Link Layer - Ethernet

Seminar Internet-Protokolle

Jens Schmüdderich Stefanie Schirmer

10.11.2002

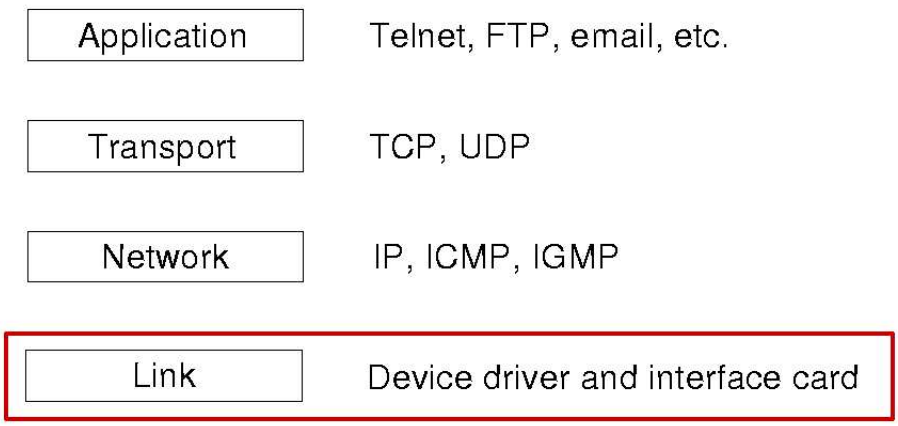
Inhaltsverzeichnis

1 Einführung in das Thema

Unser Thema ist der Link Layer, wobei bei den Protokollen der Schwerpunkt auf Ethernet liegt. Der Begriff Ethernet ist relativ bekannt, vor allem weil Ethernet für LANs (Local Area Networks) benutzt wird.

Ein kurzer Einschub über Kanäle zum Informationstransport: Um welche Arten von Verbindungen geht es im Seminar?
Grundsätzlich gibt es zwei Arten von Verbindungen: Einerseits connection-oriented/circuit-switched Kanäle und andererseits connectionless/package-switched Übertragungswege. Zur Erklärung der Begriffe helfen Beispiele. Das Telefon stellt eine circuit-switched-Verbindung bereit. Das heißt ein freier Pfad wird den Kommunikationspartnern bei Herstellung einer Verbindung garantiert (Vorteil), und auch in der Kapazität, eine menschliche Stimme zu übertragen. Andererseits muss man bezahlen, auch wenn man nichts sagt (Nachteil). Ein Netzwerk ist ein Beispiel für eine package-switched-Verbindung. Daten werden in Pakete zerstückelt, gesendet und beim Empfänger wieder zusammengesetzt. Hierbei ist gleichzeitige Kommunikation von vielen Sender-Empfänger-Paaren möglich (Vorteil). Wenn viel Kommunikation stattfindet hat ein Paar aber weniger Kapazität für sich (und muss eventuell warten) (Nachteil).
Es geht hier nur um den zweiten Teil von Verbindungen(package-switched).

2 Einordnung in das Schichtenmodell der TCP-IP Protokollfamilie



2.1 Link Layer

Die Link Layer wird auch Data Link Layer oder Network Interface Layer genannt. Sie ist die unterste Schicht des Modells, und besteht aus der Hardware im Computer und der Software im Betriebssystem. Kurz gesagt besteht sie aus Netzwerkkarte und Treiber. Diese beiden Komponeneten übernehmen zusammen alle Hardware-Details der physikalischen Verbindung. Es spielt also für die darüberliegenden Schichten keine Rolle, welche

Kabel oder andere Verbindungsmedien tatsächlich der Verbindung zugrunde liegen.
An Protokollen spielen für die Link Layer neben Ethernet noch PPP(Point-to-Point Protocol), SLIP(Serial Line IP) und andere Protokolle eine Rolle. Speziell für Ethernet und Token Ring Netzwerke gibt es ARP (Adress Resolution Protocol) und RARP (Reverse ARP), die zum Konvertieren von IP- in Netzwerkkartenadressen (MAC-Adressen) benutzt werden.

2.2 Network Layer

Die Network Layer wird auch Internet Layer genannt. Diese Schicht ist zuständig für das Verschicken von Paketen im Netzwerk, gewährleistet jedoch keinen verlässlichen Datenfluss. Es wird zwar der Versuch gestartet, zu senden, aber letztendlich gibt es keine Garantie dafür, dass die abgesendeten Daten überhaupt ankommen (unreliable, best effort).

2.3 Transport Layer

Die Transport Layer ist zuständig für Datenfluss zwischen zwei Hosts, sie garantiert also zum Teil Sicherheit in der Übertragung für die darüberliegende Schicht.
Protokolle sind hier z.B. TCP und UDP.

2.4 Application Layer

Diese Schicht ist zuständig für die Details der jeweiligen Anwendung. Protokolle der Application Layer sind z.B. Telnet, FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol).

Zusammengenommen bilden diese vier Schichten die TCP-IP-Protokollfamilie, auch Internet-Protokollfamilie genannt.
Eine stärkere Unterteilung kann noch zwischen der Application Layer und den niedrigeren Schichten gemacht werden.
Anwendungen sind meistens Prozesse. Sie befasssen sich nur mit Applikationsdetails. Die niedrigeren Schichten sind aber meistens im Kernel/Betriebssystem implementiert, und behandeln Kommunikationsdetails.
Genau diese stärkere Unterteilung an der Stelle ist beabsichtigt. Physikalische Details der Verbindung sollen für die Anwendungen unerheblich sein sein, es soll also für eine bestimmte Netzwerk-Applikation egal sein ob die Verbindung über Ethernet, über ein Token-Ring-Netzwerk, unterschiedliche Kabel oder ähnliches besteht.
Dieses verstecken von Details macht die Internet-Protokollfamilie so mächtig und nützlich. Zusammenfassend kann man sagen, dass TCP/IP auf fast jeder Art von Verbindung arbeitet.

3 Link Layer

Aus dem bisherigen kurzen Überblick kristallisieren sich drei Aufgaben für die Link Layer: Vor allem das Senden und Empfangen von IP-Datagrams/Paketen, ausserdem ARP-Anfragen und -Antworten sowie RARP-Anfragen und -Antworten. Die TCP/IP-Protokollfamilie unterstützt sehr viele unterschiedliche Link Layer (Ethernet, Token Ring, Fiber Distributed Data Interface usw.).

4 Ethernet

Ethernet ist die heute noch meistbenutzteste LAN-Technologie. Ursprünglich erfolgte die Verbindung über ein dickes Koaxialkabel (thick wire) als Bus. Mittlerweile gibt es auch schnellere Varianten (thin wire, twisted pair, fast ethernet). Das Prinzip ist jedoch immer gleich: Es gibt ein passives Kabel (Ether). Die aktiven Komponenten sind die Verbindungen zwischen den Kabeln. Wenn etwas auf das Kabel gesendet wird kann es jede angeschlossene Station empfangen (vgl. lautes rufen). Es gibt keinen Koordinator für die Nachrichten. Jeder Empfänger muss selbst entscheiden, welche Nachricht für ihn relevant ist. Zur Abstimmung der Übertragung über diesen einen Kanal benutzt Ethernet ein verbessertes Carrier Sense Protocol (siehe CSMA/CD).

5 Ethernet historisch

Als die Väter oder die Erfinder des Ethernet werden immer wieder zwei Personen genannt: Robert (Bob) M. Metcalfe und David R. Boggs. Auf der Internetseite des amerikanischen Patentamtes kann man jedoch sehen, das für das Patent Ethernet vier Entwickler eingetragen sind. Die anderen werden meistens übergangen. Entwickelt wurde Ethernet bei Xerox PARC (Palo alto Research Center), in den frühen 70er Jahren. Ein erstes Memo stammt vom Mai 1973.

Der Ethernet-Standard wurde dann 1982 von drei großen Firmen verabschiedet: Digital Equipment, INTEL und Xerox. Ergänzend zum Ethernet-Standard gibt es RFC 895 vom April 1984. Der Ethernet-Standard wird heute noch fast ungeändert benutzt.

6 CSMA/CD

CSMA/CD ist die Abkürzung für Carrier Sense Multiple Access With Collision Detect. Dabei handelt es sich erst einmal um ein System für die Regelung der Benutzung eines gemeinsamen Kanals. Dieses System wird für LANs benutzt, unter anderem auch vom Ethernet-Protokoll. CSMA/CD-Protokolle garantieren zwei Merkmale für Verbindungen:

- keine Station sendet, wenn sie den Kanal als belegt erkennt
- Abbruch bei einer Kollision – Frames, die dann ohnehin verstümmelt wären, werden nicht zu Ende übertragen, sondern es erfolgt ein sofortiger Abbruch der Übertragung

Dieses Verhalten führt zur Einsparung von Zeit und Bandbreite.

6.1 Carrier Sense

Jede Maschine entscheidet selbsttätig ob das Netzwerk frei ist. Hat eine Station nun ein Paket zu übermitteln, überprüft sie, ob gerade eine Nachricht übermittelt wird (carrier sensing). Ist alles frei, so beginnt sie mit der Übertragung. Nach Beendigung einer Übertragung muss die Station eine Unterbrechung einlegen, damit nicht eine Station das Netzwerk besetzt hält.

6.2 Multiple Access

Mehrere Maschinen sind an einem gemeinsamen (physikalischen) Netzwerk angeschlossen.

6.3 with Collision Detection

Wenn eine Station mit der Übertragung beginnt, kommt das Signal nicht überall gleichzeitig auf dem Kabel an. Also können zwei Sender gleichzeitig das Netzwerk als frei wahrnehmen und zu senden beginnen. Die beiden elektrischen Signale treffen sich, und geraten durcheinander. Keines von beiden bleibt eine lesbare Nachricht. Ein solcher Vorfall wird Kollision genannt. Nun gibt es aber einen guten Weg, damit umzugehen: Jeder Sender hört das Kabel ab um zu prüfen, ob ein fremdes Signal dazwischen kommt Das funktioniert, indem Leistung/Impuls des gesendeten Signals mit dem empfangenen verglichen wird. Das Verfahren heisst Collision detection Bei einer Kollision wird die Übertragung abgebrochen, erneut gewartet bis die Leitung frei ist (carrier sense), und wieder ein Versuch gestartet.

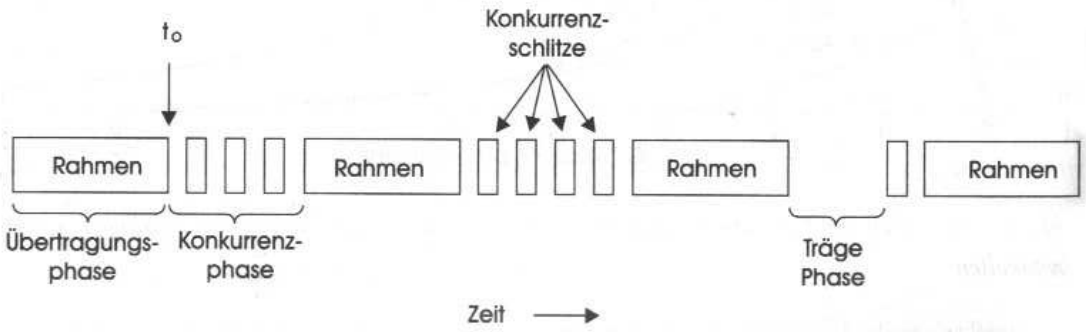
6.4 Beispielablauf

Zum Zeitpunkt t_0 ist gerade die Übertragung eines Frames beendet. Nun können andere Stationen mit dem Senden beginnen (Konkurrenz). Bei gleichzeitigem Beginn mehrerer

Stationen kommt es zu Kollisionen. Daraufhin folgt für jede beteiligte Station der Abbruch und eine zufällige Wartezeit. Wenn schliesslich eine Station allein mit dem Senden beginnt, werden die anderen warten (wegen carrier sense). Der Sender überträgt seinen Frame. Dann muss er warten um den anderen Stationen eine Chance zu geben.

Es kann also zu drei Phasen im Netzwerk kommen:

- Senden
- Konkurrenz
- Niemand sendet/Freiphase



7 Binary Exponential Backoff Algorithm

Die Wartezeit bei einer Kollision sollte geregelt werden. Es muss eine anpassungsfähige Zufallsstrategie sein, die minimale Verzögerung bei geringer Sendelast verursacht, und trotzdem stabil bei hoher Sendelast ist. Dazu wurde gleich der passende Algorithmus von Metcalfe und Boggs mitgeliefert: Der Binary Exponential Backoff Algorithm. Nach der Übertragung eines Paketes gibt es eine Phase, in der alle Sender konkurrieren. Wenn es nun zu einer Kollision kommt, dann setzen alle daran beteiligten Stationen einen bestimmten Parameter L auf 2 und wählen zufällig einen der nächsten L Sendeschlitze (Intervall, in dem eine erneute Übertragung begonnen werden darf, dieses hängt von den Eigenschaften des Netzwerks ab), um einen neuen Versuch zu starten. Bei jeder weiteren Kollision, an der die Station beteiligt ist, wird diese Zahl L verdoppelt (binary exponential). Der Effekt dieser Methode ist, dass nach k Kollisionen nur noch ein Bruchteil von 2^{-k} der Stationen versuchen zu senden. Der Algorithmus passt sich der Auslastung des Netzwerks an, bei anderen Protokollen ist das nicht unbedingt der Fall, so dass es zu regelrechten Verkehrsstaus auf der Leitung kommen kann.

Man sollte beachten, dass auch ohne Störung durch Kollisionen Frames durch andere Einflüsse nicht am Zielort ankommen müssen (Bsp. ungenügend Pufferplatz, Störungen im Kabel).

8 Die verschiedenen Ethernettypen

Prinzipiell unterscheidet man zwischen zwei verschieden Kabeltypen: Den Koaxialkabeln und Twisted Pair Kablen.

8.1 10Base5

10Base5 stellt das ursprüngliche Ethernet Design dar. Es benutzt ein 1,25cm dickes Koaxialkabel, das bis zu einer Länge von 500m funktioniert (daher die 5 hinter 10Base). Das Kabel ist außen von einem einfachen Isolationsmantel umgeben, darunter folgt eine Metallabschirmung als Schutz vor elektrischen Interferenzen. Der Zwischenraum zwischen dem Center Wire, welches das zentrale Datenkabel darstellt, und der Abschirmung ist mit Polyethylen gefüllt. An den Enden des Kabels wird zwischen Center Wire und Abschirmung ein Wiederstand angebracht, der verhindert, dass elektrische Signale reflektiert werden können.
Die Verbindung zwischen dem Kabel und einem Computer erfolgt über einen sogenannten Transceiver. Ein Transceiver ist ein kleines Gerät, dass den Ether (Bezeichnung für Kabel) nach analogen Signalen abtastet aber auch digital mit dem Computer kommunizieren kann. Es dient also der Übersetzung zwischen den beiden Komponenten: Einerseits übersetzt es analoge Signale in digitale, andererseits übersetzt es die Daten vom Computer in analoge Signale, die es auf den Ether stellt.
Zur Verbindung zwischen Transceiver und Computer wird ein sogenanntes Attachment Unit Interface Kabel (kurz AUI) verwendet. Dieses Kabel besteht aus meist fünf Leitungen, von denen eins für die Stromversorgung des Transceivers genutzt wird und die anderen für die Signalübermittlung.
Die Nachteile bei dieser Art von Verkabelung liegen einerseits in den hohen Kosten, die vor allem durch die nicht billigen Transceiver entstehen. Dazu kommt, dass diese Geräte am Ether liegen und nicht direkt am Computer. Die dadurch entstehen Schwierigkeiten einen Transceiver zu finden können den Austausch oder die Reparatur erheblich behindern. Ein weiterer Nachteil entsteht durch die schwere Abschirmung des Kabels. Sie macht das Kabel steif und schwer zu verlegen. Das selbe gilt für das AUI-Kabel.

8.2 10Base2 / Thin-Wire Ethernet

Dieses Design benutzt mit 0,5cm Dicke ein weit dünneres Kabel als sein Vorgänger, was vor allem an einer leichteren Abschirmung liegt als bei 10Base5. Auch wurden bei diesem Design die Transceiver durch einen Schaltkreis ersetzt, der direkt auf der Netzwerkkarte installiert ist, also jetzt direkt am Computer sitzt. Die Kabelenden sind hier mit BNC-Steckern versehen, mit deren Hilfe das Kabel an den Computer angeschlossen wird. Hier zeigt sich auch ein großer Unterschied zu 10Base5: Das Kabel liegt nicht mehr zentral und wird durch AUI-Kabel verbunden, sondern wird direkt an jeden Computer heran- und wieder weggeführt.
Die Vorteile bei dieser Art von Verkabelung liegen zum einen in den weit geringeren

Kosten, die vor allem durch das Wegfallen der Tranceiver und die günstigeren Kabel entstehen.
Auch sind die Kabel durch ihre höhere Flexibilität leichter zu verlegen. Durch die BNC-Stecker ist es viel einfacher, das Netzwerk um einen weiteren Computer zu erweitern, da er einfach zwischen zwei bestehende geschaltet werden kann.
Die Vorteile dieser Architektur sind aber auch ihre Nachteile: Da bei dieser Kabelart auf eine leichtere Abschirmung gesetzt wurde, ist es nicht mehr möglich, diese Kabel starken elektrischer Interferenzen auszusetzen, wie sie beispielsweise in Fabrikhalle auftreten.
Ein noch gravierenderer Nachteil besteht in dem Anschluss des Kabels: Da das Kabel zu jedem Computer hin- und wieder weggeführt wird, kann ein Nutzer, der seinen Computer vom Netz nimmt, das gesamte Netzwerk lahm legen. Eine Lösung, dieses Problem etwas zu relativieren lag in der Einführung sogenannter T-Stücke, die zwei Anschlüsse für die Kabel und einen für den Computer besaßen. So konnte ein Nutzer seinen Computer vom Netz nehmen, ohne das Kabel zu unterbrechen.

8.3 Twisted Pair Ethernet

Um den oben genannten Nachteilen zu entgehen, wurde das Twisted Pair Ethernet entwickelt. Es verwendet keine abgeschirmten Koaxialkabel mehr, sondern einfache 8-adrige verdrillte Kupferleitungen, ähnlich den Telefonleitungen. Durch diese Verdrillung der Leitungen ist eine starke Abschirmung der Kabel überflüssig, da diese durch ihre Drehung einen eigenen Schutz vor elektrischen Interferenzen besitzen. Oft reicht deswegen einfache Teflonfolie als Abschirmung aus.
Bei dieser Verkabelung werden die Computer über einen Hub (zu deutsch: Mittelpunkt) verbunden. Ein Hub ist eine kleine Box, die die Signale auf dem Ether simuliert. Es wird also an dem ursprünglichen Design festgehalten, was auch bedeutet, dass man sich die Verbindung vom Computer zum Hub wie die Verbindung vom Computer über das AUI-Kabel zum Transceiver vorstellen kann. Ein Hub ist also im Gegensatz zu einem Switch dumm – er kann nicht unterscheiden, an wen Daten adressiert sind und sie nur an diesen Computer durchschalten, sondern er leitet alle Daten an alle Hosts und überlässt diesen die Filterung.
Hierin liegt auch schon einer der wesentlichen Vorteile gegenüber den Thin-Wire Ethernets, denn ein Nutzer, der seinen Computer vom Netz nimmt, kann damit nicht mehr den Datenfluss auf dem Ether unterbrechen.
Darüber hinaus macht diese Verkabelung auch die Installation erheblich einfacher, da nur ein Hub zentral aufgestellt werden muss, an den dann jeder Rechner angeschlossen wird. Dies vereinfacht auch stark das Finden von Defekten. Bei Thin-Wire Ethernet, musste nämlich noch durch komplizierte Methoden festgestellt werden muss, wo das Kabel unterbrochen war und dann ersetzt oder geflickt werden. Bei Twisted Pair Ethernets ist die Fehlerfindung deswegen weit einfacher, da der Defekt immer in dem Kabel sein muss, dass den Computer verbindet, der keine Daten erhalten oder versenden kann. Die Kosten bei diesem Design sind ebenfalls geringer als bei den Vorgängern, was vor allem daran liegt, dass die Kupferleitungen weit billiger als Koaxialkabel sind und in den meisten Gebäuden bereits in Form von Telefonleitungen vorhanden sind.

8.4 10Base-T

10Base-T war das erste Ethernet Design, dass auf dem Twisted Pair Kabeln basierte. Es stellte mit 10Mbps aber noch keinen Gewinn an Geschwindigkeit gegenüber den Koaxialkabel-Ethernets dar, was aber auch zu seiner Entwicklung in den Siebzigern nicht notwendig war. In dieser Zeit waren nämlich nicht die Netzwerke der Engpass der Datenkommunikation sondern vielmehr die langsamen Prozessoren und Netzwerkkarten.

8.5 100Base-T / Fast Ethernet

Die oben beschriebene Situation änderte sich in den Neunziger Jahren. Durch die dramatische Zunahme der Geschwindigkeit sowohl der Prozessoren als auch der Netzwerkkarten, bildeten jetzt die Netzwerke das Nadelöhr der Kommunikation. Aus diesem Grund wurde das 10Base-T zum 100Base-T weiterentwickelt. Die Leitungen blieben zwar gleich, es konnte aber durch eine effizientere Nutzung der Leitungen eine Durchsatzrate von 100Mbps erreicht werden. Dabei wurden allerdings keine anderen Teile von Ethernet geändert, insbesondere blieb die Paketgröße gleich. Das Netz war also nicht darauf ausgelegt, eine maximale Geschwindigkeit zwischen zwei Computern, sondern eine höhere Durchsatzrate zwischen mehreren Computern zu gewährleisten.

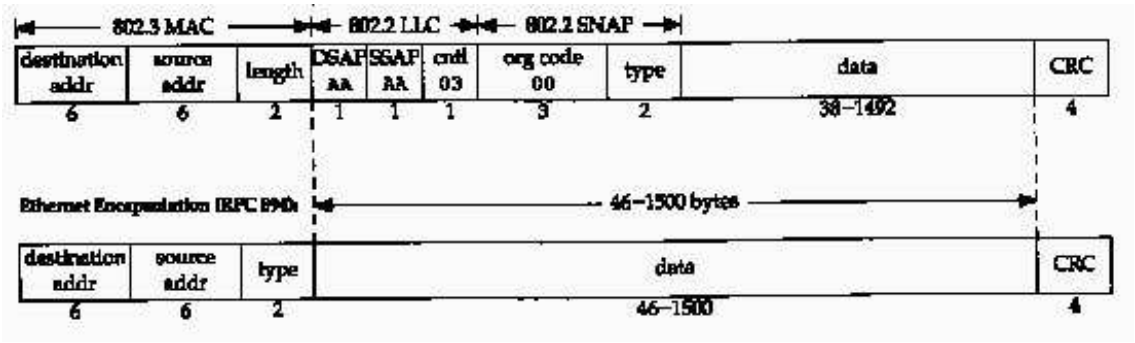
8.6 10/100 Ethernet / Dual-Speed Etherent

Durch die zunehmende Popularität der 100Mbit-Netzwerke wurde an Techniken gearbeitet, diese leichter nutzbar zu machen. Eine dieser Weiterentwicklungen stellt das 10/100 - oder Dual-Speed Ethernet dar. Dieses ist aufgrund der Extrasignale, die Fast Ethernets charakterisieren, in der Lage, die Geschwindigkeit mit der ein Netz arbeitet zu erkennen und sich automatisch auf diese anzupassen. Damit können auch Computer in einem Dual-Speed-Netzwerk betrieben werden, die nur über eine 10Mbit-Karte verfügen. Die Geschwindigkeit der Kommunikation zwischen einer 100Mbit und einer 10Mbit Karte wird dann automatisch auf 10Mbit gedrosselt.

8.7 1000BaseT / Gigabit Ethernet

Diese verhältnismäßig neue Netzwerktechnologie, die Ende der 90er Jahre entwickelt wurde, ermöglicht eine Netzgeschwindigkeit von 1000Mbps. Dieser Netzwerktyp wird für sogenannte Rückgratnetzwerke verwendet, also solche Netze, in denen die Daten von vielen anderen Netzen zusammenlaufen. Auch bei Gigabit Ethernets geht es nicht darum, eine möglichst große Geschwindigkeit zwischen zwei Computern herzustellen, vielmehr sind sie in der Lage, den Verkehr von zehn 100Mbit Netzwerken aufzunehmen und mit gleicher Geschwindigkeit weiterzuleiten.
Der Vorteil dieser Technologie liegt neben der hohen Geschwindigkeit darin, dass auch hier das Paketformat und die Paketgröße gleich geblieben sind. Deswegen ist es möglich, ein Datenpaket, welches in einem 10Mbit-Netzwerk erstellt wurde direkt durch das Gigabit Netz zu leiten, ohne dass die Daten neu verkapselt werden müssen.
Der Nachteil liegt allerdings in der viel höheren Anfälligkeit für elektrische Interferenzen.

So ist nicht gewährleistet, dass ein Kabel, welches mit 100Mbit gut arbeitete auch noch mit 1000Mbit funktioniert. Aus diesem Grund kommen hier häufig Glasfaser- Kabel zum Einsatz, da diese gegen elektrische Inteferenzen unempfindlich sind.



9 Kapselung und Aufbau eines Ethernet-Frames, Demultiplexing

9.1 Kapselung

Will eine Anwendung Daten verschicken, so müssen diese Daten jeden Layer des Vier-Schichten Models auf ihrem Weg nach unten passieren, bis sie als Stream von Bits über den Ether geschickt werden. In der TCP/IP Protocol-Suite ist es aber gängig, dass der Transportlayer nicht nur von einer Anwendung Daten erhält, sondern von mehrern. Gleiches gilt für die unteren Schichte. Es erhält also jeder Layer Daten von verschiedenen Komponenten der Oberschicht. Um diese Daten auch wieder an die richtige Komponente zurückliefern zu können, fügt jede Schicht den erhaltenen Daten einen Header oder Trailer hinzu. Diesen Prozess nennt man Kapselung oder Encapsulation.
Im Detail bedeutet das, dass eine Anwendung, die Daten über das Netz verschickt, auch wenn sie die Daten erhalten hat noch wissen muss, was mit diesen Daten geschehen soll. Deshalb speichert sie dies Informationen in einem spezifischem Header und stellt ihn den Daten voran.
Damit TCP auch nach dem Versand noch weiss, von welcher Anwendung die Daten stammen, fügt es ebenfalls einen Header mit zwei 16 Bit Ports zum Speichern der Ziel -und Ursprungsanwendung hinzu.
Bei Ethernet gibt es das Problem, dass es mehrere verschiedene Protokollfamilien gibt, die Ethernet als Link-Layer benutzen. Aus diesem Grund enthält dessen Header einen 8bit Frame Typ. Dieses Feld gibt an, welche Art von Daten transportiert werden (0800 für IP, 0806 für ARP und 8035 für RARP). Man spricht dabei von self identifying. Der Frame weiss selbst, was er transportiert und welche Protocoll Suite angewendet werden soll.
Zu Beginn des Headers steht aber zunächst das Preamble, ein 8byte großes Feld, nur aus alternierenden Einsen und Nullen bestehend. Diese Feld dient der Synchronisation

zwischen zwei Netzwerkkarten.
Ebenfalls im Header werden in zwei 6byte Adressen die Source- und Destination Hardware Adress gespeichert. Eine Hardware Adress ist eine Nummer, die jedem Computer weltweit einzigartig zugewiesen ist und auf der Netzwerkkarte gespeichert ist. Um die Einzigartigkeit der Adressen zu gewährleisten, kaufen Netzwerkkartenhersteller Blocks dieser Adressen bei IEEE und verwenden sie für ihre Netzwerkkarten. Dass die Hardwareadresse auf Netzwerkkarte gespeichert sind, hat den Nachteil, dass mit dem austauschen einer Netzwerkkarte ein Computer eine völlig andere Hardwareadresse erhalten kann. Aus diesem Grund müssen die oberen Layer von dieser Hardwareadresse unabhängig sein. Die Zuordnung zwischen der Hardware und der dazugehörenden IP-Adresse erfolgt dabei über die ARP und RARP Protokolle.
Die Hardware Adressen erfüllen aber noch einen weiteren Zweck: In allen Ethernet Netzwerken herrscht Broadcast. Das bedeutet, dass stets alle Pakete an alle Computer im Netz gesendet werden. Bei dem jeweiligen Host angekommen entscheidet dann die Hardware der Ethernetkarte anhand der Hardwareadresse, ob das jeweilige Paket auch wirklich an diesen Computer adressiert war. Falls dem so ist, werden die Daten an die nächst höhere Schicht weitergereicht, wenn nicht, wird das Paket ignoriert.
Eine Ausnahme zu dieser Regel bilden aber die Broadcast-Adressen (alle Stellen auf 1) und die sogenannten Multicast-Adressen.
Die Broadcast-Adresse wird von jeder Karte im Netz akzeptiert und die Daten weitergeleitet. Multicasting ist eine etwas eingeschränkte und spezifischere Form des Broadcasting. Beim Multicasting wird die Ethernetkarte angewiesen, alle Daten anzunehmen, die von einer gewünschten Multicast Adresse stammen.
Der Ethernetframe enthält aber zusätzlich zu dem oben genannten Headerinformationen noch einen Trailer, dem sogenannten CRC (Cyclic Redundancy Check). Hierbei handelt es sich um eine Prüfsumme, die einmal vom Empfänger aus den Daten des Frames errechnet wird (üblicherweise durch Division mit einem einfachem Polynom) und einmal vom Empfänger. Die Ergebnisse müssen dabei gleich sein, sonst hat ein Übertragungsfehler stattgefunden. Die CRC bietet keine Möglichkeit der Korrektur der Daten. Stimmt das Ergebnis nicht und sind die Daten damit als Fehlerhaft identifiziert, so werden sie weggeworfen und müssen neu angefordert werden.
Des weiteren gelten für die Daten eine bestimmte mindes- bzw. maximal Länge, die von der MTU (siehe unten) definiert werden. Sind die Daaten zu lang, so teilt IP sie in Fragmente, die alle kleiner als die maximale Größe sind. Sind sie zu kurz, so werden sie durch Einfügen von Leer-Pads auf die zulässige Mindestlänge gebracht.

9.2 Demultiplexing

Ist der Datenstrom am Zielhost eingetroffen, so müssen die Daten zu der richtigen Anwendung weitergeleitet werden. Dabei entnimmt jeder Layer den Daten dem zuhörigen Header und sucht darin nach Informationen über die Zielkomponente aus der Oberschicht. Die Daten wandern also den Stack wieder herauf, bis sie an der richtigen Applikation angekommen sind. Diesen Prozess bezeichnet man als Demultiplexing.

10 IEEE 802

Ein etwas anderer aber kompatibler Standart zum True-Ethernet bildet der etwas später vom IEEE 802 Komitee veröffentlichte IEEE 802 Standard. Er enthält die kompletten CSMA/CD-Networks, Tokenbus und Token-Ring Networks. Die Kapselung hierfür ist definiert im RFC 1042. Sie ist in großen Teilen gleich dem Ethernetstandard, nämlich bezüglich des Preambles, den Hardware-Adressen und der CRC.
An der Stelle des Type-Fields bei Ethernet findet man hier allerdings ein Length-Field, dass die Länge der folgenden Daten bis zur CRC angibt. Der Grund ist der, dass aufgrund der Collision Detection sehr viele kurze Müll-Fragmente im Ether umherirren. Um bei Daten leichter feststellen zu können, ob es sich um Müll oder um richtige Daten handelt, wird das Length-Field genutzt um zu prüfen, ob die angegebene Menge der tatsächlich erhaltenen entspricht.
Danach folgen im IEEE-Frame angaben für das LLC (Logical Link Control). Diese sind aber für diese Form der Kapselung unerheblich und erhalten einen konstanten Wert. Ähnliches gilt für die folgenden Informationen zum SNAP (Sub Network Access Protocol). Der darin enthaltene Org-Code wird auf Null gesetzt, dass dann folgende Type-Field ist das selbe wie beim True-Ethernet.
Beide Protokolle unterscheiden sich geringfügig in der zugelassenen Länge der Daten.

11 MTU und Path-MTU

Die oben genannte zulässige Maximalgröße wird bestimmt von der MTU (Maximum Transmission Unit). Dieser Wert ist nicht alleine durch die physikalische Beschaffentheit der Netzwerkmediums bestimmt, sondern vielmehr eine logische Größe, um Antworten in adäquater Zeit zu gewährleisten. So muss man sich vor Augen halten, dass bei einem 500m langem Kabel die Daten erst nach einiger Verzögerung am anderen Ende des Kabels eintreffen. Auch ist vorstellbar, dass durch eine kleinere MTU der Datenverlust möglichst gering gehalten wird, falls eine Kollision auftritt. Da die Daten auf ihrem Weg zum Empfänger sehr häufig nicht nur ein Netz, sondern mehrere passieren, hat man keine einheitliche MTU. Die sogenannte Path-MTU wird dabei nicht durch die MTU des Sender- und Empfängernetzes bestimmt, sondern vielmehr durch die kleinste MTU innerhalb aller passierter Netze. Auf Grund der Tatsache, dass die Daten im Internet aber ständig anders geroutet werden, hat man auch immer eine unterschiedliche Path-MTU.

12 Quellen

- TCP / IP illustrated Band 1 -
  W. Richard Stevens, Gary R. Wright
- Internetworking with TCP / IP -
  Douglas Comer
- Computernetzwerke -
  Andrew S. Tanenbaum