Computernetze 1

Selbststudium v1.0

Kälin Thomas, Abteilung I
WS 06 / SS 07

VORWORT

Dieses Dokument behandelt den von Andreas Rinkel aufgetragenen Selbststudiumsteil. Die Texte wurden grösstenteils von Wikipedia und dem Buch „Vernetzte IT-Systeme" (ISBN 3-8237-1141-5). Ich übernehme keine Garantie für Vollständigkeit, bzw. Korrektheit dieser Daten. Verwendung erfolgt somit auf eigene Gefahr. ☺

Sollte jemand Fehler im Dokument finden, bitte ich Ihn, dies mir mittels E-Mail (tkaelin@hsr.ch) mitzuteilen.

1. OSI-Schichten

1.1. Schicht 1 – Bitübertragungsschicht

(engl. physical layer) Die Bitübertragungsschicht ist die unterste Schicht. **Diese Schicht stellt mechanische, elektrische und weitere funktionale Hilfsmittel zur Verfügung, um physikalische Verbindungen zu aktivieren / deaktivieren, sie aufrechtzuerhalten und Bits darüber zu übertragen**. Das können zum Beispiel elektrische Signale, optische Signale (Lichtleiter, Laser), elektromagnetische Wellen (drahtlose Netze) oder Schall sein. Die für sie verwendeten Verfahren bezeichnet man als übertragungstechnische Verfahren. Geräte und Netzkomponenten, die der Bitübertragungsschicht zugeordnet werden, sind zum Beispiel die Antenne und der Verstärker, Stecker und Buchse für das Netzkabel, der Repeater, der Hub, der Transceiver, das T-Stück und der Endwiderstand (Terminator).

Auf der Bitübertragungsschicht wird die digitale Bitübertragung auf einer leitungsgebundenen oder leitungslosen Übertragungsstrecke bewerkstelligt. Die gemeinsame Nutzung eines Übertragungsmediums kann auf dieser Schicht durch statisches **Multiplexen** oder dynamisches Multiplexen erfolgen. Dies erfordert neben den Spezifikationen bestimmter Übertragungsmedien (zum Beispiel Kupferkabel, Lichtwellenleiter, Stromnetz) und der Definition von Steckverbindungen noch weitere Elemente. Darüber hinaus muss auf dieser Ebene gelöst werden, **auf welche Art und Weise überhaupt ein einzelnes Bit übertragen werden soll.**

Damit ist Folgendes gemeint: In Rechnernetzen wird heute Information zumeist in Form von Bitfolgen übertragen. Selbstverständlich sind der physikalischen Übertragungsart selbst, zum Beispiel Spannungspulse in einem Kupferkabel im Falle elektrischer Übertragung, oder Frequenzen und Amplituden elektromagnetischer Wellen im Falle von Funkübertragung, die Werte 0 und 1 unbekannt. Für jedes Medium muss daher eine Codierung dieser Werte gefunden werden, beispielsweise ein Spannungsimpuls von bestimmter Höhe oder eine Funkwelle mit bestimmter Frequenz, jeweils bezogen auf eine bestimmte Dauer. Für ein spezifisches Netz müssen diese Aspekte präzise definiert werden. Dies geschieht mit Hilfe der Spezifikation der Bitübertragungsschicht eines Netzes.

- Hardware: Modem, Hub, Repeater
- Protokolle: keine

1.2. Schicht 2 – Sicherungsschicht

(engl. data link layer, auch: Abschnittssicherungsschicht, Verbindungssicherungsschicht, Verbindungsebene, Prozedurebene) **Aufgabe der Sicherungsschicht ist es, eine sichere, weitgehend fehlerfreie Übertragung, zu gewährleisten und den Zugriff auf das Übertragungsmedium zu regeln.** Dazu dient das Aufteilen des Bitdatenstromes in Blöcke und das Hinzufügen von Folgenummern und Prüfsummen. Durch Fehler verfälschte oder verloren gegangene Blöcke können vom Empfänger durch Quittungs- und Wiederholungsmechanismen erneut angefordert werden. Die Blöcke werden auch als Frames oder Rahmen bezeichnet.

Eine so genannte Flusskontrolle macht es möglich, dass ein Empfänger dynamisch steuert, mit welcher Geschwindigkeit die Gegenseite Blöcke senden darf. Die amerikanische Ingenieursorganisation IEEE sah die Notwendigkeit, für lokale Netze auch den konkurrierenden Zugriff auf ein Übertragungsmedium zu regeln, was im OSI-Modell nicht vorgesehen ist.

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

- Hardware: Bridge, Switch (Multiport-Bridge)
- Protokolle: Ethernet, Token Ring, FDDI

1.3. Schicht 3 – Vermittlungsschicht

(engl. network layer, auch: Paketebene) **Die Vermittlungsschicht sorgt bei leitungsorientierten Diensten für das Schalten von Verbindungen und bei paketorientierten Diensten für die Weitervermittlung von Datenpaketen.** Die Datenübertragung geht in beiden Fällen jeweils über das gesamte Kommunikationsnetz hinweg und schließt die Wegesuche (Routing) zwischen den

Netzknoten mit ein. Da nicht immer eine direkte Kommunikation zwischen Absender und Ziel möglich ist, müssen Pakete von Knoten, die auf dem Weg liegen, weitergeleitet werden. Weitervermittelte Pakete gelangen nicht in die höheren Schichten, sondern werden mit einem neuen Zwischenziel versehen und an den nächsten Knoten gesendet.

Zu den Aufgaben der Vermittlungsschicht zählen der Aufbau und die Aktualisierung von Routingtabellen, sowie die Flusskontrolle. Auch die Netzadressen gehören zu dieser Schicht. Da ein Kommunikationsnetz aus mehreren Teilnetzen unterschiedlicher Technologien bestehen kann, sind in dieser Schicht auch die Umsetzungsfunktionen angesiedelt, die für eine Weiterleitung zwischen den Teilnetzen notwendig sind.

- Hardware: Router, hochwertige Switches
- Protokolle: IP, IPX

1.4. Schicht 4 – Transportschicht

(engl. transport layer, auch: Ende-zu-Ende-Kontrolle, Transport-Kontrolle) **Zu den Aufgaben der Transportschicht zählen die Segmentierung von Datenpaketen und die Stauvermeidung (engl. congestion control)**. Die Transportschicht ist die unterste Schicht, die eine vollständige Ende-zu-Ende Kommunikation zwischen Sender und Empfänger zur Verfügung stellt. Sie bietet den anwendungsorientierten Schichten 5-7 einen einheitlichen Zugriff, so dass diese die Eigenschaften des Kommunikationsnetzes nicht zu berücksichtigen brauchen.

Fünf verschiedene Dienstklassen unterschiedlicher Güte sind in Schicht 4 definiert und können von den oberen Schichten benutzt werden, vom einfachsten bis zum komfortabelsten Dienst mit Multiplexmechanismen, Fehlersicherungs- und Fehlerbehebungsverfahren.

- Protokolle: TCP, UDP

1.5. Schicht 5 – Sitzungsschicht

(engl. session layer, auch: Kommunikationssteuerungsschicht, Steuerung logischer Verbindungen, Sitzungsebene) Um Zusammenbrüche der Sitzung und ähnliche Probleme zu beheben, stellt die Sitzungsschicht **Dienste für einen organisierten und synchronisierten Datenaustausch zur Verfügung**. Zu diesem Zweck werden Wiederaufsetzpunkte, so genannte Fixpunkte (Check Points) eingeführt, an denen die Sitzung nach einem Ausfall einer Transportverbindung wieder synchronisiert werden kann, ohne dass die Übertragung wieder von vorne beginnen muss.

1.6. Schicht 6 – Darstellungsschicht

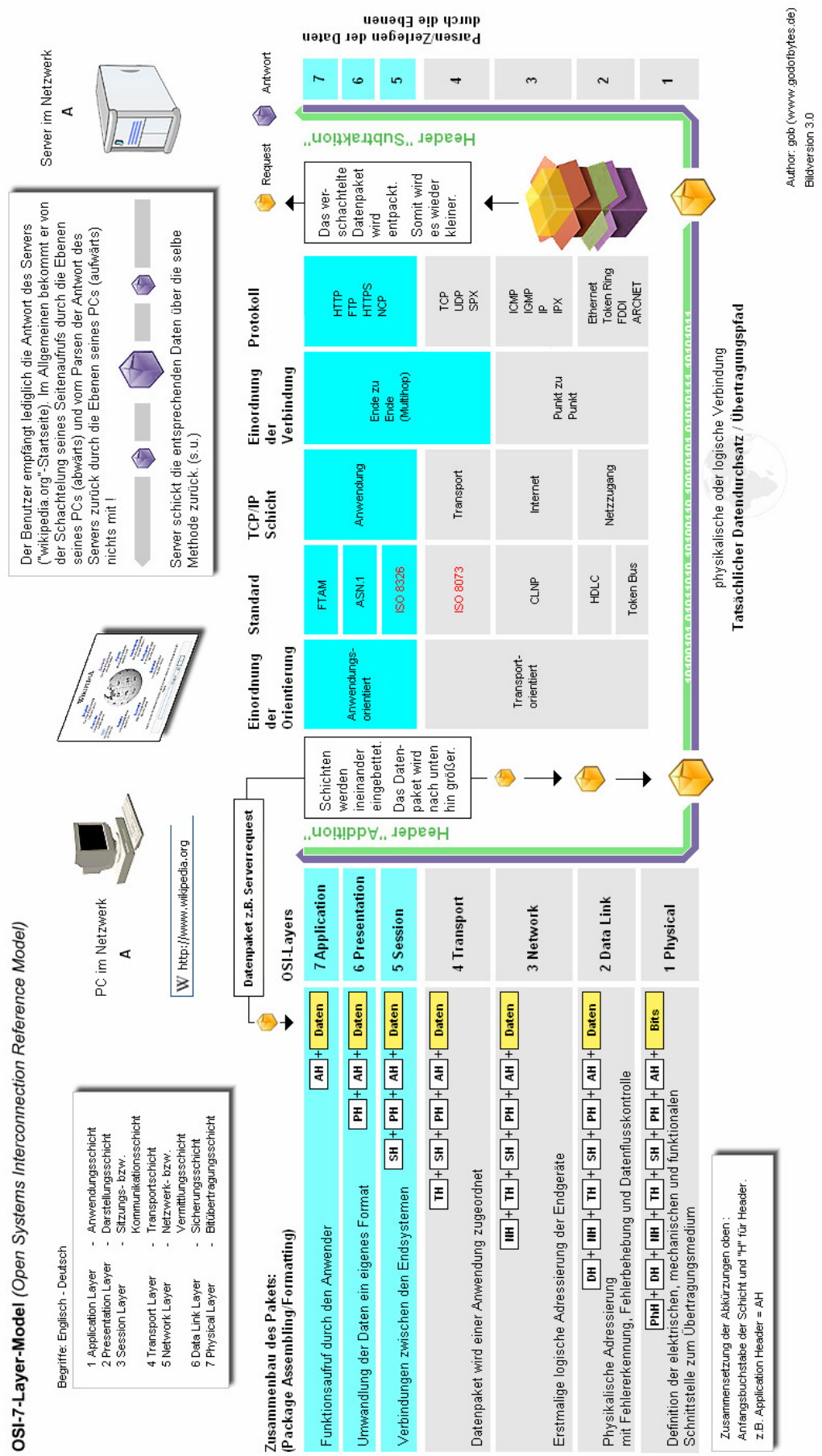
(engl. presentation layer, auch: Datendarstellungsschicht, Datenbereitstellungsebene) Die Darstellungsschicht setzt die systemabhängige Darstellung der Daten (zum Beispiel ASCII, EBCDIC) in eine unabhängige Form um und ermöglicht somit den syntaktisch korrekten Datenaustausch zwischen unterschiedlichen Systemen. Auch Aufgaben wie die **Datenkompression und die Verschlüsselung gehören zur Schicht 6**. **Die Darstellungsschicht gewährleistet, dass Daten, die von der Anwendungsschicht eines Systems gesendet werden, von der Anwendungsschicht eines anderen Systems gelesen werden können**. Falls erforderlich, agiert die Darstellungsschicht als Übersetzer zwischen verschiedenen Datenformaten, indem sie ein für beide Systeme verständliches Datenformat verwendet.

1.7. Schicht 7 – Anwendungsschicht

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

- Protokolle: HTTP, FTP

1.8. Beispiel Webseitenaufruf



2. Ethernet

2.1. Einleitung

Ethernet ist eine kabelgebundene Datennetztechnologie für lokale Datennetze (LANs). Sie ermöglicht den Datenaustausch in Form von Datenrahmen zwischen allen in einem lokalen Netz (LAN) angeschlossenen Geräten (Computer, Drucker, etc.). In seiner traditionellen Ausprägung erstreckt sich das LAN dabei nur über ein Gebäude. Ethernet-Technologie verbindet heute jedoch auch Geräte über weite Entfernungen.

Ethernet umfasst in verschiedenen Ausprägungen Festlegungen für Kabeltypen und Stecker, beschreibt die Signalisierung für die Bitübertragungsschicht und legt Paketformate und Protokolle fest. **Aus Sicht des OSI-Modells spezifiziert Ethernet sowohl die physikalische Schicht (OSI Layer 1) als auch die Data-Link-Schicht (OSI Layer 2)**. Ethernet ist weitestgehend in der IEEE-Norm 802.3 standardisiert. Es wurde ab den 1990ern zur meistverwendeten LAN-Technologie und hat alle anderen LAN-Standards wie Token Ring verdrängt, bzw. zu Nischenprodukten für Spezialgebiete gemacht. Ethernet kann die Basis für Netzwerkprotokolle, wie z. B. AppleTalk, DECnet, IPX/SPX oder TCP/IP bilden.

2.2. Bitübertragungsschicht (OSI Layer 1)

Ethernet basiert auf der Idee, dass die Teilnehmer eines LANs Nachrichten durch eine Art Funk-System versenden, allerdings nur innerhalb eines gemeinsamen Leitungsnetzes, das manchmal als Äther bezeichnet wurde (der Äther war in der Vorstellung des 19. Jahrhunderts der Stoff, durch den sich das Licht hindurch bewegte). Jeder Teilnehmer hat einen global eindeutigen 48-bit-Schlüssel, der als seine MAC-Adresse bezeichnet wird. Dies soll sicherstellen, dass alle Systeme in einem Ethernet unterschiedliche Adressen haben. Ethernet überträgt die Daten auf dem Übertragungsmedium dabei im so genannten Basisbandverfahren, d. h. in digitalem Zeitmultiplex.

2.3. CMSA/CD

In der Praxis funktioniert dieser Algorithmus bildlich wie eine Party, auf der alle Gäste ein gemeinsames Medium (die Luft) benutzen, um miteinander zu sprechen. Bevor sie zu sprechen beginnen, warten sie höflich darauf, dass der andere Gast zu reden aufgehört hat. Wenn zwei Gäste zur gleichen Zeit zu sprechen beginnen, stoppen beide und warten für eine kurze, zufällige Zeitspanne, in der Hoffnung, dass beide nicht wieder zur gleichen Zeit weitersprechen, und vermeiden so eine weitere Kollision.

Damit die Kollision festgestellt und eine Sendewiederholung initiiert werden kann, müssen die Datenframes abhängig von der Leitungslänge eine bestimmte Mindestlänge haben. Diese ergibt sich aus der physikalischen Übertragungsgeschwindigkeit (ca. 2/3 Lichtgeschwindigkeit) und der Übertragungsrate. Bei einer Übertragungsrate von 10 Mbit/s und einer maximalen Entfernung von 2,5 km zwischen zwei Stationen ist eine Mindestlänge von 64 Byte vorgeschrieben. Kleinere Datenframes müssen entsprechend aufgefüllt werden.

2.4. Broadcoast / Sicherheit

Da die gesamte Kommunikation auf derselben Leitung passiert, wird jede Information, die von einem Computer gesendet wurde, von allen empfangen. Diese Tatsache kann von Protokollen auf höheren Schichten genutzt werden, um **Broadcast- (dt. Rundruf)-Nachrichten** an alle angeschlossenen Systeme zu senden. Bei TCP/IP beispielsweise verwendet das ARP-Protokoll einen derartigen Mechanismus für die Auflösung der Schicht-2-Adressen.

Andererseits werden **Unicast-Nachrichten** (also für genau einen Empfänger) ebenso von allen angeschlossenen Computern empfangen. Die meisten Ethernet-verbundenen Geräte müssen ständig Informationen ausfiltern, die nicht für sie bestimmt sind. Dies ist eine Sicherheitslücke von Ethernet, da ein Teilnehmer mit bösen Absichten den gesamten Datenverkehr auf der Leitung mitschneiden kann, wenn er möchte. Eine häufig verwendete Abhilfe ist der Einsatz von Kryptographie (Verschlüsselung) auf höheren Protokollebenen.

In modernen, größeren Installationen werden fast ausschließlich Switches eingesetzt. Der Sicherheitsmangel wird durch die Einrichtung einer geswitchten Umgebung (wobei Switches anstatt

Hubs als Zentralstücke benutzt werden) verringert, jedoch nicht behoben. Ein möglicher Angriff auf ein geswitchtes Ethernet ist das ARP-Spoofing oder MAC-Flooding.

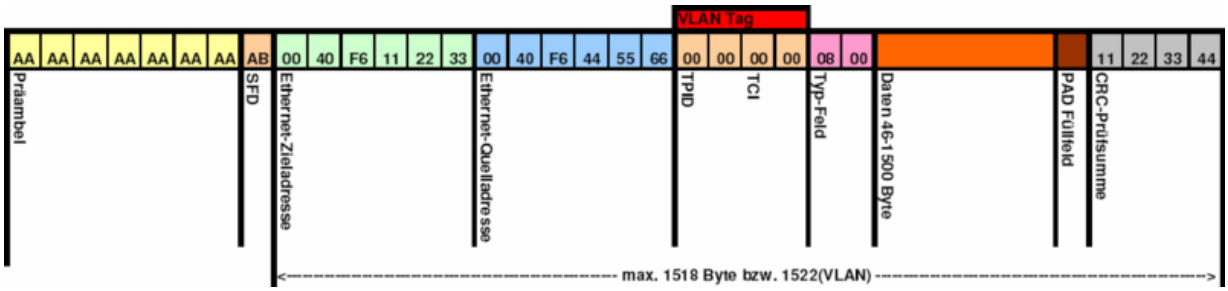
2.5. Keep-Alives

Keepalive-Nachrichten werden in Ethernet-Netzwerken verwendet, um sicherzustellen, dass eine physikalische Verbindung nicht zwischenzeitlich unterbrochen wurde. Da Ethernet ein Shared Medium ist, wird jedoch nicht überprüft, ob eine Verbindung zu einem bestimmten Teilnehmer besteht, sondern lediglich, ob Lese- und Schreibzugriff auf das Medium (OSI-Schicht 1) möglich ist. Hierzu wird ein Frame mit der eigenen MAC-Adresse im Absender- als auch Empfänger-Feld sowie dem Wert 0x9000 im EtherType-Feld gesendet. Der unmittelbare Empfang des gerade versendeten Frames stellt sicher, dass die Ethernet-Hardware korrekt funktioniert, und dass die Integrität des Übertragungsmediums sichergestellt werden kann.

2.6. Verbesserungen

Ethernet als gemeinsames Medium funktioniert gut, solange das Verkehrsaufkommen niedrig ist. Da die Chance für Kollisionen proportional mit der Anzahl der Transmitter und der zu sendenden Datenmenge ansteigt, tritt oberhalb von 50 % Auslastung vermehrt ein als Congestion bekanntes Phänomen auf, wobei regelrechte Staus entstehen und eine vernünftige Arbeit mit dem Netzwerk nicht mehr möglich ist. Um dies zu lösen und die verfügbare Bandbreite zu maximieren, wurde das Switched Ethernet entwickelt. Im Switched Ethernet werden Hubs durch Switching Hubs (Switch) ersetzt. Dadurch wird die Kommunikation im Full-Duplex-Modus möglich, d. h. Daten können gleichzeitig gesendet und empfangen werden. Außerdem wird die Collision Domain in mehrere kleinere Collision Domains (meist eine pro Peer) zerteilt, was die Anzahl an Kollisionen reduziert bzw. Kollisionen gänzlich vermeidet.

2.7. Frame-Aufbau



2.7.1. Die Präambel und SFD

Die Präambel besteht aus einer 7 Byte langen alternierenden Bitfolge (101010...1010), die der Synchronisation der Netzwerkgeräte dient. So können sich die beteiligten Geräte im Netzwerk auf eine eingehende Datenübertragung vorbereiten und sich auf den Takt des Signals synchronisieren. Anschließend folgt das eine Byte große Start Frame Delimiter (SFD). Dieses Feld (10101011) setzt die Präambel fort, die beiden letzten Bits stehen auf 1.

2.7.2. Ziel- und Quell- MAC-Adresse

Die Zieladresse identifiziert den Zielrechner, der die Daten empfangen soll. Diese Adresse kann auch eine Multicast- / Broadcast-Adresse sein. Die Quelladresse identifiziert den Sender. Jede MAC-Adresse der beiden Felder hat eine Länge von sechs Byte.

2.7.3. VLAN-Tag

Nur im Tagged-MAC-Frame folgen zusätzlich 4 Bytes als VLAN Tag. Die ersten beiden enthalten die Konstante 0x8100 (=802.1qTagType) die einen Tagged-MAC-Frame als solchen kenntlich machen. Von der Position her würde hier im Basic-MAC-Frame das Feld Ethertype stehen. Den Wert 0x8100 kann man damit auch als Ethertype für Vlan-daten ansehen. In den nächsten beiden Bytes stehen dann 3 Bitwerte für die Vlan-Priority, 1Bit Canonical Format Indicator und 12 Bit für die Vlan-ID.

2.7.4. Das Typ-Feld

Gibt Auskunft über das verwendete Protokoll der nächsthöheren Schicht innerhalb der Nutzdaten. Die Werte sind immer größer als 0x0600 (ansonsten ist das ein Ethernet-I-frame mit Längenfeld in dieser Position). Der spezielle Wert 0x8100 zur Kennzeichnung eines VLAN-Tags ist im Wertevorrat von Type reserviert.

2.7.5. Die Nutzdaten

Die Nutzdaten können pro Datenblock zwischen 0 und 1500 Byte lang sein. Sie sind die eigentlichen Informationen, die übertragen werden sollen. Die Nutzdaten werden von dem unter Type angegebenen Protokoll interpretiert.

2.7.6. Das PAD-Feld

Wird verwendet um den Ethernet-Rahmen auf die erforderliche Minimalgröße von 64 Byte zu bringen. Dies ist wichtig, um Kollisionen sicher zu erkennen. Präambel und SFD (8 byte) werden bei der erforderlichen Mindestlänge des Frames nicht mitgezählt, wohl aber ein VLAN Tag. Ein PAD-Feld wird erforderlich wenn als Nutzdaten weniger als 46 (bei einem Tagged-Frame 42) Byte zu übertragen sind. 6-Byte-Zieladresse + 6-Byte-Quelladresse + 4-Byte-VLAN-TAg + 2-Byte-Typfeld + 42-Byte-Nutzdaten + 4-Byte-CRC = 64-Byte-Mindestlänge. Das in Type angegebene Protokoll muss dafür sorgen, dass diese als Pad angefügten Bytes nicht interpretiert werden.

2.7.7. FCS (Frame Check Sequence)

Das FCS Feld stellt eine 32-Bit-CRC-Prüfsumme dar. Die FCS enthält die Prüfung des gesamten Frames, ab Zieladresse. Die Präambel, der SFD und die FCS selbst sind nicht in der FCS enthalten. Wenn ein Paket beim Sender erstellt wird, wird eine CRC-Berechnung über die gesamte Bitfolge außer der Präambel durchgeführt und die Prüfsumme an den Datenblock angehängt. Der Empfänger führt nach dem Empfang die selbe Berechnung aus. Kommt ein Rest bei der Polynomdivision heraus, geht der Empfänger von einer fehlerhaften Übertragung aus und der Datenblock wird verworfen. Zur Berechnung der CRC-32 werden die ersten 32 Bits der Mac-Adresse invertiert (zur Erkennung von fehlenden Nullen in den ersten Bits) und das Ergebnis ebenfalls invertiert (Vermeidung des Nullproblems).

2.8. Medientypen

2.8.1. 10Base2 (Cheapernet)

Koaxialkabel (RG58) mit einem Wellenwiderstand von 50 Ohm verbindet die Teilnehmer miteinander, jeder benutzt ein BNC-T-Stück zur Anbindung seiner Netzwerkkarte. An den beiden Leitungsenden sitzen **Abschlusswiderstände**. Ein Segment (das sind alle durch die BNC-T-Stücke miteinander verbundenen Koaxialkabelstücke) darf **maximal 185 Meter** lang sein. Es dürfen **maximal 30 Teilnehmer** angeschlossen werden. Zwischen 2 Teilnehmern müssen mindestens 0,5 Meter Abstand bestehen. Die Transceiver sind in der NIC (Network Interface Card) integriert. Der Abstand vom T-Stück bis zur Netzwerkkarte darf nur wenige Zentimeter betragen. Mittels Repeater können bis zu 4 weitere Netzwerksegmente angeschlossen werden. Damit ist eine maximale Gesamtlänge von 925m erreichbar.

2.8.2. 10Base5 (YellowCable)

Ein früher IEEE-Standard, der ein 10 mm dickes Koaxialkabel (RG8) mit einem Wellenwiderstand von 50 Ohm verwendet. Zum Anschluss von Geräten muss mittels einer Bohrschablone ein Loch in das Kabel gebohrt werden, durch das ein Kontakt einer Spezialklemme (Vampirklemme) des Transceivers eingeführt und festgeklammert wird. An diesen Transceiver wird mittels der AUI-Schnittstelle über ein Verbindungskabel die Netzwerkkarte des Computers angeschlossen. Dieser Standard bietet **10 Mbit/s** Datenrate bei Übertragung im Base-Band und **500 m Reichweite** mit **maximal 100 Teilnehmern**. Die Leitung hat keine Abzweigungen, und an den Enden sitzen **50 Ohm Abschlusswiderstände**. Dieser Typ ist eigentlich obsolet, aber aufgrund seiner weiten Verbreitung in den frühen Tagen noch immer in einigen Systemen in Benutzung.

2.8.3. 10Base-T (Twisted Pair)

Läuft über vier Adern (zwei **verdrillte Paare**) eines CAT-3 oder CAT-5-Kabels. Ein Hub oder Switch sitzt in der Mitte und hat für jeden Teilnehmer einen Port. Die Übertragungsgeschwindigkeit ist **10MBit/s** und die **maximale Länge eines Segments 100 Meter**. Diese Konfiguration wird auch für 100Base-T benutzt. Physikalisch sind die Steckverbindungen als 8P8C-Modularstecker und -buchsen ausgeführt, die häufig auch falsch als „RJ-45"- bzw. „RJ45"-Stecker/-Buchsen bezeichnet werden.

2.8.4. 100Base-T (Fast Ethernet)

Allgemeine Bezeichnung für die drei **100 Mbit/s-Ethernetstandards** über **Twisted-Pair-Kabel**, 100Base-TX, 100Base-T4 und 100Base-T2. Die maximale Länge eines Segments beträgt wie bei

10Base-T **100 Meter**. Die Steckverbindungen sind als 8P8C-Modularstecker und -buchsen ausgeführt und werden häufig falsch mit „RJ-45" bzw. „RJ45" bezeichnet.

2.8.5. 1000Base-T (Gigabit Ethernet)

1 Gbit/s über Kupferkabel ab Cat 5-Kabel. Die maximale Länge eines Segments beträgt wie bei 10/100Base-T **100 Meter**. Wichtige Merkmale des Verfahrens sind:

- Nutzung aller 4 Doppeladern in beide Richtungen (Echokompensation)
- Modulationsverfahren 5-PAM (Pulsamplitudenmodulation mit fünf Zuständen) übermittelt 2 Bit pro Schritt und Adernpaar
- Einsatz einer Trellis-Codierung und Scrambling
- Schrittgeschwindigkeit 125 MBaud pro Adernpaar
- Übertragungsfrequenz von 62,5 MHz
- Vollduplexbetrieb

3. CSMA/CD

3.1. Einleitung

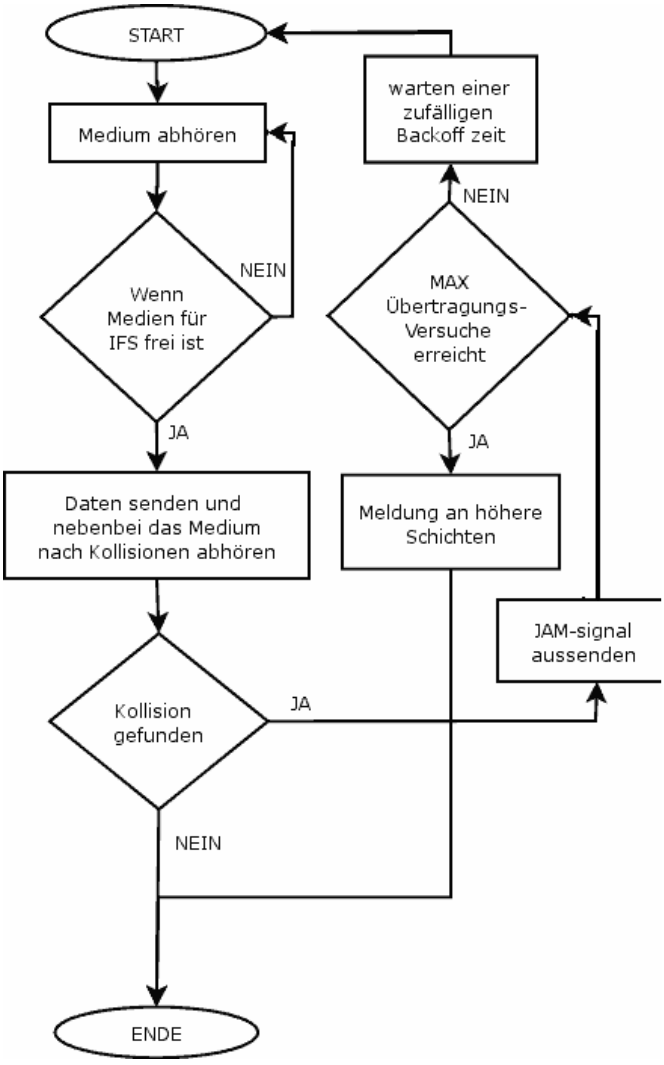
Der englische Begriff **Carrier Sense Multiple Access/Collision Detection (CSMA/CD)** bezeichnet ein Medienzugriffsverfahren, das den Zugriff verschiedener Stationen auf ein gemeinsames Übertragungsmedium im Zeitmultiplexverfahren (TDMA) beschreibt. Verwendung findet CSMA/CD beispielsweise im Bereich der Computernetzwerke beim Ethernet und ist dort als IEEE 802.3 standardisiert worden. Bei Wireless LANs oder dem im Automobilbereich verwendeten CAN-Bus wird ein ähnlicher Mechanismus namens CSMA/CA benutzt.

3.2. Kollisionen

Bei Netzwerkverfahren wie Ethernet findet eine Datenübertragung in Datagrammen (Datenframes) statt. Es wird kein endloser Datenstrom erzeugt. So wird es einerseits möglich, dass mehrere Stationen dasselbe Medium (z.B. Kabel) verwenden, andererseits entsteht dadurch die Gefahr von Kollisionen.

Da es nicht vorherbestimmt ist, zu welchem Zeitpunkt eine Station zu senden hat, **kann es geschehen, dass mehrere Sendestationen zum selben Zeitpunkt senden möchten**, wodurch sich die beiden Signale überlagern und somit stören: Keine der Stationen kann etwas Brauchbares senden. CSMA/CD ist ein Verfahren, um auf auftretende Kollisionen zu reagieren und zu verhindern, dass sie sich wiederholen.

3.3. Protokollablauf



1. **Carrier Sense = auf Signal horchen:** Zuerst muss das Medium überwacht werden.

2. Wenn das Medium eine bestimmte Zeit lang (IFS = Inter Frame Space) frei ist, beginne mit der Übertragung, andernfalls weiter mit Schritt 5.

3. **Informationsübertragung,** zugleich wird das Medium fortwährend weiter abgehört. Wenn hierbei eine Kollision entdeckt wird, beende die Datenübertragung und setze ein definiertes Störsignal (JAM) auf die Leitung (um sicherzustellen, dass alle anderen Transceiver die Kollision ebenfalls erkennen), dann weiter mit Schritt 5.

4. **Übertragung erfolgreich abgeschlossen:** Erfolgsmeldung an höhere Netzwerkschichten, Übertragungsmodus verlassen.

5. **Leitung ist belegt:** Warten, bis die Leitung wieder frei ist.

6. **Leitung ist gerade frei geworden.** Noch eine zufällige Zeit (Backoff) abwarten, dann wieder bei Schritt 1 beginnen, wenn die maximale Anzahl von Übertragungsversuchen nicht überschritten wurde.

7. **Maximale Anzahl von Übermittlungs-versuchen überschritten:** Fehler an höhere Netzwerkschichten melden, Übertragung abbrechen. Üblicherweise nach 16 Versuchen der Fall.

3.4. Backoff (Wartezeit)

Muss die Übertragung wegen eines Konflikts abgebrochen werden, so käme es unmittelbar zu einem erneuten Konflikt, wenn die beteiligten Sendestationen sofort nach dem Abbruch erneut senden würden. **Sie müssen daher im Idealfall eine unterschiedlich lange Pause einlegen**, sodass die Stationen eine Sendereihenfolge zugeordnet bekommen.

Bei Ethernet wählen die Konfliktparteien hierzu eine zufällige ganze Zahl z, welche von den bereits aufgetretenen Kollisionen abhängt. Die Sendestation wartet nun den Zeitraum von z * Slot-Time ab und sendet danach erneut, falls das Medium frei ist. Hat keine andere Station dasselbe z gezogen, gibt es also keinen Konflikt mehr.

Da die Streuung der möglichen Wartezeiten exponentiell mit der Anzahl der aufgetretenen Konflikte wächst, ist die Wahrscheinlichkeit sehr gering, dass viele Konflikte hintereinander auftreten, da die Konfliktparteien hierzu regelmäßig dieselbe Zufallszahl ziehen müssten. Daher wird nach 16 Konflikten in Folge der Sendeversuch abgebrochen und ein Systemfehler angenommen.

Der Nachteil der Methode ist, dass rechnerisch keinerlei Garantie herrscht, dass ein Paket zu einem bestimmten Zeitpunkt bereits angekommen ist. Der Übertragungserfolg hat lediglich eine gewisse Wahrscheinlichkeit. Das Verfahren ist also nicht echtzeitfähig, wie es etwa bei Token Ring der Fall ist.

3.5. Kollisionen verhindern

Aufgrund der auftretenden Kollisionen ist es nicht möglich, die theoretische Übertragungskapazität eines Mediums voll auszuschöpfen. In der Praxis kann man davon ausgehen, dass sich im günstigsten Fall etwa 70% der Nominalleistung erzielen lassen, unter ungünstigeren Bedingungen sind es unter 30%. Die Ursache ist einfach: **Je mehr Rechner sich im Netzwerk beteiligen und je höher die Auslastung steigt, desto mehr Kollisionen treten auf, folglich sinkt der reell erzielte Datendurchsatz deutlich ab.**

Nutzen nur zwei Stationen dasselbe Übertragungsmedium, schafft der Duplex-Betrieb Abhilfe. Bei Ethernet kann das Medium mittels Switch oder Bridge in mehrere Kollisionsdomänen aufgeteilt werden. Dann können pro Segment oder Kollosionsdomäne zwei Knoten (Stationen) im Duplex-Betrieb aktiv sein, ohne dass es zu Kollisionen kommt.

4. CSMA/CA

4.1. Einleitung

Der englische Begriff **Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)** bezeichnet ein Prinzip für den Zugriff mehrerer Netzwerkstationen auf dasselbe Übertragungsmedium. Es wird häufig u.a. bei drahtlosen Netzwerken (Wireless LANs) eingesetzt, findet aber abgewandelt auch bei Technologien wie ISDN Anwendung. Anders als bei CSMA/CD werden Kollisionen vermieden, statt diese zu erkennen.

4.2. Motivation für CMSA/CA bei Funknetzen

Drahtlose Netze unterscheiden sich im Bezug auf den gemeinsamen Medienzugriff durch zwei wichtige Faktoren von drahtgebundenen Netzen:

- Der Netzadapter ist nicht notwendigerweise Voll-Duplex-fähig. **Während einer eigenen Übertragung kann das Medium nicht überwacht werden**. Der Einsatz eines "Collision Detection"-Mechanismus, wie er etwa von CSMA/CD vorgesehen ist und bei Ethernet verwendet wird, würde dann fehlschlagen. Deswegen wurde CSMA/CD zu einem Mechanismus weiterentwickelt, der konsequenter dem Prinzip "listen before talk" ("erst hören, dann sprechen") folgt. An die Stelle der Kollisionserkennung ("CD") sollte die (bestmögliche) Kollisionsvermeidung ("CA") treten. Dadurch lassen sich gleichzeitige Datenübertragungen zwar nicht völlig verhindern, aber doch minimieren.
- Die Reichweite des Signals ist stark begrenzt, da die Signalstärke quadratisch mit der Entfernung abnimmt. Deshalb kann es zu Effekten wie "versteckten" oder "ausgelieferten" Endgeräten kommen.

4.2.1. Verstecktete Endgeräte

Zu einem versteckten Endgerät kommt es zum Beispiel bei folgendem Szenario: Die zwei Funkteilnehmer A und C liegen räumlich so weit auseinander, dass sie ihre Funksignale gegenseitig nicht empfangen können. Zwischen ihnen liegt die Station B. A und C senden nun zeitgleich an B und erzeugen dort einen Konflikt, können diesen aber nicht erkennen, da die Funksignale des jeweils anderen sie ja nicht erreichen. A ist für C ein verstecktes Endgerät und umgekehrt.

4.2.2. Ausgeliefertes Endgerät

Unter einem ausgelieferten Endgerät versteht man, wenn in unserem vorliegenden Szenario die Station B an A sendet und nun C an irgendeine andere Station (nicht A oder B) senden möchte. C erkennt die Signale von B und wartet, bis die Übertragung zwischen B und A vorbei ist. Da die Funkwellen von C aber A gar nicht erreichen können, wäre es gar nicht nötig zu warten: bei A könnte gar kein Konflikt auftreten. Dennoch ist C den anderen beiden Stationen ausgeliefert.

4.3. Protokollablauf

1. Zuerst wird das Medium abgehört ("Carrier Sense")
2. Ist das Medium für die Dauer eines IFS (Inter Frame Space) frei, wird gesendet. IFS wird je nach Sendeart gewählt.
3. Ist das Medium belegt, wird auf einen freien IFS gewartet und zur Kollisionsvermeidung zusätzlich um eine zufällige Backoff-Zeit verzögert.
4. Wird das Medium während der Backoff-Zeit von einer anderen Station belegt, bleibt der Backoff-Timer so lange stehen und wird nach Freiwerden des Mediums weitergezählt

5. MAC-Adresse

5.1. Einleitung

Die MAC-Adresse (Media Access Control, Ethernet-ID oder bei Apple Airport-ID und Ethernet-ID genannt) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die **zur eindeutigen Identifikation des Geräts im Netzwerk** dient.

Die MAC-Adresse wird der Sicherungsschicht, **Schicht 2 des OSI-Modells**, zugeordnet. Um die Sicherungsschicht mit der Vermittlungsschicht zu verbinden, wird zum Beispiel bei Ethernet das Address Resolution Protocol verwendet.

Netzwerkgeräte brauchen dann eine MAC-Adresse, wenn sie auf Schicht 2 explizit adressiert werden sollen, um Dienste auf höheren Schichten anzubieten. Leitet das Gerät wie ein Repeater oder Hub die Netzwerkpakete nur weiter, ist es auf der Sicherungsschicht nicht sichtbar und braucht folglich keine MAC-Adresse. Bridges und Switches untersuchen zwar die Pakete der Sicherungsschicht, um das Netzwerk physikalisch in mehrere Kollisionsdomänen aufzuteilen, nehmen aber selbst nicht aktiv an der Kommunikation teil, brauchen also ebenfalls keine MAC-Adresse.

Hubs und Switches der oberen Preisklasse verfügen über Management- und Monitoring-Dienste, die auf der Anwendungsschicht zum Beispiel über Telnet, SNMP oder HTTP genutzt werden können, daher ist solchen Geräten eine MAC-Adresse zugeordnet.

5.2. Aufbau

IEEE definiert zwei Formate von MAC-Adressen: 16 Bit und 48 Bit. In Ethernet-Frames werden 58 Adressbits verwendet.

MAC-Adressen sind sechs Byte (=48Bit) lang, die man mit einer zwölfstelligen hexadezimalen Zahl darstellt. Sie sind in zwei Bereiche aufgeteilt. An den ersten sechs Zeichen (hexadezimal) von links erkennt man den **Hersteller** der Netzwerkkarte (auch OUI = Organizationally Unique Identifier genannt). Die restlichen Zeichen sind eine fortlaufende **Seriennummer**. Die Netzwerkkartenhersteller lassen für sich bestimmte Bereiche reservieren. Dadurch sind die MAC-Adressen weltweit eindeutig.

5.2.1. Beispiele

`00-50-8b-xx-xx-xx`	`Compaq`	`00-07-E9-xx-xx-xx`	`Intel`

5.2.2. Besondere Kennungen

Das niederwertigste Bit einer MAC-Adresse gibt an, ob es sich um eine Einzeladresse oder Gruppenadresse (I/G für Individual/Group) handelt. Bei einem Broadcast oder Multicast wird I/G = 1 gesetzt, sonst und bei Quelladressen ist I/G = 0.

Das folgende Bit (genannt U/L für Universal/Local) zeigt an, dass die MAC-Adresse global eindeutig ist (U/L = 0) oder lokal administriert wird und nur dort eindeutig ist (U/L = 1).

5.3. Broadcast

Die MAC-Adresse, bei der alle 48 Bits auf 1 gesetzt sind (`ff-ff-ff-ff-ff-ff`), wird als Broadcast-Adresse verwendet, die an alle Geräte in einem LAN gesendet wird. Broadcast-Frames werden ohne besondere Maßnahmen nicht in ein anderes LAN übertragen.

6. LLC

6.1. Einleitung

Logical Link Control (LLC) ist die Bezeichnung für ein Netzwerkprotokoll der Telekommunikation, das vom IEEE standardisiert wurde. Es ist ein Protokoll, **dessen Hauptzweck in der Datensicherung auf der Verbindungsebene** liegt, und gehört daher zur **Schicht 2 des OSI-Modells**. LLC ist eine Protocol Data Unit (PDU) der OSI-Schicht 2. Sie verteilt eingehende Daten, indem sie diese an die entsprechenden Instanz-Protokolle der OSI-Schicht 3 weiterleitet. Daten, welche die OSI-Schicht 3 zur Übermittlung sendet, werden von LLC an den MAC-Layer der OSI-Schicht 2 weitergegeben. Über die LLC-Teilschicht bietet die Sicherungsschicht den Transportsystemen eine einheitliche Schnittstelle.

6.2. Aufbau

Das Protokoll LLC fügt einem gegebenen IP-Paket zwei jeweils 8 Bit große Kennzeichen namens **DSAP** (Destination Service Access Point: Einsprungadresse des Empfängers) und **SSAP** (Source Service Access Point: Einsprungadresse des Absenders) hinzu. Ausserdem existiert ein 8 oder 16 Bit grosses Feld (Control, CTRL) mit Steuerinformationen für Hilfsfunktionen wie beispielsweise Datenflusssteuerung.

6.3. LLC1 vs LLC2

LLC1 ist ein Datagrammdienst (also verbindungslos) und LLC2 ein Verbindungsdienst (also verbindungsorientiert).

7. Hub

7.1. Einleitung

Der Hub (engl.: Nabe, Knotenpunkt) bezeichnet in der Telekommunikation Geräte, die Netzwerk-Knoten sternförmig verbinden. Normalerweise wird die Bezeichnung Hub für Multiport-Repeater gebraucht. Sie werden verwendet, um Netz-Knoten oder auch weitere Hubs, z. B. durch ein Ethernet, miteinander zu verbinden.

7.2. Technisches

Ein Hub besitzt **nur Anschlüsse (auch Ports genannt) gleicher Geschwindigkeit** (mit gleichem MII aber durchaus unterschiedlichem MDI). Besitzt ein Hub beispielsweise eine BNC Kupplung und RJ45 Anschlüsse, so beträgt seine Geschwindigkeit 10Mbit half duplex. Zum Anschluss weiterer Hubs, oder Switches wird entweder ein spezieller Uplink-Port (auch X-Port oder Mid-X) oder ein gekreuztes Kabel benutzt. Ein Hub arbeitet, genauso wie ein Repeater, auf **Ebene 1 des ISO/OSI-Referenzmodells (Bitübertragungsschicht)** und wird deswegen auch Multiport-Repeater oder Repeating-Hub genannt. Das Signal eines Netzteilnehmers wird in keinem Fall analysiert, sondern **nur elektronisch aufgebessert** (entrauscht und verstärkt) und an alle anderen Netzteilnehmer weitergeleitet.

7.3. Sterntopologie / Kollisionsdomäne

Bei Einsatz eines Hubs im Netz wird durch die Verkabelung meist eine Stern-Topologie realisiert, der logische Aufbau eines Hubs entspricht, wie bei der Bus-Topologie, aber dennoch einer gemeinsamen Kollisionsdomäne. Dies bedeutet, dass durch einen Hub die maximal zur Verfügung stehende Bandbreite eines Netzes gegenüber einem Bus nicht gesteigert wird, da sich **alle Netzteilnehmer noch immer in derselben Kollisionsdomäne** befinden. Der Vorteil eines Hubs im Vergleich zum Bus liegt in der erhöhten Ausfallsicherheit. Die Störung eines Kabels legt hier nicht das gesamte Netz lahm, sondern beeinträchtigt lediglich einen einzelnen Teilnehmer, der dann nicht mehr erreichbar ist. Zusätzlich ist der Fehler viel leichter zu lokalisieren.

7.4. Kaskadierung von Hubs

Hubs können in einem Ethernet **nicht beliebig kaskadiert werden**, um eine größere Netzausdehnung zu erreichen. Eine für jede Geschwindigkeit spezifische maximale Round-Trip-Delay-Time (RTDT) darf nicht überschritten werden. Die RTDT ist die Zeit, die ein Netzwerkpaket benötigt, um vom einen Ende des Netzes zum weitenferntesten anderen Ende der Netzes zu gelangen - und wieder zurück. Wird das Netz zu groß, also die RTDT zu hoch, werden Kollisionen häufiger, unerkannte Kollisionen möglich und der gesamte Netzverkehr beeinträchtigt. Solche Störungen sind hinterlistig, da Übertragungen bei niederer Netzlast normal funktionieren können. Genauso wie bei Repeatern muss also die 5-4-3-Regel befolgt werden, um Probleme mit zu hohen Signallaufzeiten (RTDT) zu vermeiden. Auf Grund dieser Probleme werden heute fast überall Switche verwendet. Im Gigabit-Bereich (und höher) wurden daher auch keine Hubs/Repeater mehr spezifiziert.

8. Switch

8.1. Einleitung

Ein Netzwerk-Switch oder kurz nur Switch (engl. Schalter, auch Weiche), ist ein elektronisches Gerät zur Verbindung mehrerer Computer bzw. Netz-Segmente in einem lokalen Netz (LAN) und ist äußerlich ähnlich einem Hub. Da ein Switch technisch sehr ähnlich wie eine Bridge arbeitet, wird er gelegentlich **auch als Multi-Port-Bridge bezeichnet**. Switches analysieren den Netzwerkverkehr und treffen logische Entscheidungen, daher bezeichnet man einen Switch manchmal auch als **intelligenten Hub**.

8.2. Layer-2 Switches

Einfache Switches arbeiten auf **der Layer-2 bzw. Schicht 2 (Sicherungsschicht) des OSI-Modells**. Der Switch verarbeitet die 48-Bit MAC-Adressen und legt dazu eine SAT (Source Address Table) an, in der neben der MAC-Adresse auch der Port, an dem diese empfangen wurde, gespeichert wird. Im Unterschied zum Hub werden Netzwerkpakete jetzt nur noch an den Port weitergeleitet, der für die entsprechende Zieladresse in der SAT gelistet ist. Ist eine Zieladresse allerdings noch unbekannt (Lernphase), leitet der Switch das betreffende Paket an alle aktiven Ports. Im Unterschied zu Bridges haben Switches mehr als 2 Ports (meist zwischen 4 und 48 Ports) und können mehrere Ports unabhängig von einander, zeitgleich verbinden (non Blocking). Switches können natürlich auch mit Broadcasts umgehen.

Für die angeschlossenen Geräte verhält sich ein Switch transparent (nahezu unsichtbar). Aus Netzwerksicht wird die **Paketanzahl in den Segmenten drastisch reduziert**, wenn die Kommunikation vorwiegend zwischen den Geräten innerhalb eines Segments stattfindet. Muss ein Switch Pakete auf andere Segmente weiterleiten, verzögert er dagegen die Kommunikation (sog. Latenz). Bei Überlastung der Kapazität eines Segments oder zu wenig Pufferspeicher im Switch kann auch das Verwerfen von Paketen nötig sein. Dies wird durch die Protokolle in höheren Schichten, etwa TCP, ausgeglichen.

8.3. Layer-3 Switches

Auch unterscheidet man Layer-2- und Layer-3(und höher)-Switches. Layer-2-Geräte sind die älteren Modelle und verfügen nur über grundsätzliche Funktionen. Sie beherrschen meist keine Management-Funktionen (sind also "Plug and Play"-fähig), oder wenn doch, dann nur einen geringen Funktionsumfang wie Portsperren oder Statistiken. Professionelle **Layer-3(und höher)-Switches** verfügen in der Regel über Management-Funktionen, neben den grundlegenden Switch-Funktionen verfügen sie zusätzlich über Steuer- und Überwachungsfunktionen, die auch auf Informationen aus höheren Layern als Layer 2 beruhen können, wie z. B. IP-Filterung, VLAN, Priorisierung, Routing und andere Funktionen, die für die Überwachung und Steuerung eines Netzwerkes hilfreich sind. Die Steuerung dieser Switches geschieht je nach Hersteller über die Console, eine Weboberfläche, eine spezielle Steuerungssoftware oder über eine Kombination dieser drei Möglichkeiten. Bei den aktuellen nicht gemanagten (Plug and Play) Switches beherrschen die höherwertigen Geräte ebenfalls Layer-3-Funktionen wie tagged VLAN oder Priorisierung und verzichten dennoch auf eine Console oder ein sonstiges Management-Interface.

8.4. Funktionsweise

Nachfolgend wird von Layer-2-Switches ausgegangen. Die einzelnen Ports eines Switches können unabhängig voneinander Daten empfangen und senden. Diese sind entweder über einen internen Hochgeschwindigkeitsbus (Backplane-Switch) oder kreuzweise miteinander verbunden (Matrix Switch). Datenpuffer sorgen dafür, dass nach Möglichkeit keine Datenframes verloren gehen.

Ein Switch braucht nicht konfiguriert zu werden. Empfängt er ein Paket nach dem Einschalten, speichert er die MAC-Adresse des Senders und die zugehörige Schnittstelle in der Source Address Table (SAT).

Wird die Zieladresse in der SAT gefunden, so befindet sich der Empfänger im an der zugehörigen Schnittstelle angeschlossenen Segment. Das Paket wird dann an diese Schnittstelle weitergeleitet. Sind Empfangs- und Zielsegment identisch, muss das Paket nicht weitergeleitet werden, da die Kommunikation ohne Switch im Segment selbst stattfinden kann.

Falls die Zieladresse (noch) nicht in der SAT ist, muss das Paket an alle anderen Schnittstellen weitergeleitet werden. In einem IPv4-Netzwerk wird jedoch der SAT-Eintrag meist während der sowieso nötigen Antwort auf eine ARP-Adressenanfrage vorgenommen, so dass dieser Fall selten auftritt und keinerlei unnötige Pakete erzeugt. Broadcast-Adressen werden niemals in die SAT eingetragen und daher stets an alle Segmente weitergeleitet. Multicast-Adressen werden entweder wie Broadcast-Adressen verarbeitet oder, wenn das Gerät Multicasts verarbeiten kann, nur an in der SAT registrierte Multicast-Adressen geschickt.

Switches lernen also gewissermaßen die MAC-Adressen der Geräte in den angeschlossenen Segmenten automatisch.

8.5. Switch-Typen

8.5.1. Cut-Through

Eine sehr schnelle Methode, wird hauptsächlich von besseren Switches implementiert. Hierbei schaut der Switch beim eingetroffenen Frame **nur auf die Ziel-MAC-Adresse**, trifft eine Forwarding-Entscheidung und schickt den Frame entsprechend weiter. Das Frame wird **nicht auf Fehlerfreiheit geprüft**, um Zeit zu sparen. Der Switch leitet deshalb auch beschädigte Frames weiter, diese müssen dann durch andere Schicht-2-Geräte oder höhere Netzwerkschichten aufgefangen werden. Die Latenzzeit in Bit beträgt hier 112. Sie setzt sich aus der Präambel (8 Byte) und der „Destination-MAC-Adresse" (6 Byte) zusammen.

8.5.2. Store-and-Forward

Die grundlegendste, aber auch **langsamste Switching-Methode** mit der größten Latenzzeit (Verzögerungszeit). Sie wird von jedem Switch beherrscht. Der Switch empfängt zunächst den ganzen Frame (speichert diesen; „Store"), trifft wie gehabt seine Forwarding-Entscheidung anhand der Ziel-MAC-Adresse und **berechnet dann eine Prüfsumme** über den Frame, die er mit dem am Ende des Pakets gespeicherten CRC-Wert vergleicht. Sollten sich Differenzen ergeben, wird das Frame verworfen. Auf diese Weise verbreiten sich keine fehlerhaften Frames im lokalen Netzwerk. Store-and-Forward war lange die einzig mögliche Methode zu switchen, wenn Sender und Empfänger mit verschiedenen Übertragungsgeschwindigkeiten oder Duplex-Modi arbeiten oder verschiedene Übertragungsmedien nutzen. Heute gibt es auch Switches, die einen Cut-and-Store-Hybridmodus beherrschen, der vor allem beim Switchen von schnell nach langsam beschleunigend wirkt.

8.5.3. Fragment Free

Schneller als Store-and-Forward, aber langsamer als Cut-Through. Anzutreffen vor allem bei besseren Switches. Prüft, ob ein Frame die im Ethernet-Standard geforderte **minimale Länge von 64 Bytes** erreicht und schickt es dann sofort auf den Zielport, **ohne eine CRC-Prüfung** durchzuführen. Fragmente unter 64 Byte sind meist „Trümmer" einer Kollision, die kein sinnvolles Paket mehr ergeben.

8.5.4. Error-Free-Cut-Through/Adaptive Switching

Eine Mischung aus mehreren der obigen Methoden. Wird ebenfalls meist nur von teureren Switches implementiert. Der Switch arbeitet zunächst im „Cut through"-Modus und schickt das Frame auf dem korrekten Port weiter ins LAN. Es wird jedoch eine Kopie des Frames im Speicher behalten, über das dann eine Prüfsumme berechnet wird. Sollte sie nicht mit der im Frame übereinstimmen, so kann der Switch dem defekten Frame zwar nicht mehr hinterhersignalisieren, dass es falsch ist, aber er kann einen internen Counter mit der Fehlerrate pro Zeiteinheit hochzählen. **Wenn zu viele Fehler in kurzer Zeit auftreten, fällt der Switch in den Store and Forward-Modus zurück.** Wenn die Fehlerrate wieder niedrig genug ist, schaltet er in den Cut through-Modus um. Ebenso kann der Switch temporär in den Fragment-Free-Modus schalten, wenn zuviele Fragmente mit weniger als 64 Byte Länge ankommen. Besitzen Sender und Empfänger unterschiedliche Übertragungs-geschwindigkeiten oder Duplex-Modi bzw. nutzen andere Übertragungsmedien (Glasfaser auf Kupfer), so muss ebenfalls mit Store-and-Forward Technik geswitcht werden.

8.6. Port- / Segment-Switching

8.6.1. Port-Switch

Ein Port-Switch verfügt pro Port über nur einen SAT Eintrag für eine MAC-Adresse. An solch einem Anschluss dürfen folglich nur Endgeräte (Server, Router, Workstation) und keine weiteren Segmente, also keine Bridges, Hubs oder Switches (hinter denen sich mehrere MAC Adressen befinden)

angeschlossen werden. Zusätzlich gab es oft einen Uplink-Port für den diese Einschränkung nicht galt. Dieser Port hatte oft keine SAT, sondern wurde einfach für alle MAC-Adressen benutzt die nicht einem anderen lokalen Port zugeordnet waren. Solche Switches arbeiteten in der Regel nach dem Cut-Through Verfahren. Das klingt nach Systemen die nur Nachteile besaßen – dennoch gab es auch Vorteile dieser Systeme: sie kamen mit extrem wenig Speicher aus (geringere Kosten) und auf Grund der Minimalgröße der SAT konnte auch die Switching-Entscheidung sehr schnell getroffen werden.

8.6.2. Segment-Switching

Alle neueren Switches sind Segment-Switches und können **an jedem Port zahlreiche MAC Adressen verwalten**, d. h. weitere Netz-Segmente anschließen. Hierbei gibt es zwei unterschiedliche SAT Anordnungen: Entweder jeder Port hat eine eigene Tabelle von beispielsweise max. 250 Adressen. Oder es gibt eine gemeinsame SAT für alle Ports – mit beispielsweise maximal 2000 Einträgen. Vorsicht: manche Hersteller geben 2000 Adresseinträge an, meinen aber 8 Ports mit jeweils maximal 250 Einträgen pro Port.

8.7. Sicherheit

8.7.1. MAC-Flooding

Der Speicherplatz, in dem sich der Switch die am jeweiligen Port hängenden MAC-Adressen merkt, ist begrenzt. Dies macht man sich beim MAC-Flooding zu Nutze, indem man den Switch mit gefälschten MAC-Adressen überlädt, bis dessen Speicher voll ist. In diesem Fall schaltet der Switch in einen Failopen-Modus, wobei er sich wieder wie ein Hub verhält und alle Pakete an alle Ports weiterleitet. Verschiedene Hersteller haben – wieder fast ausschließlich bei Switches der mittleren bis hohen Preisklasse – Schutzmaßnahmen gegen MAC-Flooding implementiert. Als weitere Sicherheitsmaßnahme kann bei den meisten managed switches für einen Port eine Liste mit zugelassenen Absender-MAC-Adressen angelegt werden. Datenpakete mit nicht zugelassener Absender-MAC-Adresse werden nicht weitergeleitet und können das Abschalten des betreffenden Ports bewirken (Port Security).

8.7.2. ARP-Spoofing

Hierbei macht sich der Angreifer eine Schwäche im Design des ARP-Protokolls zu Nutze, welches zur Auflösung von IP-Adressen zu Ethernet-Adressen verwendet wird. Ein Rechner, der ein Paket via Ethernet versenden möchte, muss die Ziel MAC-Adresse kennen. Diese wird mittels ARP erfragt (ARP-Request Broadcast). Antwortet der Angreifer nun mit seiner eigenen MAC-Adresse zur erfragten IP (nicht seiner eigenen IP, daher die Bezeichnung Spoofing) und ist dabei schneller als der eigentliche Inhaber der IP, so wird das Opfer seine Netzwerkpakete an den Angreifer senden, welcher sie nun lesen und gegebenenfalls an die ursprüngliche Zielstation weiterleiten kann. Hierbei handelt es sich nicht um einen Fehler des Switches. Ein Layer-2-Switch kennt gar keine höheren Protokolle wie IP und ARP und kann seine Entscheidung zur Weiterleitung nur anhand der MAC-Adressen treffen. Ein Layer-3-Switch muss sich, wenn er autokonfigurierend sein soll, auf die von ihm mitgelesenen ARP-Pakete verlassen und lernt daher auch die gefälschte Adresse, allerdings kann man einen managed Layer-3-Switch so konfigurieren, dass die Zuordnung von Switchport zu IP-Adresse fest und nicht mehr von ARP beeinflussbar ist.

9. Bridge

9.1. Einleitung

Eine Bridge verbindet im Computernetz zwei Segmente auf der Ebene der **Schicht 2 (Sicherungsschicht) des OSI-Modells**. Eine Bridge kann auf der Unterschicht MAC oder der Unterschicht LLC arbeiten. Sie wird dann **MAC-Bridge** oder **LLC-Bridge** genannt. Eine weitere Unterscheidung ergibt sich durch die Art der Leitwegermittlung von Datenpaketen in Transparent Bridge und Source Routing Bridge.

9.2. Funktionsweise

Eine Bridge wird hauptsächlich eingesetzt, um **ein Netz in verschiedene Kollisionsdomänen aufzuteilen**. Somit kann die Last in großen Netzen vermindert werden, da jeder Netzstrang nur die Pakete empfängt, deren Empfänger sich auch in diesem Netz befindet.

Eine **MAC-Bridge** verbindet Netze mit gleichen Zugriffsverfahren. Die **LLC-Bridge** (auch Remote-Bridge oder Translation Bridge) wird verwendet, um zwei Teilnetze mit verschiedenen Zugriffsverfahren (z.B. CSMA/CD und Token-Passing) zu koppeln und besteht (idealisiert) aus zwei Teilen, die miteinander verbunden sind, wobei das Medium zwischen beiden Teilen hierbei egal ist. Innerhalb der LLC-Bridge findet eine Umsetzung (Translation) statt. Bei dieser Umsetzung werden alle Parameter des Quellnetzes (wie MAC-Adresse, Größe und Aufbau des MAC-Frames) an das Zielnetz angepasst, soweit diese vom Zielnetz unterstützt werden.

Eine **Transparente Bridge** lernt, welche MAC-Adressen sich in welchem Teilnetz befinden. Die Bridge lernt mögliche Empfänger, indem die Absender von Paketen in den einzelnen Teilnetzen in eine interne Weiterleitungstabelle eingetragen werden. Anhand dieser Informationen kann die Bridge den Weg zum Empfänger bestimmen. Die Absenderadressen werden laufend aktualisiert, um Änderungen sofort zu erkennen. Eine **Source Routing Bridge** besitzt keine Weiterleitungstabelle. Hier muss der Sender die Informationen zur Weiterleitung zum Ziel bereitstellen.

Ein Paket muss nur dann an alle Teilnetze gesendet werden, wenn der Empfänger nicht in dieser Tabelle eingetragen ist und das Zielnetz somit nicht bekannt ist. Ein Broadcast wird stets in alle Teilnetze übertragen.

Ein leicht verständliches Beispiel einer Bridge ist eine Laser-Bridge, die per Laserstrahl Datenaustausch zwischen zwei Gebäuden ermöglicht. In jedem Gebäude steht ein Teil, der aus einem Netzport und einer Laser Sende- und Empfangseinheit besteht, trotzdem liegen die beiden Netzports im selben logischen Netz.

Allen Bridge-Arten ist gemeinsam, dass ihre (Netz-)Ports im Promiscuous Mode arbeiten, um alle Pakete zu empfangen, **Paket-Frames überprüft werden und nur korrekte Frames weitergesendet werden.** Weiterhin wird im ungelernten Zustand jeder eingehende Frame an alle Ports gesendet (außer an den, der den Frame gesendet hat).

Bridges können redundant ausgelegt werden, um den Ausfall einer Bridge zu kompensieren. Um dabei die mehrfache Weiterleitung von Datenpaketen zu unterdrücken, muss ein passendes Komunikationsprotokoll z.B. das Spanning Tree Protocol oder Trunking, Meshing usw. unterstützt werden.

9.3. Bridge vs Switch

Switches stellen eine evolutionäre Weiterentwicklung der Bridging-Technologie dar. Überlegene Durchsatzleistung, höhere Port-Dichte, geringere Kosten pro Port und größere Flexibilität tragen dazu bei, dass sich Switches als Ersatz von Bridges, Hubs und Routern durchsetzen.

Es gibt in der Fachliteratur keine eindeutige Einteilung der Technologien, die Bridges, bzw. Switches definieren. Beide arbeiten sehr ähnlich, allgemein wurden Bridges etwa ab 1985 zum Segmentieren (verkleinern der Kollisionsdomäne) von Netzen und zum Verbinden unterschiedlicher Architekturen (z.B. Ethernet - TokenRing) entwickelt und vermarktet. Switches wurden erst viel später (1990)

entwickelt, trotz der Ähnlichkeit zu Bridges sollten sie Router ersetzen. Bei der Entwicklung von Switches lag das Hauptaugenmerk auf Performance.

Zur Verkleinerung der Kollisionsdomäne erhält ein Switch daher möglichst viele Ports, an die jeweils nur wenige Geräte - im Idealfall eines - angeschlossen wird, zusätzlich stellen ein oder mehrere sogenannte Uplink-Ports Verbindungen zum nächsten Switch bzw. Router her. Nicht modulare Switches haben in der Regel mindestens vier bis maximal etwa 48 Ports. Große "modulare" Switches können je nach Modell zu Einheiten mit mehreren hundert Ports konfiguriert werden. **Im Gegensatz zu Bridges können Switches mehrere Pakete zeitgleich zwischen verschiedenen Portpaaren übertragen**. Am Ehesten entspricht eine Bridge einem Switch im Betriebsmodus Store and Forward mit meist nur zwei Ports: a switch is a multiport bridge (ein Switch ist eine Mehrport-Bridge) - lautete noch 1990 ein Lehrspruch der Firma Cisco, seit der Übernahme von Kalpana 1994 geht man bei Cisco differenzierter mit dem Thema um.

In den Anfangszeiten gab es Port-Switches, diese können lediglich eine MAC-Adresse pro Port speichern, Bridges hingegen können stets viele MAC-Adressen in ihrer SAT speichern. Umgekehrt benötigen Bridges zum Anschluss mehrerer Geräte oft externe Verteiler z.B. Hubs.

In der Regel können Bridges und Switche Netzwerke mit verschiedenen Übertragungsgeschwindigkeiten miteinander verbinden. Bridges können meist sowohl auf MAC als auch auf LLC Basis arbeiten, Switches hingegen arbeiten meist nur auf MAC-Basis. **Switches können folglich keine unterschiedlichen Architekturen (z.B. Ethernet - Token Ring) überbrücken**. Da Ethernet den Markt dominiert, hat die Überbrückung verschiedener LAN-Architekturen nur eine geringe Bedeutung. Nicht zuletzt deshalb, sind Bridges mittlerweile Nischenprodukte.

Bei größeren Switches, genau so wie bei leistungsstarken Bridges, kann für jedes verbundene Netzwerk-Segment eine bestimmte Bandbreite festgelegt werden, auch können bestimmte Dienste priorisiert werden (FlowControl).

10. Router

10.1. Einleitung

Ein Router ist ein Vermittlungsrechner, der mehrere **Rechnernetze koppelt**, das bedeutet bei ihm eintreffende Netzwerk-Pakete eines Protokolls werden auf Basis von **Layer-3 Informationen** analysiert und zum vorgesehenen Zielnetz (auch Ziel-Subnetze) weitergeleitet oder geroutet.

10.2. Arbeitsweise

Klassische Router arbeiten auf Schicht 3 (der Netzwerkebene / Network-Layer) des OSI-Referenzmodells. Ein Router besitzt für jedes an ihn angeschlossene Netz eine Schnittstelle (auch Interface). Beim Eintreffen von Daten muss ein Router den richtigen Weg zum Ziel und damit die passende Schnittstelle bestimmen, über welche die Daten weiterzuleiten sind. Dazu bedient er sich einer **lokal vorhandenen Routingtabelle**, die angibt, über welchen Anschluss des Routers (bzw. welche Zwischenstation) welches Netzwerk erreichbar ist. Üblicherweise ist ein Eintrag in der Routingtabelle die default Route (auch Standardgateway), diese Route wird für alle Ziele benutzt, die über keinen besser passenden Eintrag in der Routingtabelle verfügen.

Professionelle Router beherrschen mittlerweile auch ein sogenanntes Policy Based Routing, dabei wird die Routingentscheidung nicht nur auf Basis des gewünschten Ziel-Netzes getroffen (Layer-3), sondern auch der gewünschte Dienst berücksichtigt. Beispielsweise kann hierdurch die default Route für Web (HTTP) eine andere sein, als die default Route für Mail (SMTP).

Für nicht routebare Protokolle muss ein Router mit einer Bridgefunktion verwendet werden, auch **BRouter** genannt. **Am Router endet sowohl die Kollisions- als auch Broadcastdomäne**. Will man trotzdem Broadcast-basierte Dienste wie DHCP benutzen, muss ein so genannter Relay Agent konfiguriert werden. Dieser sorgt dann dafür, dass Broadcasts auch über den Router hinweg ausgebreitet werden.

Außerdem sind Ein- und Mehrprotokoll-Router (auch Multiprotokoll-Router) zu unterscheiden. **Einprotokoll-Router** können nur in homogenen Umgebungen eingesetzt werden. Solche Geräte sind nur in der Lage, z. B. IP zu routen. Heute dominieren TCP/IP Router, da alle anderen Netzwerk-Protokolle nur noch eine untergeordnete Bedeutung haben und, falls sie doch zum Einsatz kommen, oft auch gekapselt werden können (NetBios, IPX). Früher hatten Mehrprotokoll-Router in größeren Umgebungen eine wesentliche Bedeutung, damals kam es eindeutig darauf an, dass mehrere Protokoll-Stacks unterstützt wurden. Ausnahmen sind auch heute Weitverkehrs- und ATM-Netze.

Wichtig ist hierbei auch die Unterscheidung zwischen gerouteten Protokollen (z. B. IP oder IPX) und Routing-Protokollen. **Routing-Protokolle** dienen der Verwaltung des Routing-Vorgangs und der Kommunikation zwischen den Routern, die z. B. ihre Routing-Tabellen austauschen (z. B. RIP oder OSPF). Geroutete Protokolle hingegen sind für die Routenauswahl und den Datenversand zuständig.

11. Spanning Tree Protocol

11.1. Funktionsweise

Das Spanning Tree Protocol (STP) **dient zur Vermeidung redundanter Netzwerkpfade (Schleifen) im LAN**, speziell in geswitchten Umgebungen.

Netzwerke sollten zu jedem möglichen Ziel immer nur einen Pfad haben, um zu vermeiden, dass Datenpakete (Frames) dupliziert werden und mehrfach am Ziel eintreffen, was zu Fehlfunktionen in darüber liegenden Netzwerkschichten führen könnte und die Leistung des Netzwerks vermindern kann. Andererseits möchte man mitunter redundante Netzwerkpfade als Backup für den Fehlerfall zur Verfügung haben. Der Spanning-Tree-Algorithmus wird beiden Bedürfnissen gerecht.

Zur Kommunikation zwischen den Switches wird das **Bridge Protokoll genutzt**. Die Bezeichnung Bridge stammt aus der Annahme, dass ein Switch eine Multiport-Bridge ist. Die Pakete dieses Protokolls werden Bridge Protocol Data Unit (BPDU) genannt.

Zunächst wird unter den Spanning-Tree-fähigen Bridges im Netzwerk eine sog. **Root Bridge** gewählt, die die Wurzel des aufzuspannenden Baumes wird und „Chef" des Netzwerks ist. Dies geschieht, indem alle Bridges ihre Bridge-ID (die jede Bridge besitzt) an eine bestimmte Multicast-Gruppe mitteilen. Die Bridge ID ist 8 Byte lang (2 Bytes Bridge Priority und 6 Bytes MAC Adresse). Die Bridge mit der niedrigsten ID wird zur Root Bridge. Sollte die Bridge Priority identisch sein, wird als ergänzendes Kriterium die MAC Adresse der Komponenten benutzt (und zwar die Bridge mit der niedrigeren MAC Adresse). Von der Root Bridge aus werden nun Pfade festgelegt, über die die anderen Bridges im Netzwerk erreichbar sind. Sind redundante Pfade vorhanden, so müssen die dortigen Bridges den entsprechenden Port deaktivieren. Die Pfade, über die kommuniziert werden darf, werden anhand von Pfadkosten bestimmt, die die dortige Bridge übermittelt. Die Kosten sind abhängig vom Abstand zur Root Bridge und dem zur Verfügung stehenden Uplink zum Ziel. Ein 10 Mbit/s-Uplink hat beispielsweise höhere Pfadkosten als ein 100 Mbit/s-Uplink zum gleichen Ziel und würde dabei unter den Tisch fallen. Auf diese Weise ist jedes Teilnetz im geswitchten LAN nur noch über eine einzige, die Designated Bridge erreichbar. In der grafischen Darstellung ergibt sich ein Baum aus Netzwerkpfaden, der dem Algorithmus seinen Namen gab.

Die Root Bridge teilt den in der Hierarchie eine Stufe unterhalb liegenden Designated Bridges im **Abstand von 2 Sekunden** mit, dass sie noch da ist, woraufhin die empfangende Designated Bridge ebenfalls an nachfolgende Bridges die entsprechende Information senden darf. Wenn diese Hello-Pakete ausbleiben, hat sich folglich an der Topologie des Netzwerks etwas geändert, und das Netzwerk muss sich reorganisieren. Diese Neuberechnung des Baumes dauert im schlimmsten Fall bis zu 30 Sekunden. Während dieser Zeit dürfen die Spanning-Tree-fähigen Bridges außer Spanning-Tree-Informationen keine Pakete im Netzwerk weiterleiten. Dies ist einer der **größten Kritikpunkte** am Spanning Tree-Algorithmus, da es möglich ist, mit gefälschten Spanning-Tree-Paketen eine Topologieänderung zu signalisieren und das gesamte Netzwerk für bis zu 30 Sekunden lahmzulegen. Um diesen potenziellen Sicherheitsmangel zu beheben, aber auch, um bei echten Topologieänderungen das Netzwerk schnell wieder in einen benutzbarem Zustand zu bringen, wurden schon früh von verschiedenen Herstellern Verbesserungen am Spanning-Tree-Algorithmus und dem dazugehörigen Protokoll erdacht. Eine davon, das Rapid Spanning Tree Protocol (RSTP) ist inzwischen zum offiziellen IEEE-Standard 802.1w geworden. Die Idee hinter RSTP ist, dass bei signalisierten Topologieänderungen nicht sofort die Netzwerkstruktur gelöscht wird, sondern erst einmal wie gehabt weiter gearbeitet wird und Alternativpfade berechnet werden. Erst anschließend wird ein neuer Baum zusammengestellt. Die Ausfallzeit des Netzwerks lässt sich so von 30 Sekunden auf unter 1 Sekunde drücken. In der 2003 zu verabschiedenden Revision des 1998 letztmalig überarbeiteten 802.1D-Standards soll das alte STP zugunsten von RSTP komplett entfallen.

11.2. Schritt-für-Schritt

1. Power-Up aller Bridges
2. Bridges stellen all ihre Anschlüsse auf Blocked
3. Jede Bridge nimmt an, sie sei Root-Bridge und sendet BPDUs (Protocol Data Unit) aus
4. Bridge mit kleinster BridgeID wird zur Root-Bridge (ID: PrioFeld + Teil der MAC)

5. Aussenden von Konfigurations-BPDUs durch die Root-Bridge
6. Jede Bridge bestimmt einen Root-Port (Port mit kleinsten Pfadkosten zur Root-Bridge. Bei Ports mit gleichen Kosten gewinnt die kleinere PortID)
7. Bestimmen der Designated Bridge (LAN wählt die Designated-Bridge. Bridge mit Root-Port ins LAN mit den tiefsten Pfadkosten)