

Unterrichtsmitschrift

Öffentliche Netze und Dienste

Michael Puff

2009-05-24

Oskar-von-Miller Schule Kassel
Fachinformatiker für Anwendungsentwicklung

Vorbemerkung

Zum Inhalt

Dieses Dokument folgt dem Unterrichtsinhalt von Herrn Sobieroj im Fach *Öffentliche Netze und Dienste*. Die eigenen Unterrichtsmitschriften sind durch Texte und Grafiken aus den angegebenen Quellen ergänzt worden.

Diese Ausarbeitung erhebt keinen Anspruch auf Vollständigkeit.

Kontaktmöglichkeiten

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

E-Mail: mail@michael-puff.de

Copyright Hinweis

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

Inhaltsverzeichnis

1	Netzwerktechnik – Grundlagen	7
1.1	Kommunikationsgrundlagen	7
1.2	Datenübertragung	7
1.2.1	Parallele- / Serielle Datenübertragung	7
1.2.2	Simplex-, Halbduplex-und Vollduplex-Betrieb	7
1.2.3	Bits und Baud	8
1.3	Fehlererkennung	8
1.3.1	Echo	8
1.3.2	Parity Check	8
1.3.3	Zyklische Blockprüfung (Cyclic Redundancy Check, CRC)	9
1.4	Modulationsarten	9
1.4.1	Amplitudenmodulation – AM	9
1.4.2	Frequenzmodulation – FM	10
1.4.3	Phasenmodulation – PM	10
1.4.4	Quadraturamplitudenmodulation – QAM	11
2	Eigenschaften von öffentlichen Netzen	13
3	Analoge Telefonie	19
3.1	Funktionsweise eines Telefons	19
3.2	Wahlverfahren	19
3.2.1	Impulswahlverfahren	19
3.2.2	Mehrfrequenzwahlverfahren	20
3.3	Das digitale und analoge Vermittlungsnetz	20
3.3.1	Digitales Vermittlungsstellennetz	21
3.3.2	Ehemaliges analoges Vermittlungsstellennetz	22
3.4	Technologie und Hardware	23
3.5	Verbindungsschema zwischen zwei Anschlüssen	23
4	Digitale Telefonie - ISDN	25
4.1	NTBA / NTPM	25
4.2	Anschlüsse	26
4.2.1	Mehrgeräteanschluss und Anlagenanschluss	26
4.2.2	Basisanschluss und Primärmultiplexanschluss (PMX)	26
4.3	S0-Bus und S0-Frame	27
4.4	Aufbau und Funktion eines ISDN-Endgerätes	29
4.5	Remote Access Service (RAS)	30
5	VoIP	31

5.1	Funktionsprinzip	31
5.2	Gesprächsübertragung	33
5.2.1	Transport der Daten	33
6	Digital Subscriber Line (DSL)	35
6.1	DSL-Grundprinzip	35
6.2	ADSL	36
6.3	VDSL	37
7	Kryptographie	41
7.1	Methoden der Kryptographie	41
7.1.1	Methoden der klassischen Kryptographie	41
7.1.2	Methoden der modernen Kryptographie	42
7.2	Symmetrische Verschlüsselung	43
7.2.1	Verfahren	43
7.3	Asymmetrische Verschlüsselung	43
7.3.1	Verfahren	44
7.4	Hybride Verschlüsselung	44
7.5	Begriffe der sicheren Kommunikation	45
8	Sicherheit von Netzwerken	47
8.1	Sicherheitsanforderungen	47
8.2	Sicherheitsmechanismen und Systeme	47
9	Malware	49
	Literaturverzeichnis	51
	Stichwortverzeichnis	53

1 Netzwerktechnik – Grundlagen

1.1 Kommunikationsgrundlagen

Unter Kommunikation versteht man den Austausch von Informationen. Dabei müssen die Kommunikationspartner über eine physische Verbindung und ein gemeinsames Protokoll, also eine Vereinbarung, wie welche Daten mit welcher Codierung übermittelt werden, verfügen.

1.2 Datenübertragung

1.2.1 Parallele- / Serielle Datenübertragung

Bei der parallelen Datenübertragung werden mehrere Bits gleichzeitig (parallel) übertragen, also auf mehreren physischen Leitungen nebeneinander oder über mehrere logische Kanäle zur gleichen Zeit.

Die Anzahl der Datenleitungen ist nicht festgelegt, wird aber meistens als ein vielfaches von 8 gewählt, so dass volle Bytes übertragen werden können (zum Beispiel 16 Leitungen ergeben 16 Bits = 2 Byte). Häufig werden zusätzliche Leitungen zur Übertragung von Metainformationen wie z. B. einer Prüfsumme (Paritätsbit), Datenflusskontrolle oder eines Taktsignals eingesetzt.

Die parallele Datenübertragung stellt das Gegenteil der seriellen Datenübertragung dar.

Bei der seriellen Datenübertragung werden Daten, sofern sie digital sind, bitweise hintereinander über ein bestimmtes Medium übertragen.

Die Übertragung über eine serielle Schnittstelle kann bitweise (je Zeitschritt ein Bit) oder auch in Bauds oder Baudrate erfolgen z. B. beim Modem. Hierbei ist nicht zwingenderweise 1 Baud mit 1 Bit per second gleichzusetzen.

1.2.2 Simplex-, Halbduplex-und Vollduplex-Betrieb

Mit Duplex (Vollduplex), Halbduplex oder Simplex bezeichnet man in der Kommunikationstechnologie die Richtungsabhängigkeit von Kommunikationskanälen.

- Simplex (SX, gerichteter Betrieb) bedeutet einen Informationstransfer in eine festgelegte Richtung (nur Senden oder Empfangen von Nachrichten), z. B. Radio, Fernsehen oder Pager.

- Halbduplex (HX, wechselseitiger Betrieb) bedeutet, dass Informationen in beide Richtungen fließen können, allerdings nicht gleichzeitig, z. B. Amateurfunk.
- Vollduplex (DX, manchmal auch FDX, gleichzeitiger Betrieb) lässt die Übertragung der Informationen in beide Richtungen zu gleicher Zeit zu, z. B. Telefonie.

[3]

1.2.3 Bits und Baud

Bit/s (bps, „bits per second“): Anzahl der übertragenen Bits pro Sekunde.

Baud: Anzahl der pro Sekunde stattfindenden Signalwechsel.

Die ältesten verwendeten Modulationsverfahren kennen nur zwei Zustände des Trägers, was der Übertragung genau eines Bits je Zustandsänderung entspricht, womit Bit- und Baudrate lange Zeit gleich waren. Neuere Modulationsverfahren erlauben mehr als zwei unterscheidbare Trägerzustände und können so mehrere Bit je Zustandsänderung übertragen. Damit ist eine höhere Bitrate bei gleicher Baudrate möglich.

[4]

1.3 Fehlererkennung

1.3.1 Echo

Bei dieser Art der Fehlererkennung werden die empfangenen Daten zum Empfänger zurück gesendet, der diese dann mit den gesendeten vergleichen kann. Dieses Verfahren erzeugt eine 100%ige Redundanz.

1.3.2 Parity Check

Bei der Parity Check Methode wird ein Prüfbit an die übertragene Bit-Folge angehängen. Dabei gibt es mehrere Möglichkeiten:

Beim Sender werden alle Bits eines Datenblocks modulo N addiert. Entsprechend lassen sich bis zu N Bitfehler erkennen. Für $N=1$ wird die Summe der Einsen (Paritätssumme) im Informationswort berechnet. Ist diese Summe gerade wird bei Even-Parity das Paritätsbit zu Null. Entsprechend ergibt eine ungerade Summe des Informationswortes das Paritätsbit Eins. (Dies gilt umgekehrt bei Odd-Parity.)

Beispiel Even-Parity: Ist für die Datenübertragung Even-Parity (Paritätssumme gerade -> Paritybit: 0, Paritätssumme ungerade -> Paritybit: 1) festgelegt, so gilt für die beiden nachfolgenden Beispiele:

- Das Informationswort 0011.1010 hat vier Einsen. Vier ist eine gerade Zahl, das Paritätskontrollbit ist also die Null, und das resultierende Codewort ist 0011.1010 0.

- Das Informationswort 1010.0100 hat hingegen eine ungerade Paritätssumme und wird in das Codewort 1010.0100 1 codiert.

Der Empfänger addiert die Bits des empfangenen Codewortes ebenfalls und überprüft, ob er denselben Code berechnet hat.

Als Erweiterung der oben dargestellten, eindimensionalen Paritätskontrolle lässt sich auch ein zwei- bzw. höherdimensionales Paritätsverfahren erstellen, welches als Erweiterung nicht nur bestimmte Fehler erkennen kann sondern auch bestimmte Fehlerkombinationen korrigieren kann. Die Paritätskontrolle wird damit zu einem fehlererkennenden und fehlerkorrigierenden Verfahren.

[6]

1.3.3 Zyklische Blockprüfung (Cyclic Redundancy Check, CRC)

Vor Beginn der Übertragung bzw. Kopie eines Blocks der Daten wird ein CRC-Wert berechnet. Nach Abschluss der Transaktion wird der CRC-Wert erneut berechnet. Anschließend werden diese beiden Prüfwerte verglichen. CRC ist so ausgelegt, dass Fehler bei der Übertragung der Daten, wie sie beispielsweise durch Rauschen auf der Leitung verursacht werden könnten, fast immer entdeckt werden.

CRC beruht auf Polynomdivision: Die Folge der zu übertragenden Bits wird als dyadisches¹ Polynom betrachtet. Die Bitfolge der Coderepräsentation der Daten wird durch ein vorher festzulegendes Generatorpolynom (das CRC-Polynom) Modulo (mod) dividiert, wobei ein Rest bleibt. Dieser Rest ist der CRC-Wert. Bei der Übertragung des Datenblocks hängt man den CRC-Wert an den originalen Datenblock an und überträgt ihn mit.

[7]

1.4 Modulationsarten

1.4.1 Amplitudenmodulation – AM

Bei der Amplitudenmodulation (Abb.: 1.1) wird das digitale Signal auf die Trägerfrequenz aufmoduliert.

Es gibt zwei Arten der Modulation:

1. Mathematisch: Trägersignal mit Nutzsignal multiplizieren
2. Praktische Realisierung: Trägersignal mit Nutzsignal addieren (überlagern) danach verzerren und filtern.

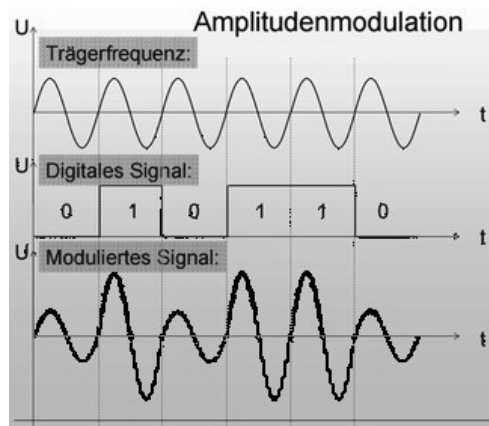


Abb. 1.1: Amplitudenmodulation

Die AM wurde zu Beginn der Rundfunktechnik eingesetzt, weil sich derartig modulierte Signale sehr einfach erzeugen und demodulieren lassen. Ebenfalls zeichnet sie sich durch einen geringen Anspruch an Bandbreite aus. So belegt bei der üblicherweise verwendeten Rundfunk-AM jeder Sender die Bandbreite $2 \cdot 4,5 \text{ kHz} = 9 \text{ kHz}$. Diesen Vorteilen stehen etliche Nachteile wie Störanfälligkeit und schlechter Wirkungsgrad gegenüber, so dass in vielen Anwendungen nun abgewandelte Modulationsverfahren genutzt werden.

[8]

1.4.2 Frequenzmodulation – FM

Die Frequenzmodulation (Abb.: 1.2) ist ein Modulationsverfahren, bei dem die Trägerfrequenz durch das zu übertragende Signal verändert wird. Die Frequenzmodulation ermöglicht gegenüber der Amplitudenmodulation einen höheren Dynamikumfang des Informationssignals. Weiterhin ist sie weniger anfällig gegenüber Störungen. Das Verfahren wurde von J. R. Carson schon 1922 mathematisch korrekt untersucht und von Edwin Howard Armstrong zuerst praktisch umgesetzt.

[9]

1.4.3 Phasenmodulation – PM

Das modulierte Sendesignal kann bei der Phasenmodulation (Abb.: 1.3) allgemein durch eine Sendefrequenz dargestellt werden, deren Frequenz sich nur dann in gewissem Umfang ändert wenn sich die zu übertragene Nutzsignalfrequenz zeitlich verändert. Durch diese Frequenzänderung wird eine Phasenverschiebung vom Sendesignal zur ursprünglichen Sendefrequenz erreicht.

¹dem Zweiersystem zugehörend

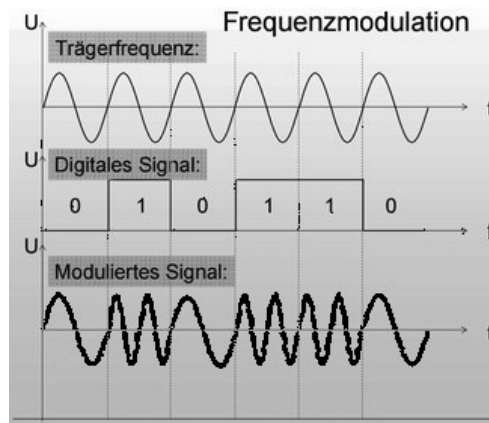


Abb. 1.2: Frequenzmodulation

Bei digitalen Signalen spricht man von Phasenumtastung, engl. Phase Shift Keying. Dabei wird die Phase einer Sinusschwingung (Träger) durch Phasenverschiebung moduliert. Man spricht von binärer Phasenmodulation, wenn zwischen zwei Phasenlagen umgeschaltet (umgetastet) wird. Typischerweise entsprechen die Phasenlagen 0° und 180° den binären Zuständen „0“ und „1“.

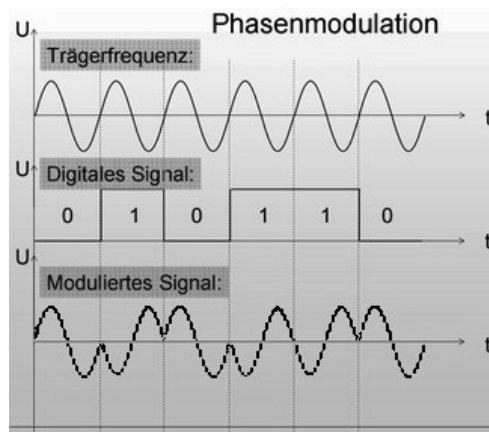


Abb. 1.3: Phasenmodulation

[10]

1.4.4 Quadraturamplitudenmodulation – QAM

Bei der Quadraturamplitudenmodulation (Abb.: 1.4) werden die Amplitudenmodulation und die Phasenmodulation miteinander kombiniert. Dabei werden zwei voneinander unabhängige Signale derselben Trägerschwingung aufgeprägt. Im Prinzip werden die Signale jeweils per Amplitudenmodulation auf einen Träger gleicher Frequenz, jedoch mit um 90° verschobener Phase, moduliert. Anschließend werden die beiden derart modulierten Trägerschwingungen addiert.

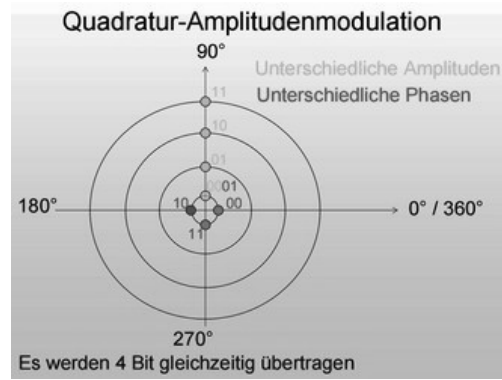


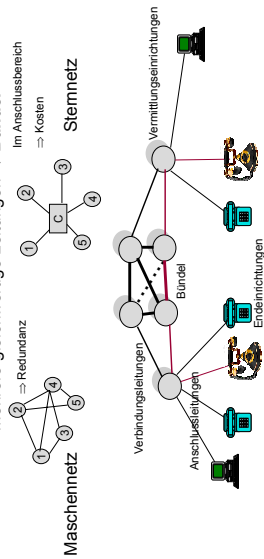
Abb. 1.4: *Quadraturamplitudenmodulation*

[11]

2 Eigenschaften von öffentlichen Netzen

Eigenschaften von Öffentlichen Netzen (1)

- **Netztopologie**
 - **Endeinrichtungen, Netzknoten**
 - **Verbindungsleitungen, Anschlussleitungen**
 - **Verkehrlenkung (Leitweglenkung)**
⇒ Suche nach optimalen Weg
 - **mehrere gleichwertige Leitungen ⇒ Bündel**
Im Anschlussbereich ⇒ Kosten



Öffentliche Netze

W.H.

1

Eigenschaften von Öffentlichen Netzen (2)

- **Anforderungen**
 - Verbindungsmöglichkeit zu einem Teilnehmer muss zu jeder Zeit möglich sein (Ausnahmen in besonderen Fällen).
 - Der Teilnehmer muss das gewünschte Ziel selbst bestimmen können.
 - Das Netz muss eine Vielzahl gleichzeitig existierender Verbindungen ermöglichen.
 - Der notwendige technische Aufwand muss begrenzt werden.

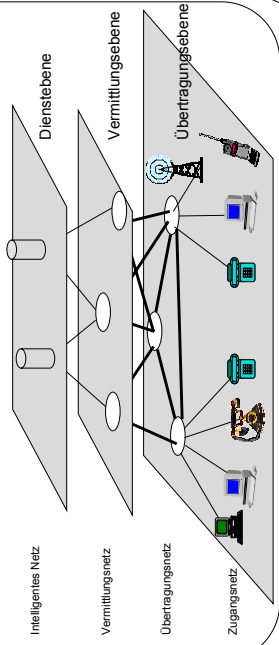
Öffentliche Netze

W.H.

2

Eigenschaften von Öffentlichen Netzen (3)

- **Netzstruktur**
 - **Übertragungsebene** (Kupferkabel, LWL, Funk, Multiplexbetrieb)
 - **Vermittlungsebene** (Vermittlung von Leitungen, Paketen und Zellen, Adressierung von Endeinrichtungen)
 - **Dienstebene** (Adressierung von Diensten, Mehrwertdienste)



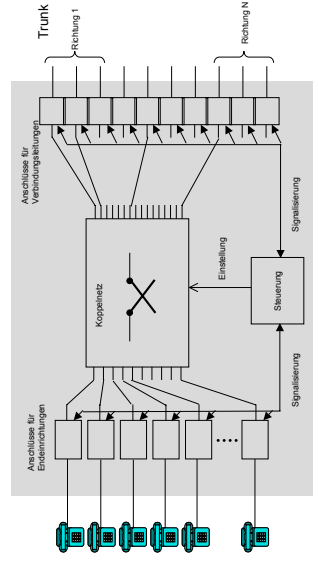
Öffentliche Netze

W.H.

3

Eigenschaften von Öffentlichen Netzen (4)

- **Teilnehmervermittlungsstelle (Beispiel Leitungsvermittlung)**



Öffentliche Netze

W.H.

4

Eigenschaften von Öffentlichen Netzen (5)

- **Übertragungsgeschwindigkeit** (33,3 bit/s – 2,5 Gbit/s ...1000Gbit/s)
- **Übertragungsmedium**
 - Kupferkabelnetze (verdritzt 2 u. 4-Adern)
 - Koaxialkabelnetze (75 Ω analog / 50 Ω digital)
 - Glasfaserkabelnetze (Monomode, Multimode, DWDM – Dense Wavelength Division Multiplexing)
 - Richtfunkstrecken
 - Digitale zelluläre Funknetze
 - Optische Übertragung mit Laser
- **Grad der Dienstintegration**
 - Dienstspezifische Netze (z.B. Telex)
 - Dienstintegrierende Netze (z.B. ISDN)
 - Overlay- Netze



Öffentliche Netze

W.H.

5

Eigenschaften von Öffentlichen Netzen (6)

- **Versorgungsgebiet**
 - Kennzeichen: sehr große Ausdehnung
->Weitverkehrsnetze
 - Ortsnetze
 - Nationale Fernnetze
 - Internationale Netze
- **Öff. Netze von Netzbetreiber verwaltet**
 - Accounting: pro Zeit / pro Datenvolumen
- **Historisch basieren Öff. Netze auf Sprachkommunikation** (Telefonnetz)



Öffentliche Netze

W.H.

6

Eigenschaften von Öffentlichen Netzen (7)

- **Verbindungsarten**
 - festgeschaltete Verbindung
 - Wählverbindung
 - Punkt-zu-Punkt-Verbindung
 - Mehrpunktverbindung (z.B. Polling, Master, Slave)
- **Vermittlung**
 - Leitungsvermittlung (circuit switching)
 - Speicher- oder Paketvermittlung (store and forward or packet switching)
- **Übertragungsarten**
 - Analoge Übertragung (Amplitudenmodulation, Frequenzmodulation, Phasenmodulation)
 - Serielle Digitale Übertragung
- **Betriebsarten**
 - Simplex (sx, Richtungsbetrieb)
 - Halbduplex (hdx, Wechselbetrieb)
 - Duplex (fdx, Gegenbetrieb)



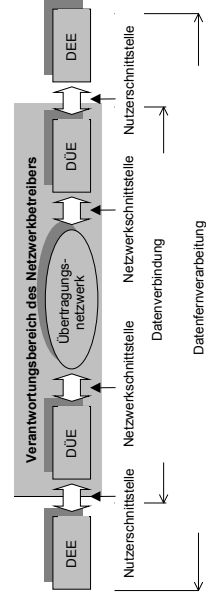
Öffentliche Netze

W.H.

7

Eigenschaften von Öffentlichen Netzen (8)

- **Struktur einer Datenübertragungsstrecke**



Öffentliche Netze

W.H.

8

<div data-bbox="239 1198 758 1870"> <h3>Eigenschaften von Öffentlichen Netzen (9)</h3> <ul style="list-style-type: none"> • Datenübertragungseinrichtungen (DÜE) <ul style="list-style-type: none"> ▪ Analogmodem (FSN) ▪ Datenfernsehgerät DFGT (X.25 Datax-P) ▪ Datenanschlußgerät DAGt (HD) ▪ ISDN-Nt (ISDN) ▪ ADSL-Modem (Internet) ▪ ... • OSI-Modell-Referenzen <ul style="list-style-type: none"> ▪ Schicht 1 (z.B. V.24, X.21) ▪ Schicht 2 (z.B. BSC, HDLC, LAP) ▪ Schicht 3 (z.B. X.25) • Prüfschleifen <ul style="list-style-type: none"> ▪ Schleifentyp 1: DEE-Prüfschleife ▪ Schleifentyp 2: Netzprüfschleife ▪ Schleifentyp 3: Lokale Prüfschleife <p style="text-align: right;">W.H. 9 Öffentliche Netze</p> </div>	<div data-bbox="239 369 758 1041"> <h3>Verbindungskategorien in Öffentlichen Netzen</h3> <p style="text-align: right;">W.H. 10 Öffentliche Netze</p> </div>
<div data-bbox="837 1198 1356 1870"> <h3>Beispiele für Verbindungen in Öffentlichen Netzen</h3> <p style="text-align: right;">W.H. 11 Öffentliche Netze</p> </div>	<div data-bbox="837 369 1356 1041"> <h3>Allgemeine Kennzeichnung von Diensten (1)</h3> <ul style="list-style-type: none"> ▪ Informationstyp <ul style="list-style-type: none"> - Sprache - Text - Daten - Stillbild - Bewegtbild ▪ Kommunikationsart <ul style="list-style-type: none"> - Individualkommunikation - Verteilungskommunikation ▪ Kommunikationsrichtung <ul style="list-style-type: none"> - Monologdienste - Dialogdienste <p style="text-align: right;">W.H. 12 Öffentliche Netze</p> </div>

Allgemeine Kennzeichnung von Diensten (2)

- **Erforderliche Bitraten**
 - Sporadische Meldungen (einige bit/s, Telemetriedienste)
 - Schmalbanddienste (≤ 64 kbit/s, Sprach- und Datendienste)
 - Schmalbanddienste (= n x 64 kbit/s, Stillbildübertragung, Sprachübertragung hoher Güte)
 - Breitbanddienste (einige Mbit/s, Bewegtbildübertragung, Bildfernsprechen)
- **Dienstmerkmale** (Dienstspezifische Nutzungseigenschaften)
- **Dienstübergänge** (Gateways)



Öffentliche Netze

W.H.

13

Dienstarten in Öffentlichen Netzen (1)

- **Trägerdienste (Bearer Services)**
 - Datenübertragungsdienste
 - überdecken nur untere Schichten (max. 1-3) des OSI-Modells (d.h. übertragungsorientiert, transparente Übertragung)
 - Beispiele: Datax-P, ISDN-Datenübertragung, Frame Relay
- **Teledienste (Tele-Services, Unified Services, Standard-Dienste)**
 - netzeigene Anwendungsdienste
 - überdecken ggf. alle 7 Schichten des OSI-Modells
 - Interne Implementierung bleibt für Nutzer transparent
 - Beispiele: Telefon, Telefax, T-Online



Öffentliche Netze

W.H.

14

Dienstarten in Öffentlichen Netzen (2)

- **Umwandlungsdienste (Conversion Services, Gateway Services)**
 - Möglichkeit zur Umwandlung zwischen Diensten
 - Beispiel: Telex-Telefax, T-Online-Telex
- **Zusatzdienste (Mehrwertdienste, Value-Added-Services)**
 - bauen auf Tele- und Trägerdiensten auf
 - Stellen zusätzliche Funktionen / Dienste bereit
 - Beispiele: Weckruf, Fernsteuerung, Televoting



Öffentliche Netze

W.H.

15

(Historische) Teledienste in Deutschland






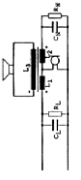

Telex	einfacher Textübertragungsdienst, Fernschreiben
Telefax	Textübertragungsdienst, Bürofernschreiben
Telebox	Mailbox-/E-mail-Dienst
BIX	Informations- und Telekommunikationsdienst, Bildschirmtext
Telefax	Fernkopierdienst
Temex	Dienst zum Fernwirken (Fernanzeigen, Fernmessen, Fernsteuern)
Fernsprechen	Sprachübertragungsdienst



Öffentliche Netze

W.H.

16

<div data-bbox="247 1198 758 1870" style="border: 1px solid black; border-radius: 15px; padding: 10px;"> <h3 style="color: red; text-align: center;">Das Fernsprechnet - Historie</h3> <ul style="list-style-type: none"> - 1861 Erfindung des Telefons von Philipp Reis - 1877 Brauchbares Telefon durch Alexander Graham Bell - 1881 erstes handvermitteltes Fernsprechart in Berlin, 48 Teilnehmer - 1889 Erfindung des Hebdrehwählers - ab ca. 1930 elektromech. Vermittlungsknoten-> analoge Durchschaltensysteme mit autom. Durchwahl (festverdrahteter Steuerung) - ab ca. 1970 rechnergest. Vermittlungsknoten -> analoger Durchschaltung mit automatische Durchwahl, SPC Stored Program Control, Zentrale Steuerung - seit ca. 1980 rechnergest. Vermittlungsknoten -> digitale Durchschaltung mit automatischer Durchwahl, rechnergesteuertes Mehrprozessorsystem - 1988 Einführung ISDN <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 10px;">  Öffentliche Netze W.H. 17 </div> </div>	<div data-bbox="247 369 758 1041" style="border: 1px solid black; border-radius: 15px; padding: 10px;"> <h3 style="color: red; text-align: center;">Hierarchischer Aufbau des Fernsprechnetzes</h3> <ol style="list-style-type: none"> 1. Nebenstellenbereich 2. Ortsnetze 3. nationales Fernnetz 4. internationales Fernnetz <ul style="list-style-type: none"> ▪ Verbindungsleitungen - Frequenzmultiplexleitungen (analog) - Zeitmultiplexleitungen (PCM-Strecken) (digital) ▪ Ortsanschlussleitungen (2 Draht-analog) <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 10px;">  Öffentliche Netze W.H. 18 </div> </div>
<div data-bbox="837 1198 1348 1870" style="border: 1px solid black; border-radius: 15px; padding: 10px;"> <h3 style="color: red; text-align: center;">Fernsprechnet-Topologie</h3> <p style="font-size: small; margin-top: 5px;">Entwicklung: 23 Weitvst. 0 HVSt.</p> <p style="font-size: small; margin-top: 5px;">Restliches Netz: Baumstruktur mit überlagerten Maschenzweigen</p> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 10px;">  Öffentliche Netze W.H. 19 </div> </div>	<div data-bbox="837 369 1348 1041" style="border: 1px solid black; border-radius: 15px; padding: 10px;"> <h3 style="color: red; text-align: center;">Fernsprechdienst und -schnittstelle</h3> <ul style="list-style-type: none"> ▪ Telefonie: internationaler Sprachdienst im Fernsprechnet, Individualdienst ▪ Sprachdienst (300-3400 Hz) ▪ Auskunftsdienst ▪ Auftragsdienst (z.B. Wecken) ▪ Service 130 ▪ Sprachdienst (Voice Mail) ▪ Konferenzverbindungen ▪ Schnittstelle: 2-Draht a/b-Schnittstelle (TAE-Anschlussdose) ▪ Gerätetechnik: Analogtelefon, Impulswahl, Tonwahl <div style="display: flex; justify-content: space-around; align-items: center; margin-top: 10px;">    </div> <div style="display: flex; justify-content: space-between; align-items: center; margin-top: 10px;">  Öffentliche Netze W.H. 20 </div> </div>

3 Analoge Telefonie

3.1 Funktionsweise eines Telefons

In Telefonapparaten wird der Schall durch ein Mikrofon in elektrische Signale gewandelt und beim Empfänger wieder als Schallwelle ausgegeben. Die Schallumwandlung auf der Senderseite kann unter Ausnutzung verschiedener physikalischer Effekte erfolgen. So ändert sich bei einem Kohlemikrofon der elektrische Widerstand unter der Einwirkung von Schallwellen. Ein Piezo-Mikrofon erzeugt unter der gleichen Einwirkung elektrische Spannungen, die in der Mikrofonkapsel gleich verstärkt werden. Mikrofone nach dem elektrostatischen Prinzip (Elektretmikrofon) werden unter anderem von der Fa. Ericsson verwendet. Schließlich erzeugt eine Membran-Spulen-Anordnung unter Ausnutzung der elektromagnetischen Induktion eine Signalspannung.

Auf der Empfangsseite sind Bauteile nach dem Membran-Spule-Prinzip, heute oft auch Lautsprecher (elektrodynamisches Prinzip) eingesetzt. Piezoelektrische Hörkapseln finden ebenso Anwendung. Welche Wandler wo zum Einsatz kommen, hängt vom Baujahr und der Preisklasse des Gerätes ab. Der Frequenzbereich des übertragenen Schalls entspricht nicht dem Bereich, der vom Menschen gehört werden kann, er ist aus Gründen der Wirtschaftlichkeit der Signalübertragung eingeschränkt. Eine ausreichende Silbenverständlichkeit ist trotzdem gegeben. Hierzu wurden in den Anfangszeiten der Fernmeldetechnik umfangreiche Untersuchungen durchgeführt.

[12]

3.2 Wahlverfahren

3.2.1 Impulswahlverfahren

Das Impulswahlverfahren (IWW) ist die heute gebräuchliche Bezeichnung im deutschen Sprachraum für das älteste Signalisierungsverfahren der automatischen Telefonvermittlung.

Früher war es das einzige Wählverfahren und brauchte daher keinen Eigennamen. Heute ist es für analoge Telefonanschlüsse weitgehend vom Mehrfrequenzwahlverfahren (MFV) abgelöst worden.

Durch das Abheben des Telefonhörers beim analogen Endgerät wird zur Vermittlungsstelle eine Stromschleife geschlossen und von der Vermittlungsstelle der Wählton zum Teilnehmer gesendet. Das Betätigen des Nummernschalters unterbricht diese Schleife entsprechend

der gewählten Ziffer: Bei Wahl der Ziffer 1 einmal, bei Ziffer 2 zweimal, ... bei Ziffer 0 zehnmal. Ein einzelner Impuls dauert 100 ms. Die gewählten Ziffern werden auf diese Weise in Wählimpulse umgesetzt, die in der Vermittlungsstelle die Schrittmagnete der Drehwähler ansteuern. Im Telefonhörer ist dies bei manchen Telefonen als eine Folge von Knackgeräuschen zu hören.

Sobald eine etwas längere Pause folgt, wartet die Telefonvermittlung auf die nächste Zahl. Hektisches Betätigen des Gabelumschalters löst daher ebenfalls eine Impulswahl aus. Dies ist der Grund, warum die Notrufnummer von ursprünglich 111 auf 110 umgestellt wurde, da es öfter vorkam, dass durch mehrmaliges Betätigen des Gabelumschalters dreimal ein Impuls abgegeben und somit die Notrufnummer gewählt wurde. Dies konnte mit 110 vermieden werden, da für die Null zehn Impulse benötigt werden.

[13]

3.2.2 Mehrfrequenzwahlverfahren

Ein Wählsignal wird in MFV durch eine Überlagerung zweier sinusförmiger Tonsignale repräsentiert, die von der Vermittlungsstelle erkannt werden.

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Tab. 3.1: MFV-Tastenbelegung

Jede Zeile repräsentiert einen tiefen Ton, jede Spalte einen hohen. Wenn die Taste „5“ gedrückt wird, ergibt sich also ein Ton aus der Überlagerung der Tonfrequenzen 1336 und 770 Hz. Damit die Vermittlungseinrichtung die gedrückte Taste sicher erkennen kann, sollte die Dauer des Tones mindestens 70 Millisekunden betragen.

Die Generierung der MFV-Töne mittels zweier Sinusgeneratoren für die Spalten- und Zeilenfrequenz ist verhältnismäßig einfach. Zur Detektion der einzelnen Frequenzen wird meist der Goertzel-Algorithmus angewendet, ein Algorithmus zum Erkennen einzelner Tonfrequenzen (Spektralkomponenten) basierend auf der diskreten Fourier-Transformation.

[14]

3.3 Das digitale und analoge Vermittlungsnetz

Linien:

grüne Linien = Sprachkanäle

rote Linien = SS7-Signalisierungsstrecken

blaue Linien = Datenstrecken

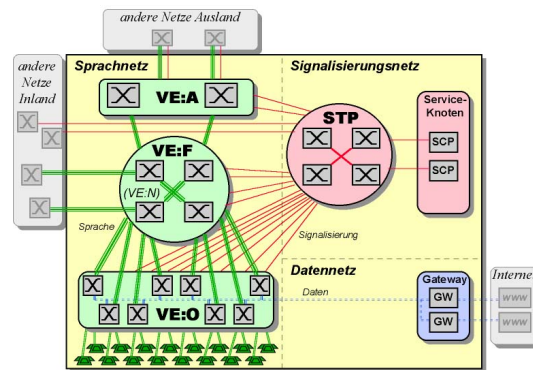


Abb. 3.1: Struktur des Festnetzes

Abkürzungen:

GW = Internet Gateway

STP = Signalling Transfer Point

SCP = Service Control Point

VE:A = Vermittlungseinheit Ausland, Auslandsvermittlungsstelle

VE:F = Vermittlungseinheit Fernverkehr, Fernvermittlungsstelle

VE:N = Vermittlungseinheit mit Netzübergangsfunktionen

VE:O = Vermittlungseinheit Ortsnetz, Ortsvermittlungsstelle

WWW = Internet-Server

3.3.1 Digitales Vermittlungsstellennetz

Heutige Telefonnetze haben im Gegensatz zu früheren keine ausgeprägte hierarchische Struktur mehr. So sind zum Beispiel im Netz der Deutschen Telekom von den ehemals vier Hierarchieebenen nur noch zwei übrig geblieben.

Fernvermittlungsstellen bilden die oberste Ebene. Diese Vermittlungsstellen sind stark miteinander vermascht. Diese Vermittlungsstellen besitzen oft Netzübergangsfunktionen, um Gespräche aus dem eigenen Netz in die Netze anderer nationaler Telefongesellschaften weiterleiten zu können.

Als Durchgangsvermittlungsstelle bezeichnet man Vermittlungsstellen, die nur Verkehr zwischen Vermittlungsstellen abwickeln, an die aber in der Regel keine Teilnehmer angeschlossen sind. Fernvermittlungsstellen sind Durchgangsvermittlungsstellen.

Auslandsvermittlungsstellen vermitteln den Verkehr zwischen unterschiedlichen Ländern. Auslandsvermittlungsstellen sind an Fernvermittlungsstellen angeschlossen. Sie haben innerhalb des eigenen Netzes keine Vermittlungsfunktion.

Ortsvermittlungsstellen bilden die unterste Ebene. Sie verwalten die Kundenanschlüsse. Mehrere Ortsvermittlungsstellen sind sternförmig an eine Fernvermittlungsstelle angeschlossen.

Eine Ortsvermittlungsstelle kann, je nach Ausbauzustand, 10.000 bis über 100.000 Teilnehmer verwalten. In großen Städten können somit mehrere Ortsvermittlungsstellen existieren. Die Identifizierung von Ortsvermittlungsstellen durch die ersten 1-3 Ziffern einer Rufnummer ist häufig noch vom ehemaligen analogen Vermittlungsnetz übernommen worden, es bedeutet, die Rufnummern eines Stadtteils beginnen immer mit identischen 1.-3. Ziffern. Eine Zuordnung bestimmter Rufnummernbereiche zu einer Vermittlungsstelle ist heute nicht mehr in allen Fällen eindeutig möglich. Zum einen werden neu vergebene Nummern nicht mehr geographisch verteilt, stattdessen werden in Deutschland die Rufnummern inzwischen blockweise an die Telefonanbieter vergeben. Zum anderen kann durch einen Umzug die Rufnummer geografisch portiert werden, also in ein fremden Rufnummernbereich mitgenommen werden. Mit Wegfall des zugehörigen Anschlusses kehrt die geografische portierte Rufnummer jedoch wieder in den ursprünglichen Vermittlungsstellenbereich zurück.

3.3.2 Ehemaliges analoges Vermittlungsstellennetz

Da jede gewählte Ziffer einer Rufnummer im analogen Netz einzeln ausgewertet wurde, war es notwendig das Netz hierarchisch aufzubauen.

Die unterste Ebene bestand im Wesentlichen aus einer oder mehreren Orts- bzw. Endvermittlungsstellen, wobei jeder Vermittlungsstelle eine oder mehrere Ziffern zugeordnet waren.

Die Ziffern 1 bis 8 waren den einzelnen Bereichen einer OVSt bzw. den EVSt'n zugeordnet; war die erste Ziffer jedoch eine 1, so konnte auf sie keine weitere 1 folgen, es sei denn, es handelte sich um eine Notruf- oder Sonderrufnummer. Zum Beispiel konnte eine VSt mit den Ziffern 2 und 3 für die Kernstadt vorgesehen sein, die 5 und 6 mit einer weiteren VSt für Stadtteile im Westen und Norden, die 7 für einen Stadtteil im Osten der Stadt und die 8 für eine angrenzende Ortschaft - ebenfalls mit eigener VSt. Diese Aufteilung hielt die Leitungslänge zu den Teilnehmern in vertretbaren Grenzen.

Durch Wahl der 0 als erste Ziffer wurde eine Verbindung in das Fernvermittlungsstellennetz (FVSt) aufgebaut, das aus drei Hierarchieebenen bestand:

1. Zentralvermittlungsstellen (ZVSt)
2. Hauptvermittlungsstellen (HVSt)
3. Knotenvermittlungsstellen (KVSt)

Die Ortsvermittlungsstellen (OVSt) gehörten nicht mehr zum Fernnetz.

Die zweite Ziffer einer Vorwahl baute eine Verbindung zur obersten Hierarchieebene (ZVSt) auf, außer es handelte sich um eine weitere 0, denn dann wurde eine Verbindung zur Auslandsvermittlungsstelle hergestellt.

Die auf die 0 folgenden Ziffern führten weiter durch die Hierarchieebenen über HVSt (3. Ziffer) und KVSt (4. Ziffer) bis zur OVSt (5. Ziffer).

Aufgrund der vorhandenen Ziffern (0 bis 9) war die Anzahl der ZVStn vorgegeben.

- 1: kein Zentralvermittlungsbereich, wurde für Sondernummern reserviert
- 2: Düsseldorf

- 3: Berlin
- 4: Hamburg
- 5: Hannover
- 6: Frankfurt am Main
- 7: Stuttgart
- 8: München
- 9: Nürnberg
- 0: Verkehrsausscheidungsziffer

Jede ZVSt konnte bis zu 10 HVStn (Hauptvermittlungsstelle) und diese wiederum bis zu 10 KVStn (Knotenvermittlungsstelle) versorgen, was sich ebenfalls aus dem vorhandenen Ziffernkontingent von 0 bis 9 erklärt.

Beispiel

Ein Teilnehmer im Ortsnetz Bad Zwischenahn hatte die Rufnummer 04403/xxxx: Die erste 4 baute einen Verbindungsweg über Hamburg (ZVSt) auf. Die zweite 4 führte diesen Verbindungsweg weiter zur HVSt in (Oldenburg) und die dann folgende 0 leitete eine Verbindung zur KVSt (in diesem Beispiel ebenfalls am Standort Oldenburg) ein. Durch Wahl der Ziffer 3 war die Verbindung zur OVSt Bad Zwischenahn vollständig aufgebaut und die Auswertung der Ortsrufnummer begann.

Wenn aber ein Teilnehmer zum Beispiel aus dem Ortsnetz Rastede, das die Vorwahl 04402 besitzt, diese Rufnummer in Bad Zwischenahn erreichen wollte, so war es unwirtschaftlich, den hierarchischen Weg über Hamburg zu belegen. Für solche Ziele wurden Querverbindungswege eingerichtet. In diesem Beispiel waren beide Ortsnetze an derselben KVSt (440 - Oldenburg) angeschlossen und der Verbindungsweg wurde nur über Oldenburg etabliert.

Querverbindungswege wurden nach wirtschaftlichen Gesichtspunkten eingerichtet und haben das in oberster Ebene existierende Maschennetz zwischen den ZVStn auf den Ebenen der HVStn und KVStn weiter verfeinert. Bei häufigem Telefonverkehr zwischen zwei Ortsnetzen gab es auch Querverbindungswege zwischen den OVStn, so dass kein hierarchischer Verbindungsaufbau mehr notwendig war.

[15]

3.4 Technologie und Hardware

3.5 Verbindungsschema zwischen zwei Anschlüssen



Abb. 3.2: Verbindungsschema zwischen zwei Anschlüssen

Abkürzungen:

TAE = Telefon-Anschlusseinheit

IAE = ISDN-Anschlusseinheit

UAE = Universelle-Anschlusseinheit

HA = Hausanschluss

SV = Strassenverteiler

OvSt = Ortsvermittlungsstelle

FvSt = Fernvermittlungsstelle

4 Digitale Telefonie - ISDN

ISDN steht für *Integrated Services Digital Network*, zu deutsch „Integriertes Sprach- und Datennetz“. Mittels ISDN werden verschiedene Dienste in einem Datennetz zusammengefasst. Vor der Einführung von ISDN gab es für jeden Dienst, wie Fernschreiber, FAX und Telefonie, eigene Netze, die mittels Gateways verbunden wurden. Durch die Digitalisierung ergibt sich auch für die Telefonie ein erweiterter Funktionsumfang und eine höhere Datenübertragungsrate.

Der Hauptunterschied zur analogen Telefonie besteht darin, dass die Signale digital übertragen werden bis zum Endgerät. daraus resultieren mehrer Vorteile:

- Übertragung mehrerer Kanäle
- Mehrere Rufnummern für einen Anschluss (*Multiple Subscriber Number*, MSN)
- MSN kann mittels der Dienstkennung für verschiedene Anwendungen genutzt werden
- Bereitstellung von vermittlungstechnischen Leistungsmerkmalen über separaten Datenkanal
- Verlustfreie Übertragung durch digital Technik
- Schnellere Datenübertragung, da kein Modem zwischen geschaltet

Allerdings besteht der Nachteil, dass ein einfaches schnurgebundenes Telefon ohne eigenständige Stromversorgung nicht vorgesehen ist. Hinzukommt, dass wenn man ein analoges Telefon anschliessen will, man einen a/b-Wandler (Terminaladapter, TA) oder eine ISDN-Anlage mit analogen Nebenstellenanschlüssen benötigt.

4.1 NTBA / NTPM

Um ein ISDN-Gerät mit der örtlichen Vermittlungstelle zu verbinden, ist eine so genannter *Netzwerk Terminierungs Basiseinheit* (NTBA) bzw. NTPM bei einem PMS¹-Anschluss, installiert sein. Der NTBA verbindet das zweiadrige Bussysteme der Vermittlungstelle mit dem vieradrigen (S0/S2M) Bussystem der ISDN-Endgeräte (Abb.: 4.1).

¹Mehrgeräteanschluss

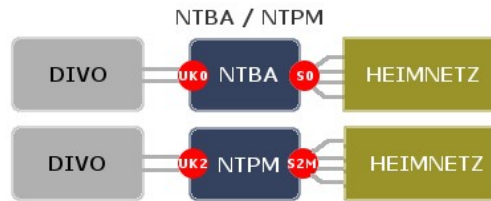


Abb. 4.1: Verbindung der Vermittlungsstelle mittels NTBA / NTPM mit dem Heimnetz

4.2 Anschlüsse

4.2.1 Mehrgeräteanschluss und Anlagenanschluss

Ein Mehrgerätanschluss (Point-to-Multipoint) bezeichnet einen Anschluss, bei dem die Endgeräte (bis zu acht) direkt an dem NTBA angeschlossen sind, während hingegen bei einem Anlagenanschluss die Endgeräte über eine Telefonanlage angeschlossen werden (Abb.: 4.2).

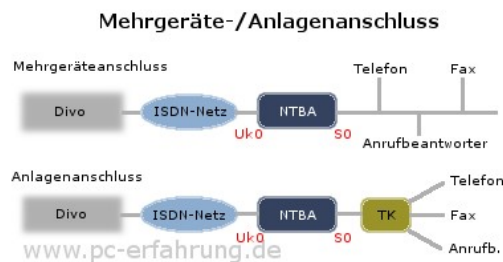


Abb. 4.2: Schema eines Mehrgeräte- bzw. Anlagenanschlusses

4.2.2 Basisanschluss und Primärmultiplexanschluss (PMX)

Basisanschluss bzw. Primärmultiplexanschluss bezeichnen Leistungsmerkmale des Dienstbieters.

Beim Basisanschluss (Abb.: 4.3) ermöglichen es zwei so genannte B-Kanäle zwei Dienste gleichzeitig in Anspruch zu nehmen. Man kann also zum Beispiel auf dem einem Kanal telefonieren und auf dem anderen Kanal im Internet surfen oder zwei Telefonate gleichzeitig führen. Ein B-Kanal verfügt über eine Bandbreite von 64 KBit/s, welche durch Kanalbündelung auf 128 KBit/s verdoppelt werden können.

Leistungsmerkmale eines Basisanschlusses:

- Verfügbar als Mehrgeräte- und Anlagenanschluss
- B-Kanäle: 2 (2×64 KBit/s)
- D-Kanal: 1 (16 KBit/s)
- Analogeschnittstelle: UK0
- Maximale Bandbreite: 192 KBit/s (3×64 KBit/s)

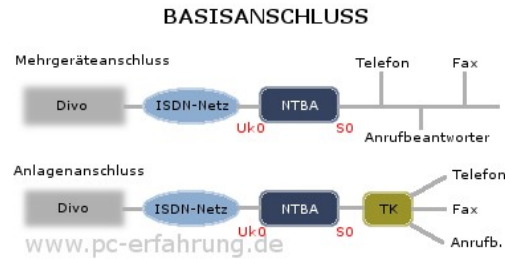


Abb. 4.3: Schema eines Basisanschlusses

Der Primärmultiplexanschluss (Abb.: 4.4) bietet 16 bis 30 Nutzkanäle (B-Kanäle) und ist nur als Anlagenanschluss verfügbar. Es wäre auch ein Mehrgeräteanschluss technisch möglich, was aber wenig Sinn macht, da maximal acht Endgeräte angeschlossen werden könnten und so die restlichen Nutzkanäle ungenutzt bleiben würden.

Leistungsmerkmale eines Primärmultiplexanschlusses:

- Verfügbar als Anlagenanschluss
- B-Kanäle: 16 - 30 (64 KBits/s)
- D-Kanäle: 1 (64 KBit/s)
- Synchronisationskanal: 1 (64 KBit/s)
- Analoge Schnittstelle: UK2
- Digitale Schnittstelle: S2M
- Maximale Bandbreite: 2048 KBit/s (32×64 KBit/s)



Abb. 4.4: Schema eines Primärmultiplexanschlusses

4.3 S0-Bus und S0-Frame

Der S0-Bus (Abb.: 4.5) ist das interne Bussystem, an dem die ISDN-Geräte angeschlossen werden.

Leistungsmerkmale des S0-Busses:

- Maximal 12 UAE²-Anschlussdosen
- Maximal 8 Endgeräte
- Maximal 4 passive Endgeräte (ohne eigenen Stromversorgung)
- Maximale Buslänge von NTBA zum UAE: 150 m
- Empfohlene Länge von UAE zum Endgerät: 10 m
- Muss mit zwei 100 Ω Widerständen terminiert werden



Abb. 4.5: Schema des S0-Busses

Die Daten werden über den S0-Bus in so genannten Frames übertragen. In einem Frame werden die zu übertragenden Daten zusammengesetzt, die dann als Frame übertragen werden (Abb.: 4.6).

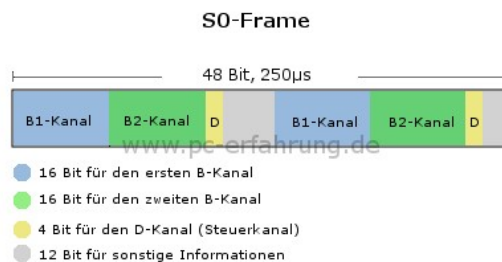


Abb. 4.6: Schema des S0-Frames

Ein S0-Frame ist 48 Bit groß, wobei 32 Bit die beiden B-Kanäle, 4 Bit der D-Kanal und die restlichen zwölf andere Steuerkanäle in Anspruch nehmen. 4000 Frames werden pro Sekunde übertragen, was einer Übertragungszeit eines einzigen Frames von $250 \mu\text{s}$ entspricht. Es gibt keine „halben“ Frames.

- Länge: 48 Bit
- Übertragung: 4000 mal pro Sekunde
- davon B-Kanal: 32 Bit (2×16 Bit)
- davon D-Kanal: 4 Bit
- davon Steuerbefehle: 12 Bit
- Übertragungsfrequenz: $250 \mu\text{s}$

Aufgaben

Aufgabe 1:

RAS-Verbindung vom Client zum Server wird über einen D-Kanal gesteuert und überwacht. Ein Befehl der Schicht 3 (D-Kanal) hat ein Datenvolumen von 765 Bit. Berechnen Sie die Zeit, die benötigt wird, um diese Daten in der Schicht zu übertragen.

In einem S0-Frame werden 4 Bits für den D-Kanal übertragen. Ein Frame benötigt $250 \mu\text{s}$ für die Übertragung. Daraus folgt die Rechnung:

²Universal-Anschluss-Einheit

$$\frac{765 \text{ Bit}}{4 \text{ Bit}} = 191,25 \rightarrow 192 \text{ Frames} \quad (4.1)$$

$$192 \times 250 \mu\text{s} = 48000 \mu\text{s} = \underline{48 \text{ ms}} \quad (4.2)$$

Aufgabe 2:

Wie lange dauert die Übertragung von 1 MB über den B-Kanal?

In einem S0-Frame werden 16 Bits für den B-Kanal übertragen. Ein Frame benötigt 250 μs für die Übertragung. Daraus folgt die Rechnung:

$$1 \times 1024 \times 1024 \times 8 \text{ Bit} = 8388608 \text{ Bit} \quad (4.3)$$

$$\frac{8388608 \text{ Bit}}{16 \text{ Bit}} = 524288 \text{ Frames} \quad (4.4)$$

$$524288 \times 250 \mu\text{s} = 131072000 \mu\text{s} = 131072 \text{ ms} = \underline{131,072 \text{ s}} \quad (4.5)$$

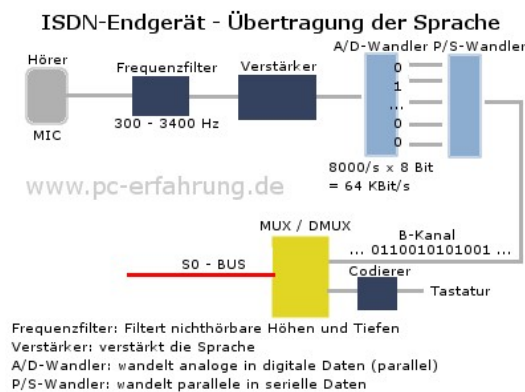
4.4 Aufbau und Funktion eines ISDN-Endgerätes

Abb. 4.7: Schema eines ISDN-Telefons

Abbildung 4.7 zeigt den groben Aufbau eines ISDN-Telefongerätes. Wenn eine Person in das Mikrophon des Telefons spricht, werden die analogen Daten von dem Frequenzfilter verarbeitet. Dieser sorgt dafür, dass die nichthörbaren Höhen und Tiefen herausgefiltert werden, ähnlich dem Verfahren der MP3-Kompression. Somit werden die Sprachdaten auf das „wesentliche“ reduziert. Im anschließenden Schritt verstärkt ein Verstärker diese wesentlichen Sprachdaten, damit sie besser verarbeitet werden können.

Nachdem die analogen Sprachdaten vorbereitet wurden, werden sie von einem Analog/Digital-Wandler in digitale Daten umgewandelt. Vorerst liegen die Daten parallel vor, es führen also 8 Adern von A/D-Wandler zum Parallel-/Seriell-Wandler. Letzterer hat nun die Aufgabe, diese Daten an den seriellen Bus zu leiten. Beim A/D-Wandler wird auch die Bandbreite des

B-Kanals deutlich, denn der A/D-Wandler verfügt über eine Abtastrate von 8000/s, was eine Datenmenge von $8000/s \cdot 8 \text{ Bit} = 64.000 \text{ Bit/s} = 64 \text{ KBit/s}$ ergibt.

Die nun digitalen Sprachdaten (B-Kanal) und die Steuersignale wie beispielsweise Tasteingaben (D-Kanäle) werden nun vom Multiplexer verarbeitet. Dieser schaltet je nachdem eine der beiden Leitungen und baut somit nach und nach einen S0-Frame auf, so dass diese dann über den S0-Bus auf die Reise geschickt werden können.

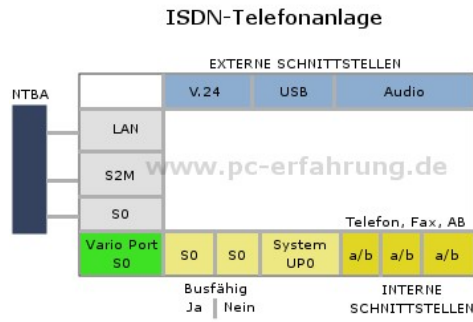


Abb. 4.8: Schema einer ISDN-Telefonanlage

4.5 Remote Access Service (RAS)

Mittels des *Remote Access Services* ist es möglich sich mittels eines Modems, ISDN oder X.25 in ein fremdes Netz einzuwählen.

Die Sicherheit wird durch folgende Punkte gewährleistet:

- MSN prüfen: Nur bestimmte Nummern dürfen sich einwählen
- Call-Back: Der Server ruft den Teilnehmer zurück, um Missbrauch von MSN-Nummern zu gewährleisten.
- Passwortabfrage: Server fragt Passwort ab. Hier gibt es auch eine Time-Out-Funktion, um Hacker-Attacken zu verhindern.

[2]

5 VoIP

Unter der IP-Telefonie, eine Kurzform für die Internet-Protokoll-Telefonie, auch Internet-Telefonie oder Voice over IP (kurz VoIP) genannt, versteht man das Telefonieren über Computernetzwerke, welche nach Internet-Standards aufgebaut sind. Dabei werden für Telefonie typische Informationen, d. h. Sprache und Steuerinformationen beispielsweise für den Verbindungsaufbau, über ein auch für Datenübertragung nutzbares Netz übertragen. Bei den Gesprächsteilnehmern können sowohl Computer, auf IP-Telefonie spezialisierte Telefonendgeräte, als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung ins Telefonnetz herstellen.

IP-Telefonie ist eine Technologie, die es ermöglicht, den Telefondienst auf dieser IP-Infrastruktur zu realisieren, so dass diese die herkömmliche Telefontechnologie samt ISDN, Netz und allen Komponenten ersetzen kann. Zielsetzung dabei ist eine Reduzierung der Kosten durch ein einheitlich aufgebautes und zu betreibendes Netz. Aufgrund der hohen Einsatzdauer klassischer Telefonesysteme und der notwendigen Neuinvestitionen für IP-Telefonie wird der Wechsel bei bestehenden Anbietern oft als lang andauernder, gleitender Übergang realisiert. Währenddessen existieren beide Technologien parallel (sanfte Migration). Daraus ergibt sich ein deutlicher Bedarf an Lösungen zur Verbindung beider Telefonesysteme (z. B. über VoIP-Gateways) und die Notwendigkeit zur gezielten Planung des Systemwechsels unter Berücksichtigung der jeweiligen Möglichkeiten für Kosten- und Leistungsoptimierung.

5.1 Funktionsprinzip

Das Telefonieren mit der IP-Telefonie kann sich für den Teilnehmer genauso darstellen wie in der klassischen Telefonie. Wie bei der herkömmlichen Telefonie teilt sich das Telefongespräch hierbei in drei grundsätzliche Vorgänge auf. Diese Vorgänge sind der Verbindungsaufbau, die Gesprächsübertragung und der Verbindungsabbau. Im Unterschied zur klassischen Telefonie werden bei VoIP aber keine dedizierten „Leitungen“ durchgeschaltet, sondern die Sprache wird digitalisiert und in kleinen Daten-Paketen transportiert.

Der Auf- und Abbau von Rufen (Rufsteuerung) erfolgen über ein von der Sprachkommunikation getrenntes Protokoll. Auch die Aushandlung und der Austausch von Parametern für die Sprachübertragung geschehen über andere Protokolle als die der Rufsteuerung.

Um in einem IP-basierten Netz eine Verbindung zu einem Gesprächspartner herzustellen, muss die aktuelle IP-Adresse des gerufenen Teilnehmers innerhalb des Netzes bekannt sein, jedoch nicht notwendigerweise auf der Seite des Anrufers. Geographisch feste Anschlüsse wie im Festnetz gibt es in rein IP-basierten Netzen nicht. Die Erreichbarkeit des Angerufenen wird, ähnlich wie in Mobilfunknetzen, durch eine vorangegangene Authentifizierung des

Gerufenen, und einer damit verbundenen Bekanntmachung seiner momentanen Adresse, ermöglicht. Insbesondere kann dadurch ein Anschluss unabhängig vom Aufenthaltsort des Nutzers genutzt werden.

Aufgrund z. B. von Ortswechsel des Teilnehmers, Wechsel des Users am gleichen PC oder der dynamischen Adressvergabe beim Aufbau einer Netzwerkverbindung ist eine feste Zuordnung von Telefonnummern zu IP-Adressen nicht möglich. Die allgemein angewandte Lösung besteht darin, dass die IP-Telefonie-Teilnehmer bzw. deren Endgeräte ihre aktuelle IP-Adresse bei einem Dienstrechner (Server) unter einem Benutzernamen hinterlegen. Der Verbindungsrechner für die Rufsteuerung, oder manchmal sogar das Endgerät des Anrufers selbst, kann dann bei diesem Server die aktuelle IP-Adresse des gewünschten Gesprächspartners über den angewählten Benutzernamen erfragen und damit die Verbindung aufbauen.

Verbindungsaufbau mit SIP

Ein verbreitetes Signalisierungsprotokolle ist das Session Initiation Protocol (SIP).

Die Teilnehmer besitzen bei SIP eine SIP-Adresse (ähnlich einer E-Mail-Adresse) im Uniform-Resource-Identifier-Format (URI-Format), wie zum Beispiel „sip:12345@beispiel-server.de“. SIP-Endgeräte müssen sich einmalig während der Startphase bei einem SIP-Registrar-Server registrieren. Zum Aufbau einer Verbindung schickt das Endgerät des Anrufers eine Nachricht an diesen Server, der dem DNS unter dem Domainnamen „beispiel-server.de“ bekannt ist. Dieser Verbindungswunsch wird durch den Server an das Endgerät des Angerufenen weitergeleitet. Sofern diese Nachricht dort verarbeitet werden kann, schickt das Endgerät eine entsprechende Nachricht zurück an den Server, der diese an den Anrufer weiterleitet. Zu diesem Zeitpunkt klingelt das Endgerät des Angerufenen, der Anrufer hört ein Freizeichen.

Eine direkte Kommunikation zwischen den beiden Endgeräten hat bis jetzt noch nicht stattgefunden. Im Rahmen dieses Austauschs zum Aufbau einer Session werden zwischen den Endgeräten alle relevanten Informationen über Eigenschaften und Fähigkeiten ausgetauscht. Für das eigentliche Telefongespräch ist der Server nicht mehr notwendig, die Endgeräte senden sich ihre Daten direkt zu, d. h., der Datenaustausch im Rahmen des Gespräches läuft am Server vorbei. Für die Übertragung dieser Daten in Echtzeit wird üblicherweise das Real-Time Transport Protocol (RTP) eingesetzt.

Zur Beendigung des Gesprächs sendet eines der Endgeräte eine SIP-Nachricht an den Server, der diese an den anderen Teilnehmer weitergibt. Beide Endgeräte beenden dann die Verbindung.

Neben dem SIP Protokoll zum Verbindungsaufbau gibt es noch verschiedene Rufnummernsysteme.

5.2 Gesprächsübertragung

Wie bei herkömmlicher Telefonie werden die akustischen Signale der Sprache zunächst analog mit einem Mikrofon in elektrische Signale gewandelt. Diese analogen elektrischen Signale werden dann digitalisiert (kodiert). Optional können sie auch komprimiert werden, um die zu übertragende Datenmenge zu reduzieren. Der Transport der so umgewandelten Daten erfolgt dann über ein öffentliches oder privates Telekommunikationsnetz. Bedingt durch das für den Transport verwendete Verfahren der Paketvermittlung werden die Daten dazu in viele kleine Pakete aufgeteilt.

5.2.1 Transport der Daten

Im Normalfall schickt jedes Endgerät die codierten Sprachdaten unabhängig von der Signalisierung direkt über das Netzwerk an die IP-Adresse der Gegenstelle. Die Gesprächsdaten fließen also nicht über Server eines VoIP-Providers.

Der eigentliche Transport der Daten erfolgt über das Real-Time Transport Protocol (RTP), gesteuert durch das Real-Time Control Protocol (RTCP). RTP verwendet zur Übertragung in der Regel das User Datagram Protocol (UDP). UDP kommt zum Einsatz, da es ein minimales, verbindungsloses Netzwerkprotokoll ist, das nicht auf Zuverlässigkeit ausgelegt wurde wie beispielsweise das Transmission Control Protocol (TCP). Dies bedeutet, dass der Empfang der Sprachpakete nicht bestätigt wird, also keine Übertragungsgarantie besteht. Der Vorteil von UDP ist aber dessen geringere Latenzzeit gegenüber der von TCP, da nicht auf eine Bestätigung gewartet und fehlerhafte Pakete nicht neu gesendet werden und sich somit der Datenfluss insgesamt nicht zusätzlich verzögert. Eine vollkommen fehlerfreie Übertragung ist aufgrund der hohen Redundanz gesprochener Sprache und der Fähigkeit der verwendeten Codecs, Fehler zu korrigieren, unnötig. Für ein flüssiges Gespräch ist eine geringe Laufzeit viel wichtiger.

[29]

6 Digital Subscriber Line (DSL)

DSL steht für *Digital Subscriber Line*¹ und bezeichnet eine Reihe Übertragungsstandards der Bitübertragungsschicht, mit der Daten mit hohen Übertragungsraten über einfache Kupferleitungen wie die Teilnehmeranschlussleitung gesendet und empfangen werden können. Der Standard dient zur Kommunikation zwischen DSL-Modem und DSLAM², um in der Regel einen Breitband-Internetzugang über einen Internet-Zugangsserver zur Verfügung zu stellen. Die eigentliche Verbindung wird über beliebige Protokolle der weiteren Schichten hergestellt. Als Sicherungsschicht ist Ethernet oder ATM³, als Vermittlungsschicht IP üblich. Über diese Verbindung wird der Internet-Zugangsserver des Providers erreicht, der einen Internetzugang über authentifizierte Verbindungen ermöglicht.

6.1 DSL-Grundprinzip

DSL unterscheidet sich von einer herkömmlichen Internetverbindung über analoge Telefonanschlüsse (POTS⁴) oder ISDN dadurch, dass für die Datenübertragung ein weitaus größerer Frequenzbereich genutzt wird, was eine vielfach höhere Geschwindigkeit ermöglicht; die Reichweite des Signals ist durch dieses große Frequenzband jedoch stark eingeschränkt.

Bei den üblicherweise für die Privatkunden-Vermarktung vorgesehenen DSL-Varianten wie ADSL, wird der für die Festnetztelefonie verwendete Frequenzbereich ausgespart, womit DSL parallel zum normalen Telefon genutzt werden kann. Fax, analoges Telefon oder ISDN stehen auch während des DSL-Betriebs zur Verfügung. Dadurch ergeben sich neue Anwendungen, denn der Internet-Zugang ist nun wie bei einer Standleitung stets verfügbar.

Zwischen dem DSL-Modem des Kunden und der nur wenige Kilometer entfernten Vermittlungsstelle wird das analoge DSL-Signal über die Telefonleitung übertragen. Der DSL-Multiplexer DSLAM wandelt (demoduliert) das analoge Signal in ein digitales Signal, bzw. wandelt in der Gegenrichtung ein digitales Signal in ein analoges um. Das digitale Signal wird über eine breitbandige Glasfaseranbindung vom DSLAM zu einem Konzentrator und von dort in den Backbone des Providers übertragen. Siehe dazu Grafik 6.1 *Grundprinzip DSL*.

[24]

¹englisch für Digitaler Teilnehmeranschluss

²Digital Subscriber Line Access Multiplexer (deutsch: DSL-Vermittlungsstelle)

³ATM: Asynchronous Transfer Mode

⁴POTS: Plain old telephone service (analoge Telefonie)

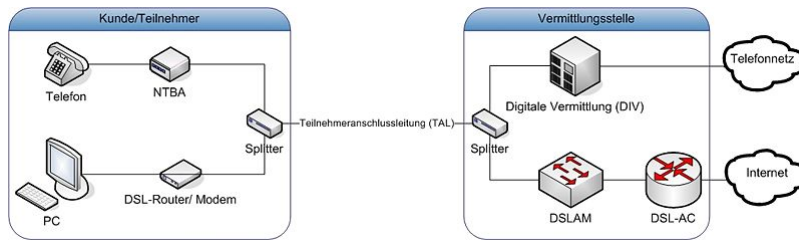


Abb. 6.1: Grundprinzip DSL

6.2 ADSL

Mit Asymmetric Digital Subscriber Line (ADSL) wird die zur Zeit häufigste Anschlusstechnik von Breitbandanschlüssen für Konsumenten bezeichnet. Sie wurde auf Basis der DSL-Technik mit der Maßgabe entwickelt, über die vorhandene Telefonanschlussleitung zu funktionieren ohne die Telefonie über den Festnetzanschluss zu beeinträchtigen und gleichzeitig den meist asymmetrischen (ungleichen) Datenratenbedürfnissen der Privatkunden nach höherer Empfangs- als Sendedatenrate nachzukommen.

Bei POTS/ISDN-Anschlussleitungen gibt es Frequenzbereiche, welche für die Telefonie nicht genutzt werden und daher brachliegen. Diese höheren Frequenzbereiche werden für ADSL verwendet.

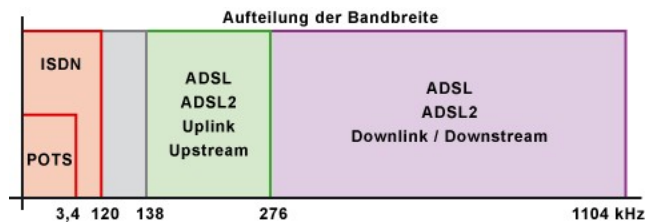


Abb. 6.2: Frequenzbereiche der Telefonleitung

Funktionsprinzipien der ADSL-Technik sind Frequenzmultiplexverfahren, Fouriertransformation und Discrete Multitone Transmission (DMT); ein ADSL-Modem enthält als wesentliche Bestandteile einen schnellen Analog-Digital-Wandler und einen digitalen Signalprozessor zur Berechnung der Fouriertransformationen für die einzelnen Frequenzen.

Damit sich die beiden Nutzungsarten der Telefonleitung nicht stören, werden die beiden Frequenzbereiche sowohl beim Teilnehmer als auch im Hauptverteiler durch eine Frequenzweiche, den sogenannten Splitter, getrennt. Grundsätzlich wird durch die ADSL-Nutzung kein Sprachkanal belegt, so dass man – anders als bei einem Internetzugang mittels herkömmlichem Telefonmodem – auch an einem Analoganschluss gleichzeitig surfen und mittels klassischer Festnetztelefonie telefonieren kann.

Die Datenübertragung im DSL Bereich erfolgt über 4,3125 kHz breiten Kanälen. Dabei werden die Kanäle im Bereich von 138-275 kHz für den Upstream (32 Kanäle) und 275-1104 kHz für den Downstream (192 Kanäle) genutzt. Wegen der schlechten Leitungsqualität – schließlich waren die Telefonleitungen nicht für die Übertragung von Signalen mit einer Bandbreite

von etwa 1 MHz vorgesehen – wird die Leitung vom Endgerät zur Vermittlungsstelle „ausgemessen“ und einzelne Bänder gegebenenfalls ausgeblendet, falls die Dämpfung zu groß ist (DSL ist nur bis zu einer Dämpfung von 50dB möglich) oder Reflexionen auftreten. Auf eine Schwingung können maximal 15 Bit aufmoduliert werden. In der Praxis werden aber nur 8 bis 12 Bit aufmoduliert. Daraus ergibt sich eine Bandbreite pro Kanal von:

$$4312 \text{ Hz} \times 15 \text{ Bit} = \underline{64680 \text{ Bit}} \quad (6.1)$$

Und für den theoretischen Up- bzw. Downstream:

$$64680 \text{ Bit} \times 32 \text{ Kanäle} = \underline{2 \text{ MBit}} \quad (6.2)$$

$$64680 \text{ Bit} \times 192 \text{ Kanäle} = \underline{12 \text{ MBit}} \quad (6.3)$$

Je weiter der Endpunkt vom DSLAM entfernt ist, desto geringer wird die nutzbare Bandbreite. Zwei parallel verlaufende Ader wirken wie eine Frequenzweiche und schneiden die oberen Frequenzen ab, so dass für die Übertragung des DSL-Signals weniger Kanäle zur Verfügung stehen.

Mit der im zunehmenden Maß von den ADSL-Anbietern eingesetzten ADSL2+ Norm geht eine Ausdehnung des verwendeten Frequenzbereichs nach oben bis 2,2 MHz einher, was bei kurzen Anschlussleitungen eine deutlich höhere Datenrate ermöglicht: generell bis zu 25 MBit/s in Empfangsrichtung und bis zu 3,5 MBit/s in Senderichtung.

Beim Aufbau der ADSL-Verbindung verständigen sich das ADSL-Modem auf Teilnehmerseite und der DSLAM zunächst auf die verwendete ADSL-Norm und handeln anschließend die Verbindungsparameter der ADSL-Verbindung aus: die Übertragungskapazität der einzelnen DMT-Frequenzträger der Kupferdoppelader wird ausgemessen, die Downstream- sowie Upstream-Übertragungsraten werden entsprechend den Vorgaben des für den Anschluss konfigurierten DSLAM-Profiles (festgelegt im Vertrag z. B. DSL2000, DSL3000, ...) ausgehandelt und auf die einzelnen Träger verteilt. Nach Fertigstellung der Verbindungsaushandlung bleibt die DSL-Verbindung bis zum Abbruch der DSL-Verbindung synchronisiert.

[25]

6.3 VDSL



Abb. 6.3: Grundprinzip VDSL

VDSL ist wie ADSL ein asymmetrisches Übertragungsverfahren, um auf kurzen Strecken Übertragungsraten zu erreichen, die deutlich höher sind als bei ADSL. Wird VDSL in einem Telefonkabelnetz eingesetzt, dann ist die Voraussetzung ein Hybrid-Netz, bestehend aus Glasfaser- und Kupferleitungen. Die Glasfaserleitungen müssen möglichst nahe an den

Kundenanschluss herangeführt werden, um auf den letzten hundert Metern über die Kupferleitung eine sehr hohe Übertragungsrate zu erzielen.

[26]

VDSL1

Bei VDSL unterscheidet man prinzipiell zwischen VDSL1 und VDSL2. Wenn in Deutschland von VDSL die Rede ist, dann ist damit VDSL2 gemeint. In den folgenden Ausführungen geht es um VDSL1.

VDSL1 ist der ADSL-Technik sehr ähnlich, aber nicht kompatibel. Als Leitungscode wird DMT⁵ in Kombination mit QAM verwendet. DMT passt die QAM-Modulation dynamisch an die Bedingungen auf der Kupferleitung an.

VDSL1 erreicht eine maximale Übertragungsgeschwindigkeit von 52 MBit/s im Downlink und 11 MBit/s im Uplink. Die nutzbare Bandbreite sinkt bei zunehmender Leitungslänge. Bei ca. 900 Meter Leitungslänge erreicht man ADSL2+-Niveau. Und schon bei 2 km Leitungslänge ist ADSL-Niveau erreicht.

[27]

VDSL2

VDSL2 ist ein schnelles Übertragungsverfahren für Breitband-Internet und Triple Play im Telefonnetz. Es hat eine deutlich höhere Übertragungsgeschwindigkeit als ADSL, ADSL2 oder ADSL2+. Allerdings wird die Geschwindigkeit nur auf einer kürzeren Distanz und nur in einem Hybridnetz erreicht. Erst der Einsatz eines Hybridnetzes, bestehend aus Glasfaser- und Kupferkabel, garantiert die angestrebten Übertragungsraten von 50 bis 100 MBit/s (symmetrisch).

Obwohl namentlich verwandt, ist VDSL1 nicht der technische Vorgänger von VDSL2. Prinzipiell gibt es einige Gemeinsamkeiten. Doch beide Verfahren sind nicht kompatibel zueinander. VDSL1 ist ein Verfahren, das sich in Deutschland nicht durchgesetzt hat. Das lag vor allem daran, weil die Reichweite und die Übertragungsgeschwindigkeit zu kurz war. Weil es in Deutschland kein VDSL1 gab, wird VDSL2 in der Öffentlichkeit manchmal als VDSL bezeichnet.

VDSL2 ist zu ADSL, ADSL2 und ADSL2+ abwärtskompatibel. Es bietet sogar einen Fallback-Modus nach ADSL/ADSL2/ADSL2+. Das macht VDSL2 so interessant für die Netzbetreiber, die bereits ADSL2 und ADSL2+ einsetzen. VDSL2 gilt technisch als der direkte Nachfolger von ADSL2+. In VDSL2 wurde die Unterstützung gleichzeitiger virtueller Verbindungen über eine physikalische Verbindung implementiert. So ist es möglich bestimmte Datenverbindungen zu priorisieren. Zum Beispiel für Telefonie oder TV. VDSL2 bietet Funktionen für Quality of Service, was für Triple Play wichtig ist. Zum Beispiel für die Übertragung von Video (TV) und Sprache (Telefonie).

⁵DMT: Discrete Multitone Transmission (Modulationsverfahren.)

Während bei ADSL eine zentrale Netzstruktur aufgebaut wurde, ist bei VDSL eine verteilte Baumstruktur gefragt. Die DSL-Vermittlungsstellen (DSLAM) wandern von der Ortsvermittlungsstelle in die Kabelverzweiger (Ortsverteiler), die am Straßenrand stehen und als passive Verteilungspunkte dienen. Das VDSL-Netz ist ein Hybrid-Netz, eine Kombination aus Glasfaser- und Kuperleitungen. Die Glasfaserkabel werden von der Ortsvermittlungsstelle bis zu den Kabelverzweigern (KVz) am Straßenrand geführt. Der DSLAM wird also vom Glasfaserkabel gespeist. Die DSLAM versorgt rund 100 Haushalte pro Schrank mit VDSL. Im Vergleich zu ADSL wird die Kuperleitung deutlich aufgebohrt. Durch die Glasfaser wird die Kuperkabelstrecke verkürzt. Die Länge des Kuperkabels zum Nutzer beträgt nur wenige hundert Meter. So kann auf der Kuperleitung eine höhere Geschwindigkeit gefahren werden. Diese Infrastruktur nennt man „Fiber to the Curb“ (FTTC). Das bedeutet „Glasfaser bis zum Bordstein“.

Übertragungsgeschwindigkeit

VDSL2 erreicht eine Übertragungsgeschwindigkeit von 100 MBit/s sowohl im Downlink, als auch im Uplink. Das bedeutet 100 MBit/s symmetrisch oder Full Duplex. Die genannten Werte, egal ob 50, 68 oder 100 MBit/s sind aber nur theoretischer Natur. Die Höhe der Übertragungsrate hängt in der Praxis sehr stark von der Länge und Qualität des Kuperkabels vom Kabelverzweiger bis zum Teilnehmeranschluss (DSL-Modem) ab. Ist die Leitungsqualität sehr gut, dann erreicht man auf 1.000 Metern bis zu 50 MBit/s. Auf 1.600 Metern sinkt die Leistung auf ADSL2+-Niveau. Ist die Teilnehmeranschlussleitung (TAL) kurz genug, dann kann man sowohl im Uplink als auch im Downlink bis zu 100 MBit/s erreichen. Ist die Leitung länger, dann reduziert sich die Übertragungsgeschwindigkeit, die mit ADSL2+ vergleichbar ist. In Deutschland erreicht VDSL2 ohne FTTC die gleiche Flächendeckung wie ADSL2+.

Um mit VDSL2 eine Übertragungsgeschwindigkeit von bis zu 100 MBit/s (symmetrisch) zu erreichen, wird der Frequenzbereich bis 30 MHz in mehrere Downlink- und Uplink-Bereiche aufgeteilt. In Deutschland wird der Frequenzbereich bis mindestens 138 kHz für POTS und ISDN ausgeblendet. Damit kann weiterhin auch analoge Telefonie oder ISDN parallel im unteren Frequenzband angeboten werden. Sicherheitshalber wird noch ein Sicherheitsabstand zwischen den Frequenzbereichen eingefügt, damit ganz sicher keine Beeinträchtigung durch andere Dienste auftreten kann.

Übertragungstechnik

VDSL2 ist der ADSL-Technologie sehr ähnlich. Die Modulation der Nutzdaten erfolgt mit DMT (Discrete Multitone Modulation). Dabei wird der genutzte Frequenzbereich auf bis zu 4096 einzelne voneinander unabhängige, zeitlich versetzte Träger unterteilt. Die Träger können wahlweise eine Bandbreite von 4,3125 kHz oder 8,625 kHz haben (abhängig vom Profil). VDSL2 ist sehr robust gegen Störungen und kann wie ADSL2 dynamisch auf Störungen reagieren. So können die DSL-Parameter ohne Verbindungstrennung zwischen DSLAM und VDSL2-Modem angepasst werden.

Zwischen VDSL2-Modem und DSLAM werden die Daten ohne ATM-Codierung übertragen. Auf eine ATM-Technik und speziellen IP-Gateways wie bei ADSL wird verzichtet. Statt dessen wird direkt mit „IP over VDSL“ oder „raw IP“ übertragen. Dadurch wird der Datendurchsatz erhöht und die Infrastrukturkosten gesenkt. Die Kabelverzweiger werden über Glasfaser-Gigabit-Ethernet angebunden. Zur Daten- und Dienste-Priorisierung werden die Dienste durch VLANs (IEEE 802.1q) voneinander getrennt.

[28]

7 Kryptographie

7.1 Methoden der Kryptographie

7.1.1 Methoden der klassischen Kryptographie

Solange für die Kryptographie noch keine elektronischen Rechner eingesetzt wurden, ersetzte man bei der Verschlüsselung (zu dieser Zeit die einzige Anwendung der Kryptographie) immer vollständige Buchstaben oder Buchstabengruppen. Solche Verfahren sind heute veraltet und unsicher.

- *Transposition*: Die Buchstaben der Botschaft werden einfach anders angeordnet.
- *Substitution*: Die Buchstaben der Botschaft werden durch jeweils einen anderen Buchstaben oder ein Symbol ersetzt. Siehe dazu: Monoalphabetische Substitution (Caesar-Verschlüsselung) und Polyalphabetische Substitution (Vigenère-Verschlüsselung).

[16]

Monoalphabetische Substitution (Caesar-Verschlüsselung)

Zum Zwecke der Verschlüsselung wird dabei jeder Buchstabe des lateinischen Standardalphabets um eine bestimmte Anzahl von Positionen zyklisch verschoben (rotiert). Die Anzahl bestimmt den Schlüssel, der für die gesamte Verschlüsselung unverändert bleibt. Es ist eine der einfachsten (und unsichersten) Formen einer Geheimschrift.

[17]

Polyalphabetische Substitution (Vigenère-Verschlüsselung)

Im Gegensatz zur monoalphabetischen Substitution werden für die Zeichen des Klartextes mehrere Geheimtextalphabete verwendet.

Das Schlüsselwort sei „AKEY“, der Text „geheimnis“. Vier Caesar-Substitutionen verschlüsseln den Text. Die erste Substitution ist eine Caesar-Verschlüsselung mit dem Schlüssel „A“. „A“ ist der erste Buchstabe im Alphabet. Er verschiebt den ersten Buchstaben des zu verschlüsselnden Textes, das „g“, um 0 Stellen, es bleibt „G“. Der zweite Buchstabe des Schlüssels, das „K“, ist der elfte Buchstabe im Alphabet, er verschiebt das zweite Zeichen des Textes, das „e“, um zehn Zeichen. Aus „e“ wird ein „O“ (siehe Tabelle). Das dritte Zeichen des Schlüssels („E“) verschiebt um 4, „Y“ um 24 Stellen. Die Verschiebung des nächsten Buchstabens des Textes beginnt wieder bei „A“, dem ersten Buchstaben des Schlüssels:

Text: geheimnis
 Schlüssel: AKEYAKEYA
 Chiffre: GOLCIWRGS

		Text																										
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
S c h ü s s e l	1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	G e h e i m t e x t
	2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
	3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
	4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
	5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
	6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
	7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
	8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
	9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
	10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
	11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
	12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
	13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
	14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
	15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
	16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
	17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
	18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
	19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
	20	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
	21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
	22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
	23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
	24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
	25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	
	26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	

Abb. 7.1: Vigenère-Quadrat

[18]

7.1.2 Methoden der modernen Kryptographie

Entsprechend der Arbeitsweise von Computern arbeiten moderne kryptographische Verfahren nicht mehr mit ganzen Buchstaben, sondern mit den einzelnen Bits der Daten. Dies vergrößert die Anzahl der möglichen Transformationen erheblich und ermöglicht außerdem die Verarbeitung von Daten, die keinen Text repräsentieren. Fast alle asymmetrischen kryptographischen Verfahren basieren auf Operationen in mathematischen Strukturen, wie z.B. endlichen Körpern, elliptischen Kurven oder Gittern. Ihre Sicherheit basiert dann auf der Schwierigkeit bestimmter Berechnungsprobleme in diesen Strukturen.

7.2 Symmetrische Verschlüsselung

Die symmetrische Verschlüsselung ist eine Verschlüsselung, welche im Gegensatz zu einer asymmetrischen Verschlüsselung den gleichen Schlüssel zur Ver- und Entschlüsselung verwendet. Bei manchen symmetrischen Verfahren (z.B. IDEA) ist es dafür zunächst notwendig, den Verschlüsselungs-Schlüssel in einen Entschlüsselungs-Schlüssel zu transformieren.

Der große Nachteil symmetrischer Verfahren liegt in der Nutzung ein- und desselben Schlüssels zur Ver- und Entschlüsselung, d. h. neben der verschlüsselten Information muss auch der Schlüssel übermittelt werden. Das Problem beim Einsatz symmetrischer Verfahren ist, dass der Schlüssel über einen sicheren Kanal übertragen werden muss, denn die Sicherheit des Verfahrens hängt von der Geheimhaltung des Schlüssels ab.

7.2.1 Verfahren

- *AES*: (Advanced Encryption Standard) oder Rijndael: der US-amerikanische Verschlüsselungsstandard, Nachfolger des DES; von Joan Daemen und Vincent Rijmen entwickeltes Blockverschlüsselungsverfahren.
- *DES*: (Data Encryption Standard) oder Lucifer: bis zum Oktober 2000 der Verschlüsselungsstandard der USA. Das Verfahren, wurde 1974 von IBM entwickelt. Die Version für Privatanwender heißt Data Encryption Algorithm (DEA).
- *Triple-DES*: Eine Weiterentwicklung des DES-Verfahrens; dreimal langsamer, aber um Größenordnungen sicherer.
- *Blowfish*: 1993 von Bruce Schneier entwickeltes Blockverschlüsselungsverfahren, unpatentiert
- *Twofish* Blockverschlüsselungsverfahren, vom Counterpane Team; wird u.a. in Microsoft Windows eingesetzt.
- *RC2, RC4, RC5, RC6* („*Rivest Cipher*“: Mehrere Verschlüsselungsverfahren von Ronald L. Rivest.

[19]

7.3 Asymmetrische Verschlüsselung

Eine asymmetrische Verschlüsselung ist eine Verschlüsselung, bei dem jeder der kommunizierenden Parteien ein Schlüsselpaar besitzt, das aus einem geheimen Teil (privater Schlüssel) und einem nicht geheimen Teil (öffentlicher Schlüssel) besteht. Der private Schlüssel ermöglicht es seinem Inhaber zum Beispiel, Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren. Der öffentliche Schlüssel ermöglicht es jedermann, Daten für den Schlüsselinhaber zu verschlüsseln, dessen digitale Signaturen zu prüfen oder ihn zu authentifizieren. Im Gegensatz zu einem symmetrischen Kryptosystem müssen die kommunizierenden Parteien keinen gemeinsamen geheimen Schlüssel kennen.

Asymmetrische Kryptosysteme werden daher auch als Public-Key-Verfahren bezeichnet.

Vorteile:

- Geheimnis bleibt möglichst klein halten, da jeder Benutzer nur seinen eigenen privaten Schlüssel geheim halten braucht.
- Verminderung des so genannten Schlüsselverteilungsproblems.

Nachteile:

- Der asymmetrischen Algorithmen ist sehr langsam.
- Eine Nachricht an mehrere Empfänger muss jedes mal mit dessen öffentlichen Schlüssel verschlüsselt werden.
- Sicherheit beruht auf unbewiesenen Annahmen.
- Ungewissheit über die Echtheit des öffentlichen Schlüssels

7.3.1 Verfahren

RSA: RSA ist nach seinen Erfindern Ronald L. Rivest, Adi Shamir und Leonard Adleman benannt.

[20]

7.4 Hybride Verschlüsselung

Unter Hybrider Verschlüsselung versteht man eine Kombination aus asymmetrischer Verschlüsselung und symmetrischer Verschlüsselung. Hybride Verschlüsselungsverfahren werden z. B. bei der Datenübertragung zwischen zwei Gegenstellen in einem Netzwerk verwendet. Das Verfahren kommt unter anderem bei den Netzwerkprotokollen IPsec und SSL zum Einsatz.

Der Verbindungsaufbau geschieht dort in der Regel mit Hilfe von Schlüsselpaaren (asymmetrisch), die eigentliche Datenübertragung erfolgt zugunsten niedrigerer Anforderung an die Rechenleistung auf beiden Seiten mit demselben Schlüssel (symmetrisch). Beim Verbindungsaufbau wird dabei ein Sessionkey ausgetauscht, der dann für die symmetrische Verschlüsselung benutzt wird. Das asymmetrische Verfahren wird also nur zum sicheren Austausch des „symmetrischen Schlüssels“ benutzt. Damit werden die Vorteile beider Verfahren genutzt - die hohe Geschwindigkeit für die symmetrische Verschlüsselung der Nutzdaten und die sicherere asymmetrische Verschlüsselung für den kleinen Session Key.

Siehe dazu Abbildung 7.2 auf Seite 45.

[22]

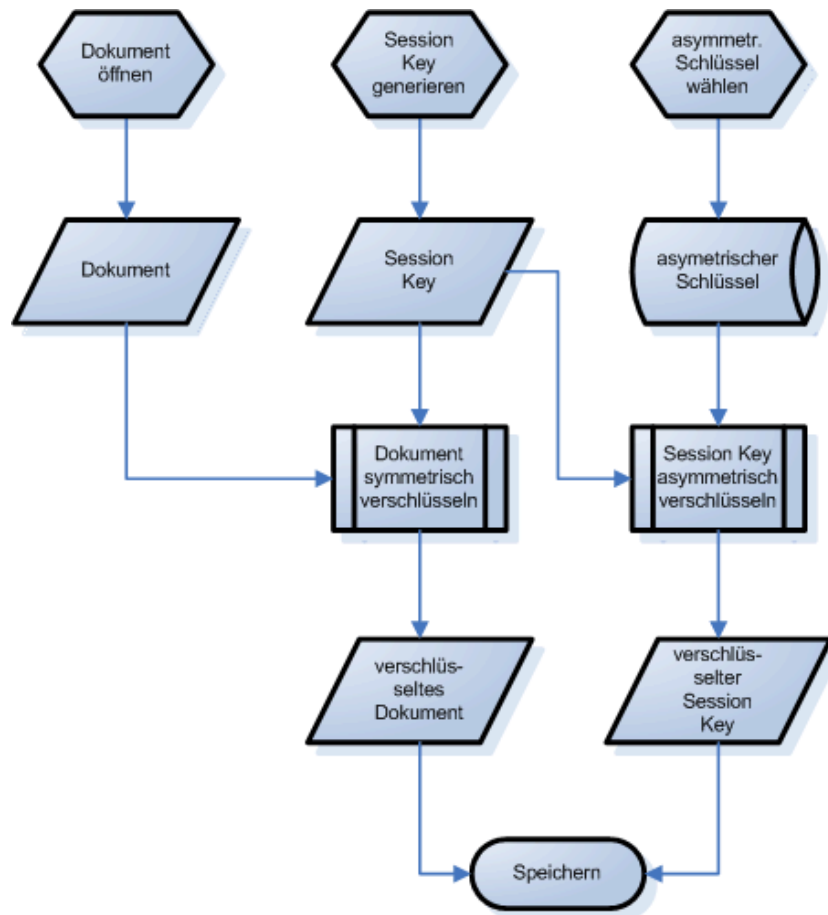


Abb. 7.2: Beispiel für ein hybrides Verschlüsselungsverfahren

7.5 Begriffe der sicheren Kommunikation

Vertraulichkeit: Daten können nicht mitgelesen werden. Die Vertraulichkeit der Kommunikation wird durch eine Verschlüsselung der Daten erreicht.

Integrität: Daten wurden nicht verändert. Die Integrität wird durch Anhängen eines Hash-Wertes sichergestellt.

Authentizität: Absender ist, der für den er sich ausgibt. Um sicherzustellen, dass die Daten wirklich vom Absender kommen, signiert der Absender seine Daten mit einer digitalen Signatur, die er mit Hilfe seines privaten Schlüssels erzeugt hat. Der Empfänger kann nun die Signatur mit dem öffentlichen Schlüssel des Absenders überprüfen.

Zertifikat: Als Zertifikat bezeichnet man eine Kombination der Sicherstellung der Integrität und der Authentizität.

Siehe dazu die weiterführenden Links: *Sichere Kommunikation per E-Mail:* <http://www-user.uni-bremen.de/~werres/old/secure.html> und *Verschlüsselung und elektronische Unterschrift im Internet:* <http://www.astelter.de/5.html>.

8 Sicherheit von Netzwerken

8.1 Sicherheitsanforderungen

Je nach Situation, Umgebung oder Anforderungen kann es verschiedene Sicherheitsanforderungen an ein System geben:

- Vertraulichkeit
- Integrität
- Authentizität
- Verfügbarkeit
- Zugriffskontrolle
- Verbindlichkeit
- Anonymität

8.2 Sicherheitsmechanismen und Systeme

Es gibt verschiedene Sicherheitsmechanismen und Systeme, um ein System (Rechner, Netzwerk, etc.) abzusichern:

- Verschlüsselungssysteme (DES, RSA, etc.)
- Message Authentication und Digitale Signatur
- Key Management, Authentication: PKI, Kerberos, etc.
- IP-Security: IPSec, VPN
- Web Security: SSL / TLS
- Email: PGP, S/MIME
- Payment: SET
- Intrusion Detection
- Schutz vor Malware (Viren, Würmer, etc.)
- Firewalls
- etc.

9 Malware

Als Malware (Kofferwort aus engl. malicious, „böartig“ und Software) bezeichnet man Computerprogramme, welche vom Benutzer unerwünschte und ggf. schädliche Funktionen ausführen. Da ein Benutzer im Allgemeinen keine schädlichen Programme duldet, sind die Schadfunktionen gewöhnlich getarnt oder die Software läuft gänzlich unbemerkt im Hintergrund. Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder die technische Kompromittierung der Sicherheitssoftware oder anderen Sicherheitseinrichtungen (wie z. B. Firewalls und Antivirenprogramme) eines Computers sein.

Malware wird unterschieden in folgende Typen:

- *Computerviren* sind die älteste Art der Malware, sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben.
- Ein *Computerwurm* ähnelt einem Computervirus, verbreitet sich aber direkt über Netze wie das Internet und versucht, in andere Computer einzudringen.
- Trojanisches Pferd (kurz: *Trojaner*) ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, böartigen Teil, oft *Spyware* oder eine *Backdoor*. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.
- Eine *Backdoor* ist eine verbreitete Schadfunktion welche üblicherweise durch Viren, Würmer oder Trojanische Pferde eingebracht und installiert wird. Es ermöglicht Dritten einen unbefugten Zugang („Hintertür“) zum Computer, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft genutzt, um den kompromittierten Computer als Spamverteiler oder für Denial-of-Service-Angriffe zu missbrauchen.
- *Rootkits* sind eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Computersystem auf dem kompromittierten System installiert wird, um zukünftige Logins des Eindringlings zu verbergen und Prozesse und Dateien zu verstecken.
- Ein *KeyLogger* ist eine Hard- oder Software, die dazu verwendet wird, die Eingaben des Benutzers an einem Computer mitzuprotokollieren und dadurch zu überwachen oder zu rekonstruieren.

[23]

Literaturverzeichnis

- [1] Hüsler, Martin: *Netzwerktechnik-Grundlagen (Präsentation)*. Fachhochschule Solothurn, Wintersemester 2004/2005
- [2] Wikipedia: *ISDN - Grundlagen, Technik und Aufbau*.
<http://www.pc-erfahrung.de/hardware/hardware-isdn.html>, Stand: 2008-01-04
- [3] Wikipedia: *Baud*.
http://de.wikipedia.org/wiki/Duplex_%28Nachrichtentechnik%29, Stand: 2008-01-7
- [4] Wikipedia: *Baud*.
<http://de.wikipedia.org/wiki/Baudrate>, Stand: 2008-01-04
- [5] Wikipedia: *Integrated Services Digital Network*.
<http://de.wikipedia.org/wiki/Isdn>, Stand: 2008-01-04
- [6] Wikipedia: *Paritätsbit*.
<http://de.wikipedia.org/wiki/Parit%C3%A4tsbit>, Stand: 2008-01-07
- [7] Wikipedia: *Zyklische Redundanzprüfung*.
http://de.wikipedia.org/wiki/Cyclic_Redundancy_Check, Stand: 2008-01-04
- [8] Wikipedia: *Frequenzmodulation*.
<http://de.wikipedia.org/wiki/Amplitudenmodulation>, Stand: 2008-01-06
- [9] Wikipedia: *Frequenzmodulation*.
<http://de.wikipedia.org/wiki/Frequenzmodulation>, Stand: 2008-01-06
- [10] Wikipedia: *Phasenmodulation*.
<http://de.wikipedia.org/wiki/Phasenmodulation>, Stand: 2008-01-06
- [11] Wikipedia: *Quadraturamplitudenmodulation*.
<http://de.wikipedia.org/wiki/Quadraturamplitudenmodulation>, Stand: 2008-01-06
- [12] Wikipedia: *Telefon*.
<http://de.wikipedia.org/wiki/Telefon>, Stand: 2008-01-07
- [13] Wikipedia: *Impulswahlverfahren*.
<http://de.wikipedia.org/wiki/Impulswahlverfahren>, Stand: 2008-01-07
- [14] Wikipedia: *Mehrfrequenzwahlverfahren*.
<http://de.wikipedia.org/wiki/Mehrfrequenzwahlverfahren>, Stand: 2008-01-07
- [15] Wikipedia: *Vermittlungsstelle*.
<http://de.wikipedia.org/wiki/Vermittlungsstelle>, Stand: 2008-01-07

- [16] Wikipedia: *Symmetrisches Kryptosystem*.
<http://de.wikipedia.org/wiki/Kryptografie>, Stand: 2008-01-07
- [17] Wikipedia: *Polyalphabetische Substitution*.
<http://de.wikipedia.org/wiki/Verschiebechiffre>, Stand: 2008-01-07
- [18] Wikipedia: *Polyalphabetische Substitution*.
<http://de.wikipedia.org/wiki/Vigen%C3%A8re-Chiffre#Vigen.C3.A8re-Verschl.C3.BCsselung>, Stand: 2008-01-07
- [19] Wikipedia: *Symmetrisches Kryptosystem*.
http://de.wikipedia.org/wiki/Symmetrische_Verschl%C3%BCsselung, Stand: 2008-01-07
- [20] Wikipedia: *Asymmetrisches Kryptosystem*.
http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem, Stand: 2008-01-07
- [21] Wikipedia: *RSA-Kryptosystem*.
<http://de.wikipedia.org/wiki/RSA-Kryptosystem>, Stand: 2008-01-07
- [22] Wikipedia: *Hybride Verschlüsselung*.
<http://de.wikipedia.org/wiki/RSA-Kryptosystem>, Stand: 2008-01-31
- [23] Wikipedia: *Malware*.
<http://de.wikipedia.org/wiki/Malware>, Stand: 2008-04-15
- [24] Wikipedia: *Digital Subscriber Line*.
<http://de.wikipedia.org/wiki/DSL>, Stand: 2008-05-22
- [25] Wikipedia: *Asymmetric Digital Subscriber Line*.
<http://de.wikipedia.org/wiki/ADSL>, Stand: 2008-05-22
- [26] Das ELEktronik KOmpendium: *VDSL - Very High Speed Digital Subscriber Line*.
<http://www.elektronik-kompodium.de/sites/kom/0305237.htm>, Stand: 2008-05-22
- [27] Das ELEktronik KOmpendium: *VDSL 1*.
<http://www.elektronik-kompodium.de/sites/kom/1302131.htm>, Stand: 2008-05-22
- [28] Das ELEktronik KOmpendium: *VDSL 2*.
<http://www.elektronik-kompodium.de/sites/kom/0305236.htm>, Stand: 2008-05-22
- [29] Wikipedia: *IP-Telefonie*.
<http://de.wikipedia.org/wiki/Voip>, Stand: 2009-03-27

Stichwortverzeichnis

- Advanced Encryption Standard (AES), 43
- Amplitudenmodulation (AM), 9
- Anlagenanschluss, 26
- Auslandsvermittlungsstelle, 21
- authentizität, 45

- Backdoor, 49
- Basisanschluss, 26
- Baud, 7
- Baudrate, 7
- Bitfehler, 8
- Blockprüfung, 9
- Blowfish, 43
- Bussystem, 27

- Cäsar-Verschlüsselung, 41
- Computervirus, 49
- Computerwurm, 49
- CRC *siehe* Blockprüfung 9

- Data Encryption Standard (DES), 43
- Datenübertragung, 7
 - parallel, 7
 - seriell, 7
- Dienstkennung, 25
- Duplex, 7
 - Halbduplex, 7
 - Simplex, 7
 - Vollduplex, 7
- Durchgangsvermittlungsstelle, 21

- Even-Parity, 8

- Fehlereerkennung, 8
- Fernvermittlungsstelle, 21
- Frequenzmodulation (FM), 10

- Impulswahlverfahren, 19
- Integrated Services Digital Network (ISDN), 25
- Integrität, 45

- IP-Telefonie, 31
- ISDN-Anlage, 25
- ISDN-Endgerät, 25, 29

- Keylogger, 49
- Kommunikation, 7
- Kryptographie, 41

- Lucifer *siehe* Data Encryption Standard (DES) 43

- Malware, 49
- Mehrfrequenzwahlverfahren, 20
- Mehrgeräteanschluss, 26
- Modulationsverfahren, 8
- Multiple Subscriber Number (MSN), 25

- Nebenstellenanschluss, 25
- Netzwerk Terminierungs Basiseinheit (NT-BA), 25

- Odd-Parity, 8
- Ortsvermittlungsstelle, 21

- Paritätskontrollbit, 8
- Paritätssummer, 8
- Parity Check, 8
- Paritybit, 8
- Phasenmodulation (PM), 10
- Point-to-Multipoint, 26
- Primärmultiplexanschluss, 26, 27
- Public-Key-Verfahren, 43

- Quadraturmodulation (QAM), 11

- Real-Time Control Protocol, 33
- Real-Time Transport Protocol, 32, 33
- Remote Access Service (RAS), 30
- Rijndael *siehe* Advanced Encryption Standard (AES) 43
- River Cipher (RC*), 43

Rootkit, 49

S0-Bus, 27

S0-Frame, 27, 28

Session Initiation Protocol, 32

Sicherheitssoftware, 49

SIP *siehe* Session Initiation Protocol 32

Spyware, 49

Steuerkanal, 28

Substitution, 41

Telefonanlage, 26

Telefonapparat, 19

Telefonie

- analog, 19
- digital, 25

Telefonnetz, 21

Transposition, 41

Triple-DES, 43

Trojaner *siehe* Trojanisches Pferd 49

Trojanisches Pferd, 49

Twofish, 43

UDP *siehe* User Datagram Protocol 33

User Datagram Protocol, 33

Vermittlungsnetz

- digital, 21

Verschlüsselung

- asymmetrisch, 43
- symmetrisch, 43

Verschlüsselungen

- hybride, 44

Vertraulichkeit, 45

Vignère-Verschlüsselung, 41

Voice over IP, 31

VoIP *siehe* Voice over IP 31

Zertifikat, 45