1995.

[15] Atkinson, R. IP Encapsulation Security Payload. Tech. rep., Network Working Group, 1995.

[16] Atkinson, R. RFC1825: Security Architecture for the Internet Protocol. Tech. rep., Network Working Group, 1995.

[17] Atkinson, R. RFC1826: IP Authentication Header. Tech. rep., Network Working Group, 1995.

[18] Atkinson, R. RFC1827: IP Encapsulating Security Payload (ESP). Tech. rep., Network Working Group, 1995.

[19] Badach, A. *High Speed Internetworking: Grundlagen und Konzepte für den Einsatz von FDDI und ATM*, 1. ed. Addison-Wesley, 1994. ISBN 3-89319-713-3, Studentenbilbliothek Pd Bad P8532T E02.

[20] Badach, A. *High Speed Internetworking: Grundlagen, Kommunikationsstandards, Technologien der Shared und Switched LANs*, 2. ed. Addison Wesley Longman, 1997. ISBN 3-8273-1232-9, Studentenbibliothek Pd Bad P8532T A2 E02.

[21] Balenson, D. RFC1423: Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers. Tech. rep., Network Working Group, 1993.

[22] Ballew, S. M. *Managing IP Networks with Cisco Routers*, 1 ed. O'Reilly & Associates, Inc., Cambridge u.a., 1997, ch. 5.

[23] Bell, E. RFC2674: Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions. Tech. rep., Network Working Group, 1999.

[24] Berson, S. Classical RSVP and IP over ATM. Tech. rep., USC/Information Sciences Institute, 1996.

[25] Borowka, P. *Brücken und Router: Wege zum strukturierten Netzwerk*, 2 ed. Datacom Buchverlag, Bergheim, 1995, ch. 4, pp. 174–344.

[26] Borowska, P. VPNs - Modeerscheinung oder Zukunftstechnik? Computerwoche Nr.2, Seite 13, June 1999.

[27] Bosse, M. VLAN. `http://www.sbsk.de/atm_bosse/ATMTheme/vlan.htm`, September 1997.

[28] Braden, R. RFC 1122 Requirements for Internet Hosts. Tech. rep., IETF, Oktober 1989.

[29] Braden, R. RFC 2205 Resource Reservation Protokoll, RSVP. Tech. rep., IETF, September 1997.

[30] Braden, R., Clark, D., and Shenker, S. RFC 1633 Integrated Services in the Internet Architecture. Tech. rep., IETF, June 1994.

[31] Braden, R., Estrin, D., Berson, S., Herzog, S., and Zappala, D. The Design of the RSVP Protocol. Tech. rep., USC/Information Sciences Institute, 1995.

[32] Callas, J. RFC2440: OpenPGP Message Format. Tech. rep., Network Working Group, 1998.

[33] Callon, R., Doolan, P., Feldman, N., Fredette, A., Swallow, G., and Viswanathan, A. A Framework for Multiprotocol Switching. Tech. rep., Network Working Group, 1999.

[34] Campbell, A., Coulson, G., and Hutchison, D. A Qualitiy of Service Architecture. *Computer Communication Review 24* (April 1994), 6–27.

[35] Chen, W. Y. *DSL: Simulation Techniques and Standards Development for Digital Subscriber Lines*. Technology Series. MacMillan Technical Publishing, 1998.

[36] Ciampa, R. Layer 3 Switching: An Introduction. `http://www.3com.com/technology/tech_net/white_papers/pdf/50066001a.pdf`, 1998.

[37] Cisco. Configuration Examples Related to VLAN Features. Catalyst 1900 Series and Catalyst 2820 Series Enterprise Edition Software Configuration Guide, `http://www.cisco.com/`.

[38] Cisco. Planing and Implementing a VLAN Configuration. VlanDirector User Guide, `http://www.cisco.com/`.

[39] Cisco. Cisco Inelligent Networking. White Papers, `http://www.cisco.com/`, 1998.

[40] Cisco. Cisco Directions for the VPN-Enabled Enterprise Network. White Papers, `http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/tech/cvpnn_wp.htm`, October 1999.

[41] Cisco. Cisco VLAN Roadmap. `http://www.cisco.com/warp/public/538/7.html`, April 1999.

[42] Cisco. Managing Virtual Private Networks—An Introduction to VPNs. White Papers, `http://www.cisco.com/warp/public/cc/sol/mkt/ent/vpne/tech/mnvpn_wp.htm`, October 1999.

[43] Cisco-Systems. Introduction: Quality of Service Overview. `http://www-search.cisco.com/univercd/cc/td/doc/product/software/ios120/%12cgcr/qos_c/qcintro.pdf`.

[44] Clark, D., Shenker, S., and Zhang, L. Supporting Real-Time Application in an Integrated Services Packet Architecture, August 1992.

[45] Conta, A. Transmission of IPv6 Packets over IPv6 and IPv4 Tunnels Specification. Tech. rep., Network Working Group, 1997.

[46] Conta, A., and Deering, S. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6). Tech. rep., Network Working Group, 1995.

[47] Costanzo, A. RFC1505: Encoding Header Field for Internet Messages. Tech. rep., Network Working Group, 1993.

[48] Deering, S., and Hinden, R. Internet Protocol, Version 6 Specification. Tech. rep., Network Working Group, 1997.

[49] Dierks, T. RFC2246: The TLS Protocol Version 1.0. Tech. rep., Network Working Group, 1999.

[50] Dittler, H. P. *IPv6 das neue Internet-Protokoll.* dpunkt.verlag, 1998.

[51] Eberspaecher, J., and Vogel, H. J. *GSM - Global System of Mobile Communication. Vermittlung, Dienste und Protokolle in digitalen Mobilfunknetzen.* Stuttgart: Teubner Verlag, 1997.

[52] Elkins, M. RFC2015: MIME Security with Pretty Good Privacy (PGP). Tech. rep., Network Working Group, 1996.

[53] Ellermann, U. IPv6 und Firewalls. `http://www.cert.dfn.de/team/ue/fw/ipv6fw/home.html`, 1996.

[54] Endres, J. DSL - Die Schnelle Leitung. *c't* (1998).

[55] Endres, J., and Fremerey, F. Volles Rohr. *c't* (1998).

[56] Ennovate. Multiprotocol Label Switching - MPLS. Tech. rep., techguide.com, 1999.

[57] Ernst, N., and Kossel, A. Schnelle Welle. *c't* (1998).

[58] Finlayson, R. RFC2588: IP Multicast and Firewalls. Tech. rep., Network Working Group, 1999.

[59] Fischer, V., and Gogl, H. *ATM - Die Technik des B-ISDN*, vol. 1.1. March 1998.

[60] Fox, B. RFC2685: Virtual Private Networks Identifier. Tech. rep., Network Working Group, 1999.

[61] Galvin, J. RFC1847: Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. Tech. rep., Network Working Group, 1995.

[62] Gärtner, J. Synchrone Digitale Hierarchie. Tech. rep., 1999.

[63] Golmie, N., Saintillan, Y., and Su, D. H. A Review of Contention Resolution Algorithms for IEEE 802.14 Networks. *IEEE Communication Surveys* (1998).

[64] Gombotz, R. Realisierung von Dienstgüten auf kupferbasierten Verteilernetzen am Beispiel von ADSL. Tech. rep., TU-München, Forschungs- und Lehreinheit Informatik XIII, 1998.

[65] Green, T. Intelogis PLUG-IN Technology. Tech. rep., Intelogis, 1998.

[66] Hamzeh, K. RFC2637: Point-to-Point Tunneling Protocol (PPTP). Tech. rep., Network Working Group, 1999.

[67] Hanks, S. RFC1701: Generic Routing Encapsulation (GRE). Tech. rep., Network Working Group, 1994.

[68] Hegering, P. D. H.-G. Management von ATM-Netzen und VLANs. `http://www.gerhardmueller.de/docs/ManagementATM/ManagementATM.html`, September 1997.

[69] Hein, M. *Ethernet*, 2. ed. Internat. Thomson Publ., 1998. ISBN 3-8266-4041-1, Studentenbibliothek Pd Hei P8745T A2 E04.

[70] Hein, M. *TCP/IP Internet-Protokolle im professionellen Einsatz.* Thomson Publishing, 1998.

[71] Hinden, R., and Deering, S. IP Version 6 Adressing Architecture. Tech. rep., Network Working Group, 1998.

[72] Huitema, C. *Routing in the Internet.* Prentice Hall, Englewood Cliffs, NJ, 1995, ch. 4, 5, pp. 65–133.

[73] IEEE. Draft Standard P802.1Q/D9. Tech. rep., IEEE, 1998.

[74] Inc., S. Portbasierende VLAN'S. `http://www.stemmer.de/magazin/artikel/vlans.html`.

[75] Jacobson, V. Modified TCP Congestion Avoidance and Control. `ftp://ftp.isi.edu/end2end/end2end-interest-1990.mail`, April 1990.

[76] Jacobson, V., and Karels, M. J., Eds. *Congestion Avoidance and Control* (November 1988), SIGCOMM '88, SIGCOMM.

[77] Jamin, S., Shenker, S., Zhang, L., and Clark, D. Admission Control Algorithm for Predictive Real-Time Service. In *Proceedings of 3rd International Workshop on Network and Operating System Support for Digital Audio and Video* (November 1992).

[78] JAMOUSSI, B. RFC2340: Nortel's Virtual Network Switching (VNS) Overview. Tech. rep., Network Working Group, 1998.

[79] KALISKI, B. RFC1424: Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services. Tech. rep., Network Working Group, 1993.

[80] KARABEK, M. S. *Data Communications in ATM Networks.* PhD thesis, Technical University of Aachen, July 1998.

[81] KARN, P. RFC1829: The ESP DES-CBC Transform. Tech. rep., Network Working Group, 1995.

[82] KAUFELLS, F.-J. *Lokale Netze*, 11. ed. MITP-Verlag GmbH, 1999. ISBN 3-8266-4059-4, Studentenbibliothek Pd Kau P5357T A11 E02.

[83] KELLY, F. P. Stochastic Models of Computer Communication Systems. *Journal of the Royal Statistical Society B 47* (March 1985), 379–395.

[84] KENT, S. RFC1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management. Tech. rep., Network Working Group, 1993.

[85] KENT, S. RFC2401: Security Architecture for the Internet Protocol. Tech. rep., Network Working Group, 1998.

[86] KENT, S. RFC2402: IP Authentication Header. Tech. rep., Network Working Group, 1998.

[87] KENT, S. RFC2406: IP Encapsulating Security Payload (ESP). Tech. rep., Network Working Group, 1998.

[88] KOBLITZ, N. *A Course in Number Theory and Cryptography.* Springer, 1994.

[89] KOSSEL, A. Teure Umwege. *c't* (1998).

[90] KRAWCZYK, H. RFC2104: HMAC: Keyed-Hashing for Message Authentication. Tech. rep., Network Working Group, 1997.

[91] KRÜGER, G., AND SCHILLER, J. *Vorlesung Mobilkommunikation: Kapitel 4: Drahtlose Telekommunikationssysteme.* Universität Karlsruhe, 1999.

[92] LEECH, M. RFC1928: SOCKS Protocol Version 5. Tech. rep., Network Working Group, 1996.

[93] LEECH, M. RFC1929: Username/Password Authentication for SOCKS V5. Tech. rep., Network Working Group, 1996.

[94] LIN, Y.-D. On IEEE 802.14 Medium Access Control Protocol. *IEEE Communication Surveys* (1998).

[95] LIN, Y.-D., HUANG, C.-Y., AND YIN, W.-M. Allocation and Scheduling Algorithms for IEEE 802.14 and MCNS in Hybrid Fiber Coaxial Networks. *IEEE Communication Surveys* (submitted).

[96] LIN, Y.-D., YIN, W.-M., AND HUANG, C.-Y. Comparing IEEE 802.14 and MCNS Standards for Hybrid Fiber Coaxial Networks. *IEEE Communication Surveys* (submitted).

[97] Linn, J. RFC1421: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. Tech. rep., Network Working Group, 1993.

[98] Lucent. Secure Virtual Private Networks for Enterprise. Tech. rep., February 1999.

[99] Marks, D. R. ATM from A to Z: A Definitive Glossary for Enterprise Network Managers. *Data Communications* (December 1994), 113–122.

[100] Massmann, J., and Yivadinovic, D. Daten im Strom. *c't* (1998).

[101] Mazanec, M. Virtual Private Network unter Linux: FreeS/WAN, IPsec. `http://www.mazanec.com/vpn/`, 1999.

[102] McCann, J., Deering, S., and Mogul, J. Path MTU Discovery for IP version 6. Tech. rep., Network Working Group, 1996.

[103] McMahon, P. RFC1961: GSS-API Authentication Method for SOCKS Version 5. Tech. rep., Network Working Group, 1996.

[104] Metzger, P. RFC1828: IP Authentication using Keyed MD5. Tech. rep., Network Working Group, 1995.

[105] Oehler, M. RFC2085: HMAC-MD5 IP Authentication with Replay Prevention. Tech. rep., Network Working Group, 1997.

[106] Ooms, D., Livens, W., Sales, B., Ramalho, M., Acharya, A., Griffoul, F., and Ansari, F. Framework for IP-Multicast in MPLS. Tech. rep., MPLS Working Group, 1999.

[107] Partridge, C. Using the Flow Label Field in IPv6. Tech. rep., Network Working Group, 1995.

[108] PNNI1.0. Private Network-Network Interface Specification Version 1.0 (PNNI 1.0). Tech. rep., The ATM Forum, Technical Committee, March 1996.

[109] Postel, J. RFC 791 Internet Protocol. Tech. rep., IETF, September 1981.

[110] Postel, J. RFC 793 Transmission Control Protocol. Tech. rep., IETF, September 1981.

[111] Proebster, W. E. *Rechnernetze.* R. Oldenbourg Verlag, 1998.

[112] RFC2328. OSPF Version 2. Tech. rep., Network Working Group, April 1998.

[113] Rigney, C. RFC2058: Remote Authentication Dial In User Service (RADIUS). Tech. rep., Network Working Group, 1997.

[114] Rigney, C. RFC2059: RADIUS Accounting. Tech. rep., Network Working Group, 1997.

[115] Rosen, E. C., Rekhter, Y., Tappan, D., Farinacci, D., Fedorkow, G., Li, T., and Conta, A. MPLS Label Stack Encoding. Tech. rep., Network Working Group, 1999.

[116] Ruffen, D. RFC2643: Cabletron's SecureFast VLAN Operational Model, Version 1.8. Tech. rep., Network Working Group, 1999.

[117] Sandte, H. Streckenerweiterung. *c't* (1998).

[118] SCHILL, A., HESS, R., KÜMMEL, S., HEGE, D., AND LIEB, H. *ATM-Netze in der Praxis*, first edition ed. Addison Wesley, 1997.

[119] SCHMOLL, M., BAUER, D., AND ANDERS, J. Schnelles Kupfer. *c't* (1998).

[120] SCHULTZ, S. SDH Pocket Guide. Tech. rep., Wandel & Goltermann GmbH & Co.

[121] SCHULZKI-HADDOUTI, C. Internet-Renner. *c't* (1998).

[122] SEEBODE, K. Rund um die Welt. *PC Magazin Plus*, 9 (September 1999), 10–12.

[123] SHENKER, S., PATRIDGE, C., AND GUERRIN, R. RFC 2212 Specification of Guaranteed Quality of Service. Tech. rep., IETF, September 1997.

[124] SHENKER, S., AND WROCLAWSKI, J. RFC 2212 General Characterzation Parameters for Integrated Services Network Elements. Tech. rep., IETF, September 1997.

[125] SHILL, A., KÜHN, S., AND BREITNER, F. Internetworking over ATM: Experiences with IP/IPng and RSVP. *Computer Networks and ISDN Systems 28* (1996), 1915–1927.

[126] SIERING, P. Nachgemessen, HDSL, ADSL, Satellit und Kabelmodem im Vergleich. *c't* (1998).

[127] SIMPSON, W. RFC1661: The Point-to-Point Protocol (PPP). Tech. rep., Network Working Group, 1994.

[128] STEVENS, W. R. *TCP/IP Illustrated, Volume 1: The Protocols*, 1 ed. No. ISBN 0-201-63346-9. Addison Wesley, 1994.

[129] STEVENS, W. R. RFC 2001 TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms. Tech. rep., IETF, January 1997.

[130] SWALLOW, G. PNNI: Weaving a Multivendor ATM Network. *Data Communications* (December 1994), 102–110.

[131] SWARS, H. VLAN - virtuelle lokale Netzwerke. `http://www.fh-fulda.de/~klingebiel/nbs-kolloquium/vlan/index.htm`, June 1998.

[132] TANENBAUM, A. S. *Computer Networks*, third edition ed. Prentice Hall, Inc., 1996.

[133] TANENBAUM, A. S. *Computer Networks*, 3 ed. No. ISBN 0-13-349945-6. Prentice Hall PTR, 1996.

[134] TANENBAUM, A. S. *Computer Networks*. Prentice Hall PTR, 1996.

[135] TANENBAUM, A. S. *Computernetzwerke*, third edition ed. Markt & Technik Verlag, 1998.

[136] THAYER, R. RFC2411: IP Security Document Roadmap. Tech. rep., Network Working Group, 1998.

[137] TOWNSLEY, W. RFC2661: Layer Two Tunneling Protocol "L2TP". Tech. rep., Network Working Group, 1999.

[138] UNKNOWN. VIRTUAL PRIVATE NETWORKS. `http://amir.fullerton.edu/msis410/Projects/Group12/vpnpaper.htm`.

[139] UNKNOWN. VPN - Virtual Private Network - Eine Einführung. `http://www.tip.co.at/HTML-Texte/WatchGuard/VPN\%20-\%20Virtual\%20Priva%te\%20Network.htm`, May 1999.

[140] VALENCIA, A. RFC2341: Cisco Layer Two Forwarding (Protocol) "L2F". Tech. rep., Network Working Group, 1998.

[141] WALKE, B. *Mobilfunknetze und ihre Protokolle, Band1: Grundlagen, GSM, UMTS und andere zellulare Mobilfunknetze.* Stuttgart: Teubner Verlag, 1998.

[142] WALKE, B. *Mobilfunknetze und ihre Protokolle, Band2: Buendelfunk, schnurlose Telefonsysteme, W-ATM, HIPERLAN, Satellitenfunk, UPT.* Stuttgart: Teubner Verlag, 1998.

[143] WOLPERT, M. VPN - Virtuelle Private Netze. `http://www.fh-fulda.de/~klingebiel/nbs-kolloquium/vpn/index.htm`, June 1998.

[144] WRIGHT, G. R., AND STEVENS, W. R. *TCP/IP Illustrated, Volume 2: The Implementation*, 1 ed. No. ISBN 0-201-63354-X. Addison Wesley, 1995.

[145] WROCLAWSKI, J. RFC 2211 Specification of th Controlled-Load Network Element Service. Tech. rep., IETF, September 1997.

[146] ZHANG, L., DEERING, S., ESTRIN, D., SHENKER, S., AND ZAPPALA, S. A New Resource ReserVation Protocol. *IEEE Network Magazin* (1993).

[147] ZIFFDAVIS. Netzwerk & Internet: Sicher über IP. `http://www.zdnet.de/technik/artikel/nw199902/ipsec_01wc.html`, February 1999.

[148] ZIMMER, T. Virtuelle private Netze – weltweite LANs. `http://www.uni-karlsruhe.de/~unol/vpn/t15_txt.html`, January 1999.

[149] ZIVADINOVIC, D., AND KOSSEL, A. Megabit-weise Internet. *c't* (1998).

Index