SelfLinux-0.13.1

Lokale Netze

Autor: Guido EhlertMatthias Kleine (*guido@ge-soft.dekleine_matthias@gmx.de*)
Formatierung: Frank Börner (*frank@frank-boerner.de*)

Inhaltsverzeichnis

1 Einleitung

2 Ethernet

2.1 Thick Ethernet (10Base5)
2.2 Thin Ethernet (10Base2)
2.3 10BaseT
2.4 Fast Ethernet (100BaseT)
2.5 Funktionsweise

3 FDDI

4 Token Ring

5 ATM - Asynchronus Transfer Mode

6 Netzwerk-Hardware

6.1 Netzwerk-Interface
6.2 Repeater
6.3 Bridges
6.4 Hubs
6.5 Switches
6.6 Router

1 Einleitung

Wie bereits angedeutet, gibt es eine große Anzahl von Technologien zum Aufbau lokaler Netze (Local Area Networks kurz LANs). Als wichtigste Vertreter sollen im Folgenden Ethernet (mit all seinen Varianten), Token Ring, FDDI und ATM detailliert vorgestellt werden.

Allen LAN-Typen ist gemein, dass man für den Anschluss an das Netzwerk natürlich über entsprechende Hardware, in den meisten Fällen eine Netzwerkkarte des jeweiligen Typs im lokalen Rechner, verfügen muss.

2 Ethernet

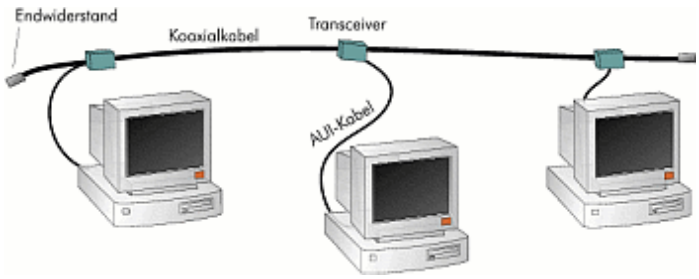
Das Ethernet wurde 1973 am Xerox PARC als Teil eines umfangreichen Forschungsprojektes für verteilte Systeme entwickelt und sollte die Vorteile einer schnellen, lokalen Vernetzung mit niedrigen Fehlerraten und ohne Verzögerungen aufzeigen.

Auf Grund seiner Einfachheit und der kostengünstigen Hardware hat Ethernet bis heute eine starke Verbreitung gefunden und ist in seinen Variationen in sehr vielen LANs anzutreffen.

2.1 Thick Ethernet (10Base5)

Das Original-Ethernet (festgelegt im Standard IEEE 802.3) besteht aus einem Koaxial-Kabel mit einem halben Zoll (1,27 cm) Durchmesser, an das die Rechner über sogenannte "Transceiver" angeschlossen sind. An jedem Ende des Kabels befindet sich ein Endwiderstand von 50 Ohm, der auch als "Terminator" bezeichnet wird (siehe Abbildung). Über ein derartiges Netzwerk lassen sich Geschwindigkeiten bis 10 Mbps (Megabit pro Sekunde) erreichen.

Ein Kabel mit einem derartigen Durchmesser ist etwas unhandlich, daher wird diese Art des Ethernets auch als "Thick Ethernet" oder "10Base5" bezeichnet.



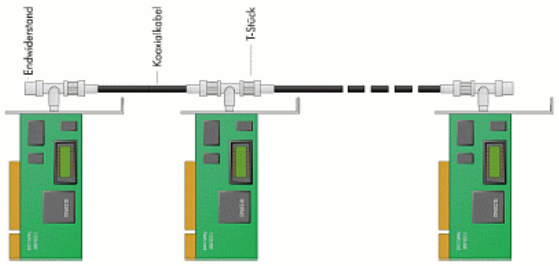
Thick Ethernet

Hinweis:
Den tatsächlich erreichbaren Übertragungswert in Megabyte pro Sekunde erhält man, indem man den Megabit-Wert durch die Zahl 8 dividiert. Diese maximalen Transferraten werden in der Praxis auch nur selten erreicht. Überhaupt ist die Frage nach der notwendigen Geschwindigkeit eines Netzes eng mit der Frage nach den tatsächlich genutzten Anwendungen verbunden.

2.2 Thin Ethernet (10Base2)

Das beim "Thin Ethernet" verwendete Koaxialkabel ist dünner, billiger und einfacher zu handhaben. Der Anschluss an die Netzwerkkarte des Rechners erfolgt über ein sogenanntes "T-Stück", an das links und rechts ein Netzwerkkabel angeschlossen wird, während die `untere' Seite des T's mit der Netzwerkkarte verbunden ist.

Am Anfang und am Ende des Kabelstrangs befinden sich auch hier Endwiderstände von 50 Ohm (Terminatoren). Die Steckverbindungen erfolgen über BNC-Anschlüsse. Mit einem Thin Ethernet kann man Geschwindigkeiten bis 10 MBit erreichen.



Thin Ethernet mit Koaxialverkabelung

2.3 10BaseT

Im Gegensatz zum normalen Thin Ethernet mit seiner Busstruktur ist ein 10BaseT-Netz sternförmig aufgebaut. Von einem Verteiler, dem sogenannten "Hub", führen Twisted-Pair-Kabel zu den einzelnen Rechnern. Der Anschluss erfolgt über RJ45-Stecker, wie sie auch oft bei Telefonen verwendet werden.

Diese Verkabelungsart beseitigt einen gravierenden Nachteil der Busstruktur. Wird der Bus nämlich an einer Stelle unterbrochen, sei es durch ein defektes Kabel oder eine übereifrige Reinigungskraft, ist das Netzwerk vollständig lahm gelegt. Bei einer sternförmigen Verkabelung ist bei einem Kabelschaden nur ein Rechner betroffen, die anderen können ganz normal im Netz weiterarbeiten.

Wäre 10BaseT nicht aufwendiger und teurer als die Koaxialverkabelung, wäre letztere sicher schon ganz von der Bildfläche verschwunden.

Sternförmiges Ethernet mit Hub

2.4 Fast Ethernet (100BaseT)

Der Aufbau eines "Fast Ethernets" ähnelt stark dem eines 10BaseT-Netzes. Jedoch müssen aufgrund der höheren Datengeschwindigkeit von 100 Mbps aufwendigere Twisted-Pair-Kabel der Kategorie 5 verwendet werden. Neben dem Hub müssen natürlich auch die eingesetzten Netzwerkkarten für eine Geschwindigkeit von 100

Mbps vorgesehen sein.

Übertragungsraten von bis zu 1000 Mbps erreicht man mit Hilfe von geschirmten Kabeln (Shielded Twisted Pair - STP) bzw. Glasfaserleitungen. Netzwerkkarten und Hubs für derartige Geschwindigkeiten müssen wesentlich aufwendiger konstruiert sein und sind dementsprechend teuer. Da kaum ein Rechner einen Datenstrom von 1 Gbps (enspricht 125 MByte pro Sekunde!) verarbeiten kann, werden Gigabit-Ethernets vor allem als Backbone-Leitungen verwendet, die ganze Netzwerke miteinander verbinden.

Die folgende Tabelle zeigt noch einmal eine Übersicht über alle Ethernet- Varianten:

Ethernet-Typ	Geschwindigkeit	max. Länge	Struktur	Kabelart	Anschluss am Rechner
10Base2 (Thin Ethernet)	10Mbps	185m	Bus	Koaxial	BNC-Buchse, T-Stück, (RG58, T-Stück, Endwiderstand)
10Base5 (Thick Ethernet)	10Mbps	500m	Bus	Koaxial	AUI-Buchse, Transceiver
10BaseF	10Mbps	2000m	Bus	Glasfaser	Optokoppler
10BaseT	10Mbps	100m	Stern	Twisted Pair	RJ45-Anschluss Kat.3
100BaseT	100Mbps	100m	Stern	Twisted Pair	RJ45-Anschluss Kat.5
Gigabit-Eth.	1Gbps	1Gbps	Stern	STP	Spezieller Anschluss Kat. 6
	1Gbps	500m	Stern	Glasfaser	Optokoppler

2.5 Funktionsweise

Neben der Verkabelung ist es natürlich interessant zu wissen, was auf einem Ethernet-Kabel eigentlich passiert. Jedes Gerät im Ethernet hat eine eindeutige Hardware-Adresse von 6 Byte Länge, die auch als MAC-Adresse bezeichnet wird. Das Kürzel MAC steht hier für Media Access Control. Diese Adresse hat nichts mit den IP-Nummern des TCP/IP-Protokolls zu tun (zumindest nicht direkt) und auch nichts mit den Computern der Firma Apple (auch nicht indirekt). Pakete im Ethernet enthalten immer die Hardware-Adresse des Senders und des Empfängers.

Das Versenden von Daten erfolgt über ein sogenanntes "Packet Broadcasting", d.h. jedes Paket wird einfach auf das Kabel gesendet. Alle anderen Stationen erhalten, bzw. `sehen' dieses Paket, es wird jedoch nur von dem festgelegten Empfänger entgegengenommen und verarbeitet.

Wenn zwei Stationen gleichzeitig Daten senden, kommt es konsequenterweise zu Paketkollisionen (natürlich "rumst" es nicht im Kabel, sondern die elektrischen Impulse der beiden Sender überschneiden sich und werden damit unbrauchbar). Das Ethernet definiert drei Varianten, mit diesem Verhalten umzugehen:

* Die Stationen `lauschen' ständig am Bus und merken so, ob auf dem Kabel Datenverkehr stattfindet. Eine Station sendet erst, wenn keine Signale mehr auf dem Kabel liegen, um die laufende Übertragung nicht zu zerschmettern.
* Sollten zwei Stationen genau zum selben Zeitpunkt mit dem Senden beginnen, kommt es trotzdem zur Kollision. Während eine Station sendet, prüft sie gleichzeitig auf dem Empfangskanal, ob die Signale korrekt versendet wurden. Da alle Stationen im Netz einschließlich der Sendenden die Signale empfangen, stellt dies kein Problem dar. Erkennt die sendende Station nun, dass die Daten nicht korrekt übertragen werden, handelt es sich wahrscheinlich um eine Kollision. Die sendende Station schickt ein

Kollisionssignal in das Kabel, was bewirkt, dass alle Stationen im Netz ihre Sendetätigkeit abbrechen (die ja vorhanden sein muss, sonst hätte es keine Kollision gegeben). Nach einer zufällig bestimmten Zeit versucht die Station wieder zu senden. Die andere Station, mit der es zur Kollision kam, hat eine andere Zufallszeit ermittelt und wird dann merken, dass das Netz bereits belegt ist. Sollten beide Stationen trotzdem wieder zur selben Zeit senden, was extrem unwahrscheinlich ist, beginnt das Spiel eben wieder von vorn.

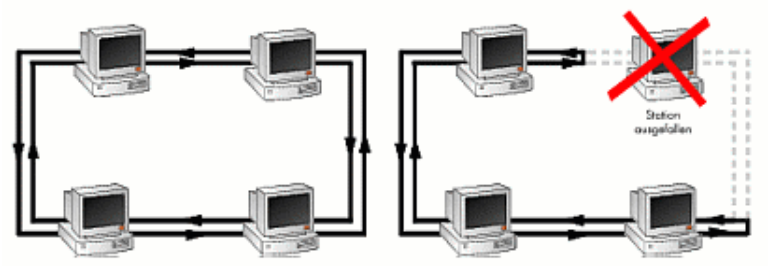
* Als Sicherungsmaßnahme wird die Prüfsumme eines Ethernet-Paketes (korrekt heißt es Ethernet-Frame) mit dem tatsächlichen Inhalt verglichen. Kommt es dabei zu Unstimmigkeiten, wird das Paket vom Empfänger abgewiesen.

3 FDDI

Die Abkürzung FDDI steht für "Fiber Distributed Data Interconnect". Dieser Netzwerktyp überträgt seine Daten nicht über Kabel, sondern über Lichtimpulse auf Glasfaserleitungen. Dies hat den Vorteil, dass die Datenübertragung nicht durch elektromagnetische Störungen beeinflusst werden kann. Außerdem ist mit Lichtimpulsen eine höhere Datenübertragungsrate möglich als bei elektrischen Signalen.

Ein FDDI-Netz ist ein Token-Ring-Netzwerk mit einer Bandbreite von 100 Megabit pro Sekunde. Um Störungen automatisch beheben zu können, besteht ein FDDI-Netz aus zwei in entgegengesetzte Richtungen laufenden Ringen. Der Datenverkehr erfolgt wie bei jedem Token-Ring-LAN über ein Token, dass ständig im Kreis läuft. Im normalen Betrieb wird von den zwei vorhandenen Ringen lediglich einer genutzt. Interessant wird das Verhalten von FDDI, wenn ein Hardware-Fehler im Netz auftritt. Wenn ein Gerät bemerkt, dass eine Kommunikation zu einem anderen Gerät im Netz nicht möglich ist, benutzt es automatisch den zweiten Ring, um den aufgetretenen Defekt zu umgehen. Wird der Ring also, aus welchen Gründen auch immer, an einer Stelle unterbrochen, leiten die zwei benachbarten Stationen den Datenverkehr automatisch auf den zweiten Ring um. Die Abbildung illustriert dieses Verhalten:

FDDI-Netz im normalen Betrieb (links) und bei einem Defekt (rechts): Der Netzverkehr kann trotzdem weiter durchgeführt werden.



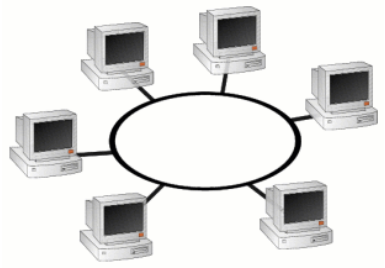
4 Token Ring

Token-Ring-Netze wurden relativ früh entwickelt, sind jedoch nicht so stark verbreitet wie andere LAN-Technologien. Die logische Struktur dieses Netztyps entspricht, wie der Name schon sagt, der eines geschlossenen Ringes. Die tatsächliche Struktur muss dem nicht entsprechen, Token-Ring-Netze sind auch mit sternförmiger Verkabelung möglich. Beschränken wir uns also auf die Art der Datenübertragung:

Um die Funktionsweise von Token-Ring-Netzwerken zu verstehen, kann man das Beispiel eines Güterzuges heranziehen, der immer wieder eine Kreisstrecke befährt und regelmäßig an allen Stationen vorbeikommt. Die Lokomotive stellt hierbei das sogenannte "Token"-Paket dar. Je nachdem ob Waggons, also Daten, angehängt wurden, wird die Lokomotive als frei oder belegt gekennzeichnet. Möchte eine Station nun Daten versenden, prüft sie, ob das Token frei ist. Ist dies der Fall, wird das Token als belegt gekennzeichnet, mit der Zieladresse versehen und die Daten angehängt. Unser Zug fährt weiter im Kreis, bis er die festgelegte Zielstation erreicht hat und trennt sich dort von seinen Daten. Das Token wird wieder als frei gekennzeichnet und kann erneut Daten transportieren.

So geht das Token ständig von Rechner zu Rechner. Ist der Inhalt des Datenpakets nicht für den jeweiligen Rechner bestimmt, sendet er das Token weiter. So ist gewährleistet, dass jede Station die gleichen Chancen hat, Daten senden zu können. Anders als beim Ethernet gibt es hier nicht das Problem mit den Paketkollisionen, da ja

immer nur ein Paket unterwegs ist.



Token Ring Netzwerk

5 ATM - Asynchronus Transfer Mode

Bei ATM handelt es sich um eine verbindungsorientierte Hochgeschwindigkeitsnetzwerk-Technologie, die sowohl in lokalen Netzen als auch in Wide Area Networks (WANs) zum Einsatz kommt. Üblicherweise meint "Hochgeschwindigkeit" Netzwerke mit Datentransferraten von 100 Mbps und höher. ATM kann je nach darunter liegender Netzwerktechnik Transferraten bis in den Gigabit-Bereich erreichen. Entsprechend teuer ist auch die für ATM erforderliche Hardware.

Um derartig hohe Geschwindigkeiten erreichen zu können, verwendet ATM mehrere spezielle Hardware- und Software-Techniken:

* Ein ATM-Netzwerk besteht aus einem oder mehreren ATM-Switches, die mit Host-Rechnern oder wiederum mit weiteren ATM-Switches verbunden sein können.
* ATM benutzt optische Medien wie Glasfaserleitungen zur Datenübertragung, auch als Verbindung zwischen Hosts und ATM-Switch.
* Pakete (sog. "Cells") in der untersten Schicht von ATM-Netzwerken haben eine feste Länge. Da jedes Paket exakt dieselbe Größe hat, können ATM-Cells sehr schnell verarbeitet werden.

ATM unterscheidet sich stark von den bisher beschriebenen paketorientierten Netzwerken. Im Gegensatz zu ihnen ist ATM verbindungsorientiert angelegt und eignet sich daher auch zur Übertragung von Sprache (große Teile des Telefonnetzes bauen auf ATM-Backbones auf). Doch bleiben wir bei Rechnernetzen: Möchte ein Host eine Verbindung zu einem anderen aufbauen, kontaktiert er den nächsten ATM-Switch und teilt ihm seinen Verbindungswunsch samt Adresse des Zielrechners mit. Der Switch versucht nun, eine Verbindung zu diesem herzustellen. Dabei entsteht eine Art Pfad über weitere Switches. Ersterer Switch legt nun für diese Verbindung bzw. diesen Pfad eine eindeutige Nummer fest und teilt dem Host diese mit. Ist eine Verbindung einmal aufgebaut, sind Übertragungen mit garantierter Bandbreite darüber möglich. Eine Verbindung bleibt bestehen, bis einer der beiden Partner diese trennt, also 'auflegt'.

Möchte der Host nun Daten versenden, schickt er diese samt Verbindungsnummer (die Verbindung besteht bereits) zum Switch. Dieser hat die Nummer gespeichert und weiß, an welchen Switch er die Daten weiterschalten und welche ID-Nummer er dort benutzen muss. Der nächste Switch tut genau dasselbe bis die Daten irgendwann beim Zielrechner angekommen sind. Dabei weiß jeder Switch nur, an wen er die Daten einer bestimmten Verbindung weiterleiten muss. Er hat keine Information über die Herkunft oder den letztendlichen Empfänger. Dies sorgt dafür, dass im Netz sehr wenig Overhead (Verwaltungsdaten) durch die Leitungen geschoben wird, was der Geschwindigkeit direkt zugute kommt.

6 Netzwerk-Hardware

Für ein funktionierendes Netzwerk, bedarf es einiger technischer Geräte. Für ein kleines Netzwerk sind dies im einfachsten Fall zwei Netzwerkkarten und ein Kabel. Bei größeren Netzwerken tauchen aber bereits Bezeichnungen wie Router, Hubs, Switches und ähnlich 'selbsterklärende' Begriffe in nicht geringer Anzahl auf, mit denen ein normaler Anwender selten etwas anzufangen weiß. Genau diese Bezeichnungen werden in diesem Kapitel näher erläutert.

6.1 Netzwerk-Interface

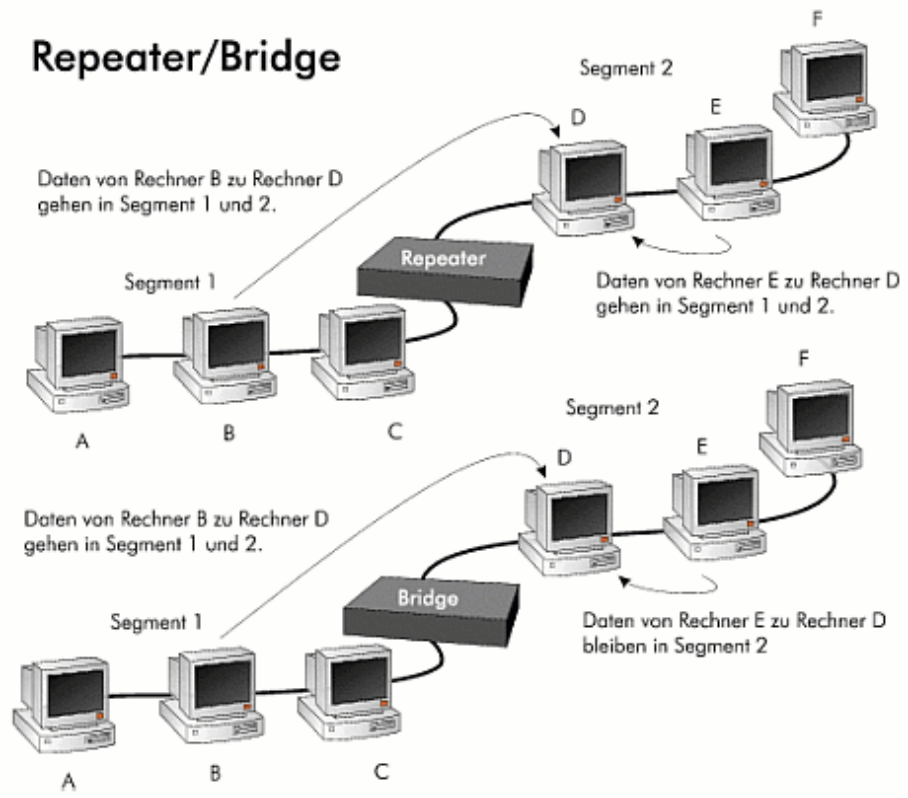
Um einen Computer an einem Netzwerk teilhaben zu lassen, benötigt er natürlich mindestens eine Netzwerkkarte, auch als "Network Interface Card (NIC)" bezeichnet. Diese Karte muss zu dem vorhandenen Netzwerk passen. Es gibt verschiedenste Ausführungen, vom 10MBit-Ethernet bis zur ultraschnellen Glasfaserübertragung ist alles dabei. Bei Ethernet-Netzwerkkarten ist eine Hardware-Adresse auf der Karte `eingebrannt', die diese Karte weltweit eindeutig im Netzwerk identifiziert. Diese Adresse wird auch als "MAC-Adresse" (MAC für Media Access Control) bezeichnet. MAC-Adressen werden den Hardwareherstellern von einer zentralen Stelle zugewiesen. Anhand der Adresse lässt sich dort auch der Hersteller der Hardware ermitteln. Wenn die Karte dann noch im Betriebssystem des Rechners ordentlich eingerichtet wurde, steht einem Betrieb im Netz nichts mehr im Wege. Netzwerkkarten sind entweder aus Platzgründen bereits auf dem Motherboard des Rechners fest eingebaut oder werden als separate Steckkarten verkauft. Für ihren Betrieb ist in der Regel eine passende Treibersoftware nötig.

6.2 Repeater

Repeater werden vor allem in busförmigen Ethernets (sprich: Koaxialkabel) verwendet. Ihre einzige Funktion ist die empfangenen Signale zu verstärken und weiterzugeben. So ist es möglich, ein Koaxial-Ethernet in mehrere Segmente zu teilen, um mehr als 185 Meter maximale Kabellänge zu erreichen. In einem Netzwerk können maximal drei solcher Segmente gebildet werden. Diese Segmente erscheinen den angeschlossenen Rechnern aber wie ein Netz, da ja die elektrischen Impulse von der einen Seite des Repeaters auf der anderen nur verstärkt werden. Repeater agieren daher im OSI-Schichtenmodell in der Schicht 1, also rein hardwarebasiert.

6.3 Bridges

Im Gegensatz zu Repeatern entscheiden Bridges anhand der MAC-Adresse des Empfängers, ob sie ein Paket oder Frame in das nächste Segment weiterleiten. Bridges werden vor allem zur Segmentierung und Geschwindigkeitssteigerung von Netzwerken eingesetzt, da sie im Gegensatz zu Repeatern das Signal nicht einfach verstärken, sondern auch filtern. Sie arbeiten auf dem Level 2 des OSI-Schichtenmodells.



Wirkungsweise von Repeatern und Bridges

6.4 Hubs

Ein Hub wird auch als "Konzentrator" oder "Verteiler" bezeichnet. In sternförmig aufgebauten Netzwerken bildet er den zentralen Punkt. Kabel führen immer von einem Port des Hubs zu einem Rechner im Netz, so dass letztendlich eine Art Stern entsteht (siehe Abbildung im Abschnitt Lokale Netze).

Statt eines Rechners kann man an einen Hub auch einen weiteren Hub anschließen, so dass weitere Anschlüsse zur Verfügung stehen. Hubs gibt es für Twisted-Pair-Ethernet mit üblicherweise 5 bis 24 Ports. Sie können entweder für Geschwindigkeiten von 10 oder 100 Mbps konstruiert sein. Es sind auch Dual-Speed-Hubs erhältlich (10 und 100Mbps). Diese beinhalten aber eigentlich zwei getrennte Hubs, die switch-artig miteinander gekoppelt und entsprechend teurer sind. Auch Hubs leiten den Netzwerkverkehr lediglich von einer Station auf alle anderen weiter, so dass sich alle am Hub angeschlossenen Stationen die Bandbreite teilen müssen. Sie arbeiten nur auf dem untersten Hardware-Level der Schicht 1 des OSI Modells.

6.5 Switches

Im Vergleich zu Hubs sind Switches schon etwas intelligenter. Äußerlich sind sie von Hubs nicht zu unterscheiden, im Inneren verbirgt sich allerdings eine ganz andere Technik. Im Gegensatz zu einem Hub, wo sich alle Rechner die gesamte Bandbreite des Netzes teilen müssen, kann jeder an einen Switch angeschlossene Host die volle Bandbreite nutzen. Dementsprechend schneller sind geswitchte Netze.

Doch wie funktioniert dies im Einzelnen? Im Gegensatz zum Hub, leitet ein Switch Pakete nur an den Switch-Port weiter, an dem sich der Empfänger befindet. Statt also ein Paket von Rechner A zu Rechner B an alle Ports und damit in das gesamte Netz zu "blasen", wird es nur zu dem Port geschaltet, an dem Rechner B angeschlossen ist. Damit entsteht eine Art virtuelle Verbindung zwischen den beiden Kommunikationspartnern. So wird unnötige Netzlast in den anderen Segmenten vermieden und die Geschwindigkeit gesteigert. Switches sind auf der Schicht 2 (Sicherungsschicht) des OSI-Modells einzuordnen.

6.6 Router

Der Begriff "Router" (darüber, ob man dieses Wort als `Ruter' oder 'Rauter` ausspricht, konnte sich noch niemand so recht einigen, daher sind beide Varianten akzeptabel) bezeichnet Geräte, die zwei oder mehrere Netzwerke miteinander verbinden. Hierbei ist ein Router dafür zuständig, die Pakete aus einem Netz in das andere zu leiten. Im Gegensatz zu Bridges können sie völlig unterschiedliche Netzwerkmedien, z.B. Token Ring und FDDI, miteinander verbinden.

Damit das Routing über mehrere Netze funktioniert, hält jeder Router eine Routingtabelle vor, die Einträge in Form von Netzwerkadressen enthält. Anhand dieser Tabelle leitet er Pakete in das korrekte Netzsegment weiter. Ein Router kann dabei ein Rechner sein, der mit mehreren Netzwerkkarten ausgestattet und mit jeder Karte an je ein Netzwerk angeschlossen ist. Es gibt aber auch spezielle Geräte, die für das Routing optimiert wurden und eine wesentlich höhere Anzahl Pakete routen können. Als Beispiel sei hier das Routing im Internet erwähnt, wo jede Anfrage durch etliche Netze geleitet werden muss. Um nachzuvollziehen, über welche Hosts eine Anfrage weitergeleitet wird, kann man das Programm traceroute (bzw. tracert unter Windows) verwenden.

Router arbeiten auf Schicht 3 des OSI-Schichtenmodells, da sie bereits Entscheidungen anhand von konkreten Adressen treffen.