

Vorlesungsmodul Rechnernetze 2

- VorlMod ReNetze2 -

Matthias Ansorg

10. Oktober 2003 bis 21. März 2004

Zusammenfassung

Studentische Mitschrift zur Vorlesung Rechnernetze 2 bei Prof. Dr. Wolfgang Schmitt (Wintersemester 2003/2004) im Studiengang Informatik an der Fachhochschule Gießen-Friedberg. Die Veranstaltung »Rechnernetze 2« ist nach Prüfungsordnung äquivalent zu »Lokale Netze«, hat jedoch einen etwas anderen Inhalt. Lokale Netze bilden jedoch einen Schwerpunkt von etwa 25%. Diese studentische Mitschrift ist vollständig identisch zum offiziellen Skript [2] der Veranstaltung gegliedert.

Die Veranstaltung besteht aus 3 SWS Vorlesung und 1 SWS Übung. Übungen finden etwa alle 14 Tage statt und beinhalten dem Stoff entsprechend wenige Rechenaufgaben und keine Praxis am Computer.

- **Bezugsquelle:** Die vorliegende studentische Mitschrift steht im Internet zum Download bereit. Quelle: Persönliche Homepage Matthias Ansorg :: InformatikDiplom <http://matthias.ansorgs.de/InformatikAusblgd/>.
- **Lizenz:** Diese studentische Mitschrift ist public domain, darf also ohne Einschränkungen oder Quellenangabe für jeden beliebigen Zweck benutzt werden, kommerziell und nichtkommerziell; jedoch enthält sie keinerlei Garantien für Richtigkeit oder Eignung oder sonst irgendetwas, weder explizit noch implizit. Das Risiko der Nutzung dieser studentischen Mitschrift liegt allein beim Nutzer selbst. Einschränkend sind außerdem die Urheberrechte der angegebenen Quellen zu beachten.
- **Korrekturen und Feedback:** Fehler zur Verbesserung in zukünftigen Versionen, sonstige Verbesserungsvorschläge und Wünsche bitte dem Autor per e-mail mitteilen: Matthias Ansorg <<mailto:matthias@ansorgs.de>>.
- **Format:** Die vorliegende studentische Mitschrift wurde mit dem Programm L^AT_EX (graphisches Frontend zu L^AT_EX) unter Linux geschrieben und mit pdfL^AT_EX als pdf-Datei erstellt. Grafiken wurden mit dem Programm xfig unter Linux erstellt und als pdf-Dateien exportiert.
- **Dozent:** Prof. Dr. Wolfgang Schmitt. Er hielt die Veranstaltung im WS 2003/2004 zum ersten Mal. Prof. Müller hält einmal pro Woche in den Semesterferien eine Sprechstunde, die er auf seiner persönlichen Homepage bekannt gibt.
- **Verwendete Quellen:** .
- **Klausur:** Es gibt keine alten Klausuren, weil Prof. Schmitt die Vorlesung zum ersten mal hält. Die alten Klausuren von Herrn Müller sind nur bedingt relevant, weil dort keine Protokollarchitektur behandelt wurde, dafür einige Dinge intensiver behandelt wurden.
Die Klausur hat zwei Teile, die je etwa 50% zählen (bisher zählte Teil A mehr).
 - In Teil A darf man Unterlagen benutzen: Skript, Übungsaufgaben, alles was man handschriftlich selbst angefertigt hat. Diese Aufgaben werden ähnlich den Übungsaufgaben sein, bei denen ein Skript zugelassen ist. Es gibt eine Lösung zu einer solchen Aufgabe im Netz.
 - In Teil B darf man nichts benutzen. Die Fragen orientieren sich aber genau an denen, die in den Kapiteln »Fragen zur Lernkontrolle« enthalten sind. Das ermöglicht eine sehr gezielte Vorbereitung. Dabei geht es um den Typ der Fragen, d.h. um ihre Detailtiefe, es werden aber nicht buchstabengetreu dieselben Fragen sein.

Wichtiger Stoff: Die Klausur wird mindestens eine Aufgabe enthalten, bei der das Protokoll oder sonst der Typ eines Ethernet-Frames zu identifizieren ist. Den Entscheidungsbaum zur Protokollidentifizierung sollte man also mit Unterlagen beherrschen.

Inhaltsverzeichnis

I Schichten, Dienste und Protokolle

4

1	Grundbegriffe und statische Struktur des OSI-Referenzmodells	4
2	Funktionsprinzipien - dynamische Struktur des OSI-Referenzmodells	4
3	Spezifizierung von Instanzen durch erweiterte endliche Automaten	4
3.1	Endlicher und erweiterter endlicher Automat	5
3.2	Zustandsübergangdiagramm	5
3.3	Zustandsübergangstabelle	5
3.4	Zeitdiagramm	5
3.5	Einführung in SDL	5
4	Literatur	5
II	Lokale Datenkommunikation	5
5	Einführung	6
5.1	LAN, MAN und CPN	6
5.2	Charakteristische Eigenschaften von LANs	6
5.3	Verfahren zur Mediumzugriffssteuerung	6
5.4	Standardisierung	6
5.5	Aufgaben und Fragen zur Lernkontrolle	6
6	Ethernet	6
6.1	Historie	6
6.2	Ethernet im OSI-Schichtenmodell	6
6.3	IEEE Ethernet Arbeitsgruppen und Teilbereiche des Ethernet Standards	6
6.4	Ethernet 10BASE5	6
6.4.1	Komponenten und Systemkenngößen	6
6.4.2	MAC-Protokoll CSMA/CD	6
6.4.3	Rahmenformate, Adressen und Fehlerbehandlung	6
6.4.4	Späte Kollisionen	6
6.4.5	Logical Link Control (LLC)	7
6.4.6	Verwendung der Rahmenformate in Standardprotokollen	7
6.4.7	Architektur eines Ethernet-Anschlusses	7
6.5	Nachfolgeentwicklungen	7
6.5.1	Ethernet 10BASE2	7
6.5.2	Ethernet 10BASE-T	7
6.5.3	Fast Ethernet 100BASE-T	7
6.5.4	Gigabit-Ethernet - 1000BASE-X	7
6.5.5	Auto-Negotiation-Funktion	8
6.6	Switched-Ethernet	8
6.6.1	Entwicklungsgeschichte und Begriffsbildung	8
6.6.2	Grundstruktur eines Ethernet-Switches	8
6.6.3	Eigenschaften von Switched-Ethernet	8
6.6.4	Realisierungsformen der Vermittlungseinheit	8
6.6.5	Schleifenfreie Wegelenkung	8
6.7	Aufgaben und Fragen zur Lernkontrolle	8
7	Token-Verfahren	9
7.1	Zugriffsverfahren Token-Passing	9
7.2	Token-Bus	9
7.3	Token-Ring	9
8	Architekturen für Netzwerktreiber	9
8.1	Problemstellung	9
8.2	NDIS	9
8.3	ODI	9

9	Literatur	9
10	Anhang 1: Kabelspezifikationen	10
III	IP-Routing	10
11	Netzübergänge und Internetworking	10
IV	TCP und UDP	10
12	TCP	11
12.1	Dienste	11
12.2	Paketformat	11
12.3	Ablaufsteuerung	11
13	UDP	11
13.1	Dienste	11
13.2	Paketformat	11
V	Dienste und Protokolle der Anwendungsschicht	11
14	WWW	11
15	E-Mail	11
16	FTP	11
VI	Netzsicherheit und Firewalls	11
VII	Übungsaufgaben	12
17	Übungsaufgaben Typ »Klausuraufgaben Teil A« (mit Unterlagen)	12
17.1	Modulo 8-Zähler als (erweiterter) endlicher Automat	12
17.2	Das Protokoll LAPB	12
17.3	Zustandstabelle eines Signalisierungsprotokolls	14
17.4	Verbindungsauf- und -abbau bei TCP	15
17.5	Transportprotokoll in SDL	16
17.6	Geldautomat in SDL	16
17.7	Truncated Binary Exponential Backoff	17
17.8	Jabber-Schutzfunktion	18
17.9	Unterschiedliche Spanning Trees am Beispiel	18
17.10	Entscheidungsbaum zur Bestimmung des Protokolls der Daten	18
18	Übungsaufgaben Typ »Klausuraufgaben Teil B« (ohne Unterlagen)	18
18.1	Begriffe LAN, MAN, CPN	18
18.2	Eigenschaften von LANs	19
18.3	Medienzugriffssteuerung: Definition und Verfahren	20
18.4	LAN-Referenzmodell	20
18.5	Shared Medium LAN	21
18.6	Grundaufbau eines Ethernet LANs	21
18.7	Kurzbezeichnungen für Ethernet LANs	21
18.8	Slot-Time, Round Trip Delay und Mindeststrahlenlänge	22
18.9	Prinzip bei CSMA/CD als Flussdiagramm	22
18.10	Kollisionserkennung bei 10BASE5	23
18.11	Backoff-Algorithmus	23

18.12 Kollisionsdomäne	23
18.13 Flussdiagramm beim Empfang eines Ethernet-Rahmens	23
18.14 Aufbau von Ethernet-Rahmen	24
18.15 Aufbau einer MAC-Adresse	25
18.16 Aufbau der LLC-Schicht	25
18.17 Aufgabe von L-SAP-Adressen	25
18.18 Arten von Encapsulation	26
18.19 Aufgaben von Komponenten und Schnittstellen im Ethernet	26
18.20 SQE-Test	27
18.21 Wozu Hubs?	27
18.22 Der MDI-X-Port	27
18.23 Der Link-Integrity-Test	27
18.24 Die Auto-Negotiation-Funktion	28
18.25 Frame Extension und Frame Bursting	28
18.26 Komponenten und Merkmale des Switched-Ethernet	28
18.27 Wie funktioniert schleifenfreie Wegelenkung?	28
18.28 Wurzel-Port	29
18.29 designierter Knoten	29
18.30 TCP-Checksum bei Ethernet nötig?	29

Teil I

Schichten, Dienste und Protokolle

1 Grundbegriffe und statische Struktur des OSI-Referenzmodells

Dieses Kapitel aus [2] ist identisch mit [1], Teil »Systemarchitekturen für die offene Datenkommunikation«, Kapitel 2.1.

Das OSI-Referenzmodell kann man sich durch folgende Begriffshierarchie verständlicher machen:

1. Das OSI-Referenzmodell enthält mehrere ...
2. Schichten. Eine Schicht enthält mehrere ...
3. Systeme. Ein System enthält mehrere ...
4. Instanzen. Eine Instanz enthält mehrere ...
5. SAPs. Ein SAP enthält mehrere ...
6. Dienste. Ein Dienst enthält mehrere ...
7. Dienstprimitive¹.

2 Funktionsprinzipien - dynamische Struktur des OSI-Referenzmodells

Dieses Kapitel aus [2] ist identisch mit [1], Teil »Systemarchitekturen für die offene Datenkommunikation«, Kapitel 2.2.

3 Spezifizierung von Instanzen durch erweiterte endliche Automaten

Die unterschiedlichen Möglichkeiten, endliche und erweiterte endliche Automaten darzustellen, sind »Zustandsübergangsdiagramm«, »Zustandsübergangstabelle« und »Zeitdiagramm«. Sie sind i.A. semantisch nicht gleichwertig, sondern auf unterschiedlichen Einsatz spezialisiert. So beschreibt z.B. nur die Zustandsübergangstabelle den gesamten (erweiterten) endlichen Automaten, ist jedoch oft sehr unübersichtlich und damit für manch Zwecke unbrauchbar.

¹Dies soll bloß eine *logische* Hierarchie formulieren, denn »Dienste werden ihrem Benutzer über Folgen von Dienstprimitiven zur Verfügung gestellt.« [2, Teil 1, Kap. 2].

3.1 Endlicher und erweiterter endlicher Automat

Dieses Kapitel aus [2] ist identisch mit [1], Teil »Systemarchitekturen für die offene Datenkommunikation«, Kapitel 2.3.1.

Man kann jeden Rechner als »endlichen Automaten« betrachten. Das heißt, die Menge der Ereignisse und die Menge der Zustände haben endlich viele Elemente.

3.2 Zustandsübergangsdiagramm

Dieses Kapitel aus [2] ist identisch mit [1], Teil »Systemarchitekturen für die offene Datenkommunikation«, Kapitel 2.3.2.

Legende

- Zustände werden gleichwertig durch Kreise, Ellipsen oder Rechtecke dargestellt. Die unterschiedlichen Repräsentationen werden nicht in einem Diagramm gemischt.
- Zustände werden benannt, manchmal auch durchnummeriert.
- Zustandsübergänge werden durch gerichtete Kanten dargestellt.
- Ereignisse, die einen Zustandsübergang auslösen, werden an die gerichteten Kanten geschrieben.

Zustandsübergangsdiagramme haben das Problem, dass man nicht alle gegebenen Informationen hineinschreiben kann, wenn man sie übersichtlich halten will. Mit Zustandsübergangsdiagrammen kann man kleine Automaten vollständig beschreiben, inkl. Ausgaben. Bei größeren Automaten wie Protokollen dienen sie dazu, einen Überblick zu vermitteln. Die detaillierte, vollständige Beschreibung steht dann in Zustandsübergangstabellen.

Ein Protokollstapel kann nun durch eine Menge von gekoppelten Automaten dargestellt werden. Aber Achtung: nur verbindungsorientierte Protokolle haben Zustände und können durch einen endlichen Automaten dargestellt werden. Verbindungslose Protokolle wie IP haben dagegen kein Ablaufgeschehen.

3.3 Zustandsübergangstabelle

Dieses Kapitel aus [2] ist identisch mit [1], Teil »Systemarchitekturen für die offene Datenkommunikation«, Kapitel 2.3.3.

Auch genannt »Zustandsübergangsmatrix«.

3.4 Zeitdiagramm

Dieses Kapitel aus [2] ist identisch mit [1], Teil »Systemarchitekturen für die offene Datenkommunikation«, Kapitel 2.3.4.

Sie geben nur den typischen Ablauf bestimmter Dienste an. Solche Diagramme werden in den Spezifikationen für Protokolle oft dargestellt.

3.5 Einführung in SDL

4 Literatur

Teil II

Lokale Datenkommunikation

5 Einführung

5.1 LAN, MAN und CPN

5.2 Charakteristische Eigenschaften von LANs

5.3 Verfahren zur Mediumzugriffssteuerung

5.4 Standardisierung

5.5 Aufgaben und Fragen zur Lernkontrolle

6 Ethernet

6.1 Historie

6.2 Ethernet im OSI-Schichtenmodell

6.3 IEEE Ethernet Arbeitsgruppen und Teilbereiche des Ethernet Standards

6.4 Ethernet 10BASE5

6.4.1 Komponenten und Systemkenngößen

Die Endwiderstände bei Ethernet-LANs auf Kupferkabel dienen dazu, die Nachricht vom Medium zu nehmen, indem die Energie der Nachricht im abschließenden Wellenwiderstand verbraten wird.

6.4.2 MAC-Protokoll CSMA/CD

6.4.3 Rahmenformate, Adressen und Fehlerbehandlung

6.4.4 Späte Kollisionen

6.4.5 Logical Link Control (LLC)

6.4.6 Verwendung der Rahmenformate in Standardprotokollen

6.4.7 Architektur eines Ethernet-Anschlusses

6.5 Nachfolgeentwicklungen

6.5.1 Ethernet 10BASE2

6.5.2 Ethernet 10BASE-T

6.5.3 Fast Ethernet 100BASE-T

PMD Geläufigste Komponente aus dieser Schicht ist ein elektro-optischer Wandler zur Anpassung der Signale auf Glasfaser.

MII Wie das AUI als Sub-D Buchse definiert, jedoch mit wesentlich mehr Adernpaaren. Diese Schnittstelle ist bei den meisten Ethernet-Karten on board, d.h. es existiert keine Sub-D Buchse. Diese Schnittstelle kann jedoch auch nach außen geführt werden.

Regeln zur physikalischen Netztopologie Wird das gesamte Netz von einer zentralen Bridge, Switch oder Router gemanaged, so nennt man diese Architektur »collapsed backbone«. Dies ist zur Zeit die gängigste Technologie für 100BASE-T Ethernet. Die Bezeichnung leitet sich von dem Unterschied zur älteren »backbone«-Architektur her: dabei war jede Etage eine Kollisionsdomäne und über einen Switch auf dieser Etage an den etagenverbindenden Bus (»backbone«) angeschlossen. Bei »collapsed backbone« wurde der etagenverbindende Bus mit seinen Switches in der zentralen Bridge, Switch oder Router zusammengefasst.

Diese beiden Architekturen haben jeweils Vor- und Nachteile: ein Netz nach »collapsed backbone« fällt mit dem zentralen Knoten komplett aus, während ein Netz nach »backbone« nur etagenweise ausfallen kann, wenn die dortigen Router ausfallen.

Pro Segment dürfen bei Ethernet 100BASE-T nur noch 2 Stationen verwendet werden, gegenüber 100 Stationen in der ersten Version des Ethernet.

Kenngößen von 100BASE-FX Diese Technologie wird verwendet, um größere Entfernungen zu überbrücken. Als Kabeltypen können Multimode- oder Singlemode-Glasfasern verwendet werden.

Vollständig geschichtete Netze verwenden nicht mehr CSMA/CD als Zugriffstechnologie, es gibt keine Kollisionsdomänen mehr. Glasfasertechnologie ist nach wie vor eine verhältnismäßig teure Technologie, sie wird deshalb nur im kommerziellen Bereich bei größeren Entfernungen eingesetzt. Besonders Singlemode-Fasern sind teuer im Handling (Anschluss technik usw.) und werden hauptsächlich im TK-Sektor für hohe Bitraten auf langen Segmenten eingesetzt.

6.5.4 Gigabit-Ethernet - 1000BASE-X

Der Gigabit-Ethernet-Allianz gehörten etwa 120 Firmen an. Sie spezifizierten Gigabit-Ethernet hauptsächlich für LWL-Kabel. IEEE fügte eine Spezifikation für Kupferkabel hinzu. Nur wenige Gigabit-Ethernet Netze verwenden CSMA/CD als Zugriffsverfahren, problematisch dabei ist die dann verwendete vergrößerte minimale Rahmenlänge, die zur Kollisionserkennung nötig ist, aber Overhead für das Netz bedeutet. Die meisten Gigabit-Ethernet-Netze sind vollständige geschichtete Netze, ohne Kollisionsdomänen und somit ohne Frame Extension zur Vergrößerung der minimalen Rahmenlänge.

Schon bei Erfindung der LANs existierten Switches und waren das gängige Vermittlungsverfahren. CSMA/CD wurde dabei als Fortschritt angesehen. Mit der Zeit wurde jedoch die Switch-Technologie wesentlich billiger und somit wieder konkurrenzfähig. Sie hat gegenüber CSMA/CD viele Vorteile für die Netzstruktur. Bei Verzicht auf CSMA/CD entfallen z.B. alle Längenbeschränkungen aufgrund von Kollisionsdomänen.

Dispersion Dispersion ist eine Eigenschaft von Lichtwellenleitern. Man unterscheidet Phasendispersion und Modendispersion. Je kleiner der Kerndurchmesser, desto geringer die Modendispersion. Denn die Anzahl der Wellentypen sinkt dabei. Wellentypen unterscheiden sich z.B. durch die Polarisation (Schwingungsebene) des Lichts.

Das Bandbreitenlängenprodukt Die über ein LWL-Kabel übertragbare Bandbreite hängt von der Länge des Kabels ab: die Signalqualität wird durch die Dispersion, je länger das Kabel ist. Hersteller drücken den Einfluss der Dispersion kompakt im Bandbreitenlängenprodukt aus: das Produkt von Kabellänge und Signalfrequenz darf im Einsatzfall diesen Wert nicht überschreiten. Ein LWL-Kabel mit einem Bandbreitenlängenprodukt von $1000\text{MHz}\cdot\text{km}$ darf also bei einer Signalfrequenz von 1GHz maximal 1km lang sein, bei einer Signalfrequenz von 500MHz maximal 2km .

Das Leistungsbudget Eine LWL-Verbindung besteht nicht nur aus der Faser, sondern auch aus der Laserdiode. Bei der Verbindung zwischen Laserdiode und Faser entstehen die ersten Leistungsverluste. Auch durch die Koppel-elemente auf dem Leitweg geht Leistung verloren. Der Leistungsverlust wird durch das Leistungsbudget als Norm begrenzt. Die Einheit ist dBm : dB bedeutet das Verhältnis von eingespeister zu abgegebener Leistung, und »m« steht für eine normierte eingespeiste Leistung von 1mW .

Kenngößen von 1000BASE-CX Die Idee war hier, Gigabit-Ethernet über Kupferkabel zu realisieren. Als Kabeltyp wird ein doppeltes Twinax-Kabel verwendet: eine Kombination zweier Twinax-Kabel, die wiederum aus zwei parallelen Koax-Kabeln bestehen.

6.5.5 Auto-Negotiation-Funktion

Sie ist ein standardisiertes Verfahren zum Feststellen und Konfigurieren der verwendeten Ethernetvariante. Diese Funktion ist nur anwendbar, wenn das Übertragungsmedium Kupfer ist - bei Glasfaser sind unterschiedliche Wellenlängen im Einsatz, weshalb dort eine Auto-Negotiation-Funktion von der Hardware her aufwändig zu implementieren wäre.

6.6 Switched-Ethernet

6.6.1 Entwicklungsgeschichte und Begriffsbildung

6.6.2 Grundstruktur eines Ethernet-Switches

6.6.3 Eigenschaften von Switched-Ethernet

6.6.4 Realisierungsformen der Vermittlungseinheit

6.6.5 Schleifenfreie Wegelenkung

6.7 Aufgaben und Fragen zur Lernkontrolle

7 Token-Verfahren

7.1 Zugriffsverfahren Token-Passing

Von allen erfundenen Verfahren zur Mediumzugriffssteuerung haben nur CSMA/CD (bei 90%) und Token Passing (10%) wesentliche Marktbedeutung. Token-Verfahren funktionieren nicht nach dem Broadcast-Prinzip. Sondern es gibt Ende-zu-Ende-Verbindungen von genau einem Transmitter einer Station zu genau einem Transmitter einer anderen Station. Damit waren Token-Verfahren von Anfang an besser mit optischen Medien nutzbar, denn bei Glasfaser muss das Signal stets ausgekoppelt werden, es kann nicht einfach abgehört werden.

Das System ist sowohl für Bus- als auch für Ringsysteme anwendbar. Token Passing wurde auch für beide Topologien standardisiert: Token Bus und Token Ring. Bei Bussystemen gibt es keine Ende-zu-Ende-Verbindungen wie in einem Ringsystem, sondern passive Ankopplung beim Abhören.

Token-Systeme sind gegenüber CSMA/CD komplexe Systeme. Ethernet dagegen sollte von Anfang an einfach und robust werden. Bei der Entwicklung komplexer hardwarebasierter Systeme ist es aber oft so, dass einmal eine Anfangshürde genommen werden muss, danach die Systeme immer billiger werden und die entwickelte Komplexität gut beherrschbar wird.

Als Vorteile von Token Passing werden angegeben:

- Echtzeitfähigkeit: es kann garantiert werden, dass in einer bestimmten Zeit jede Station einmal den Token erhalten hat.
- Prioritätssysteme: ermöglicht Zeittransparenz und damit Sprachtransfers usw.
- Keine Probleme mit kollisionsbedingten Ausdehnungsbeschränkungen. Denn die Pakete werden in jeder Station untersucht und neu generiert.

Nachteile:

- Das System ist komplex und damit immer teurer als CSMA/CD.

7.2 Token-Bus

7.3 Token-Ring

Token Ring spielt im Gegensatz zu Token Bus eine Rolle. Die Ankopplung ist im Gegensatz zu Token Bus nicht passiv, sondern aktiv. Das heißt, jede Station wirkt als Repeater.

Ein weiteres Token Passing Verfahren ist FDDI. Aber selbst im MAN-Bereich hat sich dieses System nicht durchgesetzt, denn die Telekom entschied sich für DQDB (double queue, double bus). Grund dafür war, dass sich ATM als Weitverkehrstechnik in der Telekommunikation durchgesetzt hat und DQDB eine ganz ähnliche Rahmenstruktur hat.

8 Architekturen für Netzwerktreiber

8.1 Problemstellung

8.2 NDIS

8.3 ODI

9 Literatur

10 Anhang 1: Kabelspezifikationen

Teil III

IP-Routing

11 Netzübergänge und Internetworking

Ein Hub ist eine Schaltung, die das Signal regeneriert und auf mehrere Ports verteilt. Was aber sind Brücken und Switches? Es sind Elemente, mit denen man LANs unterschiedlichen Typs verbinden kann und auch Netzübergänge zu öffentlichen Netzen wie dem Internet herstellen kann.

Switches waren damals zu teuer, weshalb verteilte Vermittlung wie CSMA/CD und Token Passing Vorteile hatten, weil sie preiswerter waren. Heute hat sich das wieder geändert: Switching löst wiederum CSMA/CD ab, denn Switches sind heute billig herzustellen. Deshalb sollten Switches als eigenes Kapitel bei LANs behandelt werden, nicht bloß als Elemente zur Verbindung von LANs mit CSMA/CD.

Grundsätzliche Arten von Netzübergängen:

1. Kopplung von LANs oder LAN-Segmenten gleichen Typs
2. Kopplung von LANs unterschiedlichen Typs (etwa Ethernet zu FDDI)
3. Netzübergang von einem LAN in ein WAN/MAN und umgekehrt (etwa LAN auf ISDN, LAN auf ATM (ebenfalls von der Telekom angeboten, etwa für die Druckindustrie), LAN auf DSL)

Komponenten, die die Fälle 2 und 3 beherrschen, heißen Gateways (oder nach ITU-T: Interworking Unit), Komponenten für den Fall 1 heißen Switches, Komponenten für den Fall 2 heißen Brücken (mittlerweile synonym zu Switches). Auf Ebene 2 werden die MAC-Adressen für die Vermittlung verwendet. Router vermitteln mit IP-Adressen (moderne Router aus Geschwindigkeitsgründen aber auch anders). Sie können aber auch mit allen Informationen der Schichten 3 und 4 arbeiten, so dass auch Firewalling usw. verwendbar sind.

Router werden heute hauptsächlich für die Zustellung zum Zielnetz verwendet (Knotenpunkte, Netzübergänge und bei weiten Strecken), Switches dagegen für die Zustellung im Zielnetz (im LAN, mit MAC-Adressen).

Routingtabellen enthalten einen Eintrag »Interfaces«; dies sind die Ports, an die Pakete weitergeleitet werden, in PCs meist Ethernet-Netzwerkkarten.

Schicht-3-Router stellen eine recht langsame Vermittlungstechnik dar, weil der IP-Routing-Algorithmus aufwendig ist. Deshalb wird heute tag switching verwendet (»echtes Layer-3-Switching«): es werden virtuelle Kanäle eingerichtet, die über Hardware ausgewählt werden. Nur an den Grenzen des Netzes (edge) wird nach dem herkömmlichen Routing-Algorithmus verfahren. Besonders bei Realzeitanwendungen wie Videoströmen bringt dies große Geschwindigkeitsvorteile.

IP Routing Algorithmus Bei direkt angeschlossenen Netzen muss nach dem IP Routing Algorithmus der Algorithmus für Adressauflöschung und Versand ausgeführt werden; dieser ist abhängig vom Typ des angeschlossenen Netzes. Der Default Router (auch: Default Gateway) ist ein Rechner, an den alle Pakete weitergeleitet werden, für die weder für den Zielhost noch für dessen Netz ein passender Eintrag in der Routing-Tabelle gefunden wurde.

Es gibt einen ARP-Cache, in dem die Ergebnisse von ARP Requests zwischengespeichert werden, um überflüssige Netzlast zu vermeiden.

RARP war dazu gedacht, Netzstationen remote zu konfigurieren. Heute wird jedoch die Weiterentwicklung DHCP verwendet. Damit kann der Protokollstack dynamisch konfiguriert werden. Es gibt einen DHCP-Server, der einen Pool von IP-Adressen vorrätig hält und sie solchen Rechnern zuteilt, die sich mit ihrer MAC-Adresse dort melden.

Als IP-Adressen Mangelware wurden, wurde Subnetting eingeführt. Das bedeutet nun eigentlich »klassenloses Routing«: was der Netzanteil einer Adresse ist, wird nicht mehr durch die IP-Adresse, sondern durch die Subnetzmaske definiert. Das gilt jedoch nur innerhalb des eigenen lokalen Netzes.

Teil IV

TCP und UDP

12 TCP

12.1 Dienste

12.2 Paketformat

TCP hat als Verbindungsendpunkte Prozesse, hat also als Adressen Portadressen. Das Paar (IP-Adresse,Port) nennt man Socket («Steckdose»). TCP hat 32bit-Folgenummern, es wird nicht modulo gezählt wie bei HDLC. Auch die Quittungen bestehen aus 32bit. Das Prüfsummenfeld des TCP-Headers verwendet keinen Hamming-Code; es können keine Fehler automatisch korrigiert werden. Weil aber die heutigen Leitungen sehr geringe Bitfehlerraten haben, ist das nur ein geringer und damit vertretbarer Mehraufwand. Der Fenster-Mechanismus bei TCP ist komplexer als bei HDLC.

12.3 Ablaufsteuerung

13 UDP

13.1 Dienste

13.2 Paketformat

Teil V

Dienste und Protokolle der Anwendungsschicht

14 WWW

15 E-Mail

16 FTP

Teil VI

Netzsicherheit und Firewalls

Teil VII

Übungsaufgaben

17 Übungsaufgaben Typ »Klausuraufgaben Teil A« (mit Unterlagen)

17.1 Modulo 8-Zähler als (erweiterter) endlicher Automat

Aufgabe

1. Beschreiben Sie das Verhalten eines Modulo-8-Zählers durch einen endlichen Automaten.
2. Reduzieren Sie die Zahl der Zustände, indem Sie den Zähler durch einen erweiterten endlichen Automaten beschreiben.

Quelle: [4, Teil 1, Aufgabe 1].

Lösung

1. Der endliche Automat eines Modulo-8-Zählers hat 8 Zustände $0, 1, \dots, 7$. Alle möglichen Zustandsübergänge werden jeweils durch einen Zählimpuls I ausgelöst. Sie sind: $0 \rightarrow 1, 1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 4, 4 \rightarrow 5, 5 \rightarrow 6, 6 \rightarrow 7, 7 \rightarrow 0$. Vgl. [2, Teil 1, Kap. 3.1].
2. Den erweiterten endlichen Automaten eines Modulo-8-Zählers zeigt Abbildung 1. Vgl. [2, Teil 1, Kap. 3.1].

17.2 Das Protokoll LAPB

Aufgabe Im Folgenden wird der Austausch von Steuerdaten zwischen den DL-Instanzen einer DEE und einer DVST-P² nach der HDLC Protokollvariante LAPB (Link Access Procedure for Balanced Mode) betrachtet. Zur Beantwortung der folgenden Fragen können neben dem Skript »Rechnernetze« die im Anhang 1 [der Aufgabenblätter; Anm.] enthaltenen Informationen aus einem DATEX-P-Handbuch über die funktionalen Abläufe dieses Schicht-2-Protokolls verwendet werden.

1. Die DEE möchte einen Befehl an die DVST-P senden. Welche Adresse steht im Adressfeld des abgesendeten Blocks?
2. Welche Meldung sendet die DVST-P jeweils nach Ablauf von T_1 , wenn sie im Zustand »Senden von DM« keine Blöcke von der DEE empfängt?
3. Nach Ablauf von $N_2 \cdot T_1$ sendet die DVST-P einen SABM-Befehl mit gesetztem Poll-Bit. Geben Sie den Inhalt des Adressfeldes, die Meldung und den Wert des Final-Bits des HDLC-Blocks an, den die DEE senden muss, damit die DVST-P in den Zustand ABM übergeht.
4. Mit welchem HDLC-Block kann die DEE einen Verbindungsaufbau in der Schicht 2 erreichen und welche Antwort erwartet sie?
5. Wieviele I-Blöcke kann die DEE (DVST-P) senden, bevor sie eine Quittung von der DVST-P (DEE) erwartet?
6. Mit welchen Blöcken kann die DEE (DVST-P) alle korrekt empfangenen I-Blöcke quittieren?

Quelle: [4, Teil 1, Aufgabe 2].

²DVST-P steht für »Datenvermittlungsstelle, paketvermittelt«.

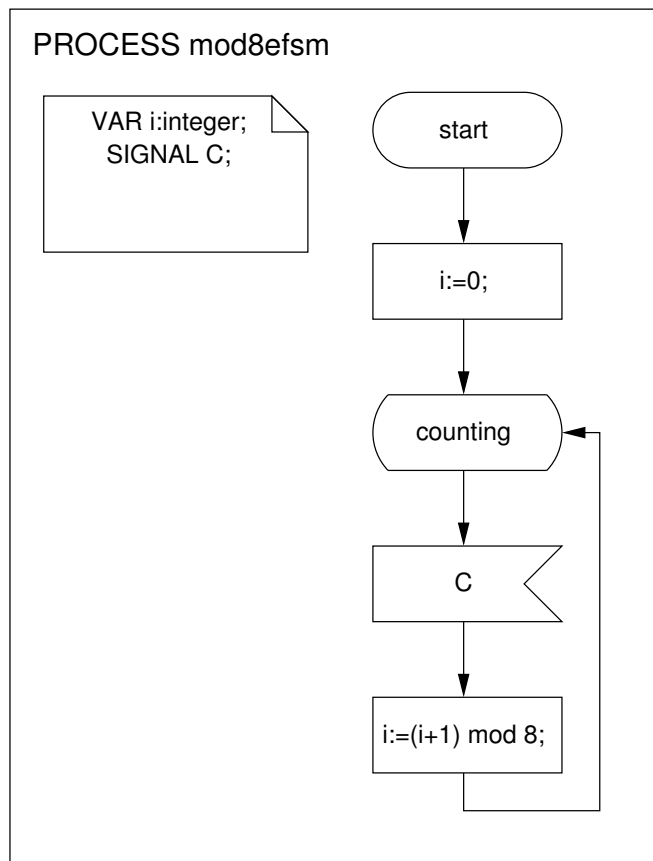


Abbildung 1: Erweiterter endlicher Automat zu einem Modulo-8-Zähler in SDL

Lösung Vergleiche [1, Teil 4, Kap. 4.3] für eine grundsätzliche Beschreibung von HDLC und LAPB. Sei im Folgenden 01_{16} die Adresse der DVST-P und 03_{16} die Adresse der DEE.

1. Wenn eine Instanz einen Befehl an eine andere Instanz richtet, enthält das Adressfeld des abgesendeten Blocks die Adresse der angesprochenen Instanz, hier die der DVST-P (01_{16}).
2. Die Meldung »DM«. Dadurch wird die DEE aufgefordert, den Übermittlungsabschnitt mit Hilfe des Befehls SABM aufzubauen.
3. Das Adressfeld enthält bei Meldungen die Adresse der sendenden Station, hier also die der DEE (03_{16}). Die Meldung muss entsprechend der Zustandsübergangstabelle »UA« sein (»unnumbered acknowledgement«). Das Final-Bit wird gesetzt, wenn im vorher empfangenen Block das Poll-Bit gesetzt war. Dies ist hier der Fall, also ist $F = 1$.
4. Befindet sich die DVST-P im Zustand »Senden von DM«, so kann die DEE durch den Befehl SABM (»set asynchronous balanced mode«) den Übermittlungsabschnitt aufbauen. Sie erwartet von der DVST-P eine Bestätigung durch »UA« (»unnumbered acknowledgement«).
5. Gefragt ist nach der Fenstergröße bei I-Blöcken. Sie kann höchstens dem Modulus (hier 8) minus 1 sein und ist im Protokoll festgelegt. Das DATEX-P-Handbuch sagt dazu: »Die maximale Anzahl von nicht bestätigten I-Blöcken darf nicht größer als 7 sein [...]«.
6. Sowohl mit S-Blöcken (»supervisory«, für Steuerungsfunktionen) als auch im Piggybacking mit I-Blöcken. Denn diese beiden Blockarten haben ein Feld »N(R)« (Empfangsfolgenummer), mit dem alle I-Blöcke bis inkl. der Sendefolgenummer $N(S) = N(R) - 1$ als korrekt empfangen quittiert werden.

17.3 Zustandstabelle eines Signalisierungsprotokolls

Aufgabe³ Die folgende Zustandstabelle beschreibt ein (fiktives) Signalisierungsprotokoll für eine Transportverbindung in einem paketvermittelten Datennetz. Geben Sie für den durch die Zustandstabelle spezifizierten Automaten das zugehörige Zustandsdiagramm an. Verwenden Sie zur Kennzeichnung der Übergänge die Notation: <Ereignis> / <Ausgabesignal>. Hinweis: Entsprechend der Darstellung in der Vorlesung, sind Ausgangssignale (SYN, FIN) in der Tabelle gerade und Folgezustände *kursiv* gedruckt.

Zustand→Ereignis↓	CLOSED	WFSYN	LISTEN	OPEN	WFFIN	WFCLOSE
ACTIV_Open	SYN <i>WFSYN</i>					
PASSIV_Open	<i>LISTEN</i>					
SYN		<i>OPEN</i>	SYN <i>OPEN</i>			
CLOSE				FIN <i>WFFIN</i>		FIN <i>CLOSED</i>
FIN				<i>WFCLOSE</i>	<i>CLOSED</i>	
TO_SYN		<i>CLOSED</i>	<i>CLOSED</i>			

Ereignisse

ACTIV_Open Anforderung von der überlagerten Schicht zum Aufbau einer Transportverbindung.

PASSIV_Open Anforderung von der Partnerinstanz zum Aufbau einer Transportverbindung.

SYN Verbindungssynchronisationszeichen: drückt durch wechselseitigen Gebrauch den Verbindungswunsch bzw. die Verbindungsbereitschaft aus.

CLOSE Anforderung/Bestätigung von der überlagerten Schicht zum Abbau einer Transportverbindung.

FIN Final-Zeichen: drückt durch wechselseitigen Gebrauch den Wunsch bzw. die Bereitschaft zum Beenden der Transportverbindung aus.

TO_SYN Anzeige eines Timeouts.

Zustände

³Dies ist eine ehemalige Klausuraufgabe.

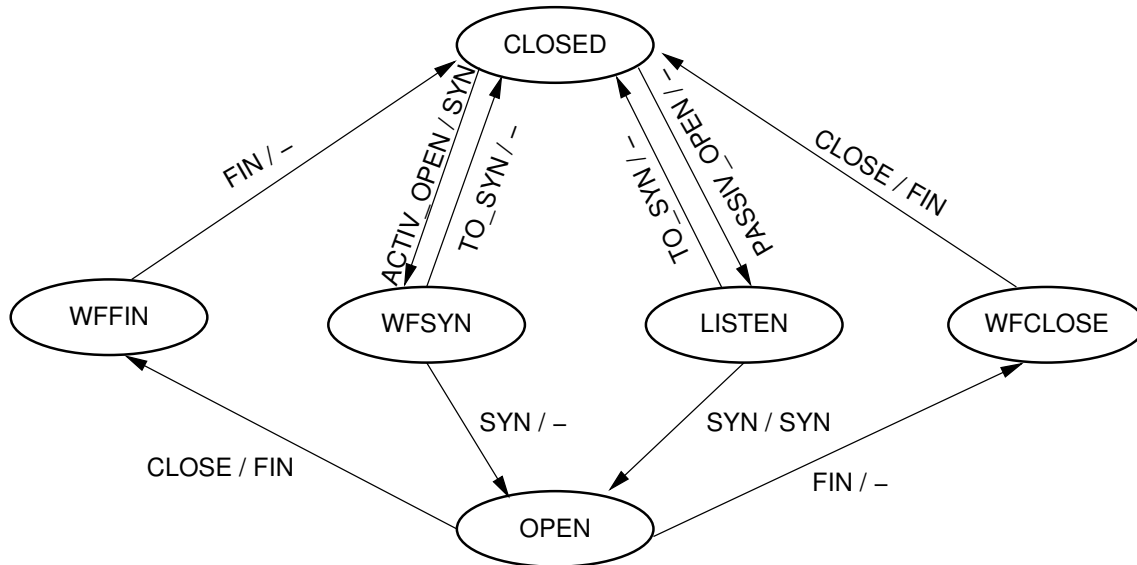


Abbildung 2: Zu Aufgabe »Zustandstabelle eines Signalisierungsprotokolls«

CLOSED Ruhezustand.

OPEN Transportverbindung hergestellt.

WFSYN Warten auf Verbindungssynchronisationszeichen.

LISTEN Zustand, in dem Transportverbindungen passiv aufgebaut werden können.

WFFIN Warten auf Bestätigung des Verbindungsabbaus durch FIN von der Partnerinstanz.

WFCLOSE Warten auf Bestätigung des Verbindungsabbaus durch CLOSE von der überlagerten Schicht.

Quelle: [4, Teil 1, Aufgabe 3].

Lösung Siehe Abbildung 2. Es entsteht eine Art vereinfachtes Zustandsübergangsdiagramm für das TCP-Protokoll. Man kann zur Lösung der Aufgabe einfach die Tabelle spaltenweise abarbeiten.

17.4 Verbindungsauf- und -abbau bei TCP

Aufgabe Das Verbindungsmanagement des im Internet verwendeten Transportprotokolls TCP (Transmission Control Protocol) wird durch das im Anhang 2a gegebene Zustandsdiagramm beschrieben. Bei den folgenden Teilaufgaben soll jeweils die Signalisierung zwischen Client und Server für einen erfolgreichen Verbindungsaufbau und -abbau betrachtet werden.

1. Vervollständigen Sie das folgende Zeitdiagramm für einen aktiven Verbindungsaufbau durch den Client.
2. Vervollständigen Sie das folgende Zeitdiagramm für einen (normalen) aktiven Verbindungsabbau durch den Client.
3. Erläutern Sie, wie die beim Verbindungsauf- und -abbau verwendeten Signalisierinformationen in den ausgetauschten TCP-Segmenten kodiert werden (Zum Layout eines TCP-Segments siehe Anhang 2b).

Quelle: [4, Teil 1, Aufgabe 4].

Lösung

1. Im Client findet ein aktiver, im Server ein aktiver Verbindungsaufbau statt. Dieser Verbindungsaufbau bei TCP wird als »Dreiwege-Handshake« bezeichnet, weil drei Nachrichten ausgetauscht werden.

Zustand Client	Nachricht (Segment)	Zustand Server
CLOSED		CLOSED
active open ↓		passive open ↓
		LISTEN
	SYN →	
SYN_SENT	SYN, ACK ←	
ESTABLISHED		SYN_RCVD
	ACK →	ESTABLISHED

2. Hier geschieht ein sog. »Vierwege-Handshake«.

Zustand Client	Nachricht (Segment)	Zustand Server
ESTABLISHED		CLOSED
close ↓	FIN →	ESTABLISHED
FIN_WAIT1		CLOSE_WAIT
	ACK ←	
FIN_WAIT2		close ↓
	FIN ←	LAST_ACK
	ACK →	
TIME_WAIT		CLOSED
↓2MSL ⁴ timeout		
CLOSED		

3. Die Signalisierinformationen sind ACK, SYN und FIN. Für jede von diesen steht im TCP-Segment ein dediziertes Bit zur Verfügung, das gesetzt wird um das entsprechende Signal zu übertragen:

ACK Bit Nummer 107

SYN Bit Nummer 110

FIN Bit Nummer 111

17.5 Transportprotokoll in SDL

Aufgabe Geben Sie für das in der Vorlesung behandelte Transportprotokoll (siehe dort Bild 3.3) eine Beschreibung der funktionalen Abläufe in SDL an. Quelle: [4, Teil 2, Aufgabe 1].

Lösung Eine bisher unvollständige Lösung zeigt Abbildung 3.

17.6 Geldautomat in SDL

Aufgabe Es ist ein Geldautomat zu entwerfen, der, vereinfacht dargestellt, folgendes leistet:

Im Ruhezustand des Automaten (A) versperrt ein Rolladen den Zugriff auf dessen Tastatur. Nach Eingabe einer Scheckkarte durch den Kunden (K) wird diese überprüft und gegebenenfalls unter Ausgabe einer Meldung zurückgewiesen. Ist die Karte zulässig, wird die Tastatur freigegeben und der Kunde zur Eingabe einer Geheimnummer aufgefordert. Nach erfolgreicher Eingabe (max. drei Fehlversuche (kommentiert), dann Einzug der Karte durch den Automaten) erscheint ein Menü der angebotenen Dienstleistungen (Hauptmenü), von denen hier nur die Abfrage des Kontostandes betrachtet werden soll. Nach Betätigung der entsprechenden Taste übermittelt der Automat die Kundendaten an den Datenbankrechner (DB) und gibt eine Meldung »Bitte Warten« aus. Nach dem Erhalt des Kontostandes von der Datenbank wird dieser dem Kunden angezeigt und gefragt, ob ein weiterer Vorgang bearbeitet werden soll. Fall »Ja«, kehrt der Automat zum Hauptmenü zurück und wartet auf eine neue Eingabe. Andernfalls gibt er die Scheckkarte aus, versperrt die Tastatur und kehrt in den Ruhezustand zurück.

Spezifizieren Sie den im Automaten ablaufenden Prozess durch ein SDL-Diagramm. Dabei sollen alle vom Kunden verursachten Zustandsübergänge zeitüberwacht werden.

Quelle: [4, Teil 2, Aufgabe 2].

Lösung

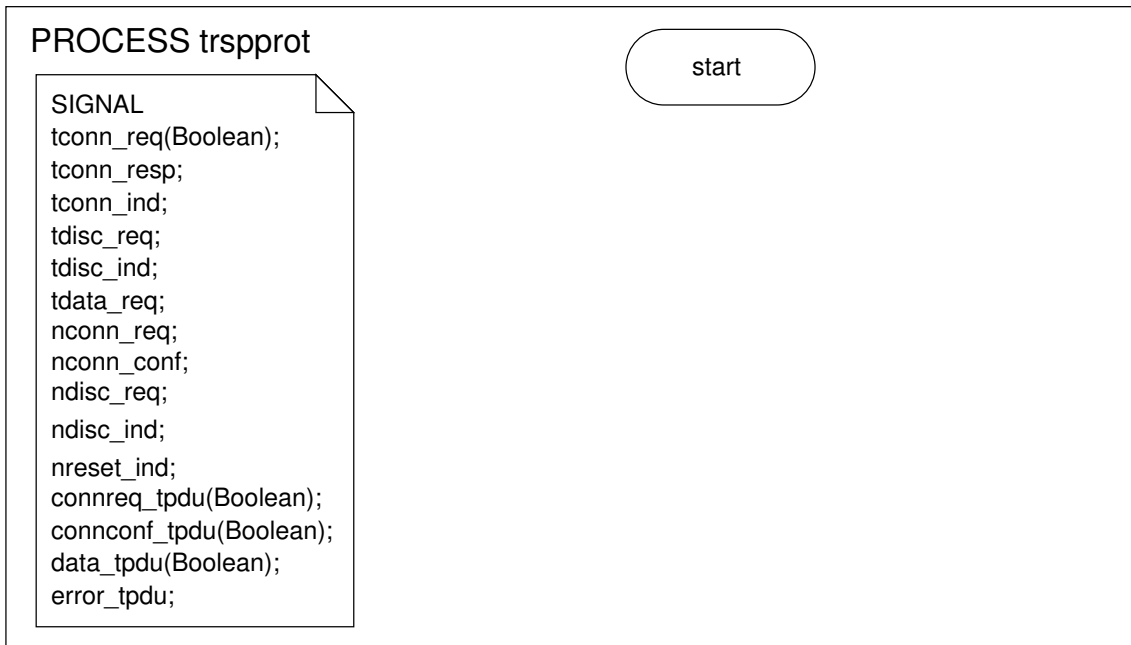


Abbildung 3: Zu Aufgabe »Transportprotokoll in SDL«

17.7 Truncated Binary Exponential Backoff

Aufgabe Erläutern Sie das Verfahren Truncated Binary Exponential Backoff. Vervollständigen Sie die folgende Tabelle. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 6d].

Lösung Ein Backoff-Verfahren ist ein Verfahren zur Kollisionsauflösung bei CSMA/CD. Truncated Binary Exponential Backoff weist dazu den kollidierten Stationen unterschiedliche Wartezeiten T_w vor ihrem nächsten Sendeversuch zu. Es gilt:

$$T_w = r \cdot T_s$$

T_s Slot-Time

r Zufallszahl im Bereich $[0, 2^{\text{Min}(n,10)} - 1]$

n Anzahl bisheriger Kollisionen für dieses Datenpaket

Wenn $n = 16$, bricht das Verfahren den Sendevorgang mit der Fehlermeldung »Excessive Collisions« ab. Die Wahrscheinlichkeit, dass eine Station mit $T_w = 0 \cdot T_s = 0$ senden darf, also sofort im nächsten Slot, beträgt:

$$p(T_w = 0) = \frac{1}{|\{0, \dots, 2^{\text{Min}(n,10)} - 1\}|} = 2^{-\text{Min}(n,10)}$$

n	Bereich der Zufallszahl r	Bereich der Wartezeit	p (Senden im nächsten Slot)
1.	$[0, 2^1 - 1] = [0, 1]$	$0 \cdot T_s \dots 1 \cdot T_s = 0 \dots 0,0512ms$	$2^{-1} = 0,5$
2.	$[0, 2^2 - 1] = [0, 3]$	$0 \cdot T_s \dots 3 \cdot T_s = 0 \dots 0,1536ms$	$2^{-2} = 0,25$
3.	$[0, 7]$	$0 \dots 0,3584ms$	$2^{-3} = 0,125$
4.	$[0, 15]$	$0 \dots 0,768ms$	$2^{-4} = 0,0625$
5.	$[0, 31]$	$0 \dots 1,59ms$	$2^{-5} = 0,3125$
6.	$[0, 63]$	$0 \dots 3,23ms$	$2^{-6} = 0,1562$
7.	$[0, 127]$	$0 \dots 6,50ms$	$2^{-7} = 0,0078$
8.	$[0, 255]$	$0 \dots 13,10ms$	$2^{-8} = 0,0039$
9.	$[0, 511]$	$0 \dots 26,20ms$	$2^{-9} = 0,002$
10.	$[0, 1023]$	$0 \dots 52,40ms$	$2^{-10} = 0,001$
\vdots	\vdots	\vdots	\vdots
15.	$[0, 1023]$	$0 \dots 52,40ms$	$2^{-10} = 0,001$
16.	n.a.	Abbruch mit »Excessive Collisions«	0

17.8 Jabber-Schutzfunktion

Aufgabe Die Jabber-Schutzfunktion geht davon aus, dass das Aussenden eines Ethernetrahmens eine Zeitspanne T_{dtmax} nicht überschreiten darf. Wird diese Zeitspanne überschritten, so bricht die MAU den Sendevorgang ab und sendet über den CI-Pfad des AUI ein SQE-Signal an den Ethernet-Controller. Dieser bricht daraufhin den Sendevorgang ab. Wie groß muss T_{dtmax} sein, wenn eine Reserve von 20% eingerechnet wird?

Quelle: Aufgabe 13 aus einer alten, nicht mehr erhältlichen Version von [2, Teil 2, Kap. 2.7].

Lösung Die *Interframe Gap* (IFG) zählt hier nicht zur Sendezeit, da die Jabber-Schutzfunktion sie nicht von bloßer Ruhe auf dem Kanal unterscheiden kann. Sei T_{dsmax} die reine Sendezeit eines Ethernetrahmens maximaler Länge l_{dmax} , dann gilt:

$$\begin{aligned} T_{dtmax} &= T_{dsmax} + 20\% \cdot T_{dsmax} \\ &= 1,2 \cdot T_{dsmax} \\ &= 1,2 \cdot \frac{l_{dmax}}{v} \\ &= 1,2 \cdot \frac{1526 \text{ Byte}}{10 \text{ Mbit} \cdot \text{s}^{-1}} = 1,2 \cdot \frac{12208 \text{ bit}}{10 \cdot 10^6 \text{ bit}} \text{s} = 1,46496 \text{ ms} \end{aligned}$$

17.9 Unterschiedliche Spanning Trees am Beispiel

Aufgabe Gegeben sei ein Netz dessen Topologie durch den folgenden Graph bestimmt ist. Knoten 1 sei der Wurzelknoten. Die Zahlen an den Kanten des Graphen seien Kostenfaktoren für die entsprechenden Verbindungsabschnitte im Netz.

1. Geben Sie einen vollständigen Baum an, für den die Anzahl der Kanten zu jedem Zielknoten minimal ist. Beschreiben Sie ihr Vorgehen als Algorithmus.
2. Geben Sie einen vollständigen Baum an, für den der Weg zu jedem Zielknoten minimale Kosten hat. Beschreiben Sie auch hier ihr Vorgehen als Algorithmus.

Quelle: [2, Teil 2, Kap. 2.7, Aufg. 18b].

Lösung Musterlösung in [6, S. 3].

17.10 Entscheidungsbaum zur Bestimmung des Protokolls der Daten

Aufgabe Entwickeln Sie einen Entscheidungsbaum für die Bestimmung des Protokolls, dem die im Datenfeld eines Ethernet-Rahmens transportierte PDU zuzuordnen ist. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 11].

Lösung Mit einem solchen Entscheidungsbaum lässt sich für jeden empfangenen Ethernet-Rahmen bestimmen, nach welchem Protokoll die Nutzdaten zu interpretieren sind. Dies leistet nahezu auch die Tabelle in [2, Teil 2, Tab. 2.8 (S. 38)]. Eine Musterlösung befindet sich in [6, S. 2].

18 Übungsaufgaben Typ »Klausuraufgaben Teil B« (ohne Unterlagen)

18.1 Begriffe LAN, MAN, CPN

Aufgabe Erklären Sie die Begriffe LAN, MAN und CPN! Quelle: [2, Teil 2, Kap. 1.5, Aufg.1].

Lösung

LAN (Local Area Network)

- Infrastruktur zu Datenkommunikation für voneinander unabhängige Teilnehmer.
- Beschränkte Ausdehnung, meist nur mehrere Gebäude oder ein Betriebsgelände.

- Meist nichtöffentlich, von den Eigentümern benutzt.
- Oft impliziert: ein Netz mit einem verbindungslosen Paketvermittlungsdienst.

MAN (Metropolitan Area Network)

- Stadtnetz, das LANs in Städten und Ballungsgebieten verbindet.
- Ausdehnung zwischen LAN und WAN.
- Meist öffentlich von den Netzbetreibern angebotene Dienste.
- Technische Unterschiede zu LANs werden durch 10-Gigabit-Ethernet schwinden.

CPN (Customer Premises Network)

- Telekommunikationsnetz moderater Größe.
- Breites Dienstspektrum möglich: Sprache, Daten, Multimedia.
- Oft öffentlich angebotene Dienste.
- Unterschied zu LANs: beliebige Vermittlungstechnik möglich.

Siehe [2, Teil 2, Kap. 1.1]

18.2 Eigenschaften von LANs

Aufgabe Nennen und erläutern Sie die charakteristischen Eigenschaften von LANs. Quelle: [2, Teil 2, Kap. 1.5, Aufg.2].

Lösung

Geringe Bitfehlerrate. Dadurch hohe semantische Transparenz.

Paketübermittlung. Der übliche Übermittlungsdienst in LANs; verbindungslos und schnell.

Niedrige Anschlusskosten. Deshalb drängen LANs von großen Unternehmen und Verwaltungen bis in die Haushalte vor. LAN-Technik ist preisgünstig weil:

- Die Komponenten durch den allgemeinen Fortschritt der Mikroelektronik, internationale Standardisierung, Massenfertigung und sicher beherrschte Fertigungsmethoden immer billiger wurden.
- Die niedrige Bitfehlerhäufigkeit einfache Protokolle ermöglicht.
- LANs sind in ihrer beschränkten räumlichen Ausdehnung und ohne öffentliche Regulierung einfach zu organisieren.

Geringe Zeittransparenz. Entwickelt für die Datenkommunikation zwischen Rechnern, bereitet die Erweiterung auf Sprachübertragung und Multimedia meist enorme Probleme.

Hohe Bitrate. Ermöglicht durch hochwertige Verkabelung und beschränkte räumliche Ausdehnung.

Dauerbetrieb möglich. Weil LANs üblicherweise ihren Benutzern gehören und somit keine Gebühren anfallen.

Verteilte Vermittlung. Das Markenzeichen der klassischen LANs, ebenso verteilter Zugriff. Heute dagegen: Switched LANs.

Zuverlässig.

Flexible in Verbindungstopologien. Es gibt keine in LANs unmögliche Verbindungstopologie.

Mehrere Netztopologien. Bus, Ring, Stern, Baum oder Kombinationen dieser reinen Topologien.

Siehe [2, Teil 2, Kap. 1.2].

18.3 Medienzugriffssteuerung: Definition und Verfahren

Aufgabe

1. Was versteht man unter »Medienzugriffssteuerung«?
2. Erläutern Sie die Verfahrensklassen »Zentrale Zugriffssteuerung«, »Wettbewerb« und »Reservierung«. Geben Sie jeweils ein Beispiel an und skizzieren Sie dessen Grundprinzip.

Quelle: [2, Teil 2, Kap. 1.5, Aufg.3].

Lösung

1. »Medienzugriffssteuerung« ist, den Zugriff mehrerer auf ein gemeinsames Übertragungsmedium zu koordinieren. Englisch: Medium Access Control (MAC).
2. Die wesentlichen Verfahrensklassen der Medienzugriffssteuerung, mit Beispiel:

Zentrale Zugriffssteuerung Funktioniert ähnlich Bussystemen: ein Arbiter koordiniert den Medienzugriff zentral. Beispiel: »Demand Priority« im 100VG-AnyLAN. Der Arbiter heißt dort Hub und arbeitet nach dem Abfrageprinzip (Polling). Er spricht die Stationen unter Berücksichtigung von Prioritäten einzeln an. Nur die jeweils angesprochene Station darf senden.

Wettbewerb Jede sendewillige Station darf senden, wenn sie das Medium für frei hält. Senden zwei Stationen gleichzeitig, werden die Pakete durch eine Kollision unbrauchbar. Kollisionen werden jedoch erkannt und die Pakete werden entsprechend einem Kollisionsauflösungsalgorithmus erneut übertragen. Beispiel: CSMA/CD im Ethernet. Netzausdehnung, Bitrate und Mindeststrahlenlänge sind dabei so abgestimmt, dass Kollisionen sicher erkannt werden können. Erkannte Kollisionen werden durch den probabilistischen Algorithmus »Truncated Binary Exponential Backoff« behandelt.

Reservierung Jede Station erhält Senderecht für eine festgelegte Maximalzeit. Die Stationen tauschen untereinander Steuerinformationen aus, um diese Reservierung vorzunehmen. Es gibt keinen zentralen Arbiter. Beispiel: Register-Einschub-Verfahren (Register Insertion) im Distributed Loop Computer Network (DLCN). Minirahmen kreisen in einem Ring, einer pro Zeitschlitz fester Länge. Freie Rahmen können von Stationen als belegt markiert und mit Daten beladen werden. Senden und Empfangen werden optimiert, indem während des Empfangs gesendet werden kann, anhängend gesendet werden kann und schon nach Prüfung des Zieladressfeldes ein Rahmen für andere Stationen weitergesendet werden kann.

Siehe [2, Teil 2, Kap. 1.3].

18.4 LAN-Referenzmodell

Aufgabe Skizzieren Sie das LAN-Referenzmodell. Geben Sie für jede Schicht deren Bezeichnung und Funktion(en) an und nennen Sie die Komponente bzw. das Gerät, in der diese Funktionen realisiert werden. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 1].

Lösung

Nr	Name	Aufgabe	Teilaufgaben
3c	Internet	Internetworking	teilnetzunabhängige Funktionen
3b	Subnetwork Enhancement	"	Anpassung an Internet-Teilschichten
3a	Subnetwork Access	"	teilnetzspezifische Funktionen
2b	Logical Link Control (LLC)		<ul style="list-style-type: none"> • Vermittlung • Multiplexen • Verbindungstypen LLC Typ 1-3 • Medienzugriffsverfahren
2a	Medium Access (MAC)		<ul style="list-style-type: none"> • MAC-Adressierung • Schnittstelle zur MAC-Schicht
1	Physical Signalling (PLS)	Bitübertragung	<ul style="list-style-type: none"> • Signalaufbereitung (Leitungskode, Modulation) • Sende- und Empfangsverfahren • Bitsynchronisation

Siehe [2, Kap. 2.2]. Schicht 3 heißt Internetworking-Schicht oder Netzwerk-Schicht. Hier ist das IP-Protokoll angesiedelt, alternativ das IPX-Protokoll oder Protokolle aus der ISO-Welt verwendet werden. ARP/RARP gehört auch zu Schicht 3.

18.5 Shared Medium LAN

Aufgabe Was versteht man unter einem *Shared-Medium-LAN*? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 2].

Lösung Shared Medium meint ein gemeinsam genutztes Medium. Alle Stationen im Netz teilen sich dasselbe Übertragungsmedium, z.B. ein Kabel oder einen Funkkanal. Die Stationen bekommen das Medium für eine kurze Zeit zugewiesen und geben es danach wieder frei. Das Gegenteil ist »Switched LAN«; dort wird das Medium durch Vermittlungsknoten in exklusiv statt gemeinsam genutzte Abschnitte geteilt. Shared Medium LANs arbeiten nach dem Prinzip der verteilten Vermittlung, Switched LANs nach dem der zentralen Vermittlung. Siehe [2, Teil 2, Kap. 1.2]

18.6 Grundaufbau eines Ethernet LANs

Aufgabe Skizzieren Sie den Grundaufbau eines Ethernet-LANs mit Koaxialkabeln als Übertragungsmedium. Erläutern Sie die Aufgaben der Komponenten *Repeater* und *Remote Repeater*. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 3].

Lösung

Repeater Um mehrere Busstrukturen zusammenzufassen, verwendet man einen Repeater. Ziel des Repeaters ist die Rückgewinnung des Signals hinsichtlich Takt, Signalform und Amplitude. Außerdem hat er Teilaufgaben des Medienzugriffs wie Kollisionserkennung und Senden des JAM-Signals.

Remote Repeater Liegen Busstrukturen örtlich 100m bis 1000m auseinander, verbindet man sie mit einem Remote Repeater. Dabei verbindet ein Link-Segment zwei Repeaterhälften. Das Link-Segment ist oft eine Glasfaserleitung.

Siehe [2, Teil 2, Kap. 2.4.1]. Zur verlangten Skizze siehe [2, Teil 2, Kap. 2.1].

18.7 Kurzbezeichnungen für Ethernet LANs

Aufgabe Erklären Sie die Kurzbezeichnung für Ethernet-LANs und geben Sie drei typische Beispiele an. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 4].

Lösung Nur für Ethernet, nicht für Token Ring und sonstige LAN-Typen, wurden solche Kurzbezeichnungen zur Kategorisierung eingeführt. Sie nennen die wichtigsten Leistungsmerkmale. Aufbau:

<Bitrate><Übertragungsverfahren><Segmentlänge>

Dabei wird die Bitrate in $Mbit \cdot s^{-1}$ und die Segmentlänge in Vielfachen von 100m angegeben. Segmentlänge ist die maximale Länge einer Busstruktur. Beim Übertragungsverfahren bedeutet BASE Basisbandübertragung und BROAD Breitbandübertragung, also modulierte Übertragung. Ab 10BASE-T wird statt der Segmentlänge das Übertragungsmedium in einem Buchstabenkode angegeben:

<Bitrate><Übertragungsverfahren>-<Übertragungsmedium>

Die drei Beispiele:

10BASE5 10MBit Bitrate, Übertragung im Basisband, Segmentlänge $5 \cdot 100m = 500m$. Das Ursprungs-Ethernet.

10BROAD36 10MBit Übertragungsrate, Übertragung im Breitband, Segmentlänge $36 \cdot 100m = 3600m$. Dies ist die einzige eingeführte Komponente, die nicht Übertragung im Basisband verwendet. Sie sollte zur Realisierung Lokaler Netze über Kabelfernsehkanaal dienen. Dieses System hat jedoch keine kommerzielle Bedeutung.

10BASE-T 10MBit Übertragungsrate, Übertragung im Basisband, Kabeltyp »Twisted Pair«.

Siehe [2, Kap. 2.3].

18.8 Slot-Time, Round Trip Delay und Mindestrahmenlänge

Aufgabe

1. Erläutern Sie die Begriffe »Slot-Time«, »Round Trip Delay« und »Mindestrahmenlänge«. Geben Sie die im Ethernetstandard festgelegten Werte für diese Größen an.
2. Ergänzen Sie:
 - Eine Vergrößerung der Bitrate erfordert eine der minimalen Paketlänge oder/und eine der maximalen Netzausdehnung.
 - Eine Vergrößerung der Netzausdehnung erfordert eine der minimalen Paketlänge oder/und eine der Bitrate.

Quelle: [2, Teil 2, Kap. 2.7, Aufg. 5].

Lösung

1. Slot-Time, Round Trip Delay und Mindestrahmenlänge:

Slot-Time $T_S = 51,2\mu s$. Es sind die kleinsten nutzbaren Zeiteinheiten im Ethernet, daher »Slot« (Schlitz). Die Slot-Time ist festgelegt als das zweifache der maximalen Signallaufzeit $\tau_{max} = 25,6\mu s$. Deshalb ist es die Zeit, die ein Sendevorgang mindestens beanspruchen muss, damit die sendende Station eine Kollisionen sicher erkennen kann. Daher ist die T_S auch die Zeit, um einen Rahmen der Länge l_{dmin} mit der Bitrate $v = 10MBit \cdot s^{-1}$ zu senden.

Round Trip Delay Synonym zu Slot-Time.

Mindestrahmenlänge $l_{dmin} = 512Bit = 64Byte$. So lang muss ein Rahmen mindestens sein, um eine Kollision sicher erkennen zu können.

2. Lückentext:

- Eine Vergrößerung der Bitrate erfordert eine *Vergrößerung* der minimalen Paketlänge oder/und eine *Verkleinerung* der maximalen Netzausdehnung.
- Eine Vergrößerung der Netzausdehnung erfordert eine *Vergrößerung* der minimalen Paketlänge oder/und eine *Verkleinerung* der Bitrate.

Der mathematische Zusammenhang macht es leichter, sich dies zu merken. Für eine sichere Kollisionserkennung soll stets gewährleistet sein:

$$l_{dmin} \stackrel{!}{\geq} v \cdot T_S \quad (1)$$

Um daraus eine Abhängigkeit von l_{dmin} , v und s_S zu erhalten, setzen wir ein $T_S = 2 \cdot \tau_{max} = 2 \cdot \frac{1}{c_L} \cdot s_S$:

$$\Rightarrow l_{dmin} \stackrel{!}{\geq} \frac{2}{c_L} \cdot v \cdot s_S \quad (2)$$

l_{dmin} minimale Rahmenlänge

v Bitrate

s_S Segmentlänge

T_S Slot Time

τ_{max} maximale Signallaufzeit

c_L Signalausbreitungsgeschwindigkeit im Medium, eine Konstante

Damit Gleichung 2 erfüllt bleibt, wenn ein Parameter geändert wird, müssen die beiden anderen wie in der Lösung zum Lückentext formuliert angepasst werden.

18.9 Prinzip bei CSMA/CD als Flussdiagramm

Aufgabe Erläutern Sie das Grundprinzip der Medienzugriffssteuerung bei CSMA/CD durch ein Flussdiagramm. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 6a].

Lösung Das gesuchte Flussdiagramm ist enthalten in [2, Teil 2, Kap. 2.4.2, Bild 2.4].

18.10 Kollisionserkennung bei 10BASE5

Aufgabe Wie erkennt man bei 10BASE5-LANs Kollisionen und was ist ein Kollisionsfragment? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 6b].

Lösung Kollisionen entstehen durch Überlagerung gleichzeitig gesendeter Signale. Die gerade sendende Station erkennt eine Kollision durch »Listen While Talking« (LWT). Die Station hört das Medium auch während des Sendevorgangs ab und vergleicht den Mittelwert der gesendeten Signale mit dem der empfangenen Signale. Der Mittelwert der gesendeten Signale ist ein Gleichspannungsanteil $U_0 \leq 1,293V$. Wenn der Mittelwert der empfangenen Signale $U_0 \geq 1,448V$ ist, so spricht die Schaltung zur Kollisionserkennung in der MAU an. Vereinfacht ausgedrückt: eine Kollision wird daran erkannt, dass etwas anderes empfangen als gesendet wird⁵. Die nicht sendenden Stationen erkennen Kollisionen am JAM-Signal, das jede sendende Station aussendet, wenn sie eine Kollision erkannt hat.

Kollisionsfragmente sind durch die Kollision unzerstörte Rahmenteile, die als Signale auf der Leitung bleiben. Nur Kollisionen erzeugen solche zerstörten Rahmen, Bitfehler ($p = 10^{-7}$) dagegen erzeugen gestörte Rahmen. Kollisionsfragmente beginnen möglicherweise als korrekter Ethernet-Rahmen, können von den Empfängern jedoch daran erkannt werden dass sie die minimale Rahmenlänge $l_{min} = 64Byte$ unterschreiten und werden dann verworfen.

Siehe [2, Teil 2, Kap. 2.4.2].

18.11 Backoff-Algorithmus

Aufgabe Was ist ein Backoff-Algorithmus? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 6c].

Lösung Mit einem Backoff-Algorithmus ermittelt eine Station nach einer Kollision die Wartezeit bis zum nächsten Sendeveruch. Ein Beispiel ist der Truncated Binary Exponential Backoff (TBEB), der Backoff-Algorithmus bei CSMA/CD. Die Wartezeit ist dabei eine Zufallszahl in einem Bereich, der von der Anzahl bisheriger Fehlversuche abhängt. Siehe [2, Teil 2, Kap. 2.4.2].

18.12 Kollisionsdomäne

Aufgabe Was ist eine Kollisionsdomäne und wodurch wird ihre maximale Ausdehnung bestimmt? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 6e].

Lösung Kollisionsdomäne heißt der Bereich eines Ethernets, in dem sich Kollisionen physikalisch ausbreiten können. Alle durch Repeater und Remote Repeater verbundenen Busstrukturen gehören zur selben Kollisionsdomäne, Bridges jedoch trennen Kollisionsdomänen. Bridges, Switches und Router trennen Kollisionsdomänen.

Die maximale Ausdehnung einer Kollisionsdomäne ist eine Vorschrift im Ethernet-Standard, die so gewählt wurde, dass eine sichere Kollisionserkennung gewährleistet ist. Dazu muss nach Gleichung 2 gelten:

$$s_S \leq \frac{1}{2} c_L \cdot \frac{l_{min}}{v} \quad (3)$$

Der Ethernet-Standard schreibt für 10BASE-T z.B. vor, dass eine Kollisionsdomäne aus einem Pfad von 5 Segmenten je maximal 100m aufgebaut sein darf, also eine Ausdehnung von maximal 500m haben kann. Siehe [2, Teil 2, Kap. 2.4.2].

18.13 Flussdiagramm beim Empfang eines Ethernet-Rahmens

Aufgabe »Entwickeln Sie ein Flussdiagramm für den Ablauf beim Empfang eines Ethernet-Rahmens.« Quelle: Aufgabe 7 aus einer alten, nicht mehr erhältlichen Version von [2, Teil 2, Kap. 2.7]. Auch in der neuen Version sollte diese Aufgabe wohl als Aufgabe 7 auftauchen, denn hier ist versehentlich überhaupt keine Aufgabe 7 enthalten.

Lösung

⁵Die Kollisionserkennung bei 10BASE-T ist einfacher: Signale auf dem Empfangsadernpaar während man selbst sendet sind eine Kollision.

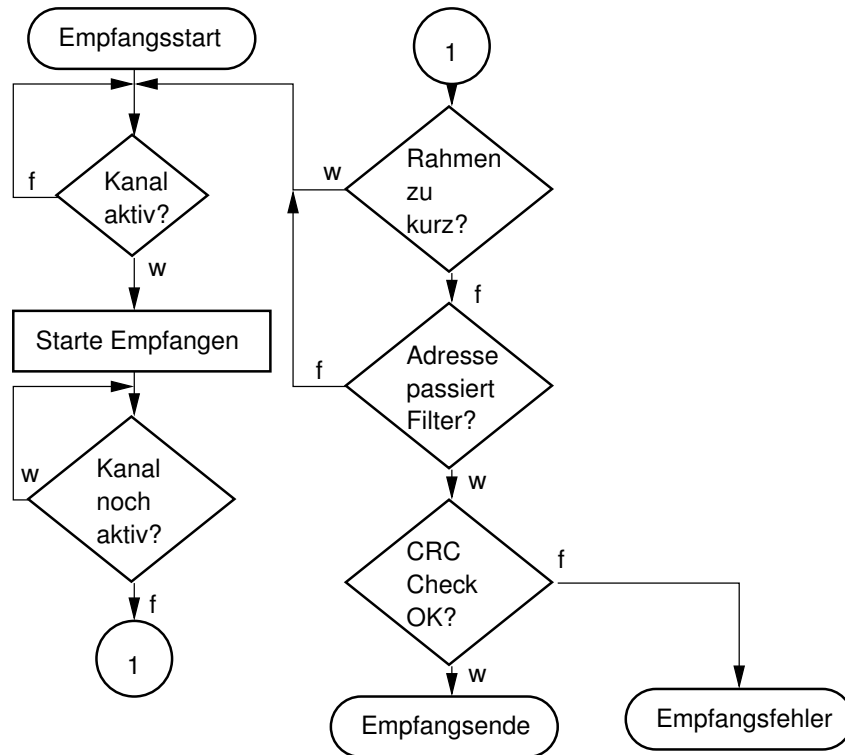


Abbildung 4: Zur Aufgabe »Flussdiagramm beim Empfang eines Ethernet-Rahmens«

18.14 Aufbau von Ethernet-Rahmen

Aufgabe

1. Skizzieren Sie den Aufbau eines Ethernet_802.3-Rahmens und erläutern Sie die Bedeutung der einzelnen Felder.
2. Worin unterscheiden sich ein Ethernet_802.3 und ein Ethernet_II-Rahmen?

Quelle: [2, Teil 2, Kap. 2.7, Aufg. 8a-b].

Lösung

1. Die Skizze zum Aufbau eines Ethernet_802.3-Rahmens ist [2, Teil 2, Kap. 2.4.3, Bild 2.6]. Darin bedeuten:

Präambel Eine Bytefolge von 7 Byte $0xAA$ dient zur Bit- und Rahmensynchronisation. Das achte Byte ist $0xAB$ und kennzeichnet den Rahmenbeginn (Start Frame Delimiter, SFD).

Empfängeradresse 6 Byte MAC-Adresse der Zielstation. Eine MAC-Adresse kann eine physikalische Adresse, eine Broadcastadresse oder eine Multicastadresse sein. Ein Empfangsfilter im Ethernet-Controller bestimmt, welche Pakete für die eigene Station relevant sind, der Rest wird verworfen.

Senderadresse 6 Byte MAC-Adresse der Quellstation. Beim Übergang in eine andere Kollisionsdomäne ersetzt der Router, die Bridge oder der Switch sie durch seine / ihre eigene MAC-Adresse in dieser Kollisionsdomäne.

Länge Die Länge der im Datenfeld enthaltenen Daten ohne Padding-Bytes, in Byte. Maximalwert 1500Byte .

Daten Enthält die transportierten Daten und evtl. Padding-Bytes, die das Datenfeld auf 46Byte und damit den Rahmen auf die minimale Rahmenlänge $l_{\text{min}} = 64\text{Byte}$ bringen.

Rahmenprüfbits Englisch Frame Check Sequence (FCS). Mit dem Generatorpolynom CRC-32 wird eine CRC-Sequenz erstellt, die alles vom Empfängeradressfeld bis zum Datenteil beinhaltet.

2. Ein Ethernet_II-Rahmen hat folgende Unterschiede zu einem Ethernet_802.3-Rahmen:

- Die Präambel besteht aus 8 Byte `0xAA`, es gibt also keinen Start Frame Delimiter.
- Das Längenfeld heißt hier Typ-Feld und identifiziert das Protokoll, mit dem die enthaltenen Daten in der Internetworking-Schicht zu interpretieren sind. Ethernet_802.3-Rahmen dagegen verwenden zu diesem Zweck die LLC-Schicht als zusätzliche Schicht.

Siehe [2, Teil 2, Kap. 2.4.3].

18.15 Aufbau einer MAC-Adresse

Aufgabe Woran erkennt man, ob es sich bei einer MAC-Adresse um eine Individual- oder um eine Gruppenadresse handelt? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 8c].

Lösung Ist das Individual/Group-Bit (I/G-Bit) einer MAC-Adresse 0, so handelt es sich um eine Individualadresse. Ist es 1, so handelt es sich um eine Gruppenadresse. Das I/G-Bit ist das MSB im ersten Byte jeder MAC-Adresse. Siehe [2, Teil 2, Kap. 2.4.3].

18.16 Aufbau der LLC-Schicht

Aufgabe Erläutern Sie die Aufgabe der LLC-Schicht und erklären Sie die Dienstypen LLC Typ 1 bis LLC Typ 3. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 9a].

Lösung Die LLC-Schicht im LAN-Referenzmodell (Schicht 2b) hat ähnliche Aufgaben wie die Sicherungsschicht im OSI-Referenzmodell (Schicht 2). Aufgrund der verteilten Vermittlung gibt es in LANs keine eigene Vermittlungsschicht, ihre Aufgaben sind ebenfalls in Schicht 2 (MAC-Schicht, LLC-Schicht) integriert. Im Einzelnen sind die Aufgaben der LLC-Schicht:

Übermittlung Die LLC-Schicht bietet hiermit den Dienst an, einen Rahmen anhand seiner MAC-Adresse zuzustellen. Dieser Dienst existiert in drei Typen und wird stets mit einem HDLC-ähnlichen Protokoll implementiert:

LLC Typ 1 Unbestätigter Datagrammdienst, d.h. verbindungslose ungesicherte Übermittlung. Die Sicherung muss von einer höheren Schicht übernommen werden, meist von TCP in der Transportschicht.

LLC Typ 2 Verbindungsorientierte Übermittlung. HDLC-ähnlicher Dienst mit Hilfe einer logischen Verbindung.

LLC Typ 3 Quittierter Datagrammdienst. Verbindungslose gesicherte Übermittlung; im Unterschied zu LLC Typ 1 werden unmittelbar Empfangsbestätigungen gesandt. Keine praktische Bedeutung.

Multiplexen Die LLC-Schicht stellt der Netzwerkschicht mehrere gemultiplexte Verbindungen zur Verfügung, jede an einem eigenen L-SAP, jede für ein anderes mögliches Protokoll der Netzwerkschicht. Die Nummer einer LLC-Verbindung identifiziert so das Protokoll, mit dem die Daten eines Ethernet_802.3-Rahmens zu interpretieren sind. Multiplexen ermöglicht es, Verbindungen mit unterschiedlichen Protokolltypen der Netzwerkschicht gleichzeitig zu haben.

Siehe [2, Teil 2, Kap. 2.4.5].

18.17 Aufgabe von L-SAP-Adressen

Aufgabe Erklären Sie den funktionalen Unterschied zwischen einer MAC-Adresse und einer L-SAP-Adresse. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 9b].

Lösung Protokollinstanzen der Netzwerkschicht realisieren ihre Verbindungen durch Dienste der LLC-Schicht. Die LLC-Schicht realisiert ihre Verbindungen durch Dienste der MAC-Schicht. Jede Schicht hat ihren Aufgaben entsprechend ihre eigene Art von Adressen:

- Eine MAC-Adresse identifiziert eine Station oder eine Gruppe von Stationen im Netz.
- Eine L-SAP-Adresse identifiziert eine Protokollinstanz oder eine Gruppe von Protokollinstanzen in einer Station. Die durch L-SAP adressierbaren Protokollinstanzen gehören zur Netzwerkschicht. Über sie wird mittelbar ein Anwendungsprozess oder eine Gruppe von Anwendungsprozessen in einer Station identifiziert.

MAC-Adressen dienen also der Zustellung eines Rahmens im Netz, L-SAP-Adressen danach der Zustellung seiner Daten innerhalb einer Station. [2, Teil 2, Kap. 2.4.5].

18.18 Arten von Encapsulation

Aufgabe Erklären Sie die funktionalen Begriffe:

1. Length Encapsulation
2. Type Encapsulation
3. Pure LLC Encapsulation
4. SNAP Encapsulation

Ordnen Sie jedem dieser Begriffe den entsprechenden Rahmentyp zu. Quelle: [2, Teil 2, Kap. 2.7, Aufg. 10].

Lösung

Length Encapsulation Verwendet von Ethernet_802.3-Rahmen = Ethernet_Raw-Rahmen. Die Daten werden ohne jede Angabe zum Protokolltyp transportiert. Nur ihre Länge wird im Längenfeld des Ethernet_802.3-Rahmens vermerkt.

Type Encapsulation Verwendet von Ethernet_II-Rahmen. Der Protokolltyp der transportierten Daten wird im Typ-Feld des Ethernet_II-Rahmens vermerkt.

Pure LLC Encapsulation Verwendet von Ethernet_802.2-Rahmen. Der Protokolltyp der transportierten Daten wird im nicht erweiterten LLC-Header durch die L-SAP-Adresse vermerkt.

SNAP Encapsulation Verwendet von Ethernet_SNAP-Rahmen. Der Protokolltyp der transportierten Daten wird im SNAP-Header vermerkt, einer Erweiterung des LLC-Headers, dessen Adressraum zu klein war. Im SNAP-Header geben die ersten drei Byte stets eine Organisation an, die letzten beiden bezeichnen das Protokoll mit einer von der Organisation definierten Codierung.

Siehe [2, Teil 2, Kap. 2.4.5-2.4.6].

18.19 Aufgaben von Komponenten und Schnittstellen im Ethernet

Aufgabe Erläutern Sie die Aufgaben der folgenden Komponenten/Schnittstellen eines Ethernet-Anschlusses:

1. Ethernet-Controller
2. Attachment Unit Interface - AUI
3. Medium Access Unit - MAU
4. Medium Dependent Interface - MDI

Quelle: [2, Teil 2, Kap. 2.7, Aufg. 12].

Lösung

1. Ethernet-Controller. Übernimmt die Aufgaben der folgenden Teilschichten:

- LLC (Logical Link Control)
- MAC (Medium Access Control)
- PLS (Physical Line Signalling)

2. Attachment Unit Interface - AUI. Übernimmt eine Teilaufgabe der Teilschicht PMA (Physical Medium Attachment), und zwar die Verbindung von Ethernet Controller und MAU mit einem Transceiverkabel. Der Ethernet Controller wird damit unabhängig von den Eigenschaften des Mediums und kann durch unterschiedliche MAUs für unterschiedliche Medientypen eingesetzt werden.

3. Medium Access Unit - MAU. Übernimmt zusammen mit dem AUI die Aufgaben der Teilschicht PMA (Physical Medium Attachment). Beinhaltet MDI und Transceiver. Aufgaben des Transceivers:

- Senden und Empfangen von Paketen im Basisband mit Manchesterkode.
- Medium abhören.
- Kollisionserkennung.
- SQE-Test
- Jabber-Schutzfunktion

4. Medium Dependent Interface - MDI. Ein Bestandteil der MAU, durch den die elektrische und mechanische Schnittstelle zum Medium genormt ist.

Siehe [2, Teil 2, Kap. 2.4.7].

18.20 SQE-Test

Aufgabe Welche Aufgabe hat der SQE-Test? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 12].

Lösung Nach jedem abgeschlossenen Sendevorgang überprüft die MAU mit dem SQE-Test (Signal Quality Error), ob ihre Schaltung zur Kollisionserkennung noch funktioniert. Siehe [2, Teil 2, Kap. 2.4.7].

18.21 Wozu Hubs?

Aufgabe Betrachtet wird das 10BASE-T-Ethernet. Welche Funktionen hat ein Hub? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 14a].

Lösung Ein Hub (engl. für »Radnabe«, »Sternverteiler«) ist in 10BASE-T-Ethernets ein Mutiport-Repeater. Für jeden Port, also für jedes angeschlossene Segment, hat er die Funktionen eines Repeaters:

- Das Signal hinsichtlich Takt, Signalform und Amplitude regenerieren.
- Kollisionen erkennen und dann das JAM-Signal aussenden.
- Eintreffende Signale an alle anderen Segmente senden.

Siehe [2, Teil 2, Kap. 2.5.2].

18.22 Der MDI-X-Port

Aufgabe Betrachtet wird das 10BASE-T-Ethernet. Was ist en MDI-X-Port? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 14b].

Lösung Das MDI (Medium Dependent Interface) bei 10BASE-T-Ethernet ist der RJ 45-Stecker. Ein MDI-X-Port ist ein Port eines Hubs oder Switches, der dieses Interface inkl. Crossover-Funktion (»X«) bietet. Diese ist dem Standard entsprechend für jeden Port eines Hubs oder Switches in der MAU ausgeführt, so dass Stationen mit 1:1-Kabel angeschlossen werden können. Eine Ausnahme ist der Uplink-Port: er stellt zusätzlich einen MDI-Port bereit. Siehe [2, Teil 2, Kap. 2.5.2].

18.23 Der Link-Integrity-Test

Aufgabe Betrachtet wird das 10BASE-T-Ethernet. Wozu dient der Link-Integrity-Test? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 14c].

Lösung Mit diesem Test stellt eine Station fest, ob sie an einen funktionierenden Übertragungsabschnitt mit mindestens einer anderen MAU angeschlossen wurde. Der Test besteht darin, bei freiem Übertragungsmedium periodisch ein Link-Test-Signal (Normal Link Pulse (NLP) mit $f = 1MHz$) zu senden und selbst solche von anderen MAUs zu erwarten. Werden davon 2 bis 10 korrekt empfangen, erkennt die MAU den Übertragungsabschnitt als korrekt und zeigt dies durch eine Link-LED an. Der Test zeigt eine physikalisch durchlässige Verbindung an, aber nicht ihre Qualität. Siehe [2, Teil 2, Kap. 2.5.2].

18.24 Die Auto-Negotiation-Funktion

Aufgabe Was leistet die Auto-Negotiation-Funktion? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 15].

Lösung Sie ermöglicht allen Stationen einer Kollisionsdomäne, die Übertragungscharakteristika entsprechend ihren gemeinsamen Möglichkeiten automatisch zu konfigurieren:

- Bitrate: 10, 100 oder $1000\text{Mbit} \cdot \text{s}^{-1}$. Jedoch nur bei Kupferkabeln als Übertragungsmedium.
- Halbduplexmodus bei Shared Medium LANs, Vollduplexmodus bei Switched LANs.
- Im Vollduplexmodus: Flusskontrolle ausgeschaltet oder eingeschaltet, symmetrisch oder asymmetrisch.

Siehe [2, Teil 2, Kap. 2.5.5].

18.25 Frame Extension und Frame Bursting

Aufgabe Was versteht man bei Gigabit-Ethernet unter *Frame Extension* und *Frame Bursting*? Was wird durch diese Maßnahmen bezweckt? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 16].

Lösung Die minimale Rahmengröße bei Gigabit-Ethernet beträgt 512Byte gegenüber 64Byte bei 10Mbit-Ethernet und 100Mbit-Ethernet. Diese Verlängerung war nötig, um trotz der höheren Bitrate im Shared Medium Betrieb eine angemessene Segmentlänge realisieren zu können. Es gibt zwei abwärtskompatible Möglichkeiten, 512Byte minimale Rahmenlänge zu erreichen:

Frame Extension An das CRC-Feld werden Symbole angehängt, die nicht mit Nutzdaten verwechselt werden können.

Frame Bursting Mehrere gleichzeitig anstehende kleine Rahmen werden unmittelbar hintereinander gesendet. Burst Limit ist 8192Byte .

Siehe [2, Teil 2, Kap. 2.5.4].

18.26 Komponenten und Merkmale des Switched-Ethernet

Aufgabe Switched-Ethernet.

1. Durch welche Funktionsmerkmale unterscheidet sich ein Switch von einem Hub?
2. Erklären Sie den Unterschied zwischen Layer-2- und Layer-3-Switching.
3. Was ist ein Mikrosegment und welche typischen Eigenschaften hat es?
4. Welche Performanz-Kenngrößen für Switches kennen Sie?
5. Was ist ein *Uplink-Port*?

Quelle: [2, Teil 2, Kap. 2.7, Aufg. 17].

Lösung

18.27 Wie funktioniert schleifenfreie Wegelenkung?

Aufgabe Was versteht man unter schleifenfreier Wegelenkung und wie erreicht man dieses Ziel? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 18a].

Lösung Switched LANs können gemaschte Netze sein. Das macht sie redundant, aber anfällig für Schleifen in den Routingtabellen, die ein Paket endlos zirkulieren lassen. Schleifenfreie Wegelenkung meint Verfahren, die solche Schleifen in den Routingtabellen verhindern.

Das Spanning Tree Protocol (STP) ist ein Beispiel eines solchen Verfahrens. Dabei wird die Netztopologie nur teilweise aktiviert, derart dass ein vollständiger Baum mit einem Wurzelknoten entsteht. Jeder Knoten hat danach genau einen Weg zum Wurzelknoten und wickelt darüber seinen Verkehr Richtung Wurzelknoten ab.

Siehe [2, Teil 2, Kap. 2.6.5].

18.28 Wurzel-Port

Aufgabe Was ist ein Wurzel-Port? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 19a].

Lösung Das Spanning Tree Protocol (STP) zur schleifenfreien Wegelenkung definiert für jeden Knoten genau einen Wurzelport. Es ist der Port des Knotens, über den der Weg mit den geringsten Kosten zum Wurzelknoten führt. Dies ist der einzige Weg des Knotens zum Wurzelknoten. Der Wurzelknoten selbst hat keinen Wurzelport. Siehe [2, Teil 2, Kap. 2.6.5].

18.29 designierter Knoten

Aufgabe Was ist ein designierter Knoten? Quelle: [2, Teil 2, Kap. 2.7, Aufg. 19b].

Lösung Das Spanning Tree Protocol (STP) zur schleifenfreien Wegelenkung bestimmt in jedem LAN⁶ genau einen der angeschlossenen Knoten als designierten Knoten. Es ist der Knoten (Switch oder Bridge), über aller Verkehr abgewickelt wird, der dieses LAN Richtung Wurzelknoten verlassen soll. Ein Knoten kann gleichzeitig in mehreren LANs designierter Knoten sein. Alle solchen LANs sind an je einem sog. designierten Port des designierten Knotens angeschlossen. Siehe [2, Teil 2, Kap. 2.6.5].

18.30 TCP-Checksum bei Ethernet nötig?

Aufgabe »Ist bei einer Übertragung über Ethernet, wo ja eine eigene CRC-Checksum verwendet wird, eine eigene Checksum der TCP-Pakete überhaupt noch nötig?« Quelle: eine Klausur von Prof. Dr. Bernd Müller, Fachbereich MNI, FH Gießen-Friedberg.

Lösung Ja, denn die CRC-Checksum in Ethernet-Rahmen bewirkt lediglich, dass fehlerhafte Rahmen verworfen werden. Es ist keinerlei Wiederanforderung enthalten (außer bei LLC-2). Das heißt, Ethernet selbst enthält keine Sicherungsschicht, es kann keine sichere Übertragung garantiert werden, wie für TCP erforderlich. Das muss mit den höheren Protokollschichten realisiert werden, hier TCP mit seiner Checksum.

Literatur

[1] Prof. Dr. Wolfgang Schmitt: Skript zu Rechnernetze 1. Dieses Skript enthält auch Stoff vom Beginn der Veranstaltung Rechnernetze 2, darin identisch zu [2]. Gliederung:

- Teil 1: Einführung
- Teil 2: Digitale Übertragungstechnik
- Teil 3: Systemarchitekturen für die offene Datenkommunikation
- Teil 4: Übertragungssteuerung

[2] Prof. Dr. Wolfgang Schmitt: Skript zu Rechnernetze 2. Dieses Skript enthält allen klausurrelevanten Stoff in ausreichender Tiefe für die Klausurvorbereitung. Es enthält alles, was in der Veranstaltung mit Beamer gezeigt wurde. Es besteht aus mehreren Teilen, die im Laufe der Veranstaltung verteilt wurden, aber auch nachträglich im Büro von Prof. Dr. Wolfgang Schmitt erhältlich sind:

- Teil 1: »Schichten, Dienste und Protokolle«. Dieser Teil des Skriptes ist 2003-12-01 vollständig..
- Teil 2: »Lokale Datenkommunikation«.
- Teil 3: »IP-Routing«. Dokument existiert nicht, Stoff wurde jedoch kurz behandelt. Der Stoff ist enthalten in [1], jedoch nicht klausurrelevant.
- Teil 4: »TCP und UDP«. Dokument existiert nicht, Stoff wurde jedoch kurz behandelt. Der Stoff ist nicht klausurrelevant.
- Teil 5: »Dienste und Protokolle der Anwendungsschicht«. Dokument existiert nicht, Stoff wurde nicht behandelt.
- Teil 6: »Netzsicherheit und Firewalls«. Dokument existiert nicht, Stoff wurde nicht behandelt.

⁶genauer: in jeder Kollisionsdomäne

- [3] Prof. Dr. W. Schmitt: »Rechnernetze II - WS 2003/2004 - Inhaltsübersicht«. Quelle: referenziert auf <http://homepages.fh-giessen.de/~hg6421/AbrufWS03.html>, direkter Link http://homepages.fh-giessen.de/%7Ehg6421/Rechnernetze_2/RNII_Inhalt.pdf.
- [4] Prof. Dr. Wolfgang Schmitt: Aufgaben zu Rechnernetze 2. Die Aufgaben bestehen aus mehreren Teilen, die im Laufe der Veranstaltung ausgeteilt wurden, aber auch nachträglich im Büro von Prof. Dr. Schmitt erhältlich sind:
- Teil 1: »Grundlagen der Protokolltechnik I - Beschreibung funktionaler Abläufe«.
 - Teil 2: »Grundlagen der Protokolltechnik II - Beschreibung funktionaler Abläufe mit SDL«
- [5] Prof. Dr. Wolfgang Schmitt: »Grundlagen der Protokolltechnik I - Beschreibung der funktionalen Abläufe - Lösungen«. Die Lösungen zu [4, Teil 1]. Sie enthalten Teile aus [4, Teil 1], jedoch nicht den Anhang mit hilfreichen Tabellen. Quelle: http://homepages.fh-giessen.de/~hg6421/Rechnernetze_2/Protokolltechnik_Loesung.pdf, referenziert auf <http://homepages.fh-giessen.de/~hg6421/AbrufWS03.html>.
- [6] Prof. Dr. Wolfgang Schmitt: »Rechnernetze II - WS 2003/2004 - Lokale Datenkommunikation - Lösungen zu den Aufgaben zur Lernkontrolle aus Abschnitt 2. 6.«. Dies sind Lösungen zu [2], Teil »Lokale Datenkommunikation«, Kapitel 2.7: »Aufgaben und Fragen zur Lernkontrolle«. Jedoch nur zu den sog. »*«-Aufgaben, d.i. zu solchen die mit Hilfe des Skriptes gelöst werden dürfen. Quelle: http://homepages.fh-giessen.de/~hg6421/Rechnernetze_2/LAN_Loesung.pdf, referenziert auf <http://homepages.fh-giessen.de/~hg6421/AbrufWS03.html>.
- [7] Comer: »Internets und Intranets«. Nach diesem Buch richtet sich diese Vorlesung. Nur im Bereich Lokale Netze wird die Thematik in dieser Veranstaltung intensiver behandelt.
- [8] Tanenbaum: »Lokale Netze«. Nach diesem Buch richtet sich der Teil »Lokale Netze« dieser Veranstaltung.
- [9] Jörg Rech: »Ethernet«. Aus diesem Buch stammen einige der in der Veranstaltung dargestellten Informationen.