LEHRBUCH

Andriy Luntovskyy
Dietbert Gütter

Moderne Rechnernetze – Übungsbuch

Aufgaben und Musterlösungen zu Protokollen, Standards und Apps in kombinierten Netzwerken

Springer Vieweg

Moderne Rechnernetze – Übungsbuch

Andriy Luntovskyy
Dietbert Gütter

Moderne Rechnernetze – Übungsbuch

Aufgaben und Musterlösungen zu Protokollen, Standards und Apps in kombinierten Netzwerken

Springer Vieweg

Andriy Luntovskyy
Berufsakademie Sachsen
Dresden, Deutschland

Dietbert Gütter
Berufsakademie Sachsen
Dresden, Deutschland

ISBN 978-3-658-25618-0 ISBN 978-3-658-25619-7 (eBook)
https://doi.org/10.1007/978-3-658-25619-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über ► http://dnb.d-nb.de abrufbar.

Planung/Lektorat: Reinhard Dapper
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Persönlichkeiten werden nicht durch schöne Reden geformt, sondern durch Arbeit und eigene Leistung.

(Albert Einstein, 1870–1955)

Vorwort

Dieses Übungsbuch ergänzt das Lehrbuch von A. Luntovskyy, D.Gütter (Vorwort: A.Schill) „Moderne Rechnernetze: Protokolle, Standards und Apps in kombinierten, drahtgebundenen, mobilen und drahtlosen Netzwerken“ um praktische Übungen und dazugehörige Musterlösungen.

Es wird als vorlesungsbegleitendes Buch zum Modul „Computernetzwerke“ im ET- und IT- Fachstudium für Studierenden und Dozenten an den technischen Hochschulen und Studienakademien Deutschlands, Österreichs und in der Schweiz sowie in weiteren deutschsprachigen Gebieten empfohlen (insb. als Lehrbuch für Fernstudium).

Von den Autoren wurden bereits zwei einschlägige Fachbücher publiziert:

1. *Andriy Luntovskyy, Dietbert Guetter, Igor Melnyk. Planung und Optimierung von Rechnernetzen: Methoden, Modelle, Tools für Entwurf, Diagnose und Management im Lebenszyklus von drahtgebundenen und drahtlosen Rechnernetzen, Lehrbuch, Vieweg + Teubner Verlag Wiesbaden, 2011, S. 435 (ISBN 978-3-8348-1458-6).*
2. *Andriy Luntovskyy, Josef Spillner. Architectural Transformations in Network Services and Distributed Systems: Service Vision. Case Studies, Lehrbuch, Springer Vieweg, 2017, XXIV, S. 344, 238 pict. (ISBN: 978-3-658-14840-9).*

In Deutschland und dem deutschsprachigen Raum (Österreich, Schweiz) ist trotz des Vorhandenseins einer breiten Literaturauswahl zu Rechnernetzen (A.Tanenbaum, R.Schreiner, H.Zisler, J.Roth etc.) bei Themen wie Verteiltes Rechnen, Cloud Computing, Datenschutzgarantierende Verteilte Systeme, Green-IT, Internet der Dinge usw. festzustellen, dass für uns als Fachexperten und aktiv unterrichtende Dozenten einige Aspekte dieser Fach- und Handbücher aus der Perspektive übergreifender Trends und Transformationen nicht ausreichend behandelt werden.

Die Analyse moderner Literatur zur erwähnten Problematik zeigte außerdem, dass die übersetzten Fach- und Handbücher mit der Auflistung und Aufzählung von Positionen existierender ITU-T-, ISO-, IEEE-Standards, Katalogdaten und Konfigurationsanleitungen oft übersättigt sind, sowie zu wenige konkrete Implementierungsbeispiele und Anwendungsfälle beinhalten.

Manche Autoren führen durchaus sinnvoll bekannten theoretischen Lernstoff vor, z. B. zugrunde liegende Methoden für Netzwerkservices, -Produkte und -Standards, aber mit geringer praktischer Illustration durch Übungsstoff, Musterlösungen, moderne (mobile) Applikationen, Einsatzbeispiele usw. Gerade für Studierenden des berufsintegrierten Studiums (staatliche Studienakademien, Berufsakademien, duale Hochschulen) sind solche naheliegenden und greifbaren Use Cases aber wichtig.

In unseren Büchern (Lehrbuch und Übungsbuch) sollen die oben erwähnte Lücken geschlossen, die angesprochene Problematik behoben sowie die bisherigen autoreigenen Bücher ergänzt und erweitert werden. Das Buch enthält Aufgaben zur Problematik von kombinierten (drahtgebundenen, mobilen und drahtlosen) Netzwerken, Netzwerkservices zu 5G, IoT, Cloud- und Fog-Diensten sowie modernen Architekturen verteilter (mobiler) Anwendungen.

Dieses Übungsbuch ergänzt das Lehrbuch von A. Luntovskyy, D.Gütter (Vorwort: A.Schill) „Moderne Rechnernetze: Protokolle, Standards und Apps in kombinierten (drahtgebundenen, mobilen und drahtlosen) Netzwerken" um praktische Übungen und dazugehörige Musterlösungen.

Die beiden Bücher mit einem stark ausgeprägten modularen Aufbau werden für das Modul „Computernetzwerke" im ET- und IT-Fachstudium für Studierende und Dozenten an den technischen Hochschulen empfohlen.

Die Übungen und Musterlösungen im begleitenden Übungsbuch werden den Teilen I, II, III im Lehrbuch zugeordnet und nach den folgenden Komplexen I, II, III aufgeteilt:

- Komplex I – Übertragungsorientierte Schichten
- Komplex II – Netzwerktechnologien und Mobile Kommunikation. Netzkopplung und Verkabelung
- Komplex III – Verarbeitungsorientierte Schichten und Netzwerkanwendungen

Komplex I (zum Teil I Lehrbuch) beinhaltet Übungen zur Einführung in das Gebiet der Rechnernetze. Die weiterführenden Komplexe II und III behandeln konkrete aktuelle Rechnernetztechnologien und verteilte Anwendungslösungen. Genauso enthalten die beiden weiteren Komplexe II und III die erforderlichen Musterlösungen.

Das Komplex II (zum Teil II Lehrbuch) begleitet mit praktischen Übungen die im Lehrbuch vermittelte Kenntnisse und Fertigkeiten, die benötigt werden, um von der Problemstellung der Datenübertragung in Netzwerken über bestimmte Netzwerkmuster (drahtgebunden, drahtlos, mobil, satellitenbasiert) zu kostengünstiger, energiesparender und effizienter Vernetzung zu gelangen.

Das Komplex III (zum Teil III Lehrbuch) setzt voraus, dass die Leser die Inhalte der Komplexe I und II beherrschen. Sie sind mit dem Aufbau und den Funktionen der relevanten Referenzmodelle (Internet, TCP/IP, OSI) vertraut und besitzen einen qualifizierten Überblick über aktuelle Protokolle lokaler Netzwerke sowie von Weitverkehrsnetzen, Zugangsnetzwerken, drahtlosen und Mobilfunknetzen.

Aufbauend auf den Komplexen I und II (Teile I und II Lehrbuch), welche die übertragungstechnischen Probleme und aktuellen Netzwerktechnologien grundlegend behandeln, erfolgt im Komplex III (Teil III Lehrbuch) eine kurze Einführung in die oberen verarbeitungsorientierten Schichten des OSI-Referenzmodells, zu den Netzwerkanwendungen, mobilen Apps, Middleware und Webservices. Des Weiteren werden die verteilten Systeme und die aktuellen Konzepte wie u. a. Grids, Clustering, IoS, Clouds und Fog Computing, Industrie 4.0 sowie IoT diskutiert.

Andriy Luntovskyy
Dietbert Gütter
Dresden, Deutschland

Danksagung

In den Inhalt des Lehrbuches wurden auch didaktisch bewährte Beispiele von Dozenten der TU Dresden und BA Dresden übernommen. Wir danken dafür Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill, Dr. habil. Josef Spillner, Dr.-Ing. Marius Feldmann, Dr. Iris Braun, Dr. Thomas Springer, Prof. Dr. Tenshi Hara und vielen weiterer unseren Kollegen, Gleichgesinnten und Mitstreitern.

Einige Beispiele wurden aus dem Wissensbestand Skripte LS Rechnernetze an der TU Dresden [3] mit Anpassungen und Erweiterungen zitiert.

Inhalte und kurzfassende Hinweise

Das Übungsbuch beinhaltet die Musterlösungen zum Übungsmaterial mit den praktischen Aufgaben. Das Material begleitet die Inhalte des Buches Teil I, II, III und erweitert die in diesen Teilen aufgeführten Beispiele.

Hinweis:
Alle Berechnungen werden in SI-Maßeinheiten bzw. mit SI-konformen Präfixen durchgeführt.

Lernziele Übungsbuch

Die nachfolgend gestellten Musterlösungen zu den praktischen Aufgaben haben das Ziel, dass Sie eine professionelle Sicherheit bei der Lösung von Problemen auf den Gebieten der Rechnernetze und der Datenübertragung erreichen.

Die weiterführenden Aufgaben zu den Komplexen I, II und III setzen voraus, dass Sie alle Kontrollfragen und Übungsaufgaben des Buches gelöst haben und selbständig die Stellungnahme ähnlicher Probleme beherrschen.

Die praktischen Aufgaben ermöglichen die schrittweise Vertiefung der erworbenen theoretischen Kenntnisse zu den Netztechnologien und Kopplungselementen, sowie zu den notwendigen Arbeitsschritten zwecks Erstellung komplexerer Netzwerklösungen sowie Konzipierung oder Analyse der Effizienz dieser oder jener Rechnernetzanwendung.

Teilweise fußt der Inhalt der Aufgaben auf dem didaktisch bewährten Übungsmaterial der TU Dresden und BA Dresden (Studienakademie Sachsen). Für die Inspiration danken die Autoren besonders den Kollegen Prof. Dr. rer. nat. habil. Dr. h. c. Alexander Schill, Dr. habil. J. Spillner und Dr.-Ing. M. Feldmann.

Die praktischen Aufgaben werden mit den begleitenden Musterlösungen angeboten.

WISSEN:

Die Studenten erhielten eine Einführung in den aktuellen Stand der Technik. Aktuelle Standards aus dem Internet, zu mobilen Netzwerken und zu Rechnernetzanwendungen stehen im Buch in den Teilen I, II und III im Mittelpunkt.

Effiziente Architekturen, Prinzipien und Systeme zu mobiler Kommunikation, Kriterien zur Optimierung von Netzwerken und Verteilten Systemen und Ideen zu modernen Technologien wie Clouds, Parallel und Fog Computing, IoS/IoT wurden weitgehend diskutiert.

Die Studierenden sind befähigt,

- die Lösungen zu Clouds, Parallel und Fog Computing, IoS/IoT zu bewerten, zu verwalten und auf der Basis einer hinreichenden konzeptionellen Fundierung in die Praxis umzusetzen.
- die Datensicherheitsaspekte von Rechnernetzanwendungen beurteilen zu können und erteilte Systeme und mobile Apps möglichst datenschutzkonform gestalten zu können.
- zur Entwicklungstrends von Architekturen von Netzwerken und Verteilten Systemen und der damit verbundenen Probleme Stellung nehmen zu können.

Inhaltsverzeichnis

Über die Autoren

Prof. Dr. habil. Andriy Luntovskyy
ist Professor an der BA Dresden. An der BA Dresden arbeitet er seit 2008. Im Zeitraum 2001 bis 2008 arbeitete Herr Luntovskyy als wiss. MA am Lehrstuhl Rechnernetze an der Technischen Universität Dresden. Seine „Alma Mater" ist die Technische Universität Kiew „Igor Sikorsky KPI" (Abschluss 1989).

Interessen-/Lehrgebiete:
1. Rechnernetze und mobile Kommunikation
2. Verteilte Systeme und angewandte Datensicherheit
3. Softwaretechnik und Betriebssysteme
4. Grundlagen der Programmierung / Informatik.

Kontakt: Staatliche Studienakademie Sachsen (BA Dresden), Andriy.Luntovskyy@ba-dresden.de

Dr. rer. nat. Dietbert Gütter (em.)
ist nebenberuflicher Dozent an der TU Dresden und an der BA Dresden. Seine „Alma Mater" ist die Technische Universität Dresden (Promotion 1974). Er arbeitete mehr als 40 Jahre in Dresden als wiss. MA am Lehrstuhl Rechnernetze an der TU Dresden, BA Dresden und anderen akademischen Institutionen.

Interessen-/Lehrgebiete:
1. Rechnernetze und Betriebssysteme
2. Netzwerkpraxis und -projektierung
3. Web-Anwendungen und Softwaretechnik
4. Informations- und Kommunikationssysteme.

Kontakt: Technische Universität Dresden, Dietbert.Guetter@tu-dresden.de

Aufgabenstellungen zu praktischen Übungen

Der Mensch tut gut daran, einen Bleistift bei sich zu tragen und die Gedanken, wenn sie kommen, niederzuschreiben.
(Sir Francis von Verulam Bacon, 1561–1626, englischer Philosoph und Staatsmann, entwarf die Methodologie der Wissenschaften)

Inhaltsverzeichnis

1 Aufgaben zum Komplex I – Übertragungsorientierte Schichten

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze – Übungsbuch*,
https://doi.org/10.1007/978-3-658-25619-7_1

1.1 Dienstelemente für einen abstrakten Telefondienst

a. Erstellen Sie ein folgendes Ablaufdiagramm für einen abstrakten Telefondienst, bei dem ein Initiatorprozess A eine Gesprächsverbindung zum Responderprozess B aufbauen will:
   - Zuerst hört der Prozess A bei einer ersten Verbindungsaufnahme ein Besetztzeichen und es kommt keine Verbindung zustande.
   - Beim zweiten Versuch wird die Verbindung zwischen Prozess A und Prozess B erfolgreich aufgebaut.
   - Die Daten werden übertragen (unbestätigter Datentransfer) und danach wird die Verbindung abgebaut.

b. Zeichen Sie das dazugehörige Zustandsdiagramm entsprechend den Vorgaben von Aufgabe a)!

1.2 Funkübertragungskanal nach Nyquist-Theorem

Über einen digitalen Funkübertragungskanal soll eine Datenrate von 160 MBit/s übertragen werden.

a. Wie groß sind Schrittgeschwindigkeit und minimale Bandbreite des (rauschfreien) Übertragungskanals, wenn pro Signalschritt 16 Bit kodiert werden können?

b. Auf welchen Wert erhöht sich die minimal erforderliche Bandbreite bei einem Signal-Rausch-Verhältnis auf dem Übertragungskanal von SNR = 1023?

1.3 Multiplexverfahren: Frequenzmultiplex vs. OFDM

a. Die Kanalbandbreite eines analogen Fernsehkanals beträgt 5,5 MHz. Wie viele Fernsehprogramme könnten durch ein Kabelverteilnetz im Frequenzmultiplex angeboten werden, wenn ein Frequenzband von 170–299 MHz nutzbar ist und zwischen den Kanälen ein Sicherheitsabstand von 1000 kHz einzuhalten ist?

b. Welche Vorteile bringt der Einsatz des OFDM-Konzepts im Vergleich zum Frequenzmultiplex?

1.4 Modulationsverfahren

a. Was ist ein Modulationsverfahren?
b. Stellen Sie die Übertragung der Bitfolge „0101100100100“ dar mit Amplitudentastung, Frequenztastung und Phasentastung!

1.5 IP-Adressen und Klassenbildung

a. Welche der vorgegebenen IPv4-Adressen sind falsch? Für richtige Adressen definieren Sie die Klassen (A, B, C, D) und tragen sie in die Tabelle ein!
b. Welche der Adressen sind Hostadressen (bitte vermerken)?
c. Welche der Adressen sind Netzwerkadressen (bitte vermerken)?
d. Welche der Adressen sind Broadcast/Multicast-Adressen (bitte vermerken)?

IP-Adresse	Klasse bzw. Typ oder fehlerhaft?
315.115.115.115	
117.117.117.117	
133.177.133.177	
115.0.0.0	
221.225.3.225	
155.122.0.0	
225.251.177.233	
235.225.235.735	

1.6 Distance Vector Routing

Gegeben sei folgendes Netzwerk (◘ Abb. 1.1):
Die Router sind in der Lage, die Übertragungskosten zu ihren Nachbarn zu bestimmen.

Im 30-Sekunden-Rhythmus senden sie ihre Distanzvektoren DV an ihre Nachbarn.

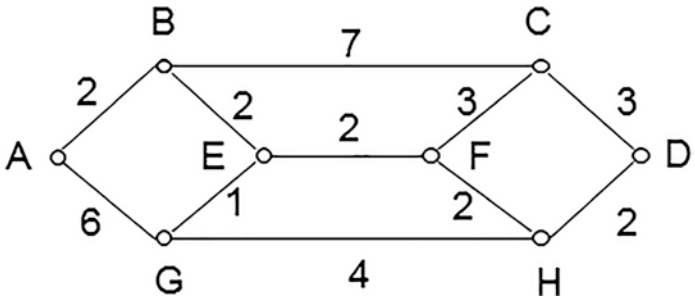


Abb. 1.1 Vermaschtes Netzwerk mit Knoten A, B, C, D, E, F, G, H

Hinweis:
Die Komponenten der Vektoren stellen die aktuelle Distanz vom Router zu den anderen Routern (Distanz zu A, Distanz zu B, …, Distanz zu H) dar.

a. Wie ändert sich die Routingtabelle des Knotens E, wenn dieser nach einem Systemausfall folgende Distanzvektoren von seinen Nachbarn erhält?
   von B (2, 0, 7, 8, 2, 4, 3, 6)
   von F (6, 4, 3, 4, 2, 0, 3, 2)
   von G (5, 3, 6, 6, 1, 3, 0, 4)
b. Nach wie viel Schritten ist der Inhalt der Routingtabelle stabil?
c. Überlegen Sie sich, ob der Inhalt der Tabelle bei zeitveränderlichen Metriken immer zu einem optimalen Ergebnis führt!

1.7 IP – Fragmentierung

Ein TCP-Segment mit 2048 Byte Nutzdaten wird an IP zur Auslieferung übergeben.

Der Übertragungsweg geht über zwei Netzwerke (Quellrechner → Router → Zielrechner).

Jedes Netzwerk hat eine Maximalgrenze MTU für die IP-Paketgröße.

Netzwerk 1 - MTU = 1024 Byte

Netzwerk 2 - MTU = 512 Byte

a. Geben Sie für die beim Empfänger ankommenden Fragmente jeweils die Größe und den Offset an.
b. Wie viele Fragmente würden erzeugt, wenn der Sender wüsste, dass die kleinste MTU auf den Pfad zum Empfänger 512 Byte beträgt?

1.8 Netto/Brutto-Datenrate in der Schichtenarchitektur

Ein Rechnernetz mit einer 7-Schichtenarchitektur habe pro Schicht einen Verlust der Datenrate von a = 15 % infolge Overhead. Wie hoch ist die Anwendungs-Übertragungsrate in einem 10Gigabit-Ethernet-LAN (10 GBit/s)?

1.9 Internet-Schichtenarchitektur und Netto-/Brutto-Verhältnis

a. Das Internet besitzt eine 4-Schichtenarchitektur und habe für die 2.Schicht einen Verlust der Datenrate von 10 % infolge Overhead. Jede nächste Schicht hat einen um 5 % höheren Overhead. Wie hoch ist die Anwendungs-Übertragungsrate (Schicht 4) in einem Gigabit-Ethernet-LAN (Netto-DR = 1000 Mbit/s)?
b. Wie groß ist das Netto-/Brutto-Verhältnis in diesem Fall?

1.10 Fehlerbehandlung durch Paritätskontrolle

Der ASCII-Basiskode ist ein Zeichendarstellungskode für Klein- und Großbuchstaben des englischen Alphabets, sowie für Ziffern, Sonder- und Steuerzeichen

Auszug (hexadezimale Darstellung)

A	B	...	O	P	Q	...	Z
0×41	0×42		0×4F	0×50	0×51		0×5A

a. Notieren Sie zeichenweise untereinander die Zeichenkette „ABCDPQRS“ in binärer 7-bit-Darstellung.
b. Fügen Sie ein Kontrollbit für gerade Parität hinzu.
c. Welche Bitfehlersituationen können erkannt und welche korrigiert werden?
d. Wie hoch ist bei einer Bitfehlerwahrscheinlichkeit von 10^{-3} die Wahrscheinlichkeit eines fehlerhaften Zeichens und wie hoch ist die Wahrscheinlichkeit, dass der Fehler nicht erkannt wird?
e. Fügen Sie ein Kontrollzeichen für gerade Blockparität hinzu.
f. Welche Bitfehlersituationen können erkannt und welche korrigiert werden?
g. Für welche Anwendungen wäre ein solcher Kode geeignet?

1.11 Fehlerkorrigierende Codes

Folgende Tabelle enthält die Kodeabbildung für die Zeichen „A“, „B“, „C“ und „D“:

A	B	C	D
000000	111000	000111	111111

a. Wie würden Sie die folgenden, zum Teil gestörten Bitfolgen interpretieren?
   - 100000
   - 001111
   - 101111
   - 000111
   - 101010
b. Wie groß ist die Hamming-Distanz des Codes?
c. Wie viele Bitfehler lassen sich erkennen und wie viele korrigieren?

1.12 Cyclic Redundancy Check (CRC)

Um Übertragungsfehler erkennen zu können, wird mit den Daten noch eine redundante Bitfolge fester Länge, die sogenannte Sicherungssequenz (Frame Check Sequence), gesendet. Diese wird durch eine Polynomdivision ermittelt, bei der der Dateninhalt durch ein sogenanntes Generatorpolynom (bzw. Prüfpolynom) „dividiert“ wird. Der Divisionsrest dient als Prüfsequenz und wird nach den letzten Informationsbits gesendet.

Die Informationsbits werden dabei sequentiell in einen Puffer (Größe = Polynomgrad plus 1) geschrieben und dann sequentiell gesendet. Im Puffer erfolgt bei jedem Takt ein bitweises Exclusiv-Oder (EXO) mit den Koeffizienten des Generatorpolynoms, falls das führende Bit im Puffer den Wert „1“ besitzt.

Im folgenden Beispiel verwenden wir aus rechentechnischen Gründen eine sehr kurze Sendebitfolge und ein sehr kleines Polynom.

Zu übertragen seien die Daten (10 Bits): 1010001101
Als Prüfmuster dient das Polynom: $x^3 + x + 1$

a. Berechnen Sie daraus die Sicherungssequenz!
b. Belegen Sie Ihr Ergebnis dadurch, dass Sie den Empfang des korrekt gesendeten Frames überprüfen!

■ **Hinweis**

Der „Quotient“ muss nicht berechnet werden, da nur der Rest benötigt wird.

1.13 Protokolle der Sicherungsschicht

a. Vergleichen Sie die Protokolle HDLC und PPP miteinander!

1.14 Überlaststeuerung

Beim Choke-Verfahren wird an einem Router eine Messreihe von relativen „Lastwerten" ermittelt. Dieser Lastwert repräsentiert z. B. die Länge einer Warteschlange. Kurzzeitige Überschreitungen einer Grenzlast (Schwellwert) werden toleriert, aber bei dauerhafter Überschreitung wird ein sogenanntes Choke-Paket an den Quellknoten gesendet. Dieser muss dann die Sendeleistung verringern (Standard 50 %) und steigert sie dann langsam wieder.

So spielt sich ein vernünftiges Gleichgewicht der Paketsenderate ein.

Periodisch wird folgende Berechnung im Router ausgeführt.

$$\text{Last}_{\text{neu}} = a * \text{Last}_{\text{alt}} + (1 - a) * \text{Last}_{\text{aktuell}}$$

Dabei bedeuten:		
	Last_{neu}	Schätzung der Last für nächsten Zeitraum
	a	Anpassungsfaktor (Konstante des „Vergessens" der Historie)
	Last_{alt}	Last des vorherigen Zeitraumes
	$\text{Last}_{\text{aktuell}}$	Wert der momentanen Last

Im folgenden Beispiel wird an einem Gateway-Rechner eine Messreihe von relativen „Lastwerten" ermittelt: {1/5/8/9/9}. Als Schwellwert wird 7.9 verwendet, als Anpassungsfaktor 0.3.

Wann wird ein Choke-Paket gesendet?

1.15 Einsatz von IP: Adressen und Subnetze

Die Kommunikation in modernen Rechnernetzen erfolgt auf der Basis der Internet-Technologie (TCP/IP). Als universelle Adressen werden IPv4-Adressen eingesetzt.

a. Erläutern Sie den Aufbau der IPv4-Adressen und die Aufteilung des Adressraums in die Klassen A–D, sowie die Aufteilung durch Netzmasken!
b. Welche Unterschiede sehen Sie in der Nutzung von MAC- und IP-Adressen?
c. Erläutern Sie den Einsatz von Subnetzmasken beim Routing! Welche Vorteile bringt die Maskierung (s. Abb. 1.2)?

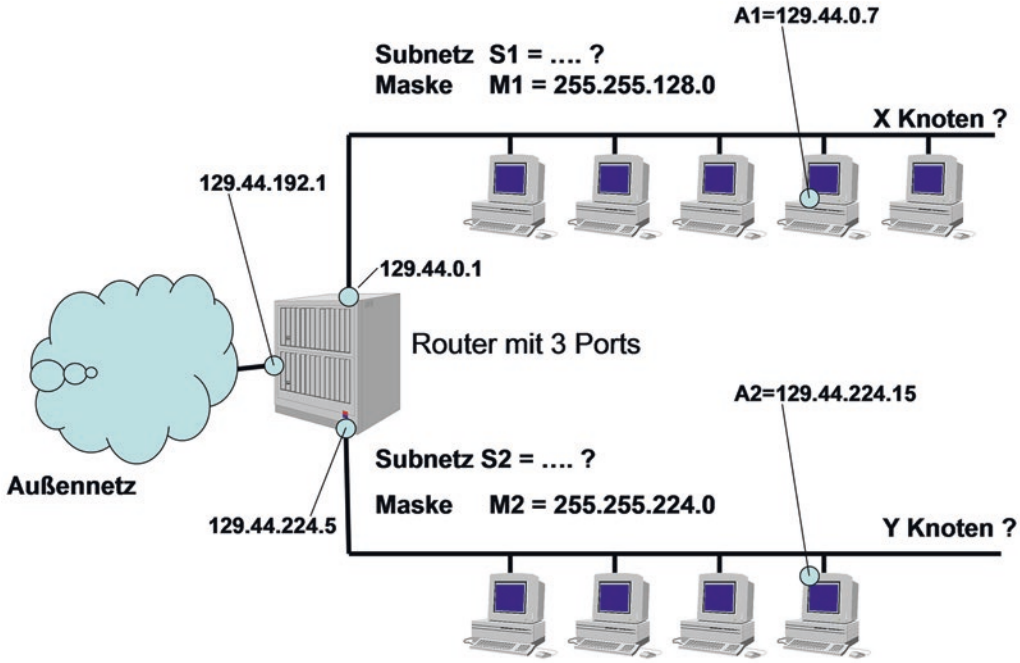


Abb. 1.2 Netzwerkszenario mit Router und Subnetting

Berechnen Sie für die gegebene Skizze:

d1) Die Knotenadresse im Subnetz S1 ist A1 = 129.44.0.7, die Subnetzmaske ist M1 = 255.255.128.0. Definieren Sie die Subnetzadresse S1! Wie hoch ist die maximale Knotenanzahl X in diesem Subnetz?

d2) Die Knotenadresse im Subnetz S2 ist A2 = 129.44.224.15, die Subnetzmaske ist M2 = 255.255.224.0. Definieren Sie die Subnetzadresse S2! Wie hoch ist die maximale Knotenanzahl Y in diesem Subnetz?

1.16 Hilfsprotokolle zum Einsatz von IP

a. Erläutern Sie Aufgaben des Hilfsprotokolls ARP!
b. Erläutern Sie Aufgaben des Hilfsprotokolls DHCP!

1.17 Weiterentwicklung von IP: IPng

Als einige der wichtigsten Weiterentwicklungen von IP, oder IP Next Generation (IPng), gelten u. a. die Protokolle IPv6 und IPsec.

a. Diskutieren Sie Vor- und Nachteile von IPv6 im Vergleich zu IPv4!
b. IPsec stellt effiziente Sicherheitsmechanismen auf der Schicht 3 dar. Diskutieren Sie diese! Wie sehen die modifizierten IPsec-Pakete aus?

1.18 Quality of Service in der Transportschicht

Die Transportschicht lässt das Aushandeln von QoS-Parametern für die Kommunikation zwischen den Endsystemen in der Phase des Verbindungsaufbaues zu.

a. Welche Parameter kommen hierfür infrage? Diskutieren Sie diese!
b. Der Nutzer des Transportdienstes benötigt die folgenden QoS-Parameter:
   kontinuierlich 1200 Byte/s,
   Verschlüsselung der zu übertragenden Daten.

Skizzieren Sie die Ablaufdiagramme für die nachfolgenden Szenarien:

b1. Der Responder kann die gewünschten Parameter erfüllen.
b2. Der Responder kann die Datenrate nur zu 75 % garantieren, nach Rücksprache mit der Anwendung akzeptiert der Initiator.
b3. Der Responder kann die Datenrate nur zu 75 % garantieren, der Initiator kann nicht akzeptieren und baut die Verbindung ab.
b4. Die Instanz zur Verschlüsselung beim Responder ist ausgefallen und es gibt keine Redundanz.

1.19 Ablauf- und Zustandsdiagramme für die Transportschicht

Ergänzen Sie die Aufgabe 1.1 um einen bestätigten Datentransfer für die Transportschicht.

Dienste müssen durch die untenstehenden Dienstprimitive realisiert werden.

Dienste	Zugehörige Dienstprimitive
Verbindungsaufbau	ConReq/ConInd/ConRsp/ConCnf
Datentransfer, bestätigt	DatReq/DatInd/DatRsp/DatCnf
Datentransfer, unbestätigt	DatReq/DatInd
Verbindungsabbau	DisReq/DisInd

c. Zeichnen Sie das Ablaufdiagramm für die Dienstfolge: Verbindungsaufbau → Datentransfer, bestätigt → Verbindungsabbau!
d. Modellieren Sie die Aufgabe a) als Zustandsdiagramm!

1.20 Übersicht der Netzwerkfunktionen und Kommunikationsschichten

Ordnen Sie die Begriffe in der ersten Spalte der folgenden Tabelle den richtigen Kommunikationsschichten (Spalten 2–6) zu. In einigen Fällen kann ein Begriff mehreren Schichten zugeordnet werden. Als Schichten stehen die OSI-Schichten Bitübertragungsschicht, Sicherungsschicht, Vermittlungsschicht, Transportschicht und die Anwendungsschicht des TCP/IP-Referenzmodells zur Verfügung (◘ Tab. 1.1).

◘ **Tab. 1.1** Netzwerkfunktionen und Kommunikationsschichten. Tabelle zum Vervollständigen

Begriff	Bitübertragungs-schicht	Sicherungs-schicht	Vermittlungs-schicht	Transport-schicht	Anwendungs-schicht
TCP als Bsp.	–	–	–	X	–
DHCP					
CSMA/CD					
BGPv4					
Client-Server-Anwendung					
DSL					
HTTPS					
IPv4					
UDP					
Koaxialkabel					
LWL					
Modem					
PPP					
Router					
Sockets					
Token Ring					
Twisted Pair					
WLAN					
Frequenz-multiplex					

1.21 Zusammenfassung Kapitel 1

Kapitel 1 bietet Ihnen praktische Aufgaben zu Komplex I (Übertragungsorientierte Schichten). Es werden physikalische Verfahren der Datenübertragung, Konzepte zum nachrichtentechnischen Kanal, Modellierung von Protokollen und Dienstelementen mithilfe Ablauf- und Zustandsdiagramme, Internet Protocol und Weiterentwicklung des Protokolls IPng diskutiert.

Außerdem werden Performance-Parameter in Netzwerken, Brutto- und Nettodatenraten sowie Parameter für QoS (Quality of Service) praktisch geübt.

Des Weiteren werden typische Adressierungsarten, Methoden für Fehlerbehandlung und Überlaststeuerung, Wegewahl/Routing in IP-Netzwerken betrachtet sowie fehlerkorrigierende Codierung und Prüfsummenverfahren (CRC) in sog. übertragungsorientierten Schichten im OSI-Referenzmodell (Layer 1 bis Layer 4) adressiert.

Aufgaben zum Komplex II – Netzwerktechnologien und Mobile Kommunikation. Netzkopplung und Verkabelung

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze – Übungsbuch*,
https://doi.org/10.1007/978-3-658-25619-7_2

2.1 Multiprotocol Label Switching (MPLS)

a. Erläutern Sie den Aufbau eines MPLS-Tunnels! Wie setzt man die Labels?
(siehe Teil II Lehrbuch, Abb. 12.6)
b. Beschreiben Sie den Gesamtablauf zwischen dem Quell-Host, den Ingress/Egress-Routern und dem Ziel-Host in Stichworten!
c. Nennen Sie die wesentlichen Unterschiede zwischen MPLS und ATM!

2.2 Ethernet und ALOHA: stochastische Medienzugriffsverfahren

a. Geben Sie die Klassifikation von Medienzugriffsverfahren an!
Welche Medienzugriffsverfahren werden als „stochastisch" bezeichnet?
b. Wie groß ist die Mindestframelänge beim „klassischen Ethernet" IEEE 802.3?
c. Wie groß müssten die Frames bei einem busförmigen Netz der Länge 100 km, einer Datenrate von 100 Mbit/s und einer Signalausbreitungsgeschwindigkeit von 200000 km/s mindestens sein?
d. Weshalb kann das CSMA/CD-Verfahren beim ALOHA-System nicht zum Einsatz kommen?

2.3 Netzwerktechnologien und WAN-Verbindungen

Im aufgeführten Beispiel (◘ Abb. 2.1) erfolgt der Zugriff zu den Diensten einer Cloud über „Thin Clients" mithilfe von Smartphones, Laptops oder PC/Desktops mit den folgenden Monatsdatenvolumina (V1, V2, V3, s. ◘ Tab. 2.1):

a. Welche Netzwerktechnologien ermöglichen diesen Zugriff? Nennen Sie 2–3 Beispiele!
b. Ergänzen Sie die unten aufgeführte Tabelle und kreuzen Sie zutreffendes an!

Konvention: 1 M = 1.000.000; 1 G = 10^9; 1 T = 10^{12}

Abb. 2.1 Netzwerkzugriff mithilfe von Smartphones, Laptops oder PC/Desktops

Tab. 2.1 Auswahl geeigneter Technologien zur Übertragung gegebener Volumina

Netzwerktyp	Typische DR, Mbit/s	V_1 = 450 TByte	V_2 = 2,3 TByte	V_3 = 5 TByte
ATM OC-3	155			
LTE	150			
DSL50	50			
HSDPA	14,4			
WLAN 802.11n	108…600			
10GbE	10.000			

Voraussetzungen Ein Monat hat im Schnitt 417 Arbeitsstunden, die durchschnittliche Auslastung der Verbindungen soll $\beta = 25\,\%$ nicht übersteigen, damit „burstartige" Belastungen abgefangen werden können (Tab. 2.1).

2.4 Netztechnologievergleich

Diskutieren Sie Vor- und Nachteile von MPLS, der Ethernet-Familie und ATM bei Einsatz als

- Last Mile Zugriff,
- Backbone,
- Lokales Netz

bezüglich
- Kosten,
- Dienstqualität (Anwendungen),
- Interoperabilität,
- Management,
- Datensicherheit.

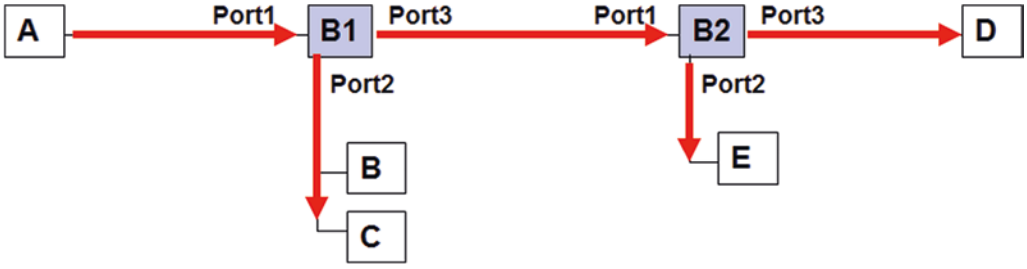
Die Ergebnisse stellen Sie bitte tabellarisch dar!

2.5 Kopplungselemente: Transparent Bridges

Gegeben sei die folgende LAN-Topologie (◘ Abb. 2.2) mit den Rechnern A…E und den transparenten Bridges B1, B2:

Wie werden die Wegewahltabellen bei transparenten Bridges aufgebaut?

a. Skizzieren Sie den Weg nacheinander gesendeter Frames mit folgenden Quell-/Zieladressen: (A/D), (B/A), (E/C), (B/E)!
b. Erfassen Sie in Tabellen, in welchen Schritten die Brücken ihre Kenntnisse über die Topologie des Netzes erwerben! Welche Informationen werten sie dazu aus?
c. Ergänzen Sie das Netz von b) um weitere Brücken, sodass alternative Wege möglich sind! Welche Probleme ergeben sich in diesem Fall für die Frameweiterleitung?
d. Benötigt man zur Lösung der Probleme von c) einen komplexen Routingalgorithmus (z. B. OSPF) oder gibt es einfachere Lösungen?



◘ **Abb. 2.2** LAN-Topologie mit Transparent Bridges

2.6 Strukturierte Verkabelung und Einsatz von Switches als Kopplungselemente (am Bsp. der Vernetzung eines Studentenwohnheims)

Für ein Studentenwohnheim mit 3 Etagen (je 10 Zimmer) mit Anschluss an das Campusnetz und an das Internet soll eine Netzkonzeption erarbeitet werden.

a. Diskutieren und vergleichen Sie mögliche Ansätze im Bereich der Verkabelung!
b. Was bedeutet der Begriff „Strukturierte Verkabelung"?
c. Wählen Sie geeignete Netztechnologien und dafür erforderliche Koppelelemente aus!

2.7 Firewall als Kopplungselement

a. Welche Basiskonzepte für die Firewalls sind Ihnen bekannt? Nennen Sie drei Firewallkonzepte und geben Sie ihre Zuordnung zu den OSI-Schichten an!
b. Nennen Sie Beispiele, bei denen die Verwendung eines Paketfilter-Firewalls ausreicht bzw. bei denen eine anwendungsbezogene Filterung erforderlich ist! Diskutieren Sie am Beispiel einer Schule.
c. Warum gibt es eine sog. demilitarisierte Zone (DMZ)?
d. In welcher Zone des Netzes können private Adressen eingesetzt werden? Welche Vorteile bringt dies?

2.8 Satellitenfunk

Wie lange dauert die Datenfunkübertragung eines Datenpakets mit Länge $L = 1000$ Byte zwischen einer terrestrischen Station und einem Satelliten (Uplink-Modus) auf der Orbithöhe $h = 1200$ km bei der maximalen Bitrate des Senders $DR = 10$ MBit/s?

a. Berechnen Sie die Gesamtzeit bei der Satellitenfunkkommunikation! Beachten Sie die korrekte und SI-konforme Umwandlung der Maßeinheiten!
b. Zu welcher Satellitenklasse (LEO, MEO, GEO) gehört der oben genannte Satellit? Welche Pro und Kontra haben Satelliten dieser Klasse?

2.9 Klassen von Satellitensystemen

Berechnen Sie die in der unten aufgeführten Tabelle (◘ Tab. 2.2) fehlenden Angaben (ggf. Satellitenhöhe h oder Umlaufperiode T).

Hinweis
Die Umlaufperiode T ergibt sich zu $T = \text{sqrt}((R + h)^3 / a)$ mit der Konstante

$$a = g * R^2/(2 * PI)^2$$

mit dem Erdradius R = 6378 km und der Konstante g = 9,81 N/kg (sqrt bedeutet Quadratwurzel).
Geben Sie Acht, dass Sie die richtigen Maßeinheiten verwenden!

a. Berechnen Sie die lineare Geschwindigkeit v_{GPS} bei der gegebenen Satellitenhöhe h_{GPS} für GPS-Erdsatelliten mit der Umlaufperiode T_{GPS}!
b. Berechnen Sie die lineare Geschwindigkeit v_{ISS} bei der gegebenen Satellitenhöhe h_{ISS} für GPS-Erdsatelliten mit der Umlaufperiode T_{ISS}!

Hinweis zu a) + b)

$$v = (2PI/T) * (R + h)$$

◘ **Tab. 2.2** Zusammenhang Satellitenhöhe und Umlaufperiode. Tabelle mit fehlenden Angeben zum Ergänzen

Typ	Satellitenhöhe h	Umlaufperiode T
GEO (Geostationary Earth Orbit Satellite)	?	24 h
MEO (Middle Earth Orbit Satellite)	7000 km	?
LEO (Low Earth Orbit Satellite)	700 km	?
GPS (Global Positioning System, US NAVSTAR-Satellite)	20.200 km	?
ISS (International Space Station)	?	92 Min

2

2.10 Frequenzspektrum und Funknetze

a. Werten Sie das nachfolgende Bild aus (◘ Abb. 2.3).

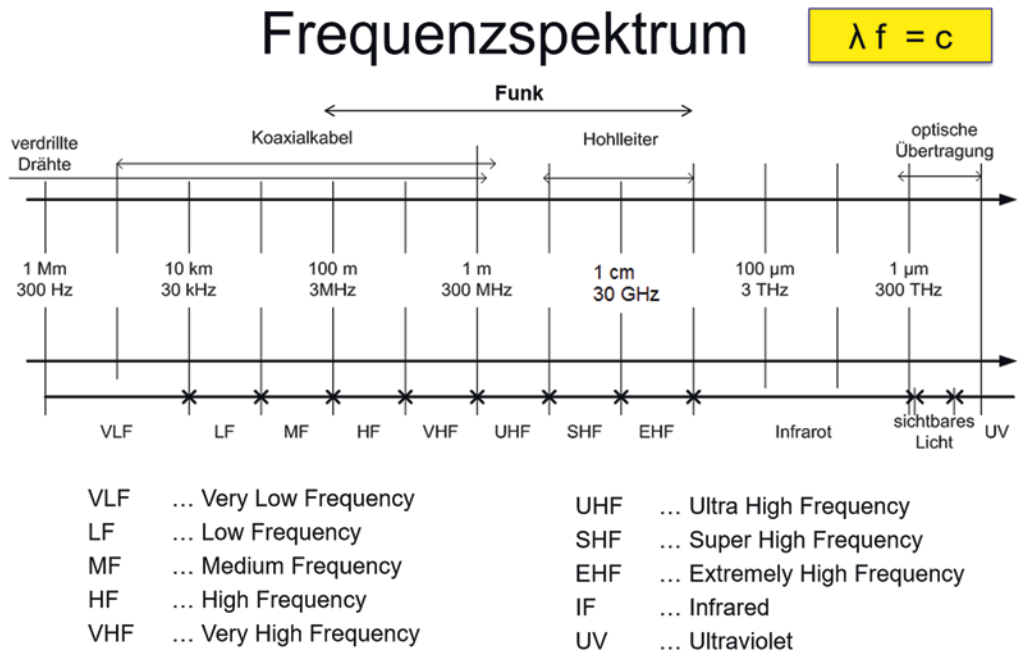
Geben Sie die Klassifikation von Frequenzbereichen und Wellenlängen an!

In welchem Frequenzbereich kommen die Funknetze zum Einsatz?

b. Welche Besonderheiten treten bei jeweiligen Wellentypen auf? Warum ist die LOS-Anforderung für Funkkommunikationssysteme von Bedeutung?

c. Typische Wellenlängen λ für Mobilfunkstandards sind nachfolgend aufgeführt:
   - GSM (890–960 MHz, 1710–1880 MHz), λ = 0,33 m (900 MHz)
   - WLAN IEEE 802.11b/g/n (2,4 GHz), λ = 0,125 m
   - WLAN IEEE 802.11a/n (5 GHz), λ = 0,06 m
   - WiMAX IEEE 802.16a (2–11 GHz), λ = 0,03 m (10 GHz)
   - WiMAX IEEE 802.16 (10–66 GHz), λ = 0,0045 m (66 GHz)

Wie hängen die Wellenlängen und Frequenzen zusammen?



◘ **Abb. 2.3** EM-Schwingungen: Frequenzbereiche und Wellenlängen

2.11 Spektraleffizienz

a. Was versteht man unter dem Begriff „Spektraleffizienz“?
b. Wie errechnet sich maximale Spektraleffizienz eines Mobilfunksystems anhand der Nyquist- Theoreme?

2.12 Antennentechnik und Funknetze

a. Was ist eine Antenne? Welche Antennenarten kennen Sie? Welche Antennenarten kommen bei WLAN zum Einsatz? Welche Antennenarten kommen beim Mobilfunk zum Einsatz?
b. Diskutieren Sie Vorteile MIMO vs. SISO! Führen Sie entsprechende Systembeispiele an!
c. Diskutieren Sie die Unterschiede zwischen den Begriffen „Richtfunk“ vs. „Rundfunk“ vs. „Sektorantennen“!
d. Was ist Handover in Mobilfunknetzen? Verdeutlichen Sie den Begriff!

2.13 Freiraumdämpfung/EIRP

Das Freiraumdämpfungsmodell (FSL, oder Free Space Loss Model) stellt das einfachste aller denkbaren Simulationsmodelle für die Ausbreitung von elektromagnetischen Wellen dar. Dabei wird angenommen, dass sich das Sendesignal kugelförmig um die Sendeantenne verteilt (isotroper Kugelstrahler).

Zu einer ersten Abschätzung der Empfangsqualität kann das Modell genutzt werden, obwohl dämpfende Umgebungsobjekte (z. B. Wände) nicht berücksichtigt werden.

Die FSL-Dämpfung kann nach folgenden Formeln berechnet werden, wobei d den Abstand zwischen Sende- und Empfangsantenne bedeutet, λ die Wellenlänge und f die Frequenz.

$$\mathrm{FRD} = \text{Sendeleistung/Empfangsleistung}$$
$$= (4\pi * \mathrm{d}/\lambda)^2 = (4\pi * \mathrm{f} * \mathrm{d}/\mathrm{c})^2$$

In der Praxis verwendet man meist die logarithmierte Form (Angabe in dB)

$$\mathrm{FRD}_{\log} = 10 * \log(\mathrm{FRD})$$
$$= 32{,}44 + 20 * \log(\mathrm{f}/\mathrm{MHz}) + 20 * \log(\mathrm{d}/\mathrm{km})$$

a. In einem WLAN ist ein Access Point im Außenbereich installiert mit der Sendefrequenz 2,4 GHz und der Sendeleistung Ptx = 30 mW. Wie groß ist die Empfangsleistung Prx in 35 m Abstand? (Wenden Sie das Modell der Freiraumdämpfung an.)

Vergleichen Sie die Ergebnisse nach den obigen zwei Formeln.

b. Ab welchem Abstand ist der Empfang nicht mehr möglich (Empfangsleistung unter 10^{-10} W)?
Der Gesetzgeber beschränkt die zulässige Sendeleistung, z. B. für WLAN 802.11b/g auf eine max. EIRP-Leistung von 100 mW. Für die Bestimmung der zulässigen Sendeleistung muss der Gewinn der verwendeten Antenne abgezogen werden.

c. Wie hoch darf die max. Sendeleistung bei IEEE 802.11g sein, wenn eine Sendeantenne mit einem Gewinn von 12 dBi eingesetzt wird?

2.14 FSL-Modelle im Mobilfunk

In der Mikrozelle eines Mobilfunknetzes im zugewiesenen Frequenzband von F = 2 GHz beträgt die minimale Empfangsleistung den Wert PRx = −92,5dBm bei der Sendeleistung von 0 dBm. Dies entspricht dem maximalen Pfadverlust PL (Path Loss) im Freien (s. Free Space Loss Model bzw. vorige Aufgabe!).

a. Schätzen Sie die maximale Reichweite d (Zellradius) für das Mobilfunknetz ab! Nutzen Sie das FSL-Ausleuchtungsmodell (Freiraumdämpfung) zum Modellieren der Pfadverluste!

b. Lösen Sie die Aufgabe bei dem minimal zulässigen Wert PRx = −72,5 dBm. Schätzen Sie die maximale Reichweite in diesem Fall ab. Wie ändert sich das Ergebnis?

Hinweis

Basierend auf dem Teil II Lehrbuch bzw. Buch [5]:

Vorsicht ist bei den Maßeinheiten geboten, z. B. liefert die Frequenzangabe in GHz:

$$\mathbf{FRD_{log} = 10 * log(FRD) = 92{,}44 + 20 * log(f/GHz) + 20 * log(d/km)}$$

2.15 Weitere Ausbreitungsaspekte in Funknetzen

a. Welche Funksignalausbreitungsaspekte soll man bei Aufbau von Funkkommunikationssystemen berücksichtigen? Geben Sie entsprechende Szenarien an.

b. Diskutieren Sie die wichtigsten Effekte der Wellenausbreitung je nach Wellenlänge!

2.16 Zusammenfassung Kapitel 2

Kapitel 2 enthält Aufgaben zu Komplex II (Netzwerktechnologien und Mobile Kommunikation. Netzkopplung und Verkabelung).

Praktische Aufgaben in Bezug auf Performance und QoS zur Vielfalt aktueller Netzwerktechnologien werden formuliert zwecks Festigung der schon gelernten Theorieansätze.

Außerdem werden stochastische (kollisionsbehaftete) Medienzugriffsverfahren für lokale Netze (Ethernet, WLAN), wie bspw. ALOHA, CSMA/CD, CSMA/CA in Betracht gezogen.

Des Weiteren wird MPLS als wichtige Integrationstechnik für Weitverkehrsnetze diskutiert. Praktische Netzwerke werden in Zusammenhang mit strukturierter Verkabelung, leistungsfähigen passiven und aktiven Kopplungselementen, wie Hubs, Bridges, Switches, Router, Access Points sowie mit den Komponenten für abgesicherten Nachrichtenverkehr (sog. Firewalls) betrachtet.

Neben drahtgebundenen Lösungen werden auch Themen wie Funknetze, mobile und SAT-basierte Systeme geübt. Weitere spezifische Aspekte, wie Dienste und Klassen von Satellitensystemen (LEO, MEO, GEO), zugelassene Frequenzspektren, Ausbreitungseffekte für Funknetze, Spektraleffizienz und Antennentechnik werden detailliert dargestellt und praxisnah geübt.

Aufgaben zum Komplex III – Verarbeitungsorientierte Schichten und Netzwerkanwendungen

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze – Übungsbuch*,
https://doi.org/10.1007/978-3-658-25619-7_3

3.1 Klassische Internetapplikationen

a. Warum ist es sinnvoll, dass einige Anwendungen anstelle des Transportprotokolls TCP das weniger leistungsfähige Protokoll UDP nutzen?
b. In welchen Fällen ist es sinnvoll, Dateien mittels des SMTP-Protokolls zu verschicken und in welchen Fällen eignet sich das Protokoll FTP besser?
c. Welche Gefahren entstehen bei Nutzung des TELNET-Protokolls?
   Zeigen Sie mögliche Maßnahmen zum Schutz auf!

3.2 Cloud Computing

In der Entwicklung der Rechnernetzwerktechnik gab es immer wieder Vorstellungen, die Funktionalität der Arbeitsstationen auf eine reine Terminalfunktion (Thin Client) zu begrenzen und alle Verarbeitungsfunktionen transparent in das Netzwerk auszulagern.

a. Vergleichen Sie die Unterschiede in der Last-/Funktionenverteilung zwischen Cloud Computing und herkömmlicher IT vs. SaaS vs. PaaS vs. IaaS!
b. Ordnen Sie die Cloud-Einsatzszenarios in der ersten Spalte der folgenden Tabelle (◘ Tab. 3.1) den richtigen Mustern von Cloud-Diensten (Spalten 2–4) zu. In einigen Fällen kann ein Begriff mehreren Mustern/ Spalten zugeordnet werden:

◘ **Tab. 3.1** Cloud-Einsatzszenarien

Dienstmuster	IaaS	PaaS	SaaS
– Cloud Backup			
– Data Center			
– VM Migration			
– Market Place			
– Hochleistungscluster für paralleles Rechnen			
– SOA Plattform			
– Test-Umgebung			
– Frontend			

3.3 Multimediale Netzwerkanwendungen und Mobilfunk

Ein Videostreaming wird mit dem Standard UXGA verwirklicht. Dieser ermöglicht die Bildauflösung von $V = 1600 \times 1200$ Pixel. Dabei wird die Farbkodierung $FT = 24$ Bit genutzt sowie die Bildfrequenz $fps = 25$ Bild/s. Diese Übertragung wird

a. zuerst ohne Kompression per Festnetzmietleitung vorgenommen.
   Wie groß muss die verfügbare Datenrate sein, wenn keine Kompression möglich ist?
b. Welche Netzwerktechnologien sind für dieses Videostreaming ohne Kompression am besten geeignet?
c. Die beschriebene Videoübertragung wird per Mobilfunk mit Kompressionsverfahren vorgenommen. Bei welchen Kompressionsraten KR ist diese Übertragung möglich, wenn die folgenden maximalen Datenraten bei Mobilfunk mittlerweile verfügbar sind. Bereichen Sie diese Werte und ergänzen Sie die angegebene Tabelle (ggf. aufrunden!):

Mobilfunknetz	Max. DR	Die zu berechnende Kompressionsrate KR
HSDPA	14,4 MBit/s	?
LTE	150 MBit/s	?

3.4 SNMP-Management

a. Angegeben seien ein Server mit installierter Managersoftware und ein Switch mit einem Agenten, zwischen denen SNMP-Nachrichten verkehren. Die beiden verweisen auf eine MIB. Ergänzen Sie das in ◘ Abb. 3.1 vorgegebene Weg-Zeit-Diagramm (Ablaufdiagramm).

3.5 Architekturwandlung in modernen Verteilten Systemen

Unsere Zeit wird durch die signifikante Architekturwandlung in Netzwerkservices und verteilten Systemen charakterisiert. Die Verarbeitungs-, Persistenz- und Anwendungsdaten werden von mehreren Servern oder Peers bereitgestellt.

a. Ergänzen Sie das unten aufgeführte Organigramm!
   Vergleichen Sie die Client-Server- und Peer-To-Peer-Architekturen (C-S/ P2P) in ◘ Abb. 3.2.
   Führen Sie jeweils 2-3 Beispiele an!

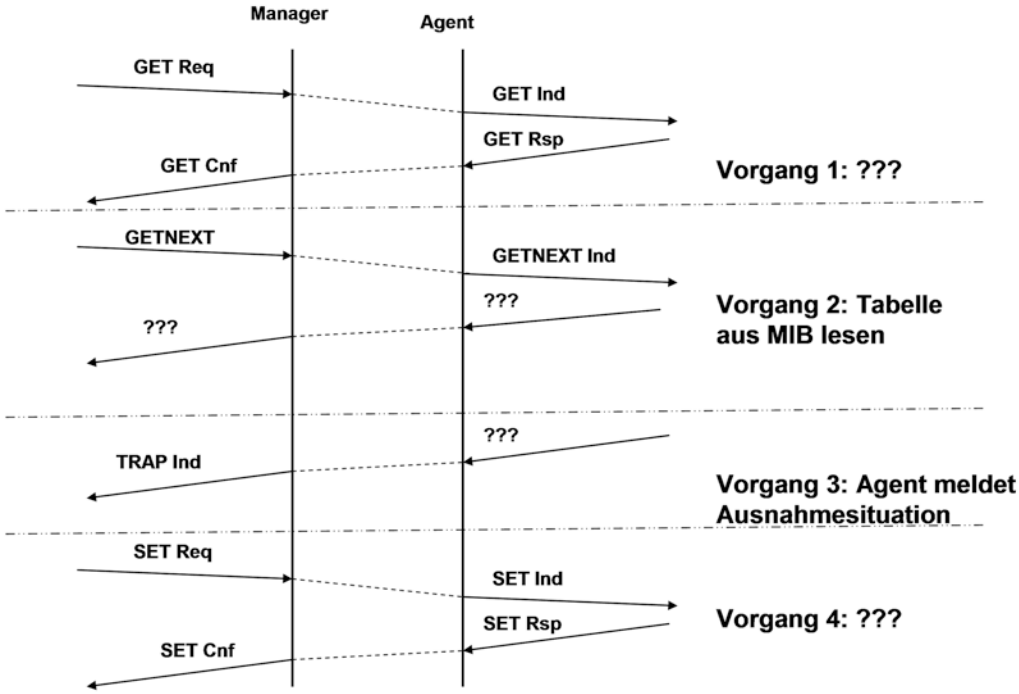


Abb. 3.1 SNMP-Ablaufdiagramm zum Vervollständigen

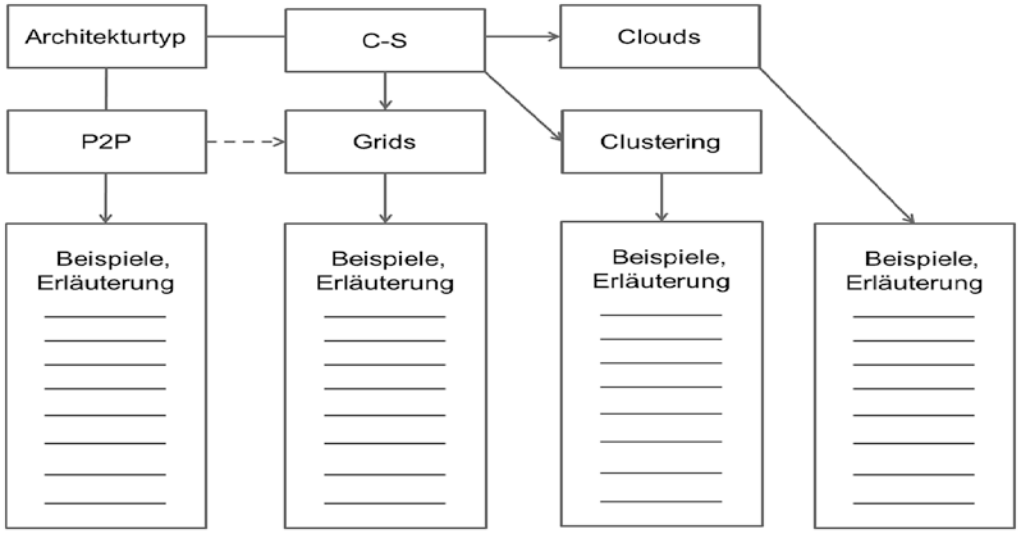


Abb. 3.2 Client-Server- und Peer-To-Peer-Architekturen

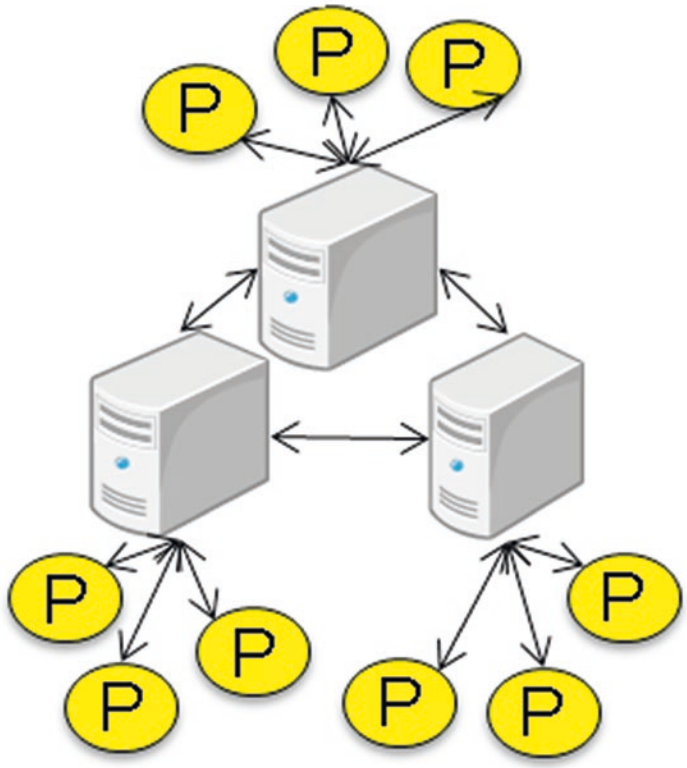


Abb. 3.3 Hybrides P2P

b. Erklären Sie die Funktionsweise von hybriden P2P/C-S-Systemen in Stichworten!
Nennen Sie jeweils drei Systembeispiele zu jedem der aufgeführten Architekturtypen mit der Erläuterung des Einsatzgebietes (s. Abb. 3.3)!

3.6 Videokonferenzen

Folgendes Szenario ist gegeben (s. Abb. 2.7, Teil III Lehrbuch): Sie möchten mit mehreren Partnern eine Videokonferenz aufbauen. Sie nutzen ein Mehrpunktkonferenzsystem mit einer sternförmigen Architektur und einer zentralen MCU (Multipoint Control Unit). Sie senden Ihr Video mit der Auflösung CIF mit einer Farbtiefe von 24 Bit/Pixel und einer Framerate von 15 fps.

a. Mit welchem Kompressionsfaktor müssen Sie ihr zu sendendes Videosignal komprimieren, wenn Sie einen Internetanschluss (Upstream: 192 kbit/s, Downstream: 2048 kbit/s) nutzen?
b. Mit wie vielen Partnern können Sie eine Videokonferenz aufbauen, wenn alle Partner Videos mit der gleichen Qualität mit dem Faktor 200:1 komprimiert senden und 10 % Overhead durch Protokoll-Header entsteht?
c. Im Regelfall sollte man aber nur maximal 60 % der zur Verfügung stehenden Bandbreite für die Videoübertragung nutzen. Wie kann die zu übertragene Datenmenge angepasst werden, damit Sie weiterhin mit allen Partnern kommunizieren können? Wie wirkt sich das auf die Qualität der Videos aus?

3.7 Fortgeschrittene Sicherheit in Netzwerken: Firewalls und CIDN

Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt und ist auch ein wichtiger Teilaspekt eines Netzwerks.

a. Vergleichen Sie die IDS/ IPS-Module (Intrusion Detection und Intrusion Prevention Systems) mit „klassischen" Firewalls! Verdeutlichen Sie die Unterschiede!
b. Nennen Sie Beispiele, bei denen die Verwendung eines Paketfilter-Firewalls ausreicht bzw. bei denen eine anwendungsbezogene Filterung erforderlich ist!
c. Wofür dient ein Circuit Relay?
d. Ergänzen Sie die folgende Tabelle (◘ Tab. 3.2) der Filtermöglichkeiten von Firewallsystemen. Ordnen Sie die Filterungsmöglichkeiten in der ersten Spalte der folgenden Tabelle den richtigen FW-Konzepten (Spalten 2–5) zu. In einigen Fällen kann ein Begriff mehreren Mustern/ Spalten zugeordnet werden:
e. Warum gibt es eine mehrstufige Firewall-Strategie? Diskutieren Sie anhand des unten aufgeführten Diagramms (◘ Abb. 3.4)!
f. Was ist CIDN?
   Welche Arten von Angriffen verhindern diese?

Tab. 3.2 Filtermöglichkeiten von Firewallsystemen. Tabelle zum Vervollständigen

Filterungsmöglichkeiten	PF (Paketfilter)	CR (Circuit Relay)	AG (Application Gateway)	Fortgeschrittenes FW-System
Zeitfensterkontrolle				
IP-Adressen und DMZ (Demilitarized Zone)				
Intrusion Detection und Intrusion Prevention Systems: IDS/IPS				
Zugelassene/verbotene Protokolle				
Malware-Blockierung, SPAM-Filter und Antiphishing				
anwendungsbezogene Authentisierung und Verschlüsselung				
Proxy für bestimmte Dienste, Proxyserver				
ausführbare Skripte, Applets, Web Services				
Web Application Firewall				
TCP-Ports und Blockierung von DDoS				

Bitte „X" falls zutreffend!

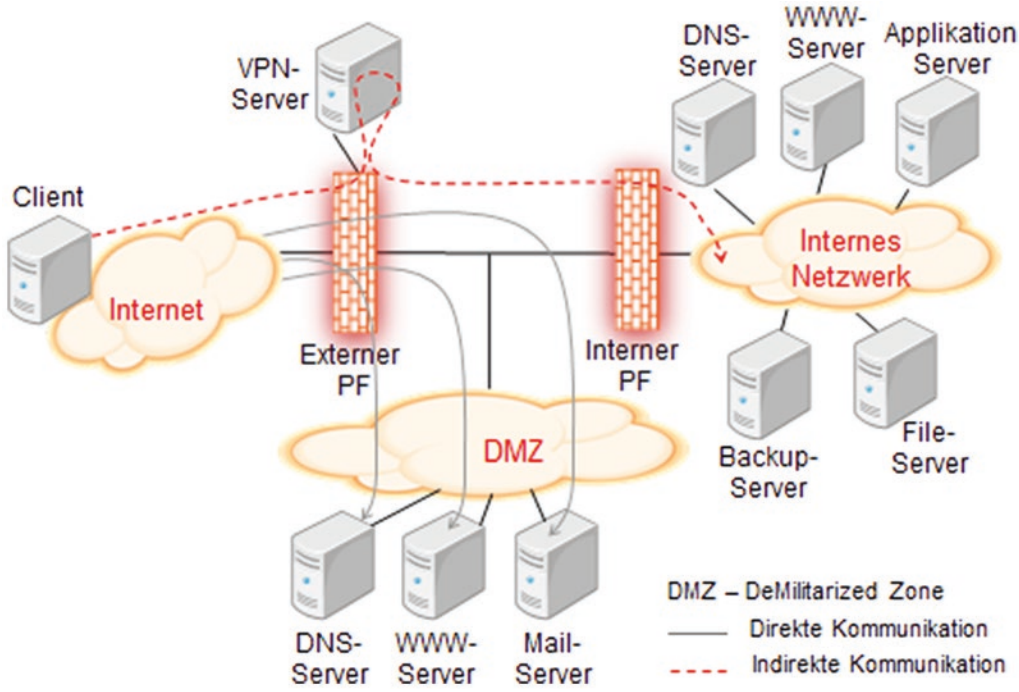


Abb. 3.4 DMZ und mehrstufige Firewall-Strategie

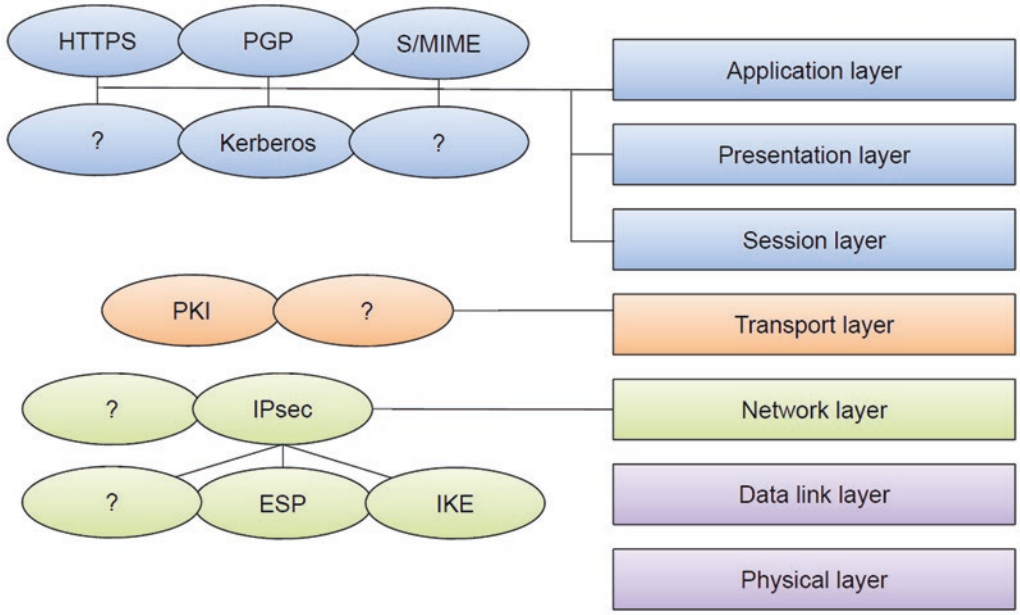
3.8 Kryptografische Absicherung in den Rechnernetzapplikationen

a. Kann es sinnvoll sein, in mehreren Netzarchitektur-Schichten Verschlüsselungsalgorithmen einzusetzen? Nennen Sie Beispiele!
b. Kann der Empfänger einer digital signierten Nachricht den Nachrichteninhalt verändern und eine passende Signatur erzeugen?
c. Wie kann man die folgende Aussage kommentieren: „TLS/SSL bietet stärkere Feingranularität bei der Absicherung für die Rechnernetzapplikationen als VPN/IPsec“.
Aus welchem Grund kann man so behaupten?

3.9 Kryptoprotokolle

Kryptoprotokolle sind Netzwerkprotokolle (i. d. R. Layer 3 bis 7), die die verschlüsselte und authentifizierte Datenübertragung über ein Computernetzwerk für die Verteilten Anwendungen garantieren.

a. Ergänzen Sie das Bild!
   Definieren Sie die fehlenden Kryptoprotokolle (◘ Abb. 3.5)!
b. Ordnen Sie die folgenden Kryptoprotokolle in der ersten Spalte der folgenden Tabelle (alphabetisch sortiert) den richtigen Kommunikationsschichten (Spalten 2–5) zu.
   Vermerk: In einigen Fällen kann ein Begriff mehreren Schichten zugeordnet werden, außerdem sind manche Begriffe gar keine Kryptoprotokolle! Als Schichten stehen die OSI-Schichten und die Schichten des TCP/IP-Referenzmodells zur Verfügung (◘ Tab. 3.3):



◘ **Abb. 3.5** Ausgewählte Kryptoprotokolle mit OSI-Schichtenzuordnung zum Vervollständigen

Tab. 3.3 Einordnung von Kryptoprotokollen. Tabelle zum Vervollständigen

Begriff	Vermittlungsschicht L3	Transportschicht L4	Anwendung L5–L7
AH			
ESP			
HTTPS			
IKE			
IPsec			
IRC			
IRCS			
PGP			
POP3			
PKI			
RSVP			
S/MIME			
SET			
Socket			
VPN			
VoIP			
TLS/SSL			

3.10 Backup und Cloud Backup

In einem Modellbetrieb bzw. KMU (Klein- und Mittelstandsunternehmen) erfolgt die Datenvollsicherung bzw. Cloud Vollbackup über die bestehenden VDSL und MPLS-Netzwerkverbindungen immer freitags um ca. 21 h. Außerdem finden weitere regelmäßige Backups statt.

Dafür werden zwei folgenden Verfahren eingesetzt:

- IB, steht für Inkrementelles Backup;
- DB, steht Differentielles Backup.

a. Ordnen Sie die Begriffe IB und DB den unten aufgeführten Bildern zu (Abb. 3.6)!
b. Diskutieren Sie jeweils zwei Pro- und zwei Contra-Argumente für die beiden Verfahren. Vergleichen Sie die beiden Verfahren anhand der angegebenen Tabelle.

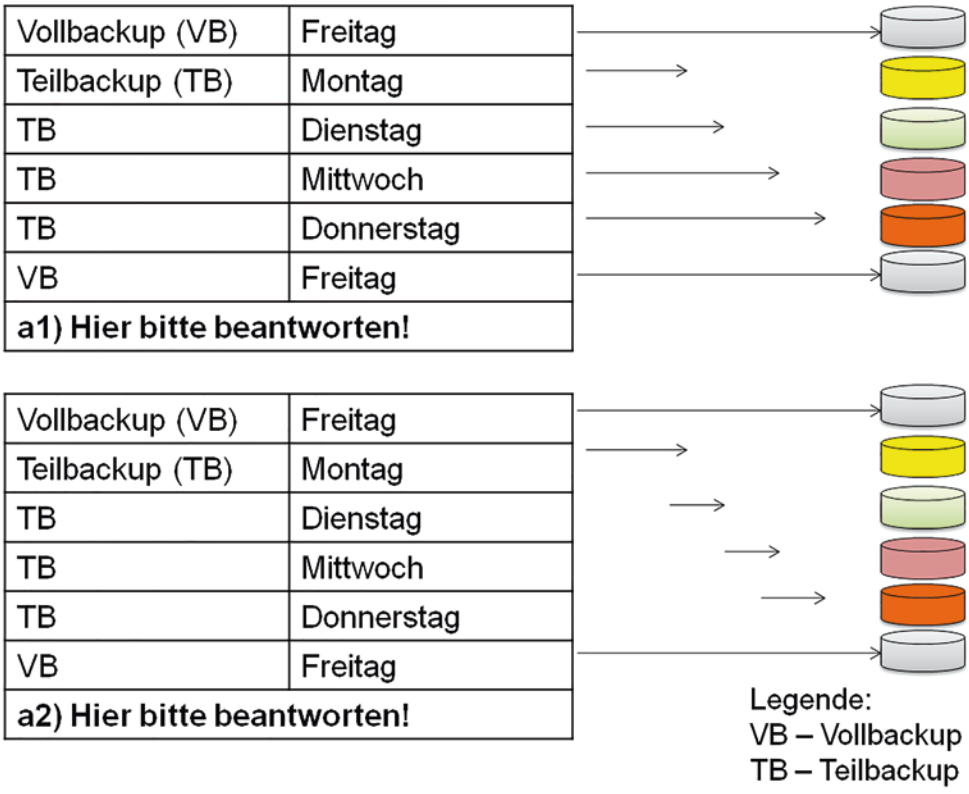


Abb. 3.6 Backup-Strategien

Die unten angegebene Tabelle ist auszufüllen!

Backup/ Datensicherungsverfahren	IB	DB
Vorteile	1. 2.	1. 2.
Nachteile	1. 2.	1. 2.

c. Nennen Sie mindestens zwei wesentliche Nachteile der Cloud Backup Lösung?

3.11 Virtualisierungsverfahren in Rechnernetzen

a. Was bedeutet der Begriff „Virtualisierung“ in aktuellen Rechnernetzen und Verteilten Systemen (Rechnerarchitekturen, Betriebssystemen und Applikationen)?

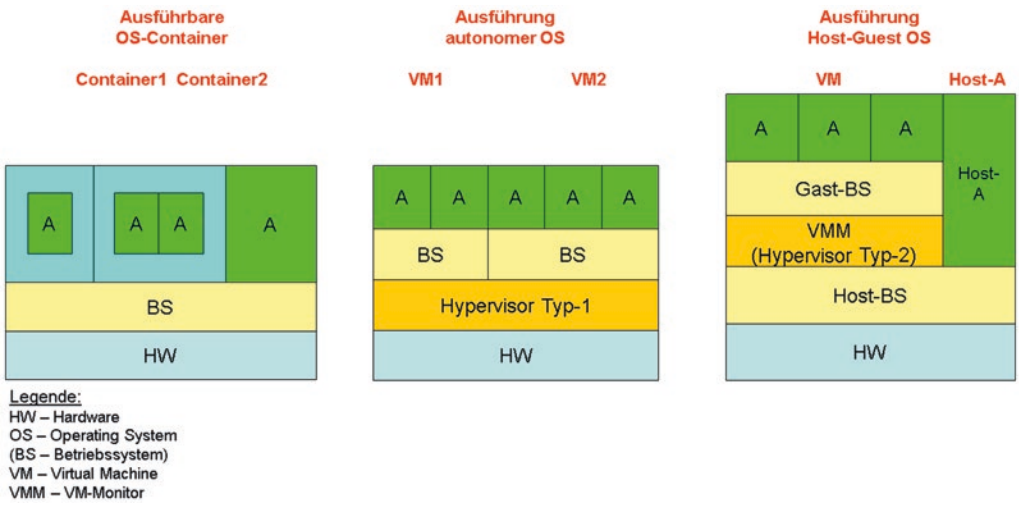


Abb. 3.7 Vergleich von Virtualisierungskonzepten: OS-Container, Hypervisor (Typ-1), VM-Monitor (Hypervisor Typ-2)

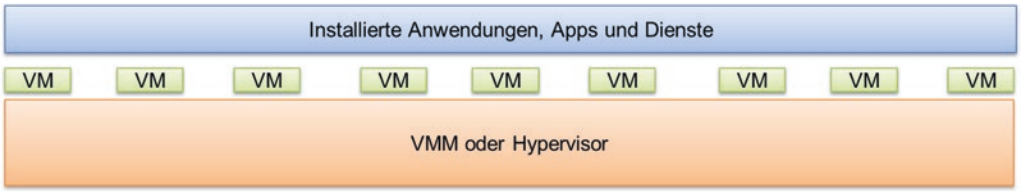


Abb. 3.8 Virtualisierungsszenario: Hypervisor oder Monitor, virtuelle Maschinen, installierte Anwendungen, Apps und Dienste

b. Existierende Virtualisierungsverfahren ermöglichen den Heterogenitätsabbau in aktuellen Rechnernetzen und im Mobilfunkumfeld (s. Abb. 3.7).
Dafür kommen die folgenden Konzepte zum Einsatz: OS-Container, Hypervisor (Typ-1) und VM-Monitor (Hypervisor Typ-2).

Welche Vorteile haben OS-Container bzw. im Mobilfunkumfeld gegenüber Hypervisor Typ-1 oder Typ-2? Nennen Sie wichtige Systembeispiele zum Konzept OS-Container!

c. Warum bietet ein Hypervisor Typ-1 eine günstigere Alternative zu einem VM-Monitor (Typ-2)? Nennen Sie mind. 2 Argumente diesbezüglich!
d. Nennen Sie mind. 3 Systembeispiele der Betriebssystemvirtualisierung (bedeutende Produkte am Markt)!
e. Ein leistungsstarker physikalischer Server in einem Mittelstandsunternehmen trägt 40 VM je mit dem Hauptspeicher 4 GB und der Festplatte 6 TB (s. Abb. 3.8)

Welche Mindestkapazitätsanforderungen und wie viel Reserve muss der Server haben? Begründen Sie den Vorschlag!

f. Wie viel Hauptspeicher insgesamt und welche gesamte Festplattenkapazität kann der phys. Server in dem Falle haben, um einen einwandfreien Betrieb von diesen 50 VM mit 10 %-Reserve zu gewährleisten? Begründen Sie den Vorschlag!

3.12 Entwicklungstrends in Rechnernetzen

a. Verdeutlichen Sie die Unterschiede zwischen IoT und IoS!
b. Was ist Fog Computing!
   Beschreiben Sie kurz die wichtigsten Netzwerktechnologien, die Fog Computing unterstützen!
c. Verdeutlichen Sie die Unterschiede zwischen Clouds und Fog Computing?
   Wie wird die Koexistenz gewährleistet?

3.13 Zusammenfassung Kapitel 3

Kapitel 3 stellt Aufgaben zu Komplex III (Verarbeitungsorientierte Schichten und Netzwerkanwendungen) zur Verfügung. Es geht um wichtige praktische Ansätze zu Rechnernetzanwendungen und deren integrierte Betrachtung an den Schichten 5–7 im OSI-Referenzmodell.

Die klassischen Basisdienste, konstruktive Besonderheiten moderner Netzwerkanwendungen und Apps im Desktop-Bereich und mobilen Umfeld sowie verbreitete Kommunikationsmodelle und Mechanismen werden diskutiert.

Durch die praxisnahen Aufgabenstellungen werden vielfältige aktuelle Internetapplikationen, Systemarchitekturen, Webanwendungen, mobile Apps, u. a. Cloud-Systeme, P2P, Fog, Systeme für Multimedia, Videostreaming und -Conferencing, Netzmanagement mittels SNMP adressiert.

Dieser Abschnitt bietet außerdem eine praktische Vorstellung über den Einsatz von Verteilten Systemen unter obligatorischer Nutzung einer effizienten Netzwerkarchitektur, über die Architekturwandlungen in aktuellen Verteilten Systemen, über die Virtualisierungsverfahren und Entwicklungstrends in Rechnernetzen.

Des Weiteren wird kryptografische Absicherung in den Rechnernetzapplikationen und angewandte Datensicherheit in Rechnernetzen diskutiert und geübt.

Musterlösungen

Probleme kann man niemals mit derselben Denkweise lösen, durch die sie entstanden sind.
(Albert Einstein, 1870–1955)

Inhaltsverzeichnis

Komplex I – Übertragungs-orientierte Schichten

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze – Übungsbuch*,
https://doi.org/10.1007/978-3-658-25619-7_4

4.1 Dienstelemente für einen abstrakten Telefondienst

a. Erstellen Sie ein Ablaufdiagramm für einen abstrakten Telefondienst, bei dem ein Initiatorprozess A eine Gesprächsverbindung zum Responderprozess B aufbauen will:
   - Zuerst hört der Prozess A bei einer ersten Verbindungsaufnahme ein Besetztzeichen und es kommt keine Verbindung zustande.
   - Beim zweiten Versuch wird die Verbindung zwischen Prozess A und Prozess B erfolgreich aufgebaut.
   - Die Daten werden übertragen (unbestätigter Datentransfer) und danach wird die Verbindung abgebaut.

b. Zeichen Sie das dazugehörige Zustandsdiagramm entsprechend den Vorgaben von Aufgabe a)!

Lösung zu 4.1a) und b)

Dienste werden durch die untenstehenden Dienstprimitive realisiert:

Dienste	Zugehörige Dienstprimitive
Verbindungsaufbau	ConReq/ConInd/ConRsp/ConCnf
Datentransfer, bestätigt	DatReq/DatInd/DatRsp/DatCnf
Datentransfer, unbestätigt	DatReq/DatInd
Verbindungsabbau	DisReq/DisInd
Verbindungsabweisung, Verbindungsabbruch	AboInd

Die nachfolgende Abbildung enthält links das Ablaufdiagramm (erfolgloser und erfolgreicher Ablauf) und rechts das Zustandsdiagramm zum aufgeführten Szenario (◘ Abb. 4.1):

4.2 Funkübertragungskanal nach Nyquist-Theorem

Über einen digitalen Funkübertragungskanal soll eine Datenrate von 160 MBit/s übertragen werden.

a. Wie groß sind Schrittgeschwindigkeit und minimale Bandbreite des (rauschfreien) Übertragungskanals, wenn pro Signalschritt 16 Bit kodiert werden können?

b. Auf welchen Wert erhöht sich die minimal erforderliche Bandbreite bei einem Signal-Rausch-Verhältnis auf dem Übertragungskanal von SNR = 1023?

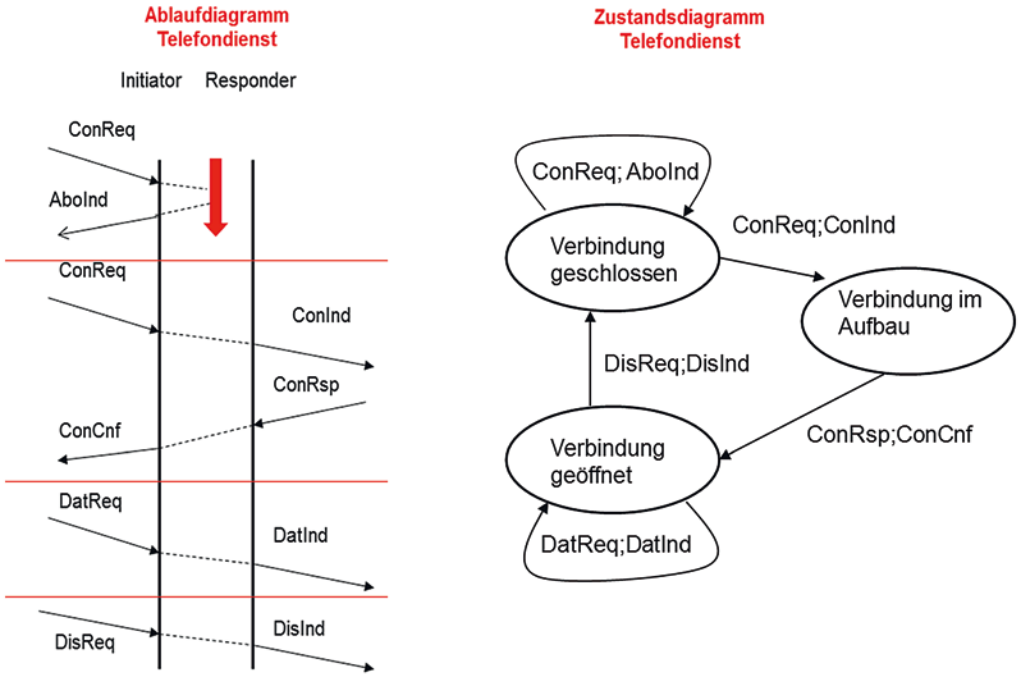


Abb. 4.1 Abstrakter Telefondienst: Ablaufdiagramm und Zustandsdiagramm

Lösung

Zu 4.2a)

Gegeben: ld S = 16 Bit

Gesucht: Schrittgeschwindigkeit (Baudrate) BR, erforderliche Bandbreite des idealen Kanals B_{ideal} sowie erforderliche Bandbreite B

Nach Nyquist-I

DR = 2 B ld S d. h. B = DR/ 2 Ld S = 160 MBit/s / 2 * 16 = 5 MHz = B_{ideal}

SR = B * ld S = 5 MHz * 16 Bit = 80.000.000 Schritte/ s = 80 MBaud

Zu 4.2b)

Gegeben: SNR = 1023; ld (1 + SNR) = ld 1024 Bit = 10 Bit

Gesucht: erforderliche Bandbreite des rauschbehafteten Kanals B_{rausch} sowie erforderliche Bandbreite B

Nach Nyquist-II

DR = B ld (1 + SNR)

d. h. B = DR/ ld (1 + SNR) = 160 MBit/s / 10 Bit = 16 MHz = B_{rausch}

Fazit

Aus dem Vergleich a) und b) folgt

Die erforderliche praktikable Kanalbandbreite B unter der Berücksichtigung der verfügbaren Codierung mit 16 Bit und des Rauschens lautet:

$$B = \max \{B_{ideal},\ B_{rausch}\} = \max \{5\ MHz, 16\ MHz\} = 16\ MHz$$

4.3 Multiplexverfahren: Frequenzmultiplex vs. OFDM

a. Die Kanalbandbreite eines analogen Fernsehkanals beträgt 5,5 MHz. Wie viele Fernsehprogramme könnten durch ein Kabelverteilnetz im Frequenzmultiplex angeboten werden, wenn ein Frequenzband von 170–299 MHz nutzbar ist und zwischen den Kanälen ein Sicherheitsabstand von 1000 kHz einzuhalten ist?
b. Welche Vorteile bringt der Einsatz des OFDM-Konzepts im Vergleich zum Frequenzmultiplex?

Lösung

Zu 4.3a)

Gegeben: Gesamtbandbreite BG = 299 − 170 MHz = 129 MHz
Gesucht: N – Anzahl verfügbarer TV-Kanäle

Dieses Band wird folgendermaßen aufgeteilt

N * 5,5 MHz + (N – 1) * 1 MHz = BG

(d. h. 1.Kanal + Sicherheitsabstand + 2.Kanal + … + N.Kanal)

5,5N + N − 1 = 129; wir lösen die Gleichung bzgl. der Variable N auf:

6,5N = 130; **N = 130 MHz/6,5 MHz = 20**

20 TV-Kanäle stehen zur Verfügung (mit 19 Abständen)!

Zu 4.3.b)

Vorteile OFDM vs. FDM

- FDM
  beim reinen Frequenzmultiplex wird die Gesamtbandbreite weniger effizient genutzt: Sicherheitsabstände vergrößern die erforderliche Bandbreite
- OFDM
  beim orthogonalem Frequenzmultiplex (OFDM) wird die Gesamtbandbreite viel effizienter genutzt: Sicherheitsabstände sind abwesend, die leichte Kanalüberlappung orthogonaler Spektren beeinflusst die DÜ minimal (Interferenzeinfluss ohne Datenratenverlust), was die erforderliche Bandbreite verringert und die Anzahl der Kanäle potentiell erhöht!

4.4 Modulationsverfahren

a. Was ist ein Modulationsverfahren?
b. Stellen Sie die Übertragung der Bitfolge „0101100100100“ dar mit Amplitudentastung, Frequenztastung und Phasentastung!

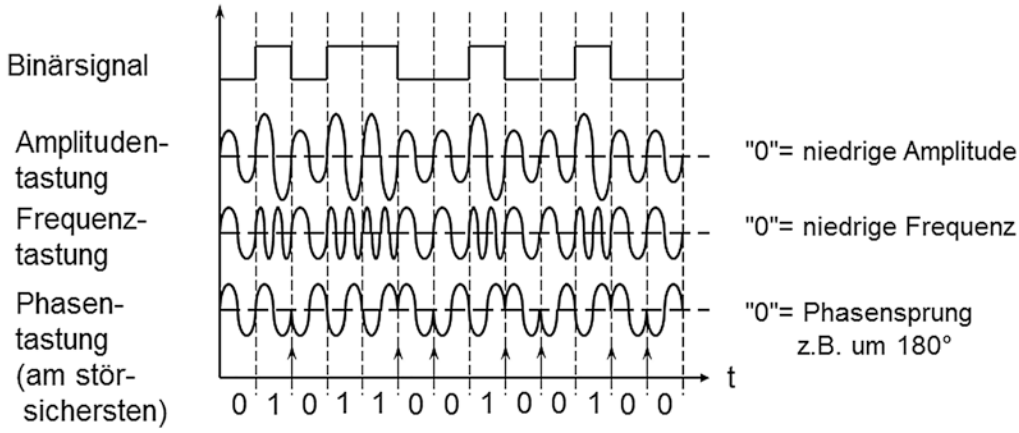
Lösung zu 4.4a)
Modulation beschreibt einen Vorgang,

- bei dem ein zu übertragendes Nutzsignal (Sprache, Daten) ein sogenanntes Trägersignal verändert (moduliert). Dadurch wird die Übertragung des niederfrequenten Nutzsignals über das höherfrequente Trägersignal ermöglicht.
- Dabei entsteht ein aufgespreiztes Frequenzband um die Frequenz des Nutzsignals.
- Die Nachricht wird empfangsseitig durch einen Demodulator wieder zurückgewonnen

Man unterscheidet dabei:

- AM – Amplitudenmodulationsverfahren/Amplitudentastung
- FM – Frequenzmodulationsverfahren/Frequenztastung
- PM – Phasenmodulationsverfahren/Phasentastung!

Lösung zu 4.4b)
s. ◘ Abb. 4.2



◘ **Abb. 4.2** Modulationsverfahren: AM, FM, PM

4.5 IP-Adressen und Klassenbildung

a. Welche der vorgegebenen IPv4-Adressen sind falsch? Für richtige Adressen definieren Sie die Klassen (A, B, C, D) und tragen sie in die Tabelle ein!
b. Welche der Adressen sind Hostadressen (bitte vermerken)?
c. Welche der Adressen sind Netzwerkadressen (bitte vermerken)?
d. Welche der Adressen sind Broadcast/Multicast-Adressen (bitte vermerken)?

IP-Adresse	Klasse bzw. Typ oder fehlerhaft?
315.115.115.115	
117.117.117.117	
133.177.133.177	
115.0.0.0	
221.225.3.225	
155.122.0.0	
225.251.177.233	
235.225.235.735	

Lösung zu 4.5a) und b) und c) und d)

IP-Adresse	Klasse bzw. Typ oder fehlerhaft?
315.115.115.115	Falsch, da 315 (Wertebereich 0 … 255)
117.117.117.117	Hostadresse Klasse A
133.177.133.177	Hostadresse Klasse B
115.0.0.0	Netzwerkadresse Klasse A
221.225.3.225	Hostadresse Klasse C
155.122.0.0	Netzwerkadresse Klasse B
225.251.177.233	Multicast-Adresse Klasse D
235.225.235.735	Falsch, da 735 (muss 0 … 255)

4.6 Distance Vector Routing

Gegeben sei folgendes Netzwerk (◘ Abb. 4.3):
Die Router sind in der Lage, die Übertragungskosten zu ihren Nachbarn zu bestimmen.

Im 30-s-Rhythmus senden sie ihre Distanzvektoren DV an ihre Nachbarn.

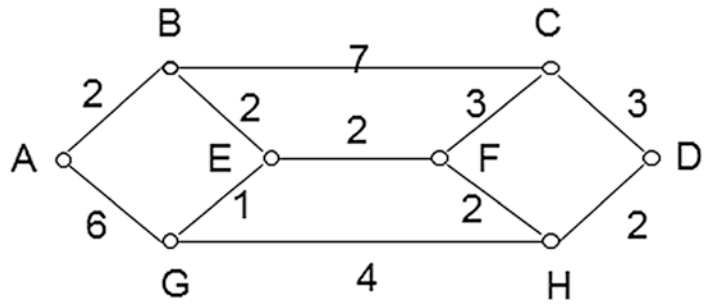


Abb. 4.3 Vermaschtes Netzwerk mit Knoten A,B,C,D,E,F,G,H

Hinweis:
Die Komponenten der Vektoren stellen die aktuelle Distanz vom Router zu den anderen Routern (Distanz zu A, Distanz zu B, …, Distanz zu H) dar.

a. Wie ändert sich die Routingtabelle des Knotens E, wenn dieser nach einem Systemausfall folgende Distanzvektoren von seinen Nachbarn erhält?
   von B (2, 0, 7, 8, 2, 4, 3, 6)
   von F (6, 4, 3, 4, 2, 0, 3, 2)
   von G (5, 3, 6, 6, 1, 3, 0, 4)
b. Nach wie viel Schritten ist der Inhalt der Routingtabelle stabil?
c. Überlegen Sie sich, ob der Inhalt der Tabelle bei zeitveränderlichen Metriken immer zu einem optimalen Ergebnis führt!

Lösung
Zu 4.6a)
Empfang Distanzvektor vom Nachbarrouter | Abstand zum Nachbarn addieren

	Tabelle nach Ausfall		**Tabelle nach DV von B (+2)**		**Tabelle nach DV von F (+2)**		**Tabelle nach DV von G (+1)**	
Ziel	**über**	**Kosten**	**über**	**Kosten**	**über**	**Kosten**	**über**	**Kosten**
A			**B**	**4**	B	4	B	4
B			**B**	**2**	B	2	B	2
C			**B**	**9**	**F**	**5**	F	5
D			**B**	**10**	**F**	**6**	F	6
E	–	0	–	0	–	0	–	0
F			**B**	**6**	**F**	**2**	F	2
G			**B**	**5**	B	5	**G**	**1**
H			**B**	**8**	**F**	**4**	F	4

Zu 4.6b)
Wenn der Graph des Netzwerkes eine Tiefe von n besitzt, verändert sich die Tabelle nicht mehr, wenn n Schritte erreicht sind. Im vorliegenden Fall also nach n = 5 Schritten.

Zu 4.6c)
Wenn eine Strecke eine bessere Bewertung erhält, konvergiert das Verfahren zum Optimum.

Wenn eine Strecke eine schlechtere Bewertung erhält, kann das Verfahren in vermaschten Netzen versagen wegen Nichtkonvertierung (Schleifen).

4.7 IP – Fragmentierung

Ein TCP-Segment mit 2048 Byte Nutzdaten wird an IP zur Auslieferung übergeben.

Der Übertragungsweg geht über zwei Netzwerke (Quellrechner → Router → Zielrechner).

Jedes Netzwerk hat eine Maximalgrenze MTU für die IP-Paketgröße.

Netzwerk 1 - MTU = 1024 Byte

Netzwerk 2 - MTU = 512 Byte

a. Geben Sie für die beim Empfänger ankommenden Fragmente jeweils die Größe und den Offset an.
b. Wie viele Fragmente würden erzeugt, wenn der Sender wüsste, dass die kleinste MTU auf den Pfad zum Empfänger 512 Byte beträgt?

Lösung
Zu 4.7a)

TCP-Segment		(mit 20-byte-Header)		→	2068 Byte
IP-Paket		(mit 20-byte Header)			2088 Byte (zu groß, wegen MTU)
Netz1	→	IP-Paket-1	1024 Byte	1004 Byte Inhalt	Offset 0
		IP-Paket-2	1024 Byte	1004 Byte Inhalt	Offset 1004
		IP-Paket-3	80 Byte	60 Byte Inhalt	Offset 2008

Router	→	IP-Paket-1-1	512 Byte	492 Byte Inhalt	Offset 0
		IP-Paket-1-2	512 Byte	492 Byte Inhalt	Offset 492
		IP-Paket-1-3	40 Byte	20 Byte Inhalt	Offset 984
		IP-Paket-2-1	512 Byte	492 Byte Inhalt	Offset 1004
		IP-Paket-2-2	512 Byte	492 Byte Inhalt	Offset 1496
		IP-Paket-2-3	40 Byte	20 Byte Inhalt	Offset 1988
		IP-Paket-3-1	80 Byte	60 Byte Inhalt	Offset 2008

Zu 4.7b)
Größerer Overhead durch kurze Pakete (Headeranteil)
Wenn kleinste MTU auf Weg bekannt, Verbesserung möglich

$$\text{5 statt 7 Pakete} \quad 4 \times (20+496)\ \text{Byte} + 1 \times (20+100)\ \text{Byte}$$

Außerdem Vermittlungsaufwand für 5 Pakete kleiner als für 7.

4.8 Netto/Brutto-Datenrate in der Schichtenarchitektur

Ein Rechnernetz mit einer 7-Schichtenarchitektur habe pro Schicht einen Verlust der Datenrate von a = 15 % infolge Overhead. Wie hoch ist die Anwendungs-Übertragungsrate in einem 10 Gigabit-Ethernet-LAN (10 GBit/s)?

Lösung

$$\begin{aligned}
&DR_1 = 10\ \text{GBit/s} = \text{Brutto-DR}\\
&DR_2 = DR_1 * (1-a) = 10 * 0{,}85 = 8{,}5\ \text{GBit/s}\\
&n = 1 \ldots 7\\
&DR_n = DR_1 * (1-a)^{(n-1)} = 10 * 0{,}85^{(n-1)}\\
&\ldots
\end{aligned}$$

Netto-DR bei der Layer 7:

$$\begin{aligned}
DR_7 &= DR_1 * (1-a)^6 = 10 * 0{,}85^6\\
&= 3{,}77\ \text{GBit/s, d. h. nur 38 \% der Brutto-DR!}
\end{aligned}$$

4.9 Internet-Schichtenarchitektur und Netto-/Brutto-Verhältnis

a. Das Internet besitzt eine 4-Schichtenarchitektur und habe für die 2. Schicht einen Verlust der Datenrate von 10% infolge Overhead. Jede nächste Schicht hat eine um 5 % höheren Overhead. Wie hoch ist die Anwendungs-Übertragungsrate (Schicht 4) in einem Gigabit-Ethernet-LAN (Netto-DR = 1000 Mbit/s)?
b. Wie groß ist das Netto-/Brutto-Verhältnis in diesem Fall?

Lösung zu 4.9a) ± b)
Gegeben
Verlustraten pro Schicht: $a_1 = 0{,}1$; $a_2 = 0{,}15$; $a_3 = 0{,}2$

Gesucht
BruttoDR; Verhältnis Netto-/Brutto
NettoDR = DR_1 = 1000 Mbit/s
$DR_2 = DR_1 * (1 - a_1)$; $DR_3 = DR_2 * (1 - a_2)$;

- **Brutto-DR**
  $DR_4 = DR_1 * (1 - a_1) * (1 - a_2) * (1 - a_3) = 1000 * 0{,}9 * 0{,}85 * 0{,}8$ = 612 MBit/s

- **Verhältnis Netto-/Brutto**
  1000 MBit/s: 612 MBit/s = 61 %

4.10 Fehlerbehandlung durch Paritätskontrolle

Der ASCII-Basiskode ist ein Zeichendarstellungskode für Klein- und Großbuchstaben des englischen Alphabets, sowie für Ziffern, Sonder- und Steuerzeichen

Auszug (hexadezimale Darstellung)

A	B	…	O	P	Q	…	Z
0×41	0×42		0×4F	0×50	0×51		0×5A

a. Notieren Sie zeichenweise untereinander die Zeichenkette „ABCDPQRS“ in binärer 7-Bit-Darstellung.
b. Fügen Sie jeweils ein Kontrollbit für gerade Parität hinzu.
c. Welche Bitfehlersituationen können erkannt und welche korrigiert werden?
d. Wie hoch ist bei einer Bitfehlerwahrscheinlichkeit von 10^{-3} die Wahrscheinlichkeit eines fehlerhaften Zeichens und wie hoch ist die Wahrscheinlichkeit, dass der Fehler nicht erkannt wird?

e. Fügen Sie ein Kontrollzeichen für gerade Blockparität hinzu.
f. Welche Bitfehlersituationen können erkannt und welche korrigiert werden?
g. Für welche Anwendungen wäre ein solcher Kode geeignet?

Lösung

Zu 4.10a) b) e)

1000001 0
1000010 0
1000011 1
1000100 0
1010000 0
1010001 1
1010010 1
1010011 0

00001001

Zu 4.10c)

- 1 Bitfehler pro Zeichen kann erkannt werden (gilt auch für das Paritätsbit)
- Korrektur ist nicht möglich
- Eine gerade Bitfehleranzahl pro Zeichen wird nicht erkannt

Zu 4.10d)

$$\text{Fehlerwahrscheinlichkeit}_{\text{Zeichen}} \approx \text{Bitanzahl}_{\text{Zeichen}} * \text{Fehlerwahrscheinlichkeit}_{\text{Bit}}$$
$$= 8 * 10^{-3}$$

2 Bitfehler werden nicht erkannt
Wahrscheinlichkeit $= 6{,}4 * 10^{-5}$

Zu 4.10f)

- 1 Bitfehler pro Zeichen kann erkannt und korrigiert werden
- Bei mehreren Bitfehlern im Block Fehlererkennung und -Korrektur u. U. nicht möglich
- Eine gerade Bitfehleranzahl pro Zeichen bzw. Bitposition wird nicht erkannt

Zu 4.10g)

Die meisten Fehler können beim Empfänger erkannt und korrigiert werden.

Nutzung sinnvoll bei Echtzeitanwendungen mit Akzeptanz einer gewissen Restfehlerrate

4.11 Fehlerkorrigierende Codes

Folgende Tabelle enthält die Kodeabbildung für die Zeichen „A“, „B“, „C“ und „D“:

A	B	C	D
000000	111000	000111	111111

a. Wie würden Sie die folgenden, zum Teil gestörten Bitfolgen interpretieren?
   - 100000
   - 001111
   - 101111
   - 000111
   - 101010
b. Wie groß ist die Hamming-Distanz des Codes?
c. Wie viele Bitfehler lassen sich erkennen und wie viele korrigieren?

Lösung

Zu 4.11a)

Für empfangene Zeichen Ermittlung des Abstandes (Zahl der Bitabweichungen zu den Kodezeichen) und Kodezuordnung

Bitfolge	Abstand zu A	Abstand zu B	Abstand zu C	Abstand zu D	Zeichen
100000	1	2	4	5	**A**
001111	4	4	1	2	**C**
101111	5	4	2	1	**D**
000111	3	6	0	3	**C**
101010	3	2	4	3	**B**

Zu 4.11b)

Die Hamming-Distanz d charakterisiert die Mindestanzahl unterschiedlicher Bitwerte in den einzelnen Kodeworten.

Zeichen	Abstand zu A	Abstand zu B	Abstand zu C	Abstand zu D
A	0	3	3	6
B	3	0	6	3
C	3	6	0	3
D	6	3	3	0

Die Hamming-Distanz des Kodes beträgt $d = 3$.

Zu 4.11c)
Die Fehlerkorrektur ist bis zu einer Bitfehleranzahl kleiner als d/2 möglich.

Die Fehlererkennung ist bis zu einer Bitfehleranzahl von (d−1) möglich.

1 Bitfehler	Erkennung und Korrektur möglich
2 Bitfehler	Erkennung möglich, aber evtl. falsche Korrektur
3 Bitfehler	Evtl. sogar fehlende Fehlererkennung

4.12 Cyclic Redundancy Check (CRC)

Um Übertragungsfehler erkennen zu können, wird mit den Daten noch eine redundante Bitfolge fester Länge, die sogenannte Sicherungssequenz (Frame Check Sequence), gesendet. Diese wird durch eine Polynomdivision ermittelt, bei der der Dateninhalt durch ein sogenanntes Generatorpolynom (bzw. Prüfpolynom) „dividiert" wird. Der Divisionsrest dient als Prüfsequenz und wird nach den letzten Informationsbits gesendet.

Die Informationsbits werden dabei sequentiell in einen Puffer (Größe = Polynomgrad plus 1) geschrieben und dann sequentiell gesendet. Im Puffer erfolgt bei jedem Takt ein bitweises Exclusiv-Oder (EXO) mit den Koeffizienten des Generatorpolynoms, falls das führende Bit im Puffer den Wert „1" besitzt.

Im folgenden Beispiel verwenden wir aus rechentechnischen Gründen eine sehr kurze Sendebitfolge und ein sehr kleines Polynom.

Zu übertragen seien die Daten (10 Bits) - 1010001101

Als Prüfmuster dient das Polynom - $x^3 + x + 1$

a. Berechnen Sie daraus die Sicherungssequenz!
b. Belegen Sie Ihr Ergebnis dadurch, dass Sie den Empfang des korrekt gesendeten Frames überprüfen!

Hinweis
Der „Quotient" muss nicht berechnet werden, da nur der Rest benötigt wird.

Lösung
Zu 4.12a)
Die Koeffizienten des Polynoms sind: 1011

Ein Generatorpolynom 3. Grades liefert einen Divisionsrest von 3 Bitstellen. Anstelle des Divisionsrestes setzen wir zunächst die Bits auf „0".

```
1010001101000  :  1011
1011
----
  001001
   1011
   ----
    01010
     1011
     ----
      001100
        1011
        ----
         1110
         1011
         ----
         101  Rest wird anstelle der Endfolge
              000 gesendet
```

Zu 4.12b)
Die empfangene Bitfolge wird durch das vereinbarte Generatorpolynom dividiert. Wenn alle Bits korrekt übertragen wurden, muss sich ein Divisionsrest von Null ergeben.

```
1010001101101 :  1011
1011
----
 001001
   1011
   ----
    01010
     1011
     ----
      001110
        1011
        ----
         1011
         1011
         ----
         000  Rest gleich Null → Empfang O.K.
```

4.13 Protokolle der Sicherungsschicht

a. Vergleichen Sie die Protokolle HDLC und PPP miteinander!

Lösung
s. ◘ Tab. 4.1

4.14 Überlaststeuerung

Beim Choke-Verfahren wird an einem Router eine Messreihe von relativen „Lastwerten" ermittelt. Dieser Lastwert repräsentiert z. B. die Länge einer Warteschlange. Kurzzeitige Überschreitungen einer Grenzlast (Schwellwert) werden toleriert, aber bei dauerhafter Überschreitung wird ein sogenanntes Choke-Paket an den Quellknoten gesendet. Dieser muss dann die Sendeleistung verringern (Standard 50 %) und steigert sie dann langsam wieder.

So spielt sich ein vernünftiges Gleichgewicht der Paketsenderate ein.

◘ **Tab. 4.1** Vergleich HDLC und PPP

Kriterium	HDLC	PPP
OSI-Schicht	Sicherungsschicht, Layer 2	Sicherungsschicht, Layer 2
Einsatz	– kommt aus der IBM-Früharchitektur für RN (Großrechnerwelt der IBM) – gut für Telefon-/Modem-Verb. geeignet – Basis für PPP	– Einwahl in das Internet über Wählleitungen zum Provider – Praktikabel
Datenübertragung	Bitorientiert Synchron	Zeichenorientiert Synchron und asynchron
Fehlererkennung/-korrektur	Frame Check Sequenz (Prüfsumme CRC-16)	Frame Check Sequenz (CRC-16)
Management-funktionalität	Supervisorframes, Mitteilung der Empfangsbereitschaft und weitere Statusinformationen	LCP Link Control und NCP Network Control (Subprotokolle): – zum Aktivieren/Testen/Beenden von Verbindungen; – zugeschnitten auf IP

Periodisch wird folgende Berechnung im Router ausgeführt.

$$\text{Last}_{neu} = a * \text{Last}_{alt} + (1 - a) * \text{Last}_{aktuell}$$

Dabei bedeuten:		
	Last_{neu}	Schätzung der Last für nächsten Zeitraum
	a	Anpassungsfaktor (Konstante des „Vergessens" der Historie)
	Last_{alt}	Last des vorherigen Zeitraumes
	$\text{Last}_{aktuell}$	Wert der momentanen Last

Im folgenden Beispiel wird an einem Gateway-Rechner eine Messreihe von relativen „Lastwerten" ermittelt: {1/5/8/9/9}. Als Schwellwert wird 7,9 verwendet, als Anpassungsfaktor 0,3.

Wann wird ein Choke-Paket gesendet?

Lösung

Beginn der Übertragung: $\text{Last}_{alt} = 0$

Relat. Lastwert	1:	Last_{neu} = 0,3 * 0 + 0,7 * 1	= 0,7
	5:	Last_{neu} = 0,3 * 0,7 + 0,7 * 5	= 3,71
	8:	Last_{neu} = 0,3 * 3,71 + 0,7 * 8	= 6,71
	9:	Last_{neu} = 0,3 * 6,71 + 0,7 * 9	= 8,31 → Senden Choke-Paket
	9:	Last_{neu} = 0,3 * 8,31 + 0,7 * 9	= 8,79 → Senden Choke-Paket
	7:	Last_{neu} = 0,3 * 8,79 + 0,7 * 7	= 7,54
	2:	Last_{neu} = 0,3 * 7,54 + 0,7 * 2	= 3,66

4.15 Einsatz von IP: Adressen und Subnetze

Die Kommunikation in modernen Rechnernetzen erfolgt auf der Basis der Internet-Technologie (TCP/IP). Als universelle Adressen werden IPv4-Adressen eingesetzt.

a. Erläutern Sie den Aufbau der IPv4-Adressen und die Aufteilung des Adressraums in die Klassen A–D, sowie die Aufteilung durch Netzmasken!
b. Welche Unterschiede sehen Sie in der Nutzung von MAC- und IP-Adressen?
c. Erläutern Sie den Einsatz von Subnetzmasken beim Routing! Welche Vorteile bringt die Maskierung (s. ◘ Abb. 4.4)?

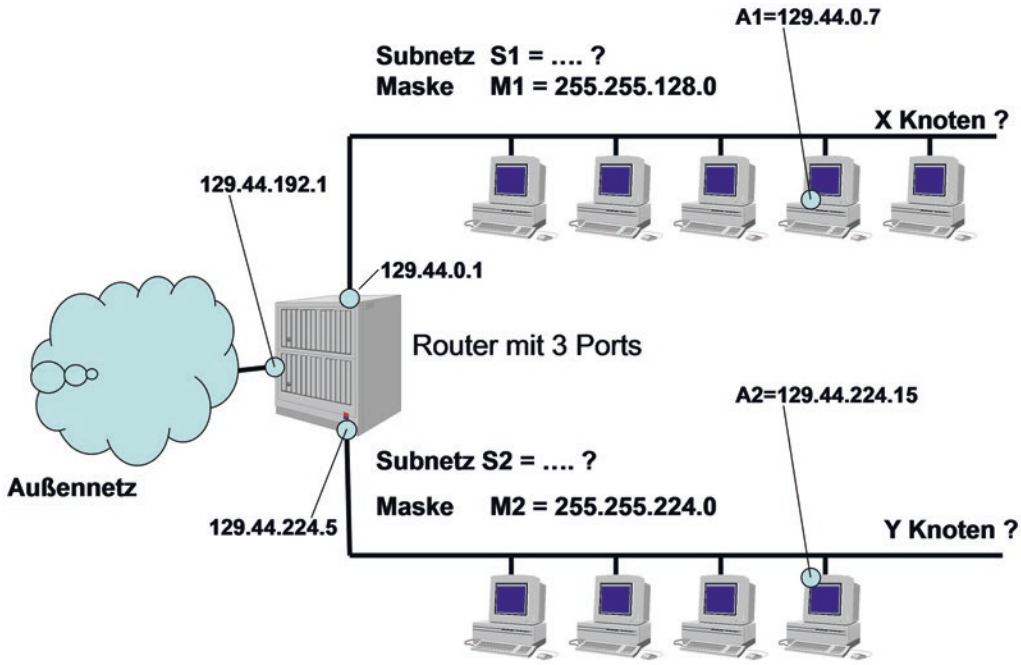


Abb. 4.4 Netzwerkszenario mit Router und Subnetting

Berechnen Sie für die gegebene Skizze:

d1) Die Knotenadresse im Subnetz S1 ist A1 = 129.44.0.7, Subnetzmaske ist M1 = 255.255.128.0. Definieren Sie die Subnetzadresse S1! Wie hoch ist die maximale Knotenanzahl X in diesem Subnetz?

d2) Die Knotenadresse im Subnetz S2 ist A2 = 129.44.224.15, die Subnetzmaske ist M2 = 255.255.224.0. Definieren Sie die Subnetzadresse S2! Wie hoch ist die maximale Knotenanzahl Y in diesem Subnetz?

Lösung
Zu 4.15a)

IPv4-Adresse (32 Bit, binär notiert), z. B. 1000 0001 . 0010 1100 . 1110 0000 . 0000 1111

IPv4-Adresse (32 Bit, dezimal notiert) 129 . 44 . 224 . 15

Damit Routingtabellen nicht zu groß werden, gibt es Gruppierungen von IP-Adressbereichen zu IP-Netzen.

Ursprünglich wurde eine starre Einteilung in Klassen A bis E praktiziert. Die 32 Bit der IP-Adresse werden dabei aufgeteilt in eine Netzadresse und eine HOST-Adresse, Je nach Klasse gibt es einen unterschiedlich großen Netzanteil.

Die Unterscheidung erfolgt dabei durch Auswertung der führenden Bits der IP-Adresse (s. Abb. 4.5).

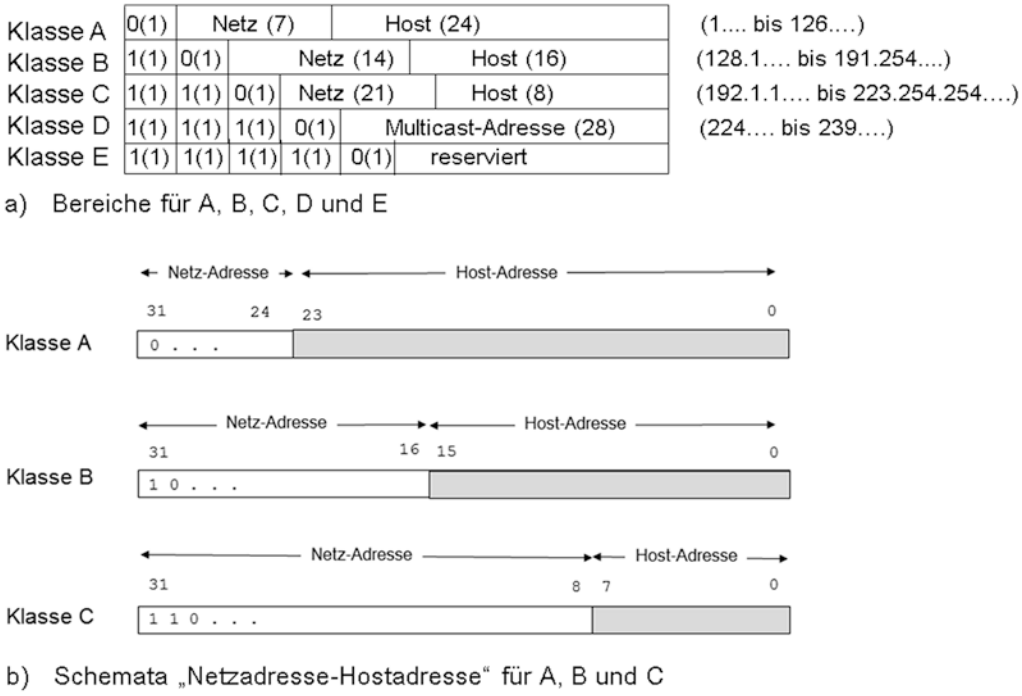


Abb. 4.5 IP-Adressen: Klassenbildung

Die HOST-Adressen „000…000“ und „111…111“ sind reserviert für Netzadresse bzw. Broadcastadresse (Sammeladresse).

Beispiel
Gegeben sei die IP-Adresse 141.76.40.123.

IPv4-Adresse (32 Bit, dezimal notiert) 141 . 76 . 40 . 123

IPv4-Adresse (32 Bit, binär notiert), z. B. 1000 1101 . 0100 1100 . 0010 1000 . 0111 1011

Die Adresse 141.76.40.123 stellt einen Rechner in einem B-Netz dar (Beginn mit „10…“) mit der Netzadresse 141.76.0.0.

Die starre Klasseneinteilung führt dazu, dass weite Bereiche des Adressraumes ungenutzt bleiben, da die Netze meist weniger Knoten besitzen als möglich. Beispielsweise bietet eine B-Adresse Platz für über 64.000 Knoten, was in der Regel nicht ausgenutzt wird.

Masken stellen wie die IP-Adressen eine 32-Bit-Zahl dar. Die Bits des Netzanteils von Adressen werden durch „1“ gekennzeichnet, die Bits des Hostanteils durch “0“.

Beispiel:

Gegeben sei die B-Netzadresse	141	.	76	.	0	.	0

Zugehörige Maske für B-Klasse 1111 1111 . 1111 1111 . 0000 0000 . 0000 000

Zu 4.15\b)

- MAC-Adressen sind Adressen in der OSI-Schicht 2.
- Sie identifizieren ein Netzinterface eines Computers in einem LAN. Für das Routing außerhalb eines LAN sind MAC-Adressen ungeeignet.
- Die Hardwarehersteller sichern die weltweite Eindeutigkeit der MAC-Adressen.
- IP-Adressen sind Adressen in der OSI-Schicht 3.
- Sie identifizieren einen Computer und sind für das weltweite Routing im Internet geeignet.
- Die Organisation IANA und ihre Unterorganisationen (RIRs) sichern die weltweite Eindeutigkeit der IP-Adressen.

Zu 4.15c)

Um die Netzbildung flexibler zu gestalten, gibt es die Möglichkeit der Unterteilung großer Netze in Subnetze mittels sogenannter Netzwerkmasken. Subnetzmasken nutzen einen Teil der Hostbits zur Unterteilung eines großen Netzes, z. B. der Klasse B, in mehrere kleinere Subnetze.

Die Erläuterung soll am Beispiel einer Universität erfolgen. Nach außen präsentiert sich die Uni als ein großes Netz, intern kann ein Subrouting zu Fakultätsnetzen erfolgen. Die Fakultäten können dann ihr Netz noch weiter unterteilen in Institutsnetze und die Institute in Lehrstuhlnetze. Dadurch ist eine hohe Flexibilität möglich, ohne dass die Routingtabellen unnötig aufgebläht werden. Da alle Subnetze der Uni Bestandteile des Uninetzes sind, genügt für die Außenwelt ein einziger Routingeintrag für alle Computer der Uni.

Allgemein gilt:

Netzadresse = IP-Adresse AND Maske

Berechnung Hostadresse über inverse Maske

Hostadresse = IP-Adresse AND (NOT) Maske

Hostanzahl $<2^{\text{Bitanzahl des HOST-Anteiles}}$ abzüglich reservierte Adressen

Reservierte Adressen: Netz- und Broadcastadresse

Beispiel:
Gegeben sei die IP-Adresse 141.76.40.123.

IPv4-Adresse (32 Bit, dezimal notiert)	141 . 76 . 40 . 123
IPv4-Adresse (32 Bit, binär notiert)	1000 1101. 0100 1100 . 0010 1000 . 0111 1011
Subnetzmaske (32 Bit, dezimal notiert)	255 . 255 . 255 . 224
Subnetzmaske (32 Bit, binär notiert)	1111 1111 . 1111 1111 . 1111 1111 . 1110 0000
Subnetz (32 Bit, dezimal notiert)	141 . 76 . 40 . 96
Host (binär notiert)	0000 0000 . 0000 0000 . 0000 0000 . 0001 1011
5 Bit Host-Anteil	$\rightarrow 2^5 - 2 = 30$ Rechner im Subnetz möglich

Bemerkung:
Heutzutage ist klassenloses Routing CIDR üblich.
Notation - IP-Adresse/Anzahl der Maskenbits, z. B. 141.76.40.123/27

Zu 4.15d)

Berechnung Subnetzadresse S1: S1 = A1 AND M1

A1 = 129.44.0.7	bzw.	1000 0001 . 0010 1100 . 0000 0000 . 0000 0111
M1 = 255.255.128.0	bzw.	1111 1111 . 1111 1111 . 1***000 0000 . 0000 0000***
→		
S1 = 129.44.0.0		1000 0001 . 0010 1100 . 0***000 0000 . 0000 0000***
X = $2^{15} - 2$		X = 32766 Knoten sind maximal im Subnetz 1 möglich.

Berechnung Subnetzadresse S2: S2 = A2 AND M2

A2 = 129.44.224.15	bzw.	1000 0001 . 0010 1100 . 1110 0000 . 0000 1111
M2 = 255.255.224.0	bzw.	1111 1111 . 1111 1111 . 111***0 0000 . 0000 0000***
→		
S2 = 129.44.224.0		1000 0001 . 0010 1100 . 111***0 0000 . 0000 0000***
Y = $2^{13} - 2$		Y = 8190 Knoten sind maximal im Subnetz 2 möglich.

4.16 Hilfsprotokolle zum Einsatz von IP

a. Erläutern Sie Aufgaben des Hilfsprotokolls ARP!
b. Erläutern Sie Aufgaben des Hilfsprotokolls DHCP!

Lösung

Zu 4.16a)

In einem LAN (OSI-Schicht 2) müssen die übertragenen Nachrichtenframes mit MAC-Adressen adressiert werden.

Die Partnerrechner sind aber anfänglich nur über ihre IP-Adresse bekannt. Eine Kommunikation wäre nur über Broadcastkommunikation möglich, was mit einer hohen Netzbelastung verbunden ist.

ARP gestattet die Ermittlung der MAC-Adresse eines Rechners, wenn seine IP-Adresse bekannt ist. Nach einmaliger(!) Anwendung von ARP kann eine Kommunikation im LAN zielgenau über die MAC-Adressennutzung erfolgen.

Intern nutzt ARP einen Broadcastruf zu einer Anfrage im LAN: „Welcher Rechner im LAN hat die IP-Adresse x?". Der angesprochene Rechner antwortet mit der Angabe der MAC-Adresse.

Zu 4.16b)

Für die ordnungsgemäße Arbeit in einem Netzwerk muss ein Rechner seine Konfigurationsparameter kennen, z. B. seine IP-Adresse, die Netzwerkmaske, die IP-Adresse eines Gateways.

Eine Möglichkeit ist die manuelle Konfiguration durch den Administrator des Netzwerkes beim Installieren der Rechnerbetriebssysteme. Dies ist jedoch aufwendig bei mobilen Nutzern, da diese bei jedem Standortwechsel neue Konfigurationsparameter benötigen.

Einen Ausweg bietet das DHCP-Protokoll. Dieses wird bei Systemstart aufgerufen zu einem Zeitpunkt, wo keine Konfigurationsparameter bekannt sind. Der DHCP-Client fordert mittels eines Broadcastrufes (über UDP) von einem DHCP-Server Konfigurationsparameter an. Der Server macht daraufhin ein Angebot, welches der Client bestätigen muss. In der Regel ist die Zuteilung von Konfigurationsparametern zeitlich befristet, z. B. für zwei Wochen.

4.17 Weiterentwicklung von IP: IPng

Als einige der wichtigsten Weiterentwicklungen von IP, oder IP Next Generation (IPng), gelten u. a. die Protokolle IPv6 und IPsec.

a. Diskutieren Sie Vor- und Nachteile von IPv6 im Vergleich zu IPv4!
b. IPsec stellt effiziente Sicherheitsmechanismen auf der Schicht 3 dar. Diskutieren Sie diese! Wie sehen die modifizierten IPsec-Pakete aus?

Lösung

Zu 4.17a)

IPv4 bietet einen Adressraum von $2^{32} \approx 4{,}3$ Mrd. IP-Adressen

- Dezimal-Punkt-Notation, z. B. *201.122.133.201*
- viele jedoch in der Praxis nicht nutzbar, da sie Sonderaufgaben dienen (z. B. Multicast) oder zu großen Subnetzen gehören

neue Eigenschaften von IPv6

- Vergrößerung des Adressraums auf $2^{128} \approx 340$ Sextillionen Adressen
- hexadezimale Notation mit Doppelpunkten, z. B. *2001:0db8:85a3:08d3:1319:8a2e:0370:7344* acht Blöcke mit einer Länge von jeweils 16 Bit
- ersten 64 Bit dienen Netzadressierung, die letzten 64 Bit zur Host-Adressierung
- Autokonfiguration von IPv6-Adressen (stateless), DHCP (stateful) für IPv6 damit in der Regel überflüssig
- Mobile IP und vereinfachte Umnummerierung („Renumbering")
- Dienste wie IPSec, QoS und Multicast „serienmäßig"
- Vereinfachung und Verbesserung der Protokollrahmen (Headerdaten) und damit des Routings

Zu 4.17b)

IPsec mit effizienten Sicherheitsmechanismen der Schicht 3

Vertraulichkeit:
Sender verschlüsselt IP-Nutzdaten (für TCP, UDP, ICMP und SNMP)
universell nutzbar:
Encryption services → DES, TripleDES oder AES zwischen VPN-Partnern (virtual private network)
Internet Key Management Protocol (IKMP), basierend auf Internet Security Association and Key Management Protocol – ISAKMP

Authentisierung:
Zielrechner kann IP-Quelladresse überprüfen

Basisprotokolle:

- Authentication Header (AH) Protocol
- Encapsulation Security Payload (ESP) Protocol.

4.18 Quality of Service in der Transportschicht

Die Transportschicht lässt das Aushandeln von QoS-Parametern für die Kommunikation zwischen den Endsystemen in der Phase des Verbindungsaufbaues zu.

a. Welche Parameter kommen hierfür infrage? Diskutieren Sie diese!
b. Der Nutzer des Transportdienstes benötigt die folgenden QoS-Parameter:
kontinuierlich 1200 Byte/s,
Verschlüsselung der zu übertragenden Daten.

Skizzieren Sie die Ablaufdiagramme für die nachfolgenden Szenarien:

b1) Der Responder kann die gewünschten Parameter erfüllen.
b2) Der Responder kann die Datenrate nur zu 75 % garantieren, nach Rücksprache mit der Anwendung akzeptiert der Initiator.
b3) Der Responder kann die Datenrate nur zu 75 % garantieren, der Initiator kann nicht akzeptieren und baut die Verbindung ab.
b4) Die Instanz zur Verschlüsselung beim Responder ist ausgefallen und es gibt keine Redundanz.

Lösung
Zu 4.18a)
QoS-Parameter sind wie folgt

- Durchsatz [Mbyte/s]
- Paketfehlerrate, bspw. 10^{-11}
- Verbindungsaufbauzeit, bspw. T = 10 ms wie bspw. bei LTE
- Wahrscheinlichkeit Transferfehler, bspw. 10^{-12}
- Prioritäten bei Übertragung, bspw. TVoP – hoch, VoIP – mittel, Email, SMS – niedrig
- Wahrscheinlichkeit Verbindungsausfall, bspw. 10^{-5}
- Verbindungsabbauverzögerung, bspw. T = 7 ms

Lösung
Zu 4.18b)
s. ◘ Abb. 4.6

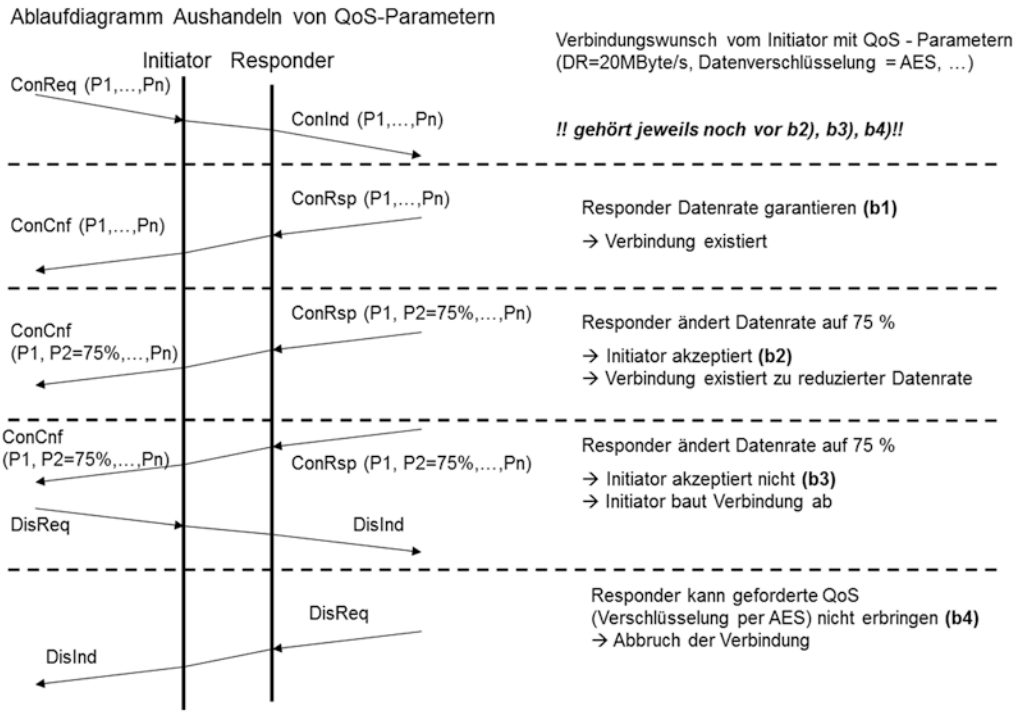


Abb. 4.6 Ablaufdiagramm mit Aushandeln von QoS-Parametern

4.19 Ablauf- und Zustandsdiagramme für die Transportschicht

Ergänzen Sie die Aufgabe 4.1 um einen bestätigten Datentransfer für die Transportschicht.

Dienste müssen durch die untenstehenden Dienstprimitive realisiert werden.

Dienste	Zugehörige Dienstprimitive
Verbindungsaufbau	ConReq/ConInd/ConRsp/ConCnf
Datentransfer, bestätigt	DatReq/DatInd/DatRsp/DatCnf
Datentransfer, unbestätigt	DatReq/DatInd
Verbindungsabbau	DisReq/DisInd

a. Zeichnen Sie das Ablaufdiagramm für die Dienstfolge: Verbindungsaufbau → Datentransfer, bestätigt → Verbindungsabbau!
b. Modellieren Sie die Aufgabe a) als Zustandsdiagramm!

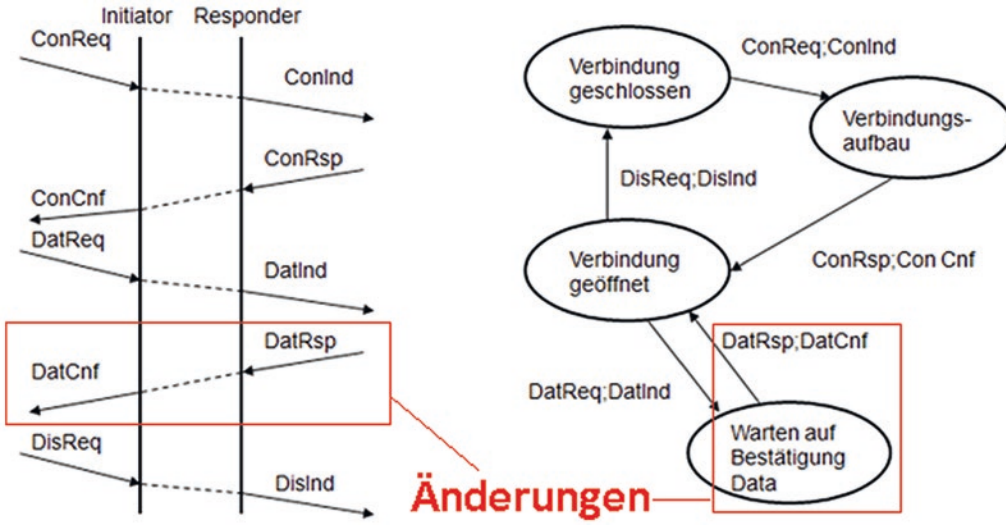


Abb. 4.7 Ablaufdiagramm und Zustandsdiagramm für die vorgegebene Dienstfolge

Lösung
Zu 4.19a) und b)
s. Abb. 4.7

4.20 Übersicht der Netzwerkfunktionen und Kommunikationsschichten

Ordnen Sie die Begriffe in der ersten Spalte der folgenden Tabelle den richtigen Kommunikationsschichten (Spalten 2–6) zu. In einigen Fällen kann ein Begriff mehreren Schichten zugeordnet werden. Als Schichten stehen die OSI-Schichten Bitübertragungsschicht, Sicherungsschicht, Vermittlungsschicht, Transportschicht und die Anwendungsschicht des TCP/IP-Referenzmodells zur Verfügung (Tab. 4.2).

Lösung
Zu 4.20
s. Tab. 4.2 und 4.3

Tab. 4.2 Netzwerkfunktionen und Kommunikationsschichten. Tabelle zum Vervollständigen

Begriff	Bitübertragungsschicht	Sicherungsschicht	Vermittlungsschicht	Transportschicht	Anwendungsschicht
TCP als Bsp.	–	–	–	X	–
DHCP					
CSMA/CD					
BGPv4					
Client-Server-Anwendung					
DSL					
HTTPS					
IPv4					
UDP					
Koaxialkabel					
LWL					
Modem					
PPP					
Router					
Sockets					
Token Ring					
Twisted Pair					
WLAN					
Frequenzmultiplex					

Tab. 4.3 Tabelle mit Ergebnissen

Begriff	Bitübertragungsschicht	Sicherungsschicht	Vermittlungsschicht	Transportschicht	Anwendungsschicht
TCP als Bsp.	–	–	–	X	–
DHCP			x		x
CSMA/CD	(x)	x			
BGPv4			x		
Client-Server-Anwendung					x
DSL	x				
HTTPS					x
IPv4			x		
UDP				x	
Koaxialkabel	x				
LWL	x				
Modem	x				
PPP		x			
Router			x		
Sockets				x	x
Token Ring	(x)	x			
Twisted Pair	x				
WLAN	x	x			
Frequenz-multiplex	x				

4.21 Zusammenfassung Kapitel 4

Der praxisorientierte Abschnitt bietet Ihnen Musterlösungen zu den Aufgabenstellungen zu Komplex I – Übertragungsorientierte Schichten. Die folgenden Themen werden geübt:

- Dienstelemente für einen abstrakten Telefondienst
- Funkübertragungskanal nach Nyquist-Theorem
- Multiplexverfahren: Frequenzmultiplex vs. OFDM
- Modulationsverfahren
- IP-Adressen und Klassenbildung
- Distance Vector Routing
- IP – Fragmentierung
- Netto/Brutto-Datenrate in der Schichtenarchitektur
- Internet-Schichtenarchitektur und Netto-/Brutto-Verhältnis
- Fehlerbehandlung durch Paritätskontrolle
- Fehlerkorrigierende Codes
- Cyclic Redundancy Check (CRC)
- Protokolle der Sicherungsschicht
- Überlaststeuerung
- Einsatz von IP: Adressen und Subnetze
- Hilfsprotokolle zum Einsatz von IP
- Weiterentwicklung von IP: IPng
- Quality of Service in der Transportschicht
- Ablauf- und Zustandsdiagramme für die Transportschicht
- Übersicht der Netzwerkfunktionen und Kommunikationsschichten.

Komplex II – Netzwerktechnologien und Mobile Kommunikation. Netzkopplung und Verkabelung

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze – Übungsbuch*,
https://doi.org/10.1007/978-3-658-25619-7_5

5.1 Multiprotocol Label Switching (MPLS)

a. Erläutern Sie den Aufbau eines MPLS-Tunnels! Wie setzt man die Labels? (siehe Teil II Lehrbuch, Abb. 12.6)
b. Beschreiben Sie den Gesamtablauf zwischen dem Quell-Host, den Ingress/Egress-Routern und dem Ziel-Host in Stichworten!
c. Nennen Sie die wesentlichen Unterschiede zwischen MPLS und ATM!

Lösung zu 5.1a)
MPLS – Multiprotocol Label Switching ist eine effiziente Integrationstechnik für aktuelle Zugangsnetze und Weitverkehrsnetze.

Die Komponenten der MPLS-Architektur sind wie folgt (s. Teil II, Abb. 12.6):
- der Quell-Host (i. d. R. in einem LAN)
- Ingress-Router und Egress-Router
- der Ziel-Host.

Ein MPLS-Tunnel wird zwischen Sender- und Empfänger-LANs (sog. Quell- und Zielsysteme) durch das Gesamtnetz ermittelt (z. B. per IP-Routing und RSVP, Resource Reservation Protocol). Am Eingang des MPLS-Tunnels agiert dabei der Ingress Router, am Ausgang agiert der Egress Router.

Der Gesamtablauf zwischen dem Quell-Host, den Ingress/Egress-Routern zu dem Ziel-Host im MPLS-Netzwerk enthält die folgenden Schritte [3]:
- Pfad („Tunnel“) durch das Gesamtnetz wird ermittelt (z. B. mittels IP-Routing)
- Label Distribution Protocol (LDP) legt Labels für diesen Pfad fest
- Ingress Router markiert eingehende Pakete gemäß Forward Equivalence Class (FEC) mit passendem Label
- Effiziente netzinterne Weiterleitung gemäß vorgegebenem Pfad (vgl. ATM) dabei Umwandlung Eingangslabel → Ausgangslabel durch jeden Switch
- Egress Router entfernt Label und leitet Pakete ins Zielsystem weiter.

Hinweis Labels unterscheiden sich prinzipiell von MAC- und IP-Adressen. Sie identifizieren keine Computer sondern einen Datenstrom.

Lösung zu 5.1b)
MPLS ermöglicht eine effiziente Weiterleitung von Paketen entlang vordefinierter Pfade (auch Hierarchie von Pfaden

möglich) gemäß ihrer sog. Forward Equivalence Class (FEC). Über die Pfade werden alle Pakete eines Datenstroms (bspw. für eine Videokonferenz) gleich behandelt. Diese Weiterleitung wird durch Labels gesteuert, die jeweils aufeinander folgende Pfadabschnitte kennzeichnen. In diese Weise garantiert MPLS erforderliche Dienstqualitäten (QoS) bei zeitkritischen Anwendungen.

Lösung zu 5.1c)
MPLS verwirklicht eine Abbildung auf existierende Netztechnologien wie historische Netze ATM, Frame Relay und auch die modernen Gigabit Ethernet und VPN. Die Effizienz von MPLS kann durch eine direkte Implementierung mittels spezieller MPLS-Hardware unmittelbar über Lichtwellenleiter (SONET) deutlich verbessert werden.

MPLS-Pakete sind wesentlich größer (Orientierung an Ethernet 1500 Byte) als ATM-Zellen mit fixierter Größe von 53 Byte. Dadurch wird der Overhead wesentlich verringert (Header-Anteil geringer) [3].

5.2 Ethernet und ALOHA: stochastische Medienzugriffsverfahren

a. Geben Sie die Klassifikation von Medienzugriffsverfahren an! Welche Medienzugriffsverfahren werden als „stochastisch“ bezeichnet?
b. Wie groß ist die Mindestframelänge beim „klassischen Ethernet“ IEEE 802.3?
c. Wie groß müssten die Frames bei einem busförmigen Netz der Länge 100 km, einer Datenrate von 100 Mbit/s und einer Signalausbreitungsgeschwindigkeit von 200.000 km/s mindestens sein?
d. Weshalb kann das CSMA/CD-Verfahren beim ALOHA-System nicht zum Einsatz kommen?

Lösung
Zu 5.2a) s. als Referenz Teil I Lehrbuch/Abschn. 3.2
- Medienzugriffsverfahren (MAC) definieren den Mehrfachzugriff auf Kanal (Shared Medium).
- Übertragungsmedien werden von den Teilnehmern im Netzverbund gemeinsam genutzt.
- Zur fehlerfreien Übertragung ist sicher zu stellen, dass nur 1 Teilnehmer Daten sendet.
- Zugriffssteuerung erforderlich (s. Klassifikation in ◘ Abb. 5.1)

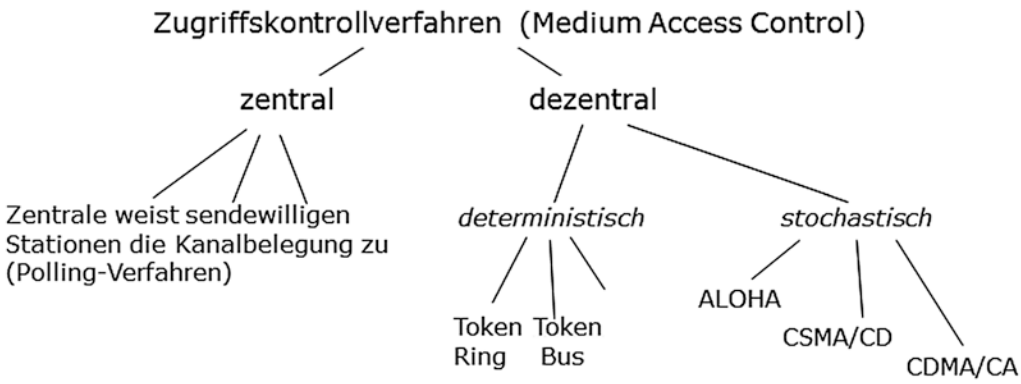


Abb. 5.1 Klassifikation MAC-Verfahren

MAC-Verfahren sind
deterministisch:
- Konventionen regeln, wann eine Station senden darf
- Sendebeginn erfolgt in Abstimmung mit anderen Stationen

oder stochastisch:
- Konventionen regeln nicht exakt, wann eine Station senden darf
- Stationen stehen in Konkurrenz um das Senderecht

Bspw. sind CSMA/CD und CSMA/CA, sowie das ALOHA-Verfahren stochastische Konkurrenzverfahren!

Zu 5.2b)
Beim „klassischen" Ethernet (busförmiges Teilmedium)
Sender und(!) Empfänger sollen eine evtl. Kollision erkennen können!

Extremfall	2 Sender an den Enden des Übertragungsmediums (Länge l) Sender 1 sendet zum Zeitpunkt t Startsignal benötigt Zeitdauer tl bis zum Ort von Sender 2 Sender 2 stellt mittels CS (Carrier Sense) bis zum Zeitpunkt (t + tl) fest: „Medium frei". Gemäß CSMA könnte er noch senden. In diesem Zeitraum ist eine Kollision möglich, danach nicht mehr, und CS liefert: „Medium besetzt".

Sender 2 stellt immer zuerst fest, dass eine Kollision vorliegt, Sender 1 aber nur, wenn er mindestens die doppelte Signallaufzeit sendet (→ Framemindestgröße)

Sendezeit:	T = F/DR	Framegröße/Datenrate
Laufzeit:	tl = l/v	Länge/Ausbreitungs-geschwindigkeit

Mit Tmin = 2 * tl ergibt sich:

F > 2 * l * DR/v

Mit den Werten l = 2,5 km, v = 200.000 km/s (Ausbreitungsgeschwindigkeit im Kabel) und DR = 10 MBit/s ergibt sich:

F > 250 Bit

IEEE 802.3:	Festlegung auf 512 Bit, bzw. 64 Byte (ohne Präambel) Daraus ergibt sich ein Zeitslot von mindestens 51,2 µs bei 10 Mbit/s.

Zu 5.2c)
Gegeben
Mit den Werten l = 100 km, v = 200.000 km/s und
DR = 100 MBit/s ergibt sich:
F > 2 * l * DR/v = 200 km * 100 MBit/s: 200.000 km/s
= 100.000 Bit = 12,5 kByte

Fazit
→ Framegröße ist deutlich zu groß, d. h. Ausdehnung des Netzes für diese Technologie zu groß
→ CSMA/CD nur für begrenzte Kabellängen geeignet

Zu 5.2d)
ALOHA – System:
- historisches Paketfunknetz, University of Hawaii, seit 1970
- Dezentrale Stationen, Kommunikation über Zentrale
- Unkoordiniertes Wettbewerbsverfahren (stochastisch)
- auch für Satellitenfunk geeignet
- f1: 407,35 MHz (Stationen => Zentrale, Uplink)
- f2: 413,475 MHz (Zentrale => Stationen, Downlink)
- Kollision auf f1 bei Zentrale, da Senden stets möglich Fehlerbehandlung durch Wiederholung, falls nach Zeit t keine Quittung auf f2
- Kein Mithören während des Sendevorgangs (CS) möglich (s. ◘ Abb. 5.2).

Diskussionsbeispiel
F = Framelänge, DR = 10 MBit/s
s = 36.000 km → Übertragungsentfernung
v = 300.000 km/s → Ausbreitungsgeschwindigkeit (≈ Lichtgeschwindigkeit)

$$\tau = \frac{36.000\ \text{km}}{300.000\ \text{km/s}} = 0{,}12\ \text{s} = 120\ \text{ms}$$

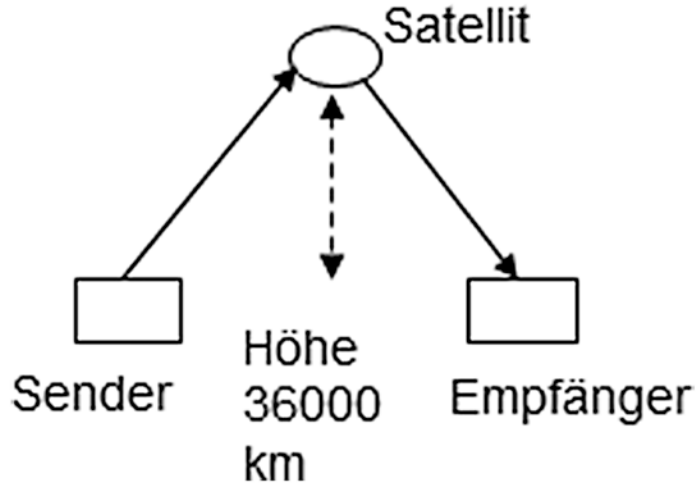


Abb. 5.2 Prinzip von ALOHA

$$F = t_s \cdot DR = 2\tau \cdot DR$$
$$F = 2 \cdot 0{,}12\ s \cdot 10 \cdot 10^6 \frac{Bit}{s}$$
$$F = 2.400.000\ bit\ =\ 2{,}4\ MBit$$
$$F = 300.000\ Byte$$

Fazit
Für eine Datenrate von 10 Mbit/s wird eine Framegröße von 300 kByte benötigt → inakzeptabel.

5.3 Netzwerktechnologien und WAN-Verbindungen

Im aufgeführten Beispiel (Abb. 5.3) erfolgt der Zugriff zu den Diensten einer Cloud über „Thin Clients" mithilfe von Smartphones, Laptops oder PC/Desktops mit den folgenden Monatsdatenvolumina (V1, V2, V3, s. Tab. 5.1):

a. Welche Netzwerktechnologien ermöglichen diesen Zugriff? Nennen Sie 2–3 Beispiele!
b. Ergänzen Sie die unten aufgeführte Tabelle und kreuzen Sie zutreffendes an!

Konvention: 1 M = 1.000.000; 1 G = 10^9; 1 T = 10^{12}

Abb. 5.3 Netzwerkzugriff mithilfe von Smartphones, Laptops oder PC/Desktops

Voraussetzungen Ein Monat hat im Schnitt 417 Arbeitsstunden, die durchschnittliche Auslastung der Verbindungen soll $\beta = 25\,\%$ nicht übersteigen, damit „burstartige" Belastungen abgefangen werden können (Tab. 5.1).

Lösung 5.3a)
Die folgenden Netzwerktechnologien ermöglichen typischerweise den Zugriff zu den Clouds:

- Mobilfunk per LTE (mobile User):
  DR = 150 Mbit/s
- Festnetzzugriff per DSL-Anschluss (Desktop-User):
  DSL = 50 MBit/s
- Zugriff über LAN und WLAN (Desktop- und BYOD-User – „Bring Your Own Device"):
  DR = 100 bis 10.000 MBit/s

Tab. 5.1 Auswahl geeigneter Technologien zur Übertragung gegebener Volumina

Netzwerktyp	Typische DR, Mbit/s	V_1 = 450 TByte	V_2 = 2,3 TByte	V_3 = 5 TByte
ATM OC-3	155			
LTE	150			
DSL50	50			
HSDPA	14,4			
WLAN 802.11n	108…600			
10GbE	10000			

Tab. 5.2 Tabelle mit Ergebnissen

Netzwerktyp	Typische DR, Mbit/s	V1 = 450 TByte	V2 = 2,3 TByte	V3 = 5 TByte
ATM OC-3	155			(x)
LTE	150			(x)
DSL50	50		x	
HSDPA	14,4			
WLAN 802.11n	108…600			x
10GbE	10000	x		

5

Lösung 5.3b)

$$\mathbf{T = 417\,h = 1{,}5\,Ms = 1{,}5 * 10^6\,s}$$

$$\mathbf{DR_{1,2,3} = 8 * V_{1,2,3}[inBit]/\beta * T = 32 * V_{1,2,3}[inBit]/T}$$

$$\mathbf{= 32 * V_{1,2,3}[inBit]/1{,}5Ms}$$

DR_1 = 32 * 450 TBit/1,5 Ms = 9600 (T/M) Bit/s = 9600 MBit/s = 9,6 GBit/s	d. h. 10 GbE
DR_2 = 32 * 2,3 TBit/1,5 Ms = 49,06 (T/M) Bit/s = 49 MBit/s	d. h. DSL50
DR_3 = 32 * 5 TBit/1,5 Ms = 106,66 (T/M) Bit/s = 107 MBit/s	d. h. WLAN 802.11n oder ATM OC3 oder LTE

Die Tabelle muss folgendermaßen aussehen (Tab. 5.2):

5.4 Netztechnologievergleich

Diskutieren Sie Vor- und Nachteile von MPLS, der Ethernet-Familie und ATM bei Einsatz als

- Last Mile Zugriff,
- Backbone,
- Lokales Netz

bezüglich

- Kosten,
- Dienstqualität (Anwendungen),
- Interoperabilität,
- Management,
- Datensicherheit.

Die Ergebnisse stellen Sie bitte tabellarisch dar!

Tab. 5.3 Tabelle mit Ergebnissen

Netzwerk	Ethernet-Familie	ATM	MPLS
Typ	LAN	Backbone im Gelände	Last Mile
Dienstqualität	Geringe Dienstqualität, Echtzeit nur durch die Erweiterung IEEE 802.1p	Dienstklassen, AAL1–5	Forward Equivalence Class, vordefinierte Pfade
Interoperabilität	+	+	++
Kosten	+	Teuer	+
Management	Per SNMP	Aufwändig, proprietär	+
Datensicherheit	Nur Klartext, da internes Netz und VPN/FW	Nur Klartext	+ (Verschlüsselung durch Egress/Ingress Router)/VPN

Losung zu 5.4
s. Tab. 5.3

5.5 Kopplungselemente: Transparent Bridges

Gegeben sei die folgende LAN-Topologie (Abb. 5.4) mit den Rechnern A…E und den transparenten Bridges B1, B2:

Wie werden die Wegewahltabellen bei transparenten Bridges aufgebaut?

a. Skizzieren Sie den Weg nacheinander gesendeter Frames mit folgenden Quell-/Zieladressen: (A/D), (B/A), (E/C), (B/E)!
b. Erfassen Sie in Tabellen, in welchen Schritten die Brücken ihre Kenntnisse über die Topologie des Netzes erwerben! Welche Informationen werten sie dazu aus?
c. Ergänzen Sie das Netz von b) um weitere Brücken, sodass alternative Wege möglich sind! Welche Probleme ergeben sich in diesem Fall für die Frameweiterleitung?
d. Benötigt man zur Lösung der Probleme von c) einen komplexen Routingalgorithmus (z. B. OSPF) oder gibt es einfachere Lösungen?

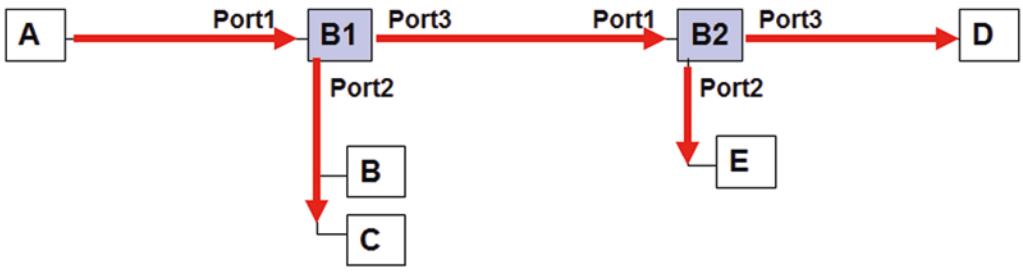


Abb. 5.4 LAN-Topologie mit Transparent Bridges

Lösung

Zu 5.5a) und b)

Die Weiterleitungstabellen der Brücken sind zunächst leer:

	Ziel-MAC	Port
	…	…
1.	A→D	B1 empfängt Frame über Port 1 Da Zielport für D unbekannt, Fluten über Port 2 und Port 3 Tabellenvermerk in B1: A erreichbar über Port 1 B2 empfängt Frame über Port 1 Da Zielport für D unbekannt, Fluten über Port 2 und Port 3 Tabellenvermerk in B2: A erreichbar über Port 1
2.	B→A	B1 empfängt Frame über Port 2 Ziel A bekannt → Ausgabe über Port 1 Tabellenvermerk in B1: B erreichbar über Port 2
3.	E→C	B2 empfängt Frame über Port 2 Da Zielport für C unbekannt, Fluten über Port 1 und Port 3 Tabellenvermerk in B2: E erreichbar über Port 2 B1 empfängt Frame über Port 3 Da Zielport für C unbekannt, Fluten über Port 1 und Port 2 Tabellenvermerk in B1: E erreichbar über Port 3
4.	B→E	B1 empfängt Frame über Port 2 Ziel E bekannt → Ausgabe über Port 3 B2 empfängt Frame über Port 1 Ziel E bekannt → Ausgabe über Port 2

Zu 5.5c) s. ◘ Abb. 5.5

Alternative Wege sind über B3 und B4 möglich, z. B. bei Ausfall von B1 oder B2.

Es ergibt sich allerdings ein Problem im Normalbetrieb. Der Aufbau der Weiterleitungstabellen in den transparenten Brücken funktioniert nicht (Zyklen) wegen der Vermaschung in der Topologie.

Zu 5.5d)

Kein komplexer Routingalgorithmus erforderlich;

Es muss lediglich eine logische Baumstruktur erreicht werden, z. B. durch Anwendung des Spanning- Tree-Protokolles.

Dabei vereinbaren die beteiligten Brücken, dass einige physisch existierende Leitungen ignoriert werden und dadurch eine Reduktion der Topologie auf einen logischen Baum erfolgt.

Auf diese Weise kann auch die vermaschte Topologie von c) genutzt werden. Bei Ausfall einer Brücke wird ein neuer Baum aufgespannt und das LAN arbeitet weiter.

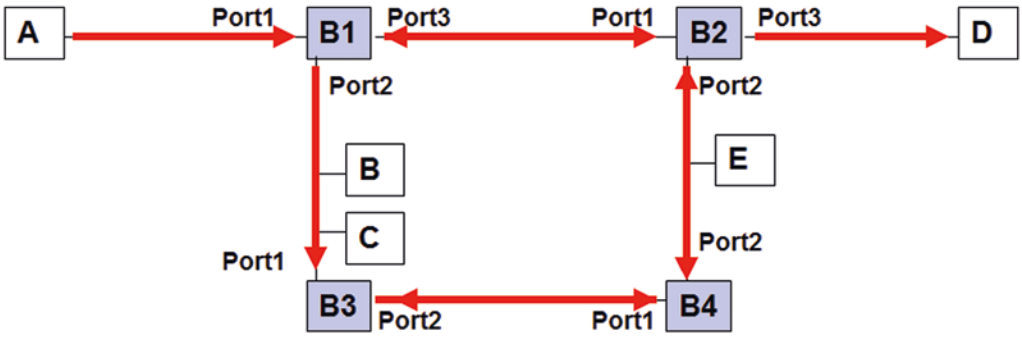


Abb. 5.5 LAN-Topologie mit vier Transparent Bridges und alternativen Wegen aufgrund der Vermaschung

5.6 Strukturierte Verkabelung und Einsatz von Switches als Kopplungselemente (am Bsp. der Vernetzung eines Studentenwohnheims)

Für ein Studentenwohnheim mit 3 Etagen (je 10 Zimmer) mit Anschluss an das Campusnetz und an das Internet soll eine Netzkonzeption erarbeitet werden.

a. Diskutieren und vergleichen Sie mögliche Ansätze im Bereich der Verkabelung!
b. Was bedeutet der Begriff „Strukturierte Verkabelung"?
c. Wählen Sie geeignete Netztechnologien und dafür erforderliche Koppelelemente aus!

Lösung

Zu 5.6a)

Verkabelung immer kostenintensiv und kurze Abschreibungsdauer

Bedarfsverkabelung (alt) vs. Strukturierte Verkabelung (aktuell)

Alter Ansatz

- Bedarfsverkabelung (Topologien Bus, Ring, Stern)
- stark an die Netzwerktechnologie angelehnt
- unflexibel, nicht an höhere Auslastung und Realtime anpassbar
- obsolete, nicht langlebig

Aktueller Ansatz

- nur strukturierte Verkabelung nach den Standards EN 50173 (EU) und EIA/TIA 568 (weltweit)
- Trennung der Bereiche: primär, sekundär, tertiär (s. Abb. 5.6)

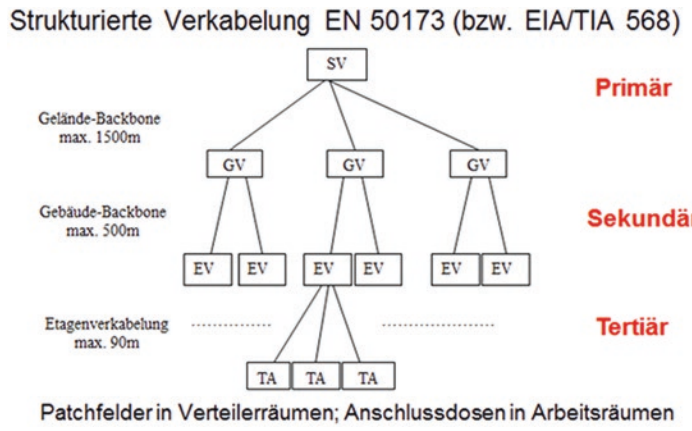


Abb. 5.6 Strukturierte Verkabelung mit Trennung der Bereiche: primär, sekundär, tertiär

Zu 5.6b)
Strukturierte Verkabelung (s. Teil II Lehrbuch)
Trennung aktive/passive Komponenten
aktive Komponenten (Switches, PC, …) austauschbar
passive Komponenten (Kabel, Trassen, Verteilerräume)
→ langlebig; anwendungsunabhängig

Topologie
Baumstruktur optimal für Wartung, flexible Nutzung
→ Koppelelemente mit Lasttrennung!!!
Switches, keine Hubs

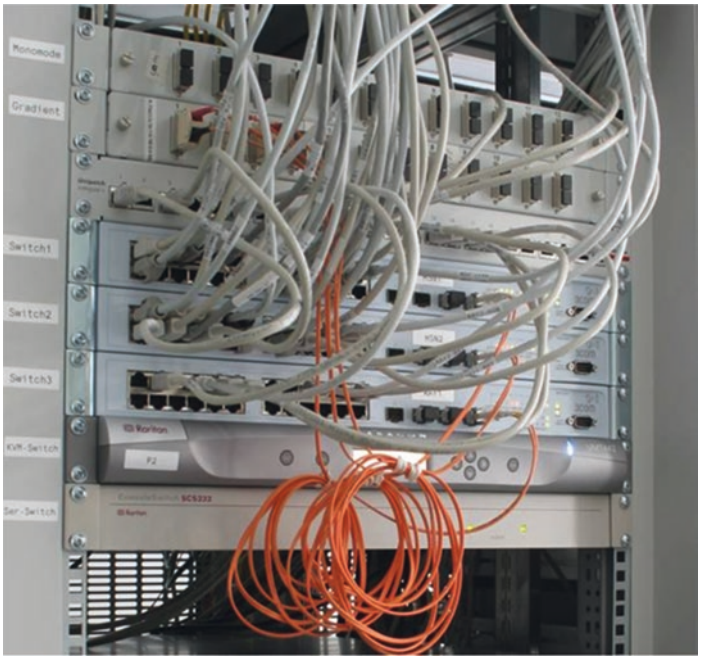
Legende
SV – Standortverteiler, GV – Gebäudeverteiler, EV – Etagenverteiler, TA – Teilnehmeranschluss

Lösung zu 3.6c)
Beispiel Studentenwohnheim
(3 Etagen, je 10 Zimmer, Internetanschluss)
- Je Etage ein Verteilerraum mit Patchfeldern, möglichst übereinander, verbunden durch Kabelschacht
- Je Etage Kabeltrasse zu Studentenzimmern (10 Kabel)
- Kabel: Patchfeld ↔ Anschlussdose im Zimmer

- Die Switches sind:

EG:	Gebäudeverteiler-Switch EG-Switch, verbunden mit GV-Switch und Arbeitsplatzrechnern im EG
OG1:Switch,	verbunden mit GV-Switch und Arbeitsplatzrechnern im OG1
OG2:Switch,	verbunden mit GV-Switch und Arbeitsplatzrechnern im OG2

- Kabel, Cu RJ-45 mind. Cat 6 (falls Länge <90 m)
  sonst LWL (Switches mit Wandlerfunktionalität erforderlich!)
- Internetanschluss
- 1 Router im EG, angeschlossen an GV-Switch
  evtl. im Verteilerraum
  NAT/PAT-Funktionalität
- DSL-Anschluss, möglichst VDSL mit Datenrate >>100 Mbit/s
- 1 IP-Adresse vom Provider
  (s. ◘ Abb. 5.7 mit einem 19”-Schrank mit Patchfeld)



◘ **Abb. 5.7** 19”-Schrank mit Patchfeld

5.7 Firewall als Kopplungselement

a. Welche Basiskonzepte für die Firewalls sind Ihnen bekannt? Nennen Sie drei Firewallkonzepte und geben Sie ihre Zuordnung zu den OSI-Schichten an!
b. Nennen Sie Beispiele, bei denen die Verwendung eines Paketfilter-Firewalls ausreicht bzw. bei denen eine anwendungsbezogene Filterung erforderlich ist! Diskutieren Sie dies am Beispiel einer Schule.
c. Warum gibt es eine sog. demilitarisierte Zone (DMZ)?
d. In welcher Zone des Netzes können private Adressen eingesetzt werden? Welche Vorteile bringt dies?

Lösung
Zu 5.7a)
s. Teil III Lehrbuch Abschn. 18.3.2
Eine Firewall (FW) ist ein Kopplungselement in den RN mit einem eingebauten Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt und ist auch ein Teilaspekt eines Sicherheitskonzepts des Unternehmens dabei. Die Zuordnung der FW-Systeme (Filterung-Funktionalität) zu den OSI-Schichten ist wie folgt:

- PF – Paketfilter (Layer 3)
- CR – Circuit Relay (Layer 4)
- AG – Application Gateway (Layer 5–7).

Das Ziel einer FW ist die mehrseitige Filterung/Blockierung unberechtigter Zugriffe in privaten Netzwerken, zu den Anwendungen und Datenbeständen auf der Basis von IP-Adressen (PF, Paketfilter), TCP/IP-Portinformationen (CR, Circuit Relay) bzw. anwendungsbezogenen Informationen (AG, Application Gateway). Die Zusammenfassung der Filtermöglichkeiten einer Firewall ist wie folgt (s. Tab. 18.3 Teil III Lehrbuch):

Weitere Lösung am Beispiel einer Schule
Zu 5.7b)
Paketfilter

- unterschiedliche Paketfilter für Lehrer-/Schülerrechner
- zeitweiliges Sperren/Erlauben Internetzugriff für Schüler
- WWW-Zugriff nur auf spezielle Bildungsserver

anwendungsbezogene Filter

- Filtern Spam-Mails
- Sperren Zugriff auf pornographische Webseiten

Zu 5.7c)
- In demilitarisierter Zone zwischen zwei Paketfiltern nur ein geringer Anteil der Computer
- besser durch Techniker kontrollierbar
- für Einsatz der öffentlich verfügbarer Dienste geeignet
- Masse der Computer abgeschottet gegen Hackerangriffe usw.

Zu 5.7d)
- private Intranetadressen im abgeschotteten Schulnetzwerk (Intranet)
- Vorteil: Einsparung (kostenpflichtiger) IP-Adressen, Abschottung einfach
- Im Gegensatz:
  In demilitarisierter Zone vollwertige IP-Adressen (weltweit eindeutig) erforderlich!

5.8 Satellitenfunk

Wie lange dauert die Datenfunkübertragung eines Datenpakets mit Länge L = 1000 Byte zwischen einer terrestrischen Station und einem Satelliten (Uplink-Modus) auf der Orbithöhe h = 1200 km bei der maximalen Bitrate des Senders DR = 10 MBit/s?

a. Berechnen Sie die Gesamtzeit bei der Satellitenfunkkommunikation!
   Beachten Sie die korrekte und SI-konforme Umwandlung der Maßeinheiten!
b. Zu welcher Satellitenklasse (LEO, MEO, GEO) gehört der oben genannte Satellit?
   Welche Pro und Kontra haben Satelliten dieser Klasse?

Lösung zu 5.8a)
Die Formeln zur Berechnung sind wie folgt:
- Gesamtzeit T = t1 + t2
- Sendezeit t1 = L/DR
- Ausbreitungszeit t2 = h/c,
  wobei c die Lichtgeschwindigkeit ist (im SI-Maßeinheitensystem gleich 299.792.458 m/s oder 299.792,458 km/s), gerundet auf 300.000 km/s.

t1 = L/DR = 8000 Bit: 10^7 Bit/s = 8 * 10^{-4} = 0.8 ms
t2 = h/c = 1200 km/300.000 km/s = 4 ms
Die Datenfunkübertragung dauert: T = 4 ms + 0,8 ms = 4,8 ms

Lösung zu 5.8b)
Laut der Tab. 13.2, Teil II Lehrbuch, gehört der Satellit zu den LEO-Systemen.

Die nichtstationären LEO-Systeme sind charakterisiert durch:

- Abstand h von der Erde von ca. 300–1800 km;
- kurze Signallaufzeiten von 5–10 ms, niedrige Sendeleistung bei Eignung für Telefonie;
- jedoch sind zur Empfangsbereichsabdeckung mehr Satelliten erforderlich (>50) bei häufigen Übergaben (Handover) in Zeiträumen von ca. 10 min.;
- kürzere Lebenserwartung (5–8 Jahre) wegen der atmosphärischen Reibung.

Systembeispiele sind: Iridium, Teledesic, Globalstar, Starlink (SpaceX/Elon Musk), ISS. ◘ Abb. 3.4 illustriert die ISS (Int. Weltraumstation) als bekanntestes LEO-Satellitensystem und der Menschheit erste Raumfahrt am 12.04.1961 (Juri Gagarin, Flugdauer = 108 min, Höhe h = ca. 400 km, LEO).

5.9 Klassen von Satellitensystemen

Berechnen Sie die in der unten aufgeführten Tabelle (◘ Tab. 5.4) fehlenden Angaben (ggf. Satellitenhöhe h oder Umlaufperiode T).

◘ **Tab. 5.4** Zusammenhang Satellitenhöhe und Umlaufperiode. Tabelle mit fehlenden Angeben zum Ergänzen

Typ	Satellitenhöhe h	Umlaufperiode T
GEO (Geostationary Earth Orbit Satellite)	?	24 h
MEO (Middle Earth Orbit Satellite)	7000 km	?
LEO (Low Earth Orbit Satellite)	700 km	?
GPS (Global Positioning System, US NAVSTAR-Satellite)	20.200 km	?
ISS (International Space Station)	?	92 min

Hinweis
Die Umlaufperiode T ergibt sich zu $T = \text{sqrt}((R + h)^3/a)$ mit der Konstante

$$a = g * R^2/(2 * PI)^2$$

mit dem Erdradius R = 6378 km und der Konstante g = 9,81 N/kg (sqrt bedeutet Quadratwurzel).
Geben Sie Acht, dass Sie die richtigen Maßeinheiten verwenden!

a. Berechnen Sie die lineare Geschwindigkeit v_{GPS} bei der gegebenen Satellitenhöhe h_{GPS} für GPS-Erdsatelliten mit der Umlaufperiode T_{GPS}!
b. Berechnen Sie die lineare Geschwindigkeit v_{ISS} bei der gegebenen Satellitenhöhe h_{ISS} für GPS-Erdsatelliten mit der Umlaufperiode T_{ISS}!

Hinweis zu 5.9 a) + b)
V = (2PI/T) * (R + h)

Lösung zu 5.9
Die Formel sind:

$T = \text{sqrt}((R + h)^3/a)$	R, h in km
$a = g * R^2/(2 * PI)^2$	T in h

Die Ergebnisse wurden in ◘ Tab. 5.5 zusammengefasst:

◘ **Tab. 5.5** Zusammenhang Satellitenhöhe und Umlaufperiode. Tabelle mit Ergebnissen

Typ	Satellitenhöhe h	Umlaufperiode T
GEO (Geostationary Earth Orbit Satellite)	Ca. 36.000 km (exakt 35.786 km)	24 h
MEO (Middle Earth Orbit Satellite)	7000 km	257 min = 4 h 17 min
LEO (Low Earth Orbit Satellite)	700 km	99 Min
GPS (Global Positioning System, US NAVSTAR-Satellite)	20.200 km	12 h
ISS (International Space Station)	Ca. 400 km (exakt 371 km)	92 min

Lösung zu 5.9 a) + b)
$\pi = 3.1415926$

GPS:

$$v = (2PI / T) * (R + h)$$
$$= (6.28319/ 12\ h) * (6378\ km + 20200\ km)$$
$$= 13916\ km/h = 232\ km/Min = \mathbf{3{,}87\ km/s}$$

ISS:

$$v = (2PI / T) * (R + h)$$
$$= (6.28319/ 92\ Min) * (6378\ km + 371\ km)$$
$$= 461\ km/Min = \mathbf{7{,}68\ km/s}$$

Exkurs

Zur Automatisierung der Berechnungen 5.9 a) … g)
kann das folgende einfache C-Programm verwendet werden:

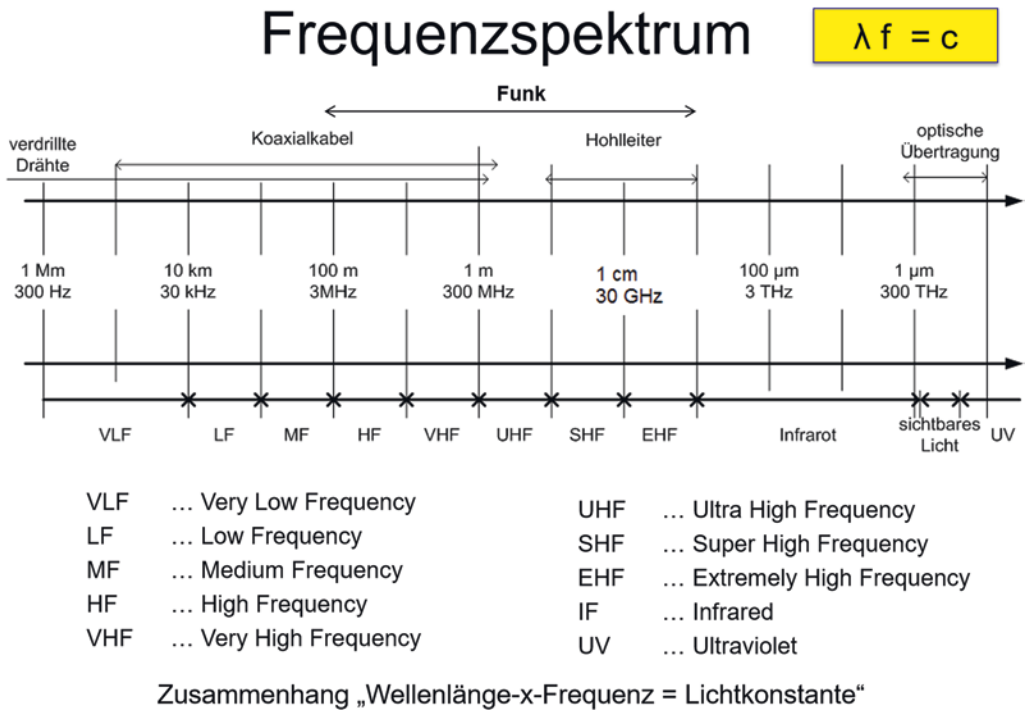
```
#include <stdio.h>
#include <stdlib.h>
#define PI 3.14159265358979
int main(void)          // ***************** SAT.c
{
 puts("Hallo SAT\n");
 double a, r, T, v;
 double g=9.81;       // Erdbeschleunigung [N/kg]
 double R=6370.0;     // Erdradius in [km]
 double h= 35786.0;  // Satellitenhöhe in [km]
bitte!
 printf("SAT Hoehe h = %.2f[km]\n", h);
 r=R+h;      // Abstand Erdmittelpunkt zum SAT
 R = R * 1000.0;   // in [m]
 r = r * 1000.0;   // in [m]
 // Folge Keplersches Gesetz: r**3/ T**2 = Const a
 a = g*R*R / (4.*PI*PI);   // Keplersche Konstante
 T = sqrt((r*r*r)/a);     // Umlaufperiode in [s]
 printf("Umlaufperiode T = %.2f[s]\n", T);
 T = T/ 3600.0; // Umlaufperiode in [h]
 printf("Umlaufperiode T = %.2f[h]\n", T);
```

```
 // Umlaufperiode in [Min]
 printf("Umlaufperiode T = %.0f[Min]\n", T*60.);
 v = (r / 1000.0) * (2. * PI) / T; // Wert r mu
ß wieder in [km] sein!
 printf("Geschwindigkeit des SAT = %.2f[km/
h]\n", v);
 printf("Geschwindigkeit des SAT = %.2f[km/
s]\n", v/3600.);
 system("PAUSE");
 return 0;
}
```

5.10 Frequenzspektrum und Funknetze

a. Werten Sie das nachfolgende Bild aus (◘ Abb. 5.8).

Geben Sie die Klassifikation von Frequenzbereichen und Wellenlängen an!



◘ **Abb. 5.8** EM-Schwingungen: Frequenzbereiche und Wellenlängen

In welchem Frequenzbereich kommen die Funknetze zum Einsatz?

a. Geben Sie die Klassifikation von Frequenzbereichen und Wellenlängen an!
   In welchem Frequenzbereich kommen die Funknetze zum Einsatz?
b. Welche Besonderheiten treten bei jeweiligen Wellentypen auf? Warum ist die LOS-Anforderung für Funkkommunikationssysteme von Bedeutung?
c. Typische Wellenlängen λ für Mobilfunkstandards sind nachfolgend aufgeführt:
   - GSM (890–960 MHz, 1710–1880 MHz), λ = 0,33 m (900 MHz)
   - WLAN IEEE 802.11b/g/n (2,4 GHz), λ = 0,125 m
   - WLAN IEEE 802.11a/n (5 GHz), λ = 0,06 m
   - WiMAX IEEE 802.16a (2–11 GHz), λ = 0,03 m (10 GHz)
   - WiMAX IEEE 802.16 (10–66 GHz), λ = 0,0045 m (66 GHz)

Wie hängen die Wellenlängen und Frequenzen zusammen?

Lösung zu 5.10a)

Die obige Abb. zeigt die maximalen Frequenzen für die in den Rechnernetzen einsetzbaren Übertragungsmedien (oberhalb dieser Frequenzen ist die Übertragung ausgeschlossen):

- Verdrillte Drähte (Twisted Pair Cat 5–7)
- Koaxialkabel (dick, dünn)
- Hohlleiter
- LWL (Lichtwellenleiter, optische Medien).

Je höher die Frequenz F ist, umso kleiner ist die Wellenlänge λ, umso mehr verhält sich eine Welle wie Licht.

Zu den Funknetzen gehören die Frequenzbereiche (s. die obige ◘ Abb. 5.8):

– HF	High Frequency	(100 m/3 MHz–10 m/30 MHz);
– UHF	Ultra High Frequency	(1 m/300 MHz–1 dm/3 GHz);
– SHF	Super High Frequency	(1 dm/3 GHz–1 cm/30 GHz);
– EHF	Extremely High Frequency	(1 cm/30 GHz–1 mm/300 GHz).

Die Funknetze werden i. d. R. im folgenden Bereich eingesetzt:

- Fmin = 3 MHz, λ = 100 m
- Fmax = 60 GHz, λ = 0,005 m = 5 mm

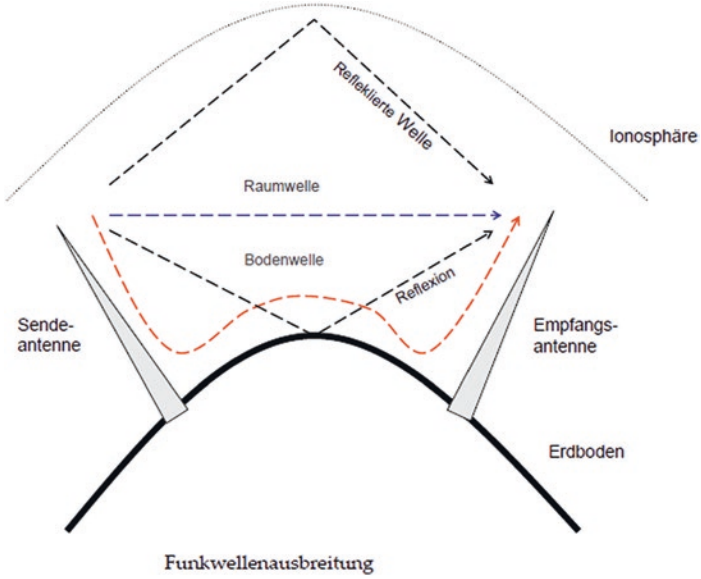


Abb. 5.9 Drei Wellentypen für die Funkwellenausbreitung

Man unterscheidet die folgenden Wellentypen (s. die nachfolgende Abb. 5.9):

- Boden- oder Oberflächenwellen
- Raumwellen
- Direktwellen

Lösung zu 5.10b)

In Abhängigkeit von der Frequenz können Funkwellen auch in Objekte eindringen bzw. diese durchdringen, je höher die Frequenz eines Signals, desto mehr verhält sich dieses wie Licht:

- Signale niedriger Frequenz (z. B. Langwellen, ca. 150–280 kHz) können Ozeane überwinden
- Kleine Objekte, wie z. B. Blätter eines Baumes, können Signale im EHF-Bereich (ab 30 GHz) blockieren.
- Wellen niedriger Frequenz (30 kHz–3 MHz), d. h. großer Wellenlänge, breiten sich der Erdkrümmung folgend als Boden- oder Oberflächenwellen aus. Sie können noch in großer Entfernung und sogar in Tunneln empfangen werden.

Bei höheren Frequenzen bilden sich vorwiegend Raumwellen aus. Die direkte Strahlung wird hier abhängig von der Rauigkeit und Leitfähigkeit der Erdoberfläche schnell gedämpft. Abhängig von ihrer Frequenz werden diese Wellen auch in der Ionosphäre gebeugt und reflektiert. Dadurch werden bei mittelgroßen Frequenzen (3 MHz–30 MHz) Reichweiten von 100 bis 150 km erreicht, während bei höheren Frequenzen (30 MHz–3 GHz)

die Reichweite aufgrund der erhöhten Durchlässigkeit der Ionosphäre in diesem Frequenzbereich geringer wird. Man spricht hier auch von Radiohorizont. Bei verstärkter Sonneneinstrahlung können Raumwellen mehrere tausend Kilometer zurücklegen.

Hinweis

- je höher Frequenz, desto höher die Datenrate (s. Teil I/ Nyquist-Theoreme)
- je höher die Frequenz eines Signals, desto mehr verhält sich dieses wie Licht

Wellen mit einer Frequenz oberhalb 3 GHz breiten sich als Direktwellen aus und sind somit näherungsweise nur innerhalb des optischen Horizonts zu empfangen. Die Erdkrümmung und die Sichtlinie sind zu berücksichtigen (LOS – line of sight in Electrical Optics; NLOS – non-line of sight).

Die Durchdringung von Objekten wird mit zunehmender Frequenz schlechter. Hindernisse, die kleiner als die Wellenlänge sind, spielen nur untergeordnete Rolle

Speziell gilt:

- Bei GSM ist die gute Durchdringung typisch. Keine Einflüsse von Objekten der Größe von Blättern und Regentropfen treten auf.
- Bei WiMAX, 5G werden sogar Objekte der Größe von Blättern und Regentropfen zu Hindernissen!

Lösung 5.10c)

Typische Wellenlängen λ für Mobilfunkstandards sind nachfolgend aufgeführt:

- GSM (890–960 MHz, 1710–1880 MHz), λ = 0,33 m (900 MHz)
- WLAN IEEE 802.11b/g/n (2,4 GHz), λ = 0,125 m
- WLAN IEEE 802.11a/n (5 GHz), λ = 0,06 m
- WiMAX IEEE 802.16a (2–11 GHz), λ = 0,03 m (10 GHz)
- WiMAX IEEE 802.16 (10–66 GHz), λ = 0,0045 m (66 GHz)

Wie hängen die Wellenlängen und Frequenzen zusammen?

$$c = \lambda * f \quad \text{mit}\, c = 300.000 \frac{\text{km}}{\text{s}} = 3 * 10^8 \frac{\text{m}}{\text{s}}$$

Bsp.:

$$\lambda_{\text{GSM}} = \frac{c}{f} = \frac{3 * 10^8 \frac{\text{m}}{\text{s}}}{900 * 10^6\,\text{Hz}} = \frac{300\,\text{m} * \text{s}}{900\,\text{s}} = 0{,}33\,\text{m}$$

Für die anderen Funknetzwerktechnologien ist die Rechnung sinngemäß.

5.11 Spektraleffizienz

a. Was versteht man unter dem Begriff „Spektraleffizienz“?
b. Wie errechnet sich maximale Spektraleffizienz eines Mobilfunksystems anhand der Nyquist- Theoreme?

Lösung zu 5.11a)
Die Spektraleffizienz nach Nyquist *SE* (Spectrum Efficiency) wird in [bit/s/Hz] gemessen und charakterisiert, wie gut die verfügbare Bandbreite durch bestimmte Netzwerkstechnologien für die Datenübertragung ausgenutzt wird.

Von besonderer Bedeutung wird diese Größe bei den Funknetzen (UMTS, HSDPA, LTE, WLAN, WiMAX etc.), da es um effiziente Nutzung der raren und preisintensiven Ressource Frequenzbandbreite geht.

Lösung zu 5.11b)
Laut Nyquist-1 und Nyquist-2, s. Formel (2.4)/Teil II Lehrbuch:
$SE = DR/B = \min [\ 2ldS, ld(1+SNR)]$

Berechnen wir die maximalen SE-Werte für die folgenden Beispiele:

UMTS:
Datenrate - DR = 2 MBit/s
Frequenzbandbreite - B = 10 MHz
$SE_{UMTS} = 0{,}2$

LTE:
Datenrate - DR = 150 MBit/s
Frequenzbandbreite - B = 5 MHz
$SE_{LTE} = 30$

5.12 Antennentechnik und Funknetze

a. Was ist eine Antenne? Welche Antennenarten kennen Sie? Welche Antennenarten kommen bei WLAN zum Einsatz? Welche Antennenarten kommen beim Mobilfunk zum Einsatz?
b. Diskutieren Sie Vorteile MIMO vs. SISO! Führen Sie entsprechende Systembeispiele an!
c. Diskutieren Sie die Unterschiede zwischen den Begriffen „Richtfunk“ vs. „Rundfunk“ vs. „Sektorantennen“!
d. Was ist Handover in Mobilfunknetzen? Verdeutlichen Sie den Begriff!

Lösung zu 5.12a)
Eine Antenne ist eine technische Anordnung zur Abstrahlung und zum Empfang elektromagnetischer Wellen zur mobilen/drahtlosen Kommunikation. Die Baugröße liegt in der Größenordnung der halben Wellenlänge, bei kurzen Wellenlängen auch ein Vielfaches und bei sehr langen auch einen Bruchteil davon und reicht von mehreren hundert Metern für den Längstwellenbereich bei unter 10 kHz bis hinab zu Bruchteilen von Millimetern für den Höchstfrequenzbereich bei über 1 THz.

Antennenarten:
Rundstrahler, Sektorantennen, Richtantennen

Die folgenden Antennentypen werden bei Wi-Fi/WLAN eingesetzt (◘ Tab. 5.6):
Beim Ausbau von Mobil-/Funknetzen werden geographische Bereiche zur Flächendeckung mit den Sektorantennen in Funkzellen aufgeteilt. Die Frequenzbänder benachbarter Funkzellen in einem Cluster werden dabei so gewählt, dass Interferenzen minimiert werden (s. ◘ Abb. 5.10).

Lösung zu 5.12b)
MIMO-Technik (Multiple Input/Multiple Output)
- Fortgeschrittene Antennentechnik
- Im Gegensatz zur herkömmlichen Technik SISO-Technik (Single Input/Single Output)
- Nutzung mehrerer Sender-/Empfängerzüge (4 x 4 bis 3D-Strukturen: 8 x 8 x 8)

Laut Nyquist
$DR_{SISO} = B * ld\ (1 + SNR)$

◘ **Tab. 5.6** Antennentypen

Einsatz	Rundstrahler	Sektorantenne	Richtantenne
Wohnungen, Privathäuser	+++	+	–
Hörsäle, Konferenzsäle	+++	+	–
Kleine Räumlichkeiten	+++	++	–
Bahnhöfe, Flughäfen	++	+++	–
Büros	+++	++	–
Flure in den Gebäuden	–	+++	++
Höfe, gekurvte Gebäudegrundrisse	+	+++	–
Städtischer Bebau (Street Canyon)	–	+++	++
Line-of-sight (LOS)	–	–	+++

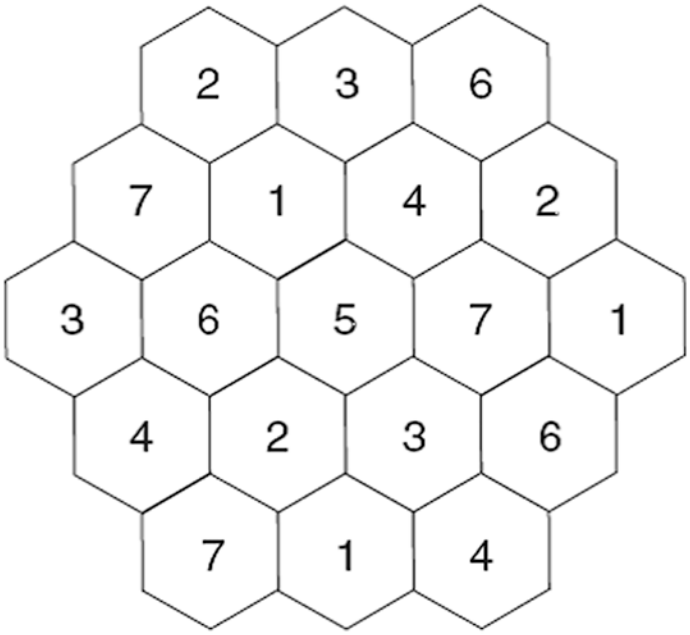


Abb. 5.10 Ein Cluster mit 7 Funkzellen ist typische für GSM-Netze

DR ist u. a. von der Verstärkung der Antenne abhängig. SNR steigt aufgrund der Verstärkung:

$SNR_{MIMO} > SNR$ (Signal nach Rauschen – Abstand).

$DR_{MIMO} = K * B * ld (1 + SNR_{MIMO})$,
DR steigert aufgrund der Multiplikation der Sender-/Empfängerzüge
Wobei
K = Produkt der Anzahl von Sender-/Empfängerzügen.

Bemerkung
Wenn $DR_{MIMO}/DR_{SISO} = K'$, dann $K' > K$, da $SNR_{MIMO} > SNR$!

Systembeispiele: LTE, WiMAX, WLAN 802.11n, ac, ad, künftig 5G

Lösung zu 5.12c)
Richtfunk vs. Rundfunk vs. Sektorantennen (s. dazugehörige obige Tab.)
Richtfunk

- überwiegende Abstrahlung elektromagnetischer Wellen in einer ausgewählten Richtung
- wird mit Richtantennen verwirklicht
  kleiner Öffnungswinkel vom Sender bzw. zum Empfänger

- Neigungswinkel bzw. LoS von Bedeutung
- i. d. R. hochfrequente Kommunikation und Direktwellen
- bei SAT-Funk größere Sendeleistungen als bei terrestrischen Funktechnologien.

Rundfunk
- wird mit horizontalen Rundstrahlern (omni-direktionale Antennen) verwirklicht
- i. d. R. niederfrequente Kommunikation mittels Raumwellen und Bodenwellen

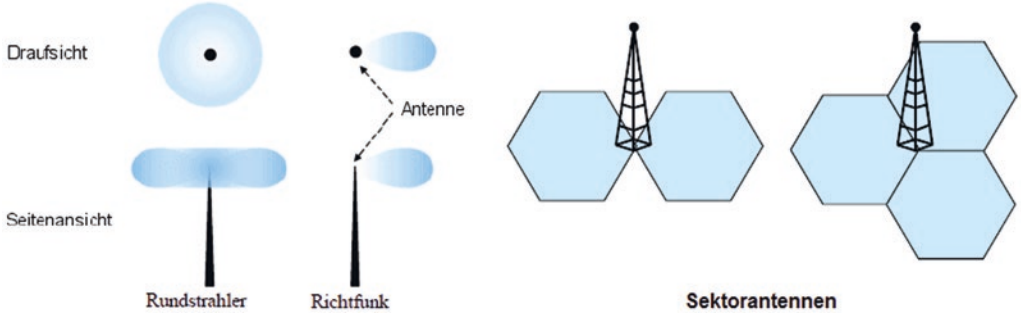
5

Sektorantennen
Mit Hilfe von speziellen Richtantennen anstelle omni-direktionalen lassen sich gezielt ausgewählte Sektoren versorgen, bspw.
- 2-Sektor-Kombination beispielsweise entlang Autobahnen oder Zugstrecken
- 6-Sektor-Kombination zur Flächendeckung (s. ◘ Abb. 5.11).

Lösung zu 5.12d)
Handover
Vorgang innerhalb eines zellularen Netzes, bei dem ein Endgerät vom Sendebereich einer Zelle A in den Sendebereich einer benachbarten Zelle B während einer Sprach- oder Datenverbindung wechselt (◘ Abb. 5.12).

Auf dem Bild:
das Gerät wechselt aus dem Empfangsbereich der Zelle A in den Empfangsbereich der Zelle B während einer Sprach/Datenverbindung

Gründe für einen Handover:
- Verlassen des Sendebereiches einer Zelle
- Überlastung oder Ausfall der aktuell benutzten Zelle
- Verbindungsqualität sinkt unter definierten Wert



◘ **Abb. 5.11** Antennentypen: Rundstrahler, Richtfunk, Sektorantennen

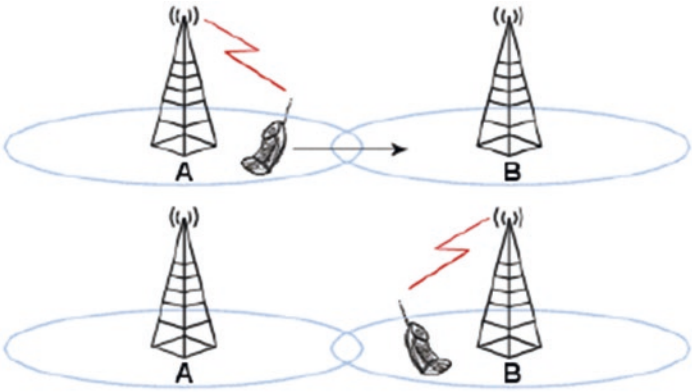


Abb. 5.12 Handover

5.13 Freiraumdämpfung/EIRP

Das Freiraumdämpfungsmodell (FSL, oder Free Space Loss Model) stellt das einfachste aller denkbaren Simulationsmodelle für die Ausbreitung von elektromagnetischen Wellen dar. Dabei wird angenommen, dass sich das Sendesignal kugelförmig um die Sendeantenne verteilt (isotroper Kugelstrahler).

Zu einer ersten Abschätzung der Empfangsqualität kann das Modell genutzt werden, obwohl dämpfende Umgebungsobjekte (z. B. Wände) nicht berücksichtigt werden.

Die FSL-Dämpfung kann nach folgenden Formeln berechnet werden, wobei d den Abstand zwischen Sende- und Empfangsantenne bedeutet, λ die Wellenlänge und f die Frequenz.

$$\begin{aligned} \text{FRD} &= \text{Sendeleistung/Empfangsleistung} \\ &= (4\pi * d/\lambda)^2 = (4\pi * f * d/c)^2 \end{aligned}$$

In der Praxis verwendet man meist die logarithmierte Form (Angabe in dB)

$$\text{FRD}_{\log} = 10 * \log(\text{FRD}) = 32{,}44 + 20 * \log(f/\text{MHz}) + 20 * \log(d/\text{km})$$

a. In einem WLAN ist ein Access Point im Außenbereich installiert mit der Sendefrequenz 2,4 GHz und der Sendeleistung Ptx = 30 mW. Wie groß ist die Empfangsleistung Prx in 35 m Abstand? (Wenden Sie das Modell der Freiraumdämpfung an.) Vergleichen Sie die Ergebnisse nach den obigen zwei Formeln.
b. Ab welchem Abstand ist der Empfang nicht mehr möglich (Empfangsleistung unter 10^{-10} W)?

Der Gesetzgeber beschränkt die zulässige Sendeleistung, z. B. für WLAN 802.11 b/g auf eine max. EIRP-Leistung von 100 mW. Für

die Bestimmung der zulässigen Sendeleistung muss der Gewinn der verwendeten Antenne abgezogen werden.

c. Wie hoch darf die max. Sendeleistung bei IEEE 802.11 g sein, wenn eine Sendeantenne mit einem Gewinn von 12 dBi eingesetzt wird?

Lösung

Zu 5.13a)

$FRD = Ptx/Prx = (4\pi d/\lambda)^2$

$$\begin{aligned} Prx = \quad Ptx/(4\pi d * f/c)^2 \quad &= 30\,mW/(4\pi * 35\,m * 2{,}4 * 10^9\,s^{-1}/ \\ &\quad (3 * 10^8\,m/s))^2 \\ &= 30\,mW/(3518{,}6)^2 \\ &= 2{,}4 * 10^{-9}\,W \end{aligned}$$

Empfangen werden nur 2,4 nW.

$$\begin{aligned} FRD &= 30\,mW/2{,}4 * 10^{-9}\,W \\ &= 12{,}5 * 10^6 \\ FRD_{log} &= 10 * \log(FRD) \\ &= 70{,}97\,dB \\ FRD_{log} &= 32{,}44 + 20 * \log(2400) + 20 * \log(0{,}035) \\ &= 70{,}92\,dB \end{aligned}$$

Beide Formeln ergeben die gleiche Dämpfung.
Die geringe Abweichung erklärt sich durch Rundungsprobleme.

Zu 5.13b)

$FRD = Ptx/Prx = (4\pi * f * d/c)^2$

$$\begin{aligned} d &= (c/4\pi * f) * \text{sqrt}\,(Ptx/Prx) \\ &= (3 * 10^8\,m/s/(4\pi * 2{,}4 * 10^9\,s^{-1})) * \text{sqrt}\left(0{,}03/10^{-10}\right) \\ &\text{sqrt}\left(0{,}03/\left(10^{-10}\right)\right) = 1{,}73 * 10^4 \\ &(3 * 10^8\,m/s/(4\pi * 2{,}4 * 10^9\,s^{-1})) = 0{,}00995 \\ d &= 0{,}00995 * 1{,}73 * 10^4\,m \\ &= 172\,m \end{aligned}$$

Zu 5.13c)

Für WLAN 802.11 b/g ist eine max. EIRP-Leistung von 100 mW gestattet.

10 lg(100 mW/1 mW)	→ maximale Sendeleistung	20 dBm
Antennengewinn (12 dBi) abziehen	→ zulässige Leistung (EIRP)	8 dBm
	bzw. $10^{0,8}$ mW	6,3 mW

5.14 FSL-Modelle im Mobilfunk

In der Mikrozelle eines Mobilfunknetzes im zugewiesenen Frequenzband von F = 2 GHz beträgt die minimale Empfangsleistung den Wert PRx = −92,5dBm bei der Sendeleistung von 0 dBm. Dies entspricht dem maximalen Pfadverlust PL (Path Loss) im Freien (s. Free Space Loss Model bzw. vorige Aufgabe!).

a. Schätzen Sie die maximale Reichweite d (Zellradius) für das Mobilfunknetz ab! Nutzen Sie das FSL-Ausleuchtungsmodell (Freiraumdämpfung) zum Modellieren der Pfadverluste!
b. Lösen Sie die Aufgabe bei dem minimal zulässigen Wert PRx = −72,5 dBm. Schätzen Sie die maximale Reichweite in diesem Fall ab. Wie ändert sich das Ergebnis?

Hinweis: Basierend auf dem Teil II bzw. Buch [5]:
Vorsicht ist bei den Maßeinheiten geboten, z. B. liefert die Frequenzangabe in GHz:
FRD_{log} = 10 * log(FRD) = 92,44 + 20 * log(f/GHz) + 20 * log(d/km)

Lösung: Zu 5.14a)
F-Band: F = 2000 MHz
FSL-Modell:
FRD_{log} = PL = 92,5 + 20 log f [GHz] + 20 log d [km];
PRx = PTx – FRD_{log}
−92,5dBm = 0dBm – FRD_{log}
d. h. Pfadverlust FRD_{log} = 92,5 dBm,
deswegen 92,5 = 92,5 + 20 log f [GHz] + 20 log d [km]
20 log f [GHz] + 20 log d [km] = 0, und aus Logarithmen-Gesetzen folgt:
(hier ohne Angabe phys. Einheiten!)
20 log f * d = 0 und log f * d = 0 und f * d = 1 und damit d [km]* 2 GHz = 1
d = 1/2 = 0,5 km = 500 m → als maximale Entfernung zur Basisstation (als Zellradius empfohlen)!

Zu 5.14b)
FSL-Modell:
F-Band: F = 2000 MHz
FRD_{log} = PL = 92,5 + 20 log f [GHz] + 20 log d [km];
PRx = PTx – FRD_{log}
−72,5dBm = 0dBm – FRD_{log}
d. h. Pfadverlust FRD_{log} = 72,5 dBm,
deswegen 72,5 = 92,5 + 20 log f [GHz] + 20 log d [km]
20 log f [GHz] + 20 log d [km] = −20, und aus Logarithmen-Gesetzen folgt:
(hier ohne Angabe phys. Einheiten!)

$20 \log f * d = -20$ und $\log f * d = -1$ und $f * d = 10^{-1} = 0{,}1$ und d [km]* 2 GHz = 0,1 und damit d = 0,1/ 2 = 0,05 km => nur 50 m als maximale Entfernung zur Basisstation!

Fazit: Kürzere Reichweite aufgrund der niedrigen Sensibilität des Empfängers!

5.15 Weitere Ausbreitungsaspekte in Funknetzen

a. Welche Funksignalausbreitungsaspekte soll man bei Aufbau von Funkkommunikationssystemen berücksichtigen? Geben Sie entsprechende Szenarien an.
b. Diskutieren Sie die wichtigsten Effekte der Wellenausbreitung je nach Wellenlänge!

Lösung

Zu 5.15a)

Bei der funktechnischen Versorgung über große Entfernungen müssen alle Effekte der Ausbreitung in Bezug auf die Landschaft und Atmosphäre berücksichtigt werden. Die Diffraktion (Beugung) hat einen bedeutenden Einfluss auf die Wellenausbreitung im Raum, wenn die physikalische Größe eines Hindernisses die Wellenlänge nicht wesentlich übersteigt (s. ◘ Abb. 5.13).

- Bei der Funkübertragung über große Entfernungen ist der Einfluss der Erdkrümmung zu berücksichtigen.
- Die Festkörper können die Elemente der Landschaft (Wälder, Berge) sowie den Bebau modellieren (s. Skizze)
- Die Festkörper reflektieren die Wellen, die rauen Fläche können diese zerstreuen (Primär, Sekundär und Tertiärwellen werden erzeugt).
- An den Kanten wird üblicherweise gebeugt außerdem zerstreut.
- Die Festkörper brechen und schwächen die Funkwellen ab. Diese können auch den sog. funktechnischen Schatten verursachen.
- Die Polarisationseffekte könnten bei den feinen Ausleuchtungsmodellen berücksichtigt werden [1, 5].

Zu 5.15b)

Die wichtigsten Effekte der Wellenausbreitung je nach Wellenlänge

1. Funkwellen bei niedriger Frequenz mit überwiegenden „Welleneigenschaften“:

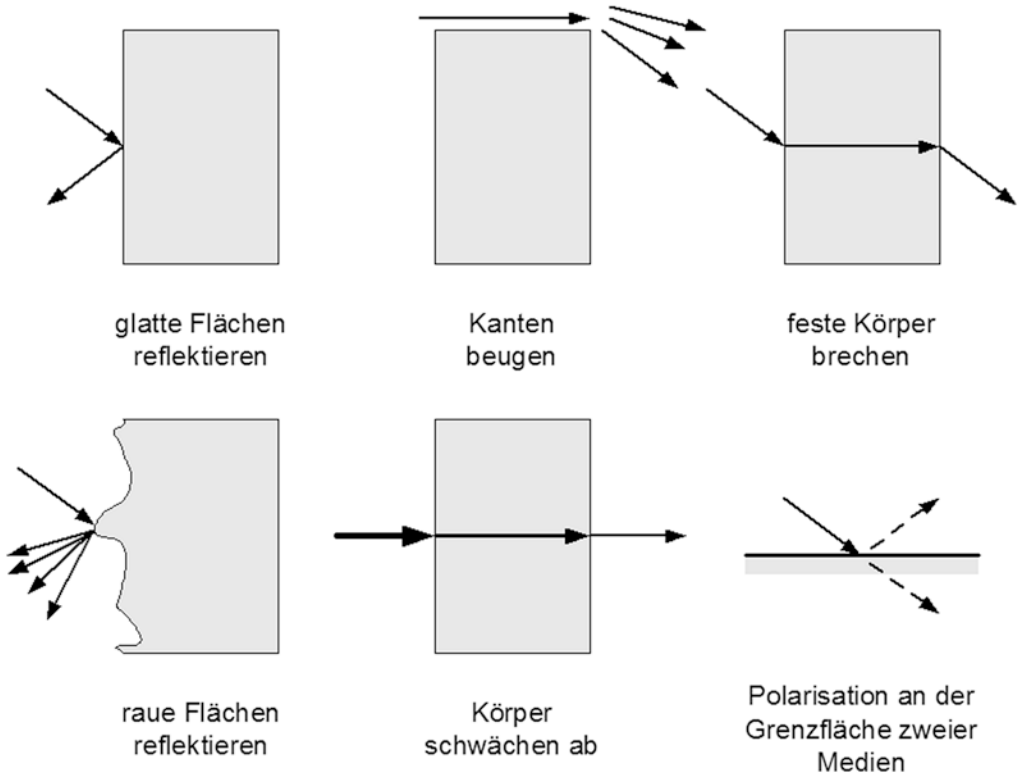


Abb. 5.13 Ausbreitungsaspekte in Funknetzen

- Es tritt Beugung, Reflektion, Brechung, Polarisation, Streuung, Abschattung und Freiraumdämpfung auf (alle frequenzabhängig)
- Abschattung und Reflexion durch Objekte verursacht, die wesentlich größer als die Wellenlänge des Signals sind
- Streuung des Signals an Objekten der Größenordnung der Wellenlänge und darunter
- Bodenwellen (Oberflächenwellen) haben niedrige Frequenz, breiten sich am Boden aus und können extrem große Entfernungen zurücklegen.

2. Je höher die Frequenz, desto mehr verhalten sich Funkwellen wie Licht:
   - Weniger Beugung, etc.
   - Raumwellen haben höhere Frequenz, dadurch auch geringere Reichweite
   - Direktwellen nur im optischen Horizont.
3. Übertragung über große Entfernungen:
   - Bodenwellen folgend der Erdkrümmung, sind sehr weit und sogar in Tunneln zu empfangen

- Raumwellen mit geringerer Beugung, Reichweite etwa 150 km (1000 km bei Sonneneinstrahlung) → nur bedingtes Folgen der Erdkrümmung
- Direktwellen nur in optischem Sichtbereich, können keiner Krümmung folgen (kaum Welleneigenschaften).

5.16 Zusammenfassung Kapitel 5

Der praxisorientierte Abschnitt bietet Ihnen Musterlösungen zu den Aufgabenstellungen zu Komplex II – Netzwerktechnologien und Mobile Kommunikation/Netzkopplung und Verkabelung. Die folgenden Themen werden geübt:

- Multiprotocol Label Switching (MPLS)
- Ethernet und ALOHA: stochastische
- Medienzugriffsverfahren
- Netzwerktechnologien und WAN-Verbindungen
- Netztechnologievergleich
- Kopplungselemente: Transparent Bridges
- Strukturierte Verkabelung und Einsatz von Switches als Kopplungselemente (am Bsp. der Vernetzung eines Studentenwohnheims)
- Firewall als Kopplungselement
- Satellitenfunk
- Klassen von Satellitensystemen
- Frequenzspektrum und Funknetze
- Spektraleffizienz
- Antennentechnik und Funknetze
- Freiraumdämpfung/EIRP
- FSL-Modelle im Mobilfunk
- Weitere Ausbreitungsaspekte in Funknetzen

Komplex III – Verarbeitungsorientierte Schichten und Netzwerkanwendungen

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze – Übungsbuch*,
https://doi.org/10.1007/978-3-658-25619-7_6

6.1 Klassische Internetapplikationen

a. Warum ist es sinnvoll, dass einige Anwendungen anstelle des Transportprotokolls TCP das weniger leistungsfähige Protokoll UDP nutzen?
b. In welchen Fällen ist es sinnvoll, Dateien mittels des SMTP-Protokolls zu verschicken und in welchen Fällen eignet sich das Protokoll FTP besser?
c. Welche Gefahren entstehen bei Nutzung des TELNET-Protokolls?
Zeigen Sie mögliche Maßnahmen zum Schutz auf!

Lösung zu 6.1a)
Warum ist es sinnvoll, dass einige Anwendungen anstelle des Transportprotokolls TCP das weniger leistungsfähige Protokoll UDP nutzen?

Protokoll TCP
- Verbindungsorientiert (Overhead durch Verbindungsaufbau/-abbau – bei längeren Datenübertragungen vernachlässigbar)
- Reihenfolgegarantie
- Flussteuerung
- keine Datenverluste (interne Fehlerkorrektur)

PRO:
- günstig für Filetransfer, Webseiten, Terminaldienste.

KONTRA:
- ungünstig für Multimediaströme (z. B. in Videokonferenzen) wegen Zeitverhalten (Übertragungswiederholungen verzögern Übertragungszeit und vergrößern Jitter, d. h. Schwankung der Ü-Zeit)
- ungünstig bei gelegentlichen, asynchronen Informationsabfragen geringen Umfangs, bspw. bei SNMP (Overhead für Verbindungsauf-/abbau fällt signifikant ins Gewicht)

Protokoll UDP
PRO:
- Nutzung von UDP mit anwendungsspezifischer Fehlerbehandlung z. B. bei Audio-/Videoübertragung keine Wiederholungen (nur Reihenfolgekorrektur), dadurch besseres Zeitverhalten, aber Akzeptanz von Datenverlusten.

Tab. 6.1 Anwendungsprotokolle

SMTP	FTP
Für wenige Empfänger	Für viele Empfänger
Einfache Zusendung	Abstimmung Sender-Empfänger
Kein Login erforderlich	Login erforderlich
Evtl. Spam-Gefahr	Evtl. Missbrauch des Logins, Lösung durch SFTP
Starke Größenbegrenzung	Geringe Größenbegrenzung
Klassische Protokolle unsicher (Passwortübertragung im Klartext usw.)	

Lösung zu 6.1b)
In welchen Fällen ist es sinnvoll, Dateien mittels des SMTP-Protokolls zu verschicken und in welchen Fällen eignet sich das Protokoll FTP besser (Tab. 6.1)?

Lösung zu 6.1c)
Welche Gefahren entstehen bei Nutzung des TELNET-Protokolls?

Zeigen Sie mögliche Maßnahmen zum Schutz auf!

TELNET – Gefahren
- jeglicher Netzverkehr (auch Passwörter) wird unverschlüsselt übertragen
- Initiator einer TELNET-Sitzung kann auf dem Partnerrechner Bedienkommandos für Betriebssystem geben
- bei Administratorrechten extrem gefährlich
- aber auch bei normalen Nutzerrechten Angriffe möglich
- evtl. Zugriffsrechte nicht ausreichend restriktiv (Dateien, Code)
- evtl. Ausnutzung von Betriebssystemschwachstellen durch Hacker
- evtl. Abhören von Passworten durch Fremde

Schutzmaßnahmen sind wichtig:
- Nutzung von Secure Shell (SSH)
- Ermöglicht sichere, authentifizierte und verschlüsselte Verbindung
- Restriktive Vergabe von Zugriffsrechten

6.2 Cloud Computing

In der Entwicklung der Rechnernetzwerktechnik gab es immer wieder Vorstellungen, die Funktionalität der Arbeitsstationen auf eine reine Terminalfunktion (Thin Client) zu begrenzen und alle Verarbeitungsfunktionen transparent in das Netzwerk auszulagern.

a. Vergleichen Sie die Unterschiede in der Last-/Funktionenverteilung zwischen Cloud Computing und herkömmlicher IT vs. SaaS vs. PaaS vs. IaaS!
b. Ordnen Sie die Cloud-Einsatzszenarios in der ersten Spalte der folgenden Tabelle (◘ Tab. 6.2) den richtigen Mustern von Cloud-Diensten (Spalten 2–4) zu. In einigen Fällen kann ein Begriff mehreren Mustern/Spalten zugeordnet werden:

Lösung 6.2a)
Die Unterschiede in der Last-/Funktionenverteilung zwischen Cloud Computing und herkömmlicher IT vs. SaaS vs. PaaS vs. IaaS lassen sich anhand der Abb. 20.16/Teil III Lehrbuch (basiert auf einer Darstellung der Fa. Microsoft) beschreiben:

- herkömmliche IT garantiert dem User nur Netzwerkdienste
- XaaS als allg. Dienstmuster ermöglicht viel mehr für die Up-To-Date-Applikationen und mobilen Apps
- Zahlreiche Verarbeitungsfunktionen werden transparent in die Cloud migriert.

Lösung 6.2b)
s. ◘ Tab. 6.3

◘ **Tab. 6.2** Cloud-Einsatzszenarien

Dienstmuster	IaaS	PaaS	SaaS
– Cloud Backup			
– Data Center			
– VM Migration			
– Market Place			
– Hochleistungscluster für paralleles Rechnen			
– SOA Plattform			
– Test-Umgebung			
– Frontend			

Tab. 6.3 Tabelle mit Ergebnissen

Dienstmuster	IaaS	PaaS	SaaS
– Cloud Backup	x		x
– Data Center	x		
– VM Migration		x	
– Market Place		x	
– Hochleistungscluster für paralleles Rechnen	x		
– SOA Plattform		x	
– Test-Umgebung		x	x
– Frontend			x

6.3 Multimediale Netzwerkanwendungen und Mobilfunk

Eine Videostreaming wird mit dem Standard UXGA verwirklicht. Dieser ermöglicht die Bildauflösung von V = 1600 × 1200 Pixel. Dabei wird die Farbkodierung FT = 24 Bit genutzt sowie die Bildfrequenz fps = 25 Bild/s. Diese Übertragung wird

a. zuerst ohne Kompression per Festnetzmietleitung vorgenommen.
   Wie groß muss die verfügbare Datenrate sein, wenn keine Kompression möglich ist?
b. Welche Netzwerktechnologien sind für diese Videostreaming ohne Kompression am besten geeignet?
c. Die beschriebene Videoübertragung wird per Mobilfunk mit Kompressionsverfahren vorgenommen. Bei welchen Kompressionsraten KR ist diese Übertragung möglich, wenn die folgenden maximalen Datenraten bei Mobilfunk mittlerweile verfügbar sind. Bereichen Sie diese Werte und ergänzen Sie die angegebene Tabelle (ggf. aufrunden!):

Mobilfunknetz	Max. DR	Die zu berechnende Kompressionsrate KR
HSDPA	14,4 MBit/s	?
LTE	150 MBit/s	?

Lösung zu 6.3a)
Speicherbedarf SB = V * FT (in Bit)
SB = (1600 * 1200 Pixel) * 24 Bit

$$\begin{aligned}\text{Datenrate DR} &= \text{SB} * \text{fps} = \text{V} * \text{FT} * \text{fps} \\ &= (1600 * 1200\ \text{Pixel}) * 24\ \text{Bit} * 25\ \text{Bild/s} \\ &= 1152\ \text{MBit/s}\end{aligned}$$

→ erforderliche Datenrate ohne Kompression = 1,152 GBit/s

Lösung zu 6.3b)
Die folgenden Netzwerktechnologien sind für Videostreaming ohne Kompression am besten geeignet:
MPLS/SONET
10GbEthernet mit Reserve

Lösung zu 6.3c)
Verfügbare DR: 150 oder 14,4 MBit/s,
Kompression ist erforderlich, ggf. aufrunden!

$KR_{LTE} = DR/DR_{LTE} = 1{,}152\ \text{GBit/s}/150\ \text{MBit/s} = 7{,}68 = 8$
Mindestens eine 8-fache Kompression ist erforderlich.

$KR_{HSDPA} = DR/DR_{HSDPA} = 1{,}152\ \text{GBit/s}/14{,}4\ \text{MBit/s} = 80$
Mindestens eine 80-fache Kompression ist erforderlich.

6.4 SNMP-Management

- Angegeben seien ein Server mit installierter Managersoftware und ein Switch mit einem Agenten, zwischen denen SNMP-Nachrichten verkehren. Die beiden verweisen auf eine MIB. Ergänzen Sie das in ◘ Abb. 6.1 vorgegebene Weg-Zeit-Diagramm (Ablaufdiagramm).

Lösung 6.4a)
s. ◘ Abb. 6.2

6.5 Architekturwandlung in modernen Verteilten Systemen

Unsere Zeit wird durch die signifikante Architekturwandlung in Netzwerkservices und verteilten Systemen charakterisiert. Die Verarbeitungs-, Persistenz- und Anwendungsdaten werden von mehreren Servern oder Peers bereitgestellt.

a. Ergänzen Sie das unten aufgeführte Organigramm!
   Vergleichen Sie die Client-Server- und
   Peer-To-Peer-Architekturen (C-S/P2P) in der ◘ Abb. 6.3.
   Führen Sie jeweils 2–3 Beispiele an!

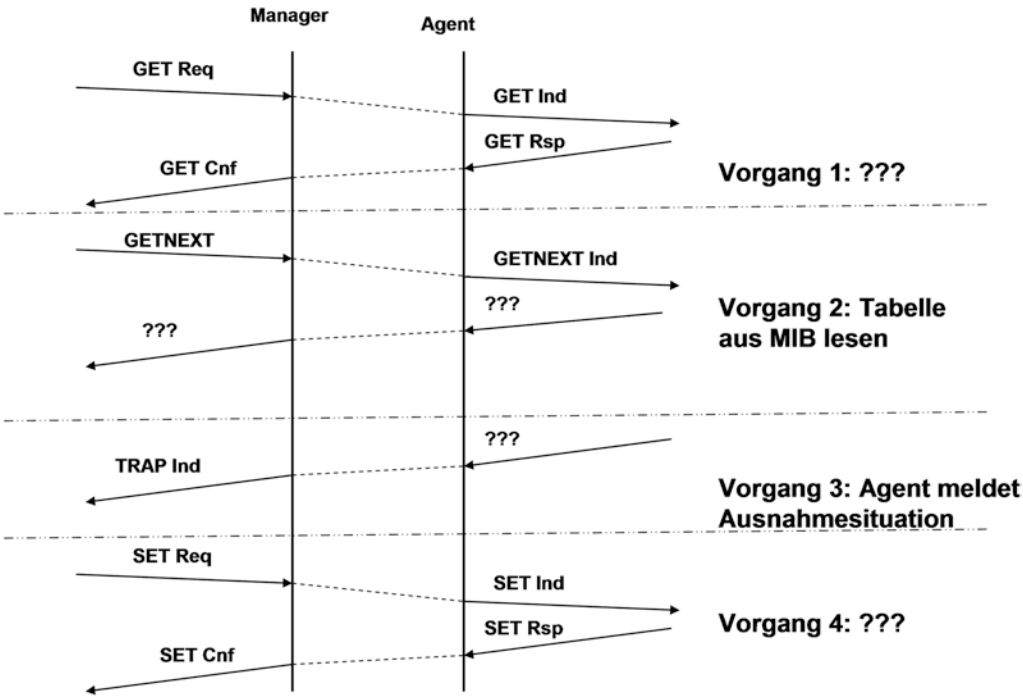


Abb. 6.1 SNMP-Ablaufdiagramm zum Vervollständigen

b. Erklären Sie die Funktionsweise von hybriden P2P/C-S-Systemen in Stichworten!
Nennen Sie jeweils drei Systembeispiele zu jedem der aufgeführten Architekturtypen mit der Erläuterung des Einsatzgebietes (s. Abb. 6.4)!

Lösung 6.5a)
s. Tab. 6.4

Lösung 6.5b)
Eigenschaften hybrider P2P/C-S-Systeme
- Performance- und Sicherheitsoptimierung durch die vorhandene Serverinfrastruktur vorhanden
- Flexibilität der Lösung
- P2P an der Peripherie

Systembeispiele hybrider P2P/C-S-Systeme
- Skype – Netzwerkdienst für VoIP, Videokonferenzen, Chat und Instant File Messaging (Clients für Desktop/Mobile)
- BOINC (Berkeley Open Infrastructure for Network Computing) – ein Grid, das an der Universität Berkeley und bei Unterstützung deren Partnern zur Kooperation mit zahlreichen wissenschaftlichen Projekten entwickelt wurde.

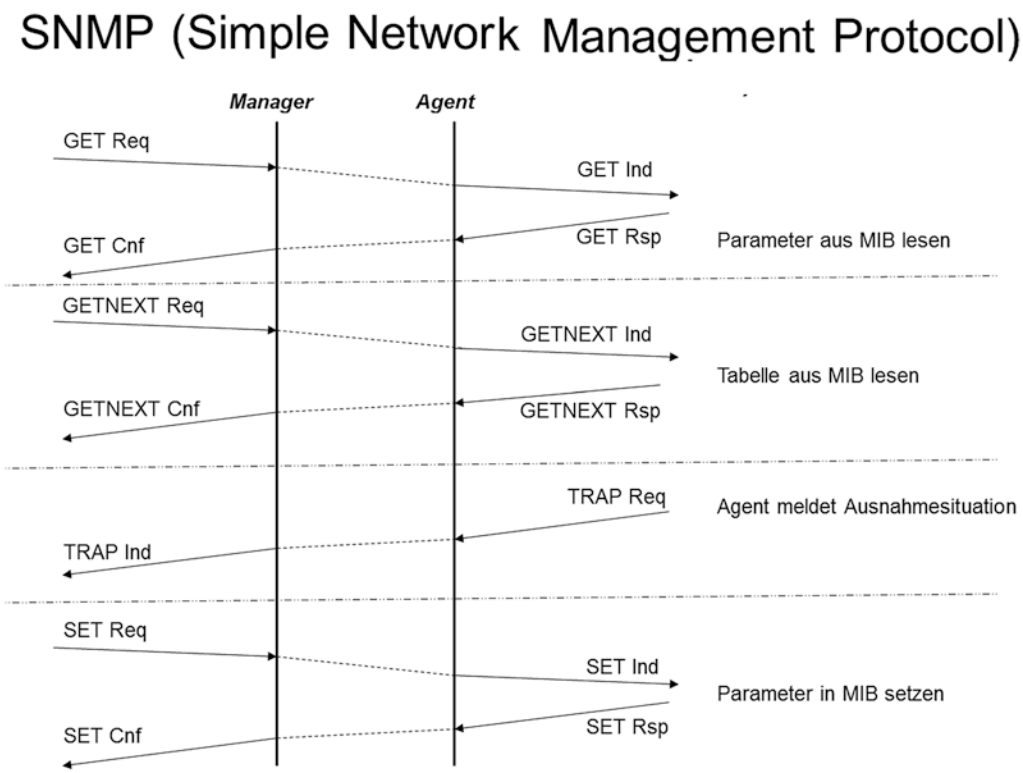


Abb. 6.2 Vollständiges SNMP-Ablaufdiagramm

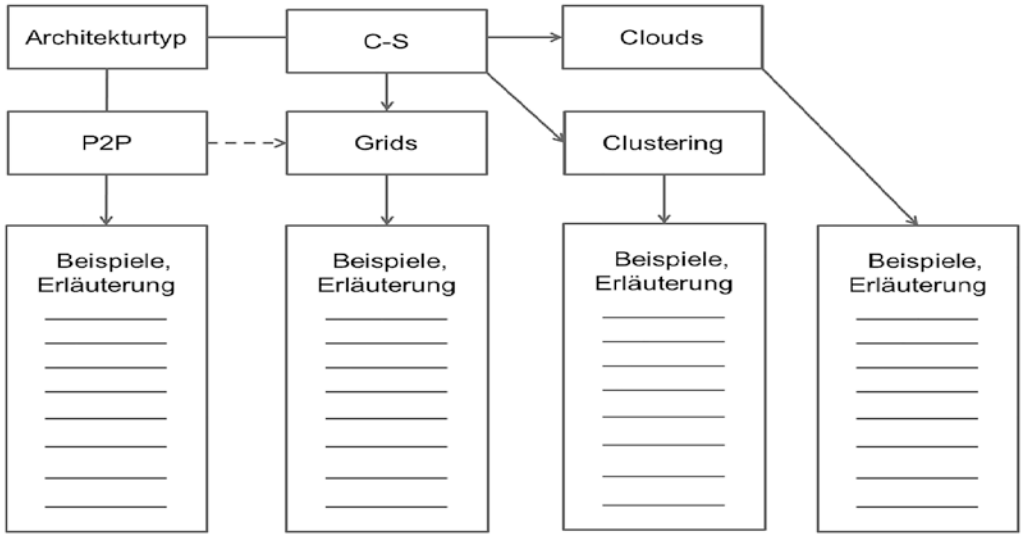


Abb. 6.3 Client-Server- und Peer-To-Peer-Architekturen

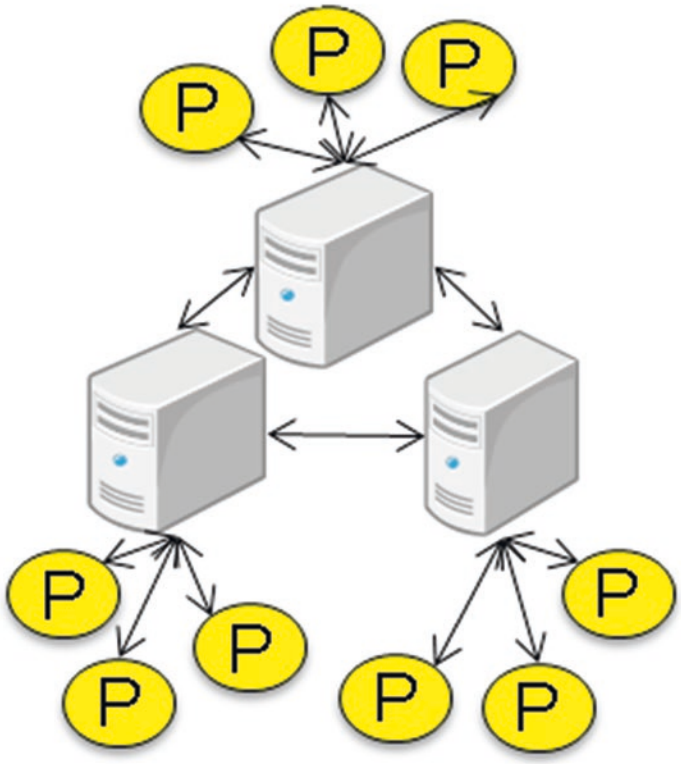


Abb. 6.4 Hybrides P2P

TOP10 der populärsten Grid-Projekte

- SETI@Home – Analyse einer Reihe von Radioteleskopdaten auf der Welt zum Zwecke der Suche nach außerirdischen Zivilisationen (Search for Extraterrestrial Intelligence).
- Einstein@Home – Testen von Hypothesen Albert Einsteins über Gravitationswellen und Suche nach Radio- und Gammastrahl-Pulsaren.
- World Community Grid – Hilfe bei der Suche nach Heilmitteln für schwere Krankheiten wie Krebs, HIV, AIDS, die Berechnung der 3D-Struktur von Proteinen und anderen Projekten (Veranstalter – IBM).
- Rosetta@Home – Berechnen der 3D-Faltungsstrukturen von Proteinen anhand der Aminosäuresequenzen für die Behandlung von Krebs, HIV, AIDS, Alzheimer-Demenz, Anthrax (sibirisches Geschwür) etc.

Tab. 6.4 Architekturen in modernen Verteilten Systemen

P2P	Grids	Clustering	Clouds
Eigenschaften			
Gleichberechtigte Partner (Peers)	C-S und P2P basiert	C-S basiert	C-S basiert
Bessere Load Balancing	Heterogene Server und Peers	Homogenität von Servern	Heterogenität, Auslagerung der Funktionalitäten in die Cloud
Flexiblere Struktur für leistungsschwächere Clients	Geografisch verteilt	Zentral	XaaS als Dienstmuster
Beispiele 1 …3			
Skype	BOINC (Berkeley Open Infrastructure for Network Computing)	TITAN (Tennessee, USA) – 17PFLOPS, 18.000 CPUs/18.000 GPUs/8 MW	Dropbox (öffentlich)
WhatsApp	OGSA (Open Grid Services Architecture) – allg. Softwarearchitektur für Grids (Webservices und Komponenten zum Aufbau von Grids)	Tianhe-2 (Guangzhou, China) – 33PFLOPS/32.000 CPUs/18 MW	Amazon EC2 (öffentlich)
BitTorrent – kollaboratives File-sharing-System. Hinweis: Das BitTorrent-Protokoll selbst ist vollkommen legal (bspw. Freeware-Distribution). Probleme entstehen bei den Usern, wenn urheberrechtswidriger Inhalt übertragen wird (illegale MM-Austauschbörsen)			MS Azur (privat)

- MilkyWay@Home – Entwicklung eines präziseren 3D-Modells der Sternströme in unserer Galaxie (Milchstraße).
- Climate Prediction – Untersuchung und Vorhersage von Klima auf der Erde.
- PrimeGrid – Suche nach sehr großen Primzahlen.
- SIMAP@Home – Erstellen einer Datenbank der Proteine für die Bioinformatik.

- Cosmology@Home – Suche nach einem Modell, das angemessen unser Universum beschreibt; steht im Einklang mit aktuellen Daten in der Astronomie und Teilchenphysik.
- Collatz Conjecture – Studien in der Mathematik, speziell um die Hypothese von Lothar Collatz zu testen, auch als „Problem 3n+1“ bekannt.

6.6 Videokonferenzen

Folgendes Szenario ist gegeben (s. Abb. 18.7, Teil III): Sie möchten mit mehreren Partnern eine Videokonferenz aufbauen. Sie nutzen ein Mehrpunktkonferenzsystem mit einer sternförmigen Architektur und einer zentralen MCU (Multipoint Control Unit). Sie senden Ihr Video mit der Auflösung CIF mit einer Farbtiefe von 24 Bit/Pixel und einer Framerate von 15 fps.

a. Mit welchem Kompressionsfaktor müssen Sie ihr zu sendendes Videosignal komprimieren, wenn Sie einen Internetanschluss (Upstream: 192 kBit/s, Downstream: 2048 kBit/s) nutzen?
b. Mit wie vielen Partnern können Sie eine Videokonferenz aufbauen, wenn alle Partner Videos mit der gleichen Qualität mit dem Faktor 200:1 komprimiert senden und 10 % Overhead durch Protokoll-Header entsteht?
c. Im Regelfall sollte man aber nur maximal 60 % der zur Verfügung stehenden Bandbreite für die Videoübertragung nutzen. Wie kann die zu übertragene Datenmenge angepasst werden, damit Sie weiterhin mit allen Partnern kommunizieren können? Wie wirkt sich das auf die Qualität der Videos aus?

Lösung (s. dazu Abb. 18.7 im Teil III mit anderen Angaben zur DR und Framerate):

Zu 6.6a)
Gegeben:
CIF (352x288 Pixel), Farbtiefe 24 bit/Pixel, Framerate 15 fps
DSL2000: Upstream: 192 kbit/s, Downstream: 2048 kbit/s

Gesucht:
Kompressionsfaktor fk

Datenvolumen des unkomprimierten Videosignals:
DV = 352 * 288 * 24 * 15 = 36.495.360 bit/s ≈ 36,5 Mbit/s

Kanal zum Senden Bandbreite 192 kbit/s
fk = 36.500 kbit/s/192 kbit/s = 190

Empfohlene Kompression mit 200:1

Zu 6.6b)
Gegeben:
Mit dem Faktor 200:1 wurde komprimiert.
10 % Overhead durch Protokoll-Header
CIF → DV = 36,5 Mbit/s, Kompressionsfaktor fk
DSL2000: Upstream: 192 kbit/s, Downstream: 2048 kbit/s

Gesucht:
Anzahl der Partner (ggf. abrunden)!

Benötigte Bandbreite:
Bnetto = 36.500 kbit/s/200 = 182,5 kbit/s

+10 % Overhead:
Bbrutto = 110 % * 182,5 kbit/s = 200,75 kbit/s

Kanal zum Empfangen: 2048 kbit/s
Anzahl der zu empfangenen Videostreams = 2048/200, 75 = 10,2

Kommunikation mit 10 Partnern möglich

Zu 6.6c)
Im Regelfall sollte man aber nur maximal 60 % der zur Verfügung stehenden Bandbreite für die Videoübertragung nutzen. Wie kann die zu übertragene Datenmenge angepasst werden, damit Sie weiterhin mit allen Partnern kommunizieren können? Wie wirkt sich das auf die Qualität der Videos aus?

Die Antwort entnehmen Sie in ◘ Tab. 6.5:

◘ **Tab. 6.5** Qualität der Videoübertragung

Reduzierung der Datenmenge durch	Auswirkungen auf die Qualität der Videos
Höhere Komprimierung	Verringerung der Bildqualität (größere Artefakte, „pixelig“)
Kleinere Framerate	Es werden weniger Bilder pro Sekunde gesendet. Bewegungen der Teilnehmer wirken ruckartig
Verringerung der Bildgröße (z. B. QCIF)	Kleineres Bild wird übertragen (z. B. 176 x 144 Pixel) (es gibt Videokonferenzsysteme, die nur den gerade Sprechenden größer, alle anderen Teilnehmer kleiner darstellen. Nachteil: Großer Rechenaufwand zur Überwachung, zu schneller Wechsel bei Diskussion zwischen mehreren Personen, nur für einseitigen Vortrag geeignet)
Verringerung der Farbtiefe	Bild wirkt blass
Reduzierung der Samplerate des Audios	Schlechte Tonqualität (klingt „dumpf“, „blechern“)

6.7 Fortgeschrittene Sicherheit in Netzwerken: Firewalls und CIDN

Eine Firewall ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt und ist auch ein wichtiger Teilaspekt eines Netzwerks.

a. Vergleichen Sie die IDS/IPS-Module (Intrusion Detection und Intrusion Prevention Systems) mit „klassischen" Firewalls! Verdeutlichen Sie die Unterschiede!
b. Nennen Sie Beispiele, bei denen die Verwendung eines Paketfilter-Firewalls ausreicht, bzw. bei denen eine anwendungsbezogene Filterung erforderlich ist!
c. Wofür dient ein Circuit Relay?
d. Ergänzen Sie die folgende Tabelle (◘ Tab. 6.6) der Filtermöglichkeiten von Firewallsystemen. Ordnen Sie die Filterungsmöglichkeiten in der ersten Spalte der folgenden Tabelle den richtigen FW-Konzepten (Spalten 2–5) zu. In einigen Fällen kann ein Begriff mehreren Mustern/Spalten zugeordnet werden:
e. Warum gibt es eine mehrstufige Firewall-Strategie? Diskutieren Sie anhand des unten aufgeführten Diagramms (◘ Abb. 6.5)!
f. Was ist CIDN?
   Welche Arten von Angriffen verhindern diese?

Lösung zu 6.7a)

- Ein Firewall-System wird als Schranke zwischen dem zu schützenden Netz (Trusted NW bzw. Internes Netzwerk, LAN/Intranet) und dem unsicheren Netz (WAN/Internet) geschaltet, sodass der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System möglich ist.
- Die Funktion einer Firewall besteht aber nicht darin, Angriffe zu erkennen. Die klassische FW soll ausschließlich Filterungsregeln für die Netzwerkkommunikation umsetzen. Für das Aufspüren von Angriffen sind sogenannte IDS/IPS-Module (Intrusion Detection und Intrusion Prevention Systems) zuständig, die durchaus auf einer Firewall aufsetzen können. Diese bilden zusammen mit dem Firewall-Modul fortgeschrittene Firewalls.

Tab. 6.6 Filtermöglichkeiten von Firewallsystemen. Tabelle zum Vervollständigen

Filterungsmöglichkeiten	PF (Paketfilter)	CR (Circuit Relay)	AG (Application Gateway)	Fortgeschrittenes FW-System
Zeitfensterkontrolle				
IP-Adressen und DMZ (Demilitarized Zone)				
Intrusion Detection und Intrusion Prevention Systems: IDS/IPS				
Zugelassene/verbotene Protokolle				
Malware-Blockierung, SPAM-Filter und Antiphishing				
anwendungsbezogene Authentisierung und Verschlüsselung				
Proxy für bestimmte Dienste, Proxyserver				
ausführbare Skripte, Applets, Web Services				
Web Application Firewall				
TCP-Ports und Blockierung von DDoS				
Bitte „X" falls zutreffend!				

Lösung zu 6.7b) + c) + d)
s. Tab. 6.7

Lösung zu 6.7e)
Unter der mehrstufigen Firewall-Strategie versteht man u.a. (s. Abb. 6.5):

- Externer PF:
  Trennung des unsicheren Internet mit diversen Risiken (Angriffe, Viren, Malware)
- Interner PF:
  Trennung/Absicherung des internen Bereiches,
  bzw. der internen Server: Backup-Server, DNS-Server, File-Server, int. WWW-Server
  Nur indirekte Kommunikation mit Autorisierung (Authentifikation und Rechtevergabe)
- Dazwischen DMZ (Demilitarized Zone):
  demilitarisierte Zone mit öffentlich verfügbaren Services, die von außen leicht erreichbar sind (s. direkte Kommunikation), aber nicht manipuliert werden dürfen!

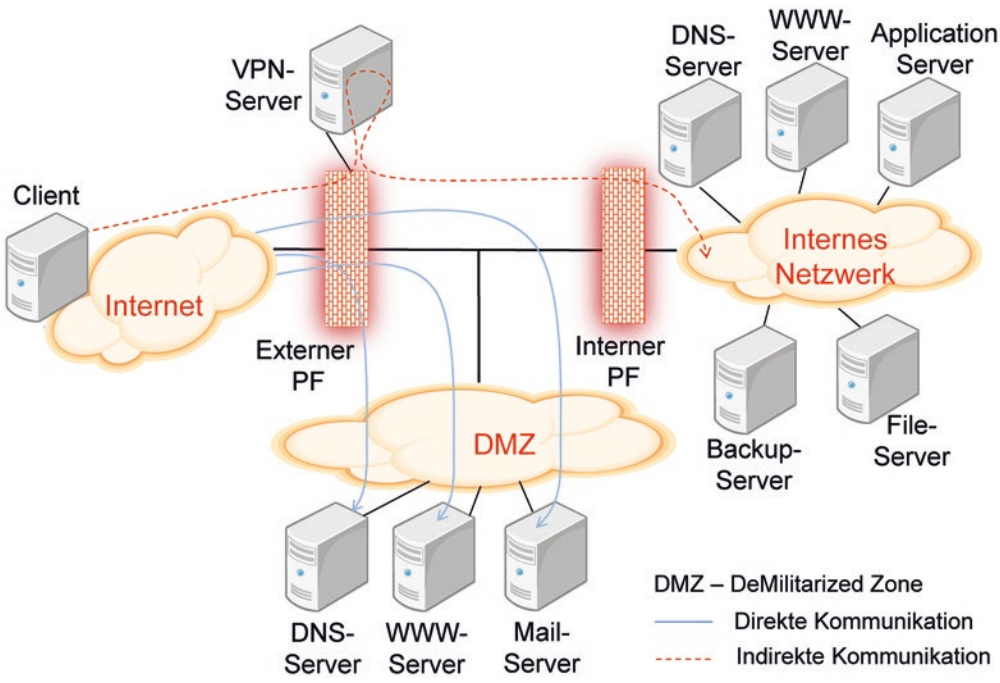


Abb. 6.5 DMZ und mehrstufige Firewall-Strategie

Tab. 6.7 Filtermöglichkeiten von Firewallsystemen. Tabelle mit Ergebnissen

Filterungsmöglichkeiten	PF	CR	AG	Fortgeschrittenes FW-System
Zeitfensterkontrolle	x	x	x	x
IP-Adressen und DMZ	x			x
Intrusion Detection und Intrusion Prevention Systems: IDS/IPS				x
Zugelassene/verbotene Protokolle	x	x	x	x
Malware-Blockierung, SPAM-Filter und Antiphishing			x	x
anwendungsbezogene Authentisierung und Verschlüsselung			x	x
Proxy für bestimmte Dienste, Proxyserver			x	x
ausführbare Skripte, Applets, Web Services			x	x
Web Application Firewall				x
TCP-Ports und Blockierung von DDoS		x		x

Lösung zu 6.7f)
Was ist CIDN?
Hinweis: s. Teil III Lehrbuch, Abschn. 18.3.3:

- Angriffe (Threats, Attacks) können 24/7 zur Störung des Betriebs moderner Daten- und Rechenzentren führen.
- Traditionelle IDS funktionieren in Isolation und sind deswegen nicht richtig wirksam, um unbekannte Bedrohungen, die immer weiter anspruchsvoller werden, zu erkennen!
- CIDN ist ein Kooperationsnetzwerk von einzelnen IDS, die paarweise ihr Wissen über Angriffe austauschen und damit die Verbesserung der Gesamtgenauigkeit und Effizienz von einzelnen IDS garantieren.

Die CIDN (Collaborative Intrusion Detection Networks) können die folgenden Arten von Angriffen verhindern:

- Eavesdropping (Lauschen-Angriffe, Abhören)
- Man-in-the-Middle (Verkleiden-Angriffe, Manipulation)
- Replay (Weiterleiten-Angriffe, Wiederholung und Vermehrung von Angriffen, u. a. Vermehren der „Malware" – Malicious Software – in Form von Viren, Trojanern, Würmen, Hoaxes, Greyware)
- Cloning (wie DDoS, Distributed Denial of Service Attack)
- Sybil-Angriffe (eine große Menge von Pseudonymen, gefälschten Identitäten, Fakes werden erzeugt)
- Newcomer-Angriffe (die Peers mit „schlechter Reputation" löschen ihre schlechte Historien, die „X-Files" mit anderen Peers im Netzwerk)
  Betrayal-Angriffe (der Vertrauensmechanismus ist robust und entspricht der sozialen Norm: „Es dauert eine lange Zeit und konsequent gutes Verhalten um hohes Vertrauen aufzubauen, während nur ein paar schlechte Handlungen es komplett ruinieren können"!
  Wenn ein vertrauenswürdiger Peer unehrlich fungiert, wird sein Vertrauenswert katastrophal fallen. Daher ist es sich schwierig für diesen Peer, andere zu täuschen oder sein früheres Vertrauen innerhalb kurzer Zeit zurück zu gewinnen!)
- Collusion-Angriffe treten auf, wenn eine Gruppe von kompromittierten oder bösartigen Peers agiert, um das CIDN zu kompromittieren.

6.8 Kryptografische Absicherung in den Rechnernetzapplikationen

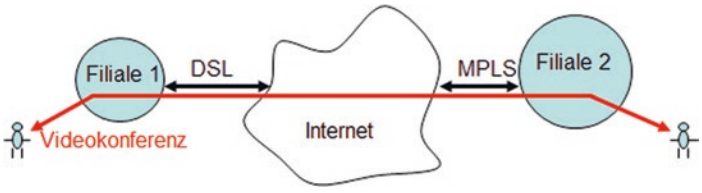
a. Kann es sinnvoll sein, in mehreren Netzarchitektur-Schichten Verschlüsselungsalgorithmen einzusetzen? Nennen Sie Beispiele!

b. Kann der Empfänger einer digital signierten Nachricht den Nachrichteninhalt verändern und eine passende Signatur erzeugen?
c. Wie kann man die folgende Aussage kommentieren: „TLS/SSL bietet stärkere Feingranularität bei der Absicherung für die Rechnernetzapplikationen als VPN/IPsec".
Aus welchem Grund kann man so behaupten?

Lösung 6.8a)
s. ◘ Abb. 6.6
Zwei Filialen einer großen Firma, über Internet verbunden
Die Filialen verschlüsseln ihren gesamten Internet-Nachrichtenverkehr:
- Layer 3 – IPsec (Schutz von Subnetzen und Netzwerken)
- Layer 4 – TLS/SSL (Schutz von Applikationen und Apps per angegebener Socket-Verbindungen)
- Layer 5–7 – PGP/Open PGP (content- und anwendungsspezifisch), um Abhören durch Konkurrenz zu verhindern.
- Mitarbeiter verschlüsseln Videokonferenz (Geheimhaltung auch firmenintern).
- Die Kompression über DSL/MPLS -Strecke führt zur Durchsatzverbesserung, Kostenreduktion
- Video-Konferenz mit anwendungsspezifischer Kompression

Lösung 6.8b)
Das Verfahren der digitalen Signatur kann viele Vorteile für E-Commerce bieten.
Bspw. der Empfänger in einem E-Commerce-Szenario kann:
- den Nachrichteninhalt ändern,
- den Inhalt verschlüsseln (mit dem öff. Schlüssel eines Anderen),
- die Check-Summe über den veränderten Nachrichteninhalt bilden.

Der Empfänger kann aber nicht:
- die passende Signatur erzeugen (privater Schlüssel des Senders erforderlich)



◘ **Abb. 6.6** Netzwerkszenario mit zwei Filialen mit DSL- und MPLS-Links

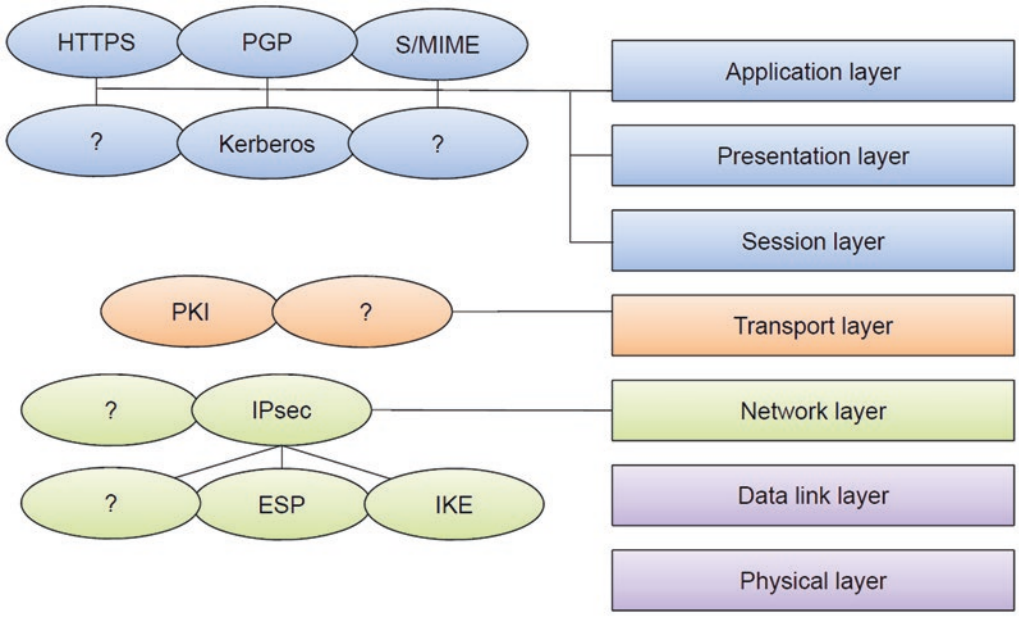
Lösung 6.8c)
TLS/SSL bietet eine stärkere Feingranularität bei der Absicherung für die Rechnernetzapplikationen als VPN/IPsec, da die angegebenen Socket-Verbindungen (Schicht 4) über die verfügbaren Ports für die Applikationen und Apps (per IP-Adresse, Port-Nummer gekennzeichnet) jeweils individuell verschlüsselt werden (Schichten 5–7).

Bei dem Protokoll IPsec werden die IP-Pakete (Schicht 3) für die Subnetze und Gesamtnetzwerke im Gegensatz dazu authentisiert und verschlüsselt.

6.9 Kryptoprotokolle

Kryptoprotokolle sind Netzwerkprotokolle (i. d. R. Layer 3 bis 7), die die verschlüsselte und authentifizierte Datenübertragung über ein Computernetzwerk für die Verteilten Anwendungen garantieren.

a. Ergänzen Sie das Bild!
   Definieren Sie die fehlenden Kryptoprotokolle (◘ Abb. 6.7)!
b. Ordnen Sie die folgenden Kryptoprotokolle in der ersten Spalte der folgenden Tabelle (alphabetisch sortiert) den richtigen Kommunikationsschichten (Spalten 2–5) zu.



◘ **Abb. 6.7** Ausgewählte Kryptoprotokolle mit OSI-Schichtenzuordnung zum Vervollständigen

Tab. 6.8 Einordnung von Kryptoprotokollen. Tabelle zum Vervollständigen

Begriff	Vermittlungsschicht L3	Transportschicht L4	Anwendung L5–L7
AH			
ESP			
HTTPS			
IKE			
IPsec			
IRC			
IRCS			
PGP			
POP3			
PKI			
RSVP			
S/MIME			
SET			
Socket			
VPN			
VoIP			
TLS/SSL			

Vermerk: In einigen Fällen kann ein Begriff mehreren Schichten zugeordnet werden, außerdem sind manche Begriffe gar keine Kryptoprotokolle! Als Schichten stehen die OSI-Schichten und die Schichten des TCP/IP-Referenzmodells zur Verfügung (Tab. 6.8):

Lösung 6.9a)
s. Abb. 6.8

Lösung 6.9b)
s. Tab. 6.9

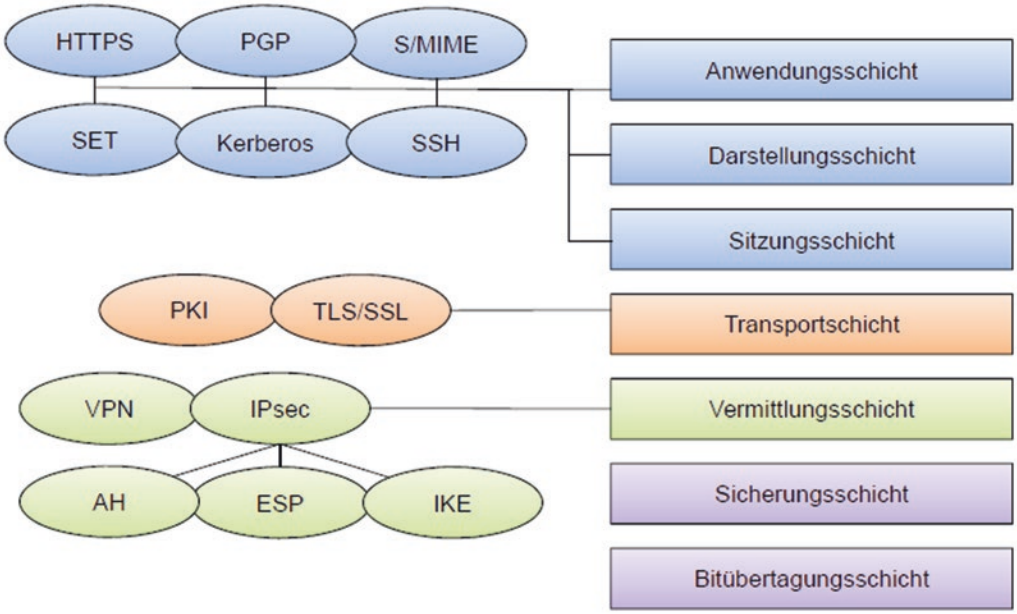


Abb. 6.8 Ausgewählte Kryptoprotokolle mit OSI-Schichtenzuordnung

Tab. 6.9 Einordnung von Kryptoprotokollen. Tabelle mit Ergebnissen

Begriff	Vermittlungsschicht L3	Transportschicht L4	Anwendung L5–L7
AH	x		
ESP	x		
HTTPS			x
IKE	x		
IPsec	x		
IRC	–	–	–
IRCS			x
PGP			x
POP3	–	–	–
PKI		x	
RSVP	–	–	–
S/MIME			x
SET			x
Socket	–	–	–
VPN	x		
VoIP	–	–	–
TLS/SSL		x	

6.10 Backup und Cloud Backup

In einem Modellbetrieb bzw. KMU (Klein- und Mittelstandsunternehmen) erfolgt die Datenvollsicherung bzw. Cloud Vollbackup über die bestehenden VDSL und MPLS-Netzwerkverbindungen immer freitags um ca. 21 h. Außerdem finden weitere regelmäßige Backups statt.

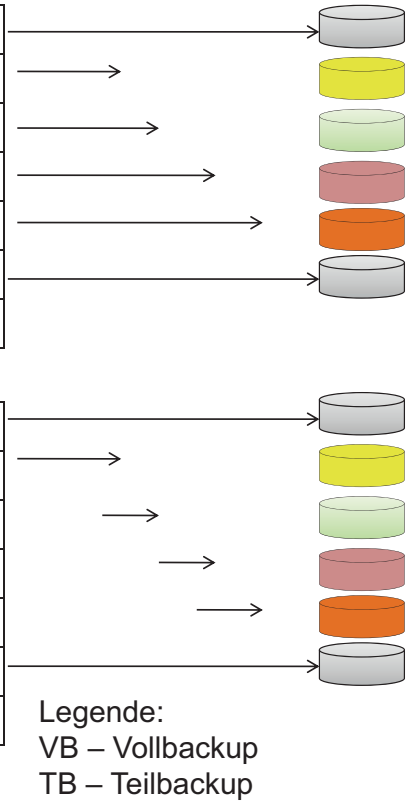
Dafür werden zwei folgenden Verfahren eingesetzt:

- IB, steht für Inkrementelles Backup;
- DB, steht Differentielles Backup.

a. Ordnen Sie die Begriffe IB und DB den unten aufgeführten Bildern zu (◘ Abb. 6.9)!
b. Diskutieren Sie jeweils zwei Pro- und zwei Contra-Argumente für die beiden Verfahren. Vergleichen Sie die beiden Verfahren anhand der angegebenen Tabelle. Die unten angegebene Tabelle ist auszufüllen!

Vollbackup (VB)	Freitag
Teilbackup (TB)	Montag
TB	Dienstag
TB	Mittwoch
TB	Donnerstag
VB	Freitag
a1) Differentiell	

Vollbackup (VB)	Freitag
Teilbackup (TB)	Montag
TB	Dienstag
TB	Mittwoch
TB	Donnerstag
VB	Freitag
a2) Inkrementell	



◘ **Abb. 6.9** Backup-Strategien

Backup/ Datensicherungsverfahren	IB	DB
Vorteile	1. 2.	1. 2.
Nachteile	1. 2.	1. 2.

c. Nennen Sie die wesentlichen Nachteile der Cloud Backup Lösung (mind. 2)?

Lösung

Zu 6.10a)

Fall a1) - beschreibt Differentielles Backup.

Fall a2) - beschreibt Inkrementelles Backup.

Zu 6.10b)

Die auszufüllende Tabelle mit jeweils zwei Pro und zwei Contra für die beiden Verfahren:

Backup/ Datensicherungsverfahren	IB	DB
Vorteile	1. Schnelles tägliches Backup 2. Weniger Medien	1. Ausfallsicherheit (+) 2. schnelleres Restore möglich
Nachteile	1. Ausfallsicherheit (−) 2. Mehr Zeit beim Restore erforderlich	1. Mehr Zeit beim täglichen Backup erforderlich 2. Mehr Speichermedien erforderlich

Zu 6.10c)

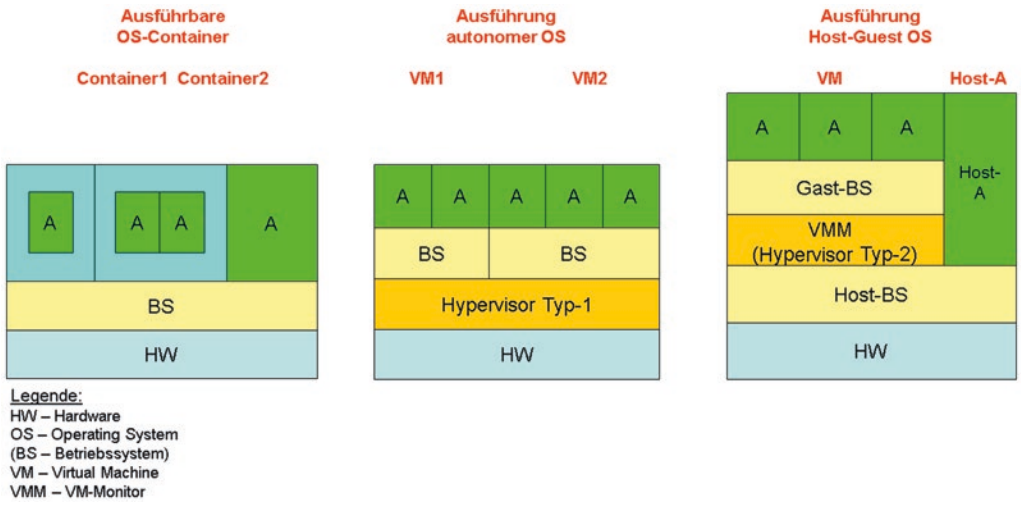
Die Cloud Backup Lösungen werden heutzutage bei den KMU (Klein- und Mittelstandsunternehmen) weitgehend favorisiert.

Die wesentlichen Nachteile der Cloud Backup Lösungen sind wie folgt:

- Ständige schnelle Netzwerkverbindung erforderlich
- Datensicherheit seitens Provider muss garantiert werden
- Vorhandensein/Bonität des Providers (Vertrauen an den Provider im großen Maße).

6.11 Virtualisierungsverfahren in Rechnernetzen

a. Was bedeutet der Begriff „Virtualisierung“ in aktuellen Rechnernetzen und Verteilten Systemen (Rechnerarchitekturen, Betriebssystemen und Applikationen)?
b. Existierende Virtualisierungsverfahren ermöglichen den Heterogenitätsabbau in aktuellen Rechnernetzen und im Mobilfunkumfeld (s. ◘ Abb. 6.10).
Dafür kommen die folgenden Konzepte zum Einsatz: OS-Container, Hypervisor (Typ-1) und VM-Monitor (Hypervisor Typ-2).
Welche Vorteile haben OS-Container bzw. im Mobilfunkumfeld gegenüber Hypervisor Typ-1 oder Typ-2?
Nennen Sie wichtige Systembeispiele zum Konzept OS-Container!
c. Warum bietet ein Hypervisor Typ-1 eine günstigere Alternative zu einem VM-Monitor (Typ-2)? Nennen Sie mind. 2 Argumente diesbezüglich!
d. Nennen Sie mind. 3 Systembeispiele der Betriebssystemvirtualisierung (bedeutende Produkte am Markt)!
e. Ein leistungsstarker physikalischer Server in einem Mittelstandsunternehmen trägt 40 VM je mit dem Hauptspeicher 4 GB und der Festplatte 6 TB (s. ◘ Abb. 6.11)
Welche Mindestkapazitätsanforderungen und wie viel Reserve muss der Server haben? Begründen Sie den Vorschlag!



◘ **Abb. 6.10** Vergleich von Virtualisierungskonzepten: OS-Container, Hypervisor (Typ-1), VM-Monitor (Hypervisor Typ-2)

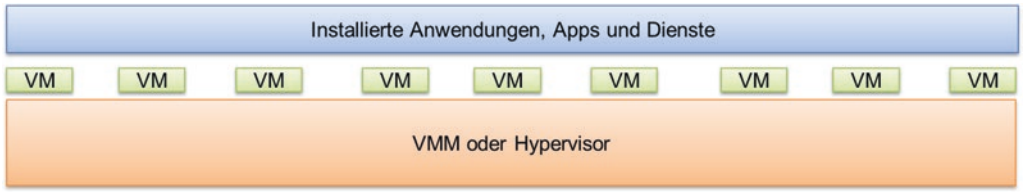


Abb. 6.11 Virtualisierungsszenario: Hypervisor oder Monitor, virtuelle Maschinen, installierte Anwendungen, Apps und Dienste

f. Wie viel Hauptspeicher insgesamt und welche gesamte Festplattenkapazität kann der phys. Server in dem Falle haben, um einen einwandfreien Betrieb von diesen 50 VM mit 10 %-Reserve zu gewährleisten? Begründen Sie den Vorschlag!

Lösung (s. Teil III Lehrbuch, Abschn. 20.6)
Zu 6.11a)
Virtualisierung bezeichnet Methoden, die es erlauben, Ressourcen eines verteilten Systems zusammenzufassen oder aufzuteilen. Primäres Ziel ist, dem User eine Abstraktionsschicht zur Verfügung zu stellen, die ihn von den eigentlichen Netzwerken/Hardware/Software isoliert.

Eine logische Schicht wird zwischen Anwender und Ressource eingeführt, um die (physischen) Gegebenheiten zu verstecken.

Existierende Virtualisierungsverfahren ermöglichen den Heterogenitätsabbau und erhöhen die Verfügbarkeit der Applikationen.

Virtualisierungsverfahren ermöglichen den Ausbau von Cloud-basierten Services (XaaS).

Zu 6.11b)
Die OS-Container im Unterschied zu einer VM:
- OS-Container stellen in sich sehr einfache Virtualisierungslösungen dar
- OS-Container ermöglichen abgeschottete und sichere Ausführung von „untypischen" Applikationen jedoch ohne Rechtevergabe an diese bspw. für Gerätetreiberinstallation und ohne Umkonfigurierungsmöglichkeiten

Systembeispiele für OS-Container sind wie folgt
im Mobilfunkumfeld:
- Dalvik JVM (Google), Sandboxes (Google, iOS)

im PC-/Desktop- Umfeld:
- Open Solaris Zoning, BSD jails, OpenVZ, Virtuozzo, Linux-VServer

Zu 6.11c) s. Skizze
Hypervisor (Typ-1) ist eine günstigere Alternative zu einem VM-Monitor (Typ-2), da
- Sparsamkeit, Performance der Virtualisierungslösung
- direkte Ausführung ohne zusätzliches Host-BS und ohne Verzögerung (keine zusätzliche Layer in der Architektur notwendig)

Zu 6.11d)
Die folgenden Produkte für Betriebssystemvirtualisierung sind heutzutage marktführend:
- Citrix-Produkte (Hypervisor-basierte Virtualisierungstechnik)
- VMWare-Produkte (VM Monitor- bzw. Hypervisor-basierte Virtualisierungstechnik)
- Microsoft Hyper-V (Hypervisor-basierte Virtualisierungstechnik)
- KVM, Kernel-based (Linux) Virtual Machine

Zu 6.11e)
Ein leistungsstarker physikalischer Server in einem Mittelstandsunternehmen mit 40 VM
RAM = 40 VM * 4 GB = 160 GB
HDD = 40 VM * 6 TB = 240 TB
+ Reserve von mind. 12.5 % für Host-BS und weitere Funktionalitäten
RAM = 20 GB
HDD = 30 TB
Gesamt:
RAM = 180 GB
HDD = 270 TB

Zu 6.11f)
Ein leistungsstarker physikalischer Server in einem Mittelstandsunternehmen mit 50 VM
RAM = 50 VM * 4 GB = 200 GB
HDD = 50 VM * 6 TB = 300 TB
+ Reserve von mind. 10 % für Host-BS und weitere Funktionalitäten
RAM = 20 GB
HDD = 30 TB
Gesamt:
RAM = 220 GB
HDD = 330 TB

6.12 Entwicklungstrends in Rechnernetzen

a. Verdeutlichen Sie die Unterschiede zwischen IoT und IoS!
b. Was ist Fog Computing!
   Beschreiben Sie kurz die wichtigsten Netzwerktechnologien, die Fog Computing unterstützen!
c. Verdeutlichen Sie die Unterschiede zwischen Clouds und Fog Computing?
   Wie wird die Koexistenz gewährleistet?

Lösung

Zu 6.12a)

Der Begriff „Internet der Dinge" (Internet of Things, Kurzform: IoT) beschreibt, dass die per IP vernetzten Gadgets (Laptops, Tablets, Smartphones) zunehmend verschwinden und durch „intelligente Gegenstände" ersetzt werden. Statt selbst Gegenstand der menschlichen Aufmerksamkeit zu sein, soll das IoT den Menschen bei seinen Tätigkeiten unmerklich unterstützen. Die immer kleineren eingebetteten Kontroller sollen Menschen im Alltag unterstützen, ohne abzulenken oder überhaupt aufzufallen (s. Abb. 20.31 im Teil III Lehrbuch).

So werden z. B. sog. Wearables, die direkt in Kleidungsstücke eingearbeitet sind, als IoT bezeichnet. Weiterhin werden intelligente Gebäudetechnik (Intelligent Home), eingebettete Gerätschaften (Embedded) mit unterschiedlichen Sensoren (Bluetooth, RFID, 6LoWPAN, …) ausgerüstet (s. Abb. 4.31). IoT ist außerdem die richtige Lösung bei den Anwendungen, die Echtzeit voraussetzen, wie Industrie-Automatisierung, Transport, Video Streaming etc.

Laut der Vorhersage von Gartner Inc. wird Internet of Things (IoT) etwa 25 Mrd. Geräte im Jahre 2025 vernetzten. Aber schon heutzutage mit dem IoT in der Kindheitsphase konkurrieren zahlreiche vernetzte Geräte weltweit um die Datenpipelines in die Clouds aufgrund der großen Datenmenge („Big Data" Problematik).

IoS (Internet of Services) ist ein herkömmlicher Begriff und bedeutet den Einsatz von Webservices und von den darauf basierten SOA in der Internetkommunikation bzw. im Cloud Computing. Mit anderen Worten steht IoS für den service-orientierter Ansatz und service-orientierte Architekturen im Internet.

IoT kann IoS verwenden.

Zu 6.12b)

Fog Computing („Fog" im Englischen „Nebel", „Trübheit") erweitert das Paradigma des Cloud Computing und verschiebt die Verarbeitung auf einen intelligenten Netzwerkknoten (Network Edge) und erlaubt dadurch eine Reihe von neuen Anwendungen, Apps und Services.

Die folgenden Merkmale von Fog Computing sind wesentlich [4]:
- Low-Latency, Location-Awareness (schnelle Reaktivierung von Knoten)
- weite geographische Verteilung
- sehr große Anzahl von Knoten und Mobilität, IPv6 empfohlen
- führende Rolle von „Wireless Access“
- Streaming- und Realtime-Anwendungen
- Knotenheterogenität.

Die wichtigsten Funktionalitäten von Fog Computing sind (alles anwenderseitig):
- Datenerfassung vor Ort
- Zwischenspeicherungen
- Kleine Anwendungen (Apps) ausführen
- Kleine Vorberechnungen vor Ort zu verrichten.

Fog Computing bietet eine passende Plattform für Weiterentwicklung von IoT-Diensten auf der Basis von folgenden bekannten und neuen Netzwerktechnologien:
- Wireless Sensors and Actuators Networks (WSNs): ZigBee, Bluetooth, EnOcean
- RFIDs
- WLAN (IEEE 802.11 ac, ad)
- 6LoWPAN
- 5G-Mobilfunk.

Zu 6.12c)
Mit dem Fog Computing werden die Services und Berechnungen an den „Rand des Netzwerks“ verschoben (zum User hin). Dabei muss ein Kompromiss gefunden werden zwischen partiellem oder komplettem Verschieben. Fog Computing heißt auch „Edge Computing“.

Auch IBM versucht mit einer ähnlichen Initiative, das traditionelle cloudbasierte Internet umzugestalten bzw. an „den Rand“ zu verschieben. Wenn über „Edge Computing“ gesprochen wird, ist damit wortwörtlich der Rand eines Netzwerkes gemeint, die Peripherie, wo das Internet endet und die reale Welt beginnt. Datenzentren sind die „Zentren“ des Netzwerkes; kleine Kontroller und typische Gadgets wie Laptops, Smartphones, Tablets, Multimediaplayer, Überwachungskameras stehen „am Rand“.

Tab. 6.10 Vergleich von Fog und Cloud Techniken [4]

Herausforderungen einer Cloud oder eines NW-Speichers	Wie dabei Fog helfen kann
Latenz als größtes Problem	+ weniger Hops
Mobilität bei der Datenerfassung beschränkt	+ Datenlokalität und lokale Caches
Bandbreitenbegrenzung	+ Vor-Ort-Bearbeitung
Zuverlässigkeit und Robustheit akzeptabel aber angesichts Big Data fraglich	+ Fast Failover
reiner Datenspeicher ohne Metainformationen für Suche	+ Location Awareness

Der Vergleich von Fog und Clouds ist Tab. 6.10 zu entnehmen:

Wie wird sich Fog Computing mittelfristig entwickeln? Der Nebel wird die Cloud nicht verdrängen. Die Frage ist nicht "Fog Computing vs. Cloud Computing", sondern es geht um die Koexistenz.

Fog Computing weist viele Vorteile auf [4]:

- ermöglicht Big Data- und Echtzeitanalyse
- Energieeffizienz,
- Performance aufgrund physischer Nähe,
- geringere Datenströme über Internet als bei Cloud-Computing,
- Sinkende Kosten bei der Datenverarbeitung (Big Data)
- Rechenleistung im Verhältnis zu Bandbreite immer günstiger (dank Raspberry Pi, Arduino Uno, Banana Pi, uvm.)
- Ersetzbarkeit bei Ausfällen
- geringere Transportkosten und geringere Latenzen
- verbesserte QoS,

aber der Datenschutz ist dabei fraglich. Die Verschlüsselung und der Einsatz von CIDN ist nachdrücklich zu empfehlen.

Dadurch wird Fog Computing zur treibenden Kraft für IoT. Mittelfristige Entwicklung liegt im IPv6-Einsatz zur effizienteren Adressierung und in der Erhöhung der Datensicherheit. Die Security-Herausforderungen wachsen. Die Authentisierung von angekoppelten Geräten in den kombinierten Strukturen muss gewährleistet werden (User+Fog+Clouds). Die Verschlüsselung und digitale Signatur wird durch eine robuste Kombination von AES+RSA+PKI sowie den Einsatz von FW und CIDN erreicht (s. Teil III Lehrbuch, Abschn. 18.3).

6.13 Zusammenfassung Kapitel 6

Der praxisorientierte Abschnitt bietet Ihnen Musterlösungen zu den Aufgabenstellungen zu Komplex III – Verarbeitungsorientierte Schichten und Netzwerkanwendungen. Die folgenden Themen werden geübt:

- Klassische Internetapplikationen
- Cloud Computing
- Multimediale Netzwerkanwendungen und Mobilfunk
- SNMP-Management
- Architekturwandlung in modernen Verteilten Systemen
- Videokonferenzen
- Fortgeschrittene Sicherheit in Netzwerken: Firewalls und CIDN
- Kryptografische Absicherung in den Rechnernetzapplikationen
- Kryptoprotokolle
- Backup und Cloud Backup
- Virtualisierungsverfahren in Rechnernetzen
- Entwicklungstrends in Rechnernetzen

Serviceteil

A. Luntovskyy und D. Gütter, *Moderne Rechnernetze – Übungsbuch*,
https://doi.org/10.1007/978-3-658-25619-7

Literatur

1. Tanenbaum, Andrew S., und David J. Wetherall. 2012. *Computernetzwerke*, 5., aktualisierte Aufl., 1040. München: Pearson Studium. (ISBN: 978-3-8689-4137-1).
2. Peterson, L.L., und B.S. Davie. 2011. *Computer networks. A system approach*, 5. Aufl., 920. Burlington, Massachusetts: Morgan Kaufmann. ISBN 978-0-12-385059-1.
3. Skripte LS Rechnernetze. 2017. ► http://www.rn.inf.tu-dresden.de.
4. Luntovskyy, Andriy, und Josef Spillner. 2017. *Architectural transformations in network services and distributed systems: Service vision. Case Studies*, XXIV, 344, 238 color pict. Heidelberg: Springer. ISBN 978-3-658-14840-9.
5. Luntovskyy, Andriy, Dietbert Guetter, und Igor Melnyk. 2011. *Planung und Optimierung von Rechnernetzen: Methoden, Modelle, Tools für Entwurf, Diagnose und Management im Lebenszyklus von drahtgebundenen und drahtlosen Rechnernetzen,* 435. Wiesbaden: V+T/ Springer Fachmedien Wiesbaden GmbH. ISBN 978-3-8348-1458-6.
6. Tanenbaum, Andrew S., und Herbert Bos. 2016. *Moderne Betriebssysteme*, 4., aktualisierte Aufl., 1313. München: Pearson Studium. (ISBN 978-3-8632-6766-7).
7. Tanenbaum, Andrew S., und Todd Austin. 2014. *Rechnerarchitektur: Von der digitalen Logik zum Parallelrechner*, 6., aktualisierte Aufl., 802. München: Pearson Studium. (ISBN 978-3-8632-6687-5).
8. Schill, Alexander, und Thomas Springer. 2012. *Verteilte Systeme – Grundlagen und Basistechnologien*, 2. Aufl., 433. Heidelberg: Springer Verlag. ISBN 978-3-642-25795-7.
9. Schneider, U. Hrsg. 2012. *Taschenbuch der Informatik*, 7. Aufl., 736. München: Carl-Hanser Verlag. ISBN 978-3-446-42638-2.
10. Kersken, Sascha. 2007. *IT-Handbuch für Fachinformatiker. Der Ausbildungsbegleiter*, 3., aktualisierte und erweiterte Aufl., 1014. Bonn: Galileo Computing. ISBN 978-3-8362-1015-7.
11. Blokland, K., J. Mengerink, M. Pol, und D. Rubruck. 2016. *Cloud-Services testen. Von der Risikobetrachtung zu wirksamen Testmaßnahmen*, 1. Aufl. Heidelberg: dpunkt. ISBN 978-3864903496.
12. OMNeT++ Discrete Event Simulator: Objective Modular Network Testbed in C++ and Simulations-Framework. 2017. ► https://omnetpp.org/. Zugegriffen: 25. Mai 2020.
13. Diskreter Event Network Simulator für das Internet NS-3. 2017. ► https://www.nsnam.org/. Zugegriffen: 25. Mai 2020.
14. Luntovskyy, Andriy. 2017. Rechnernetze im 4. Semester, Manuskript der BA Dresden (Print). Wiesbaden: Springer Vieweg.
15. Luntovskyy, Andriy. 2017. Verteilte Systeme im 5. Semester, Manuskript der BA Dresden (Print).
16. Luntovskyy, Andriy. 2017. Mobile Kommunikation und Telematik im 5. Semester, Manuskript der BA Dresden (Print), Skripte der Professur Rechnernetze. ► http://www.rn.inf.tu-dresden.de/. Zugegriffen: 25. Mai 2020.
17. Luntovskyy, Andriy. 2017. Netzwerkpraxis und neue Technologien. Wandel in Architekturen von Netzwerken und Verteilten Systemen und Telematik im 6. Semester, Manuskript der BA Dresden (Print).
18. Gütter, Dietbert. 2017. Netzwerkpraxis für Lehramt, Manuskript der TU Dresden (Print).
19. Gütter, Dietbert. 2017. Betriebssysteme und Rechnernetze, Manuskript der TU Dresden (Print).
20. Wireshark Homepage. 2017. ► https://www.wireshark.org/. Zugegriffen: 25. Mai 2020.