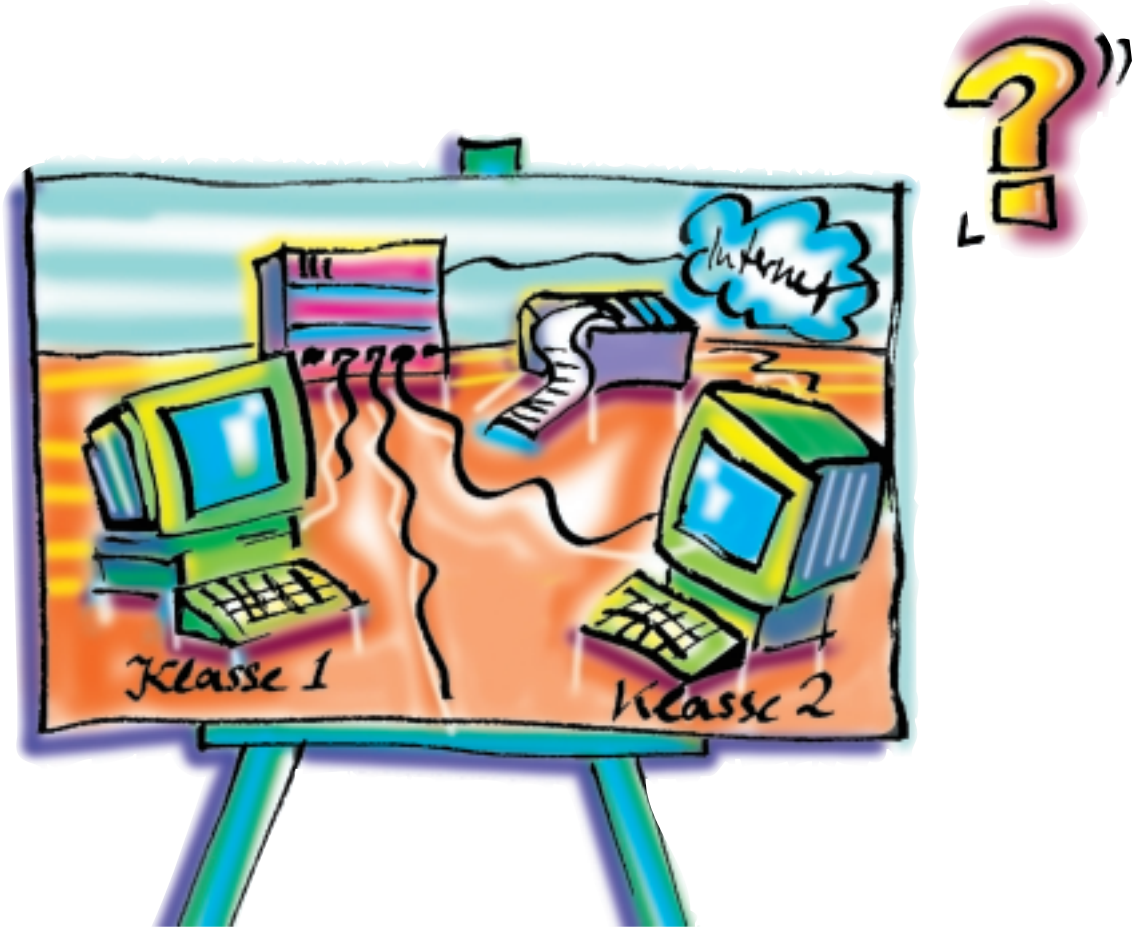
Lokale Netzwerke, Internet, kabellose Netze



Die vernetzte Schule e.V.

Netzwerkleitfaden zur Planung, für den Aufbau oder die Erweiterung eines Schulnetzwerks.

Das Ziel des Vereins „Die vernetzte Schule e.V.“ ist es, die Schulen bundesweit beim Auf- und Ausbau ihres lokalen Netzwerks und der Internet-Anbindung zu unterstützen. Die Gründer der Initiative sind davon ausgegangen, dass dies nur dann erfolgreich realisiert werden kann, wenn die Schulen, der Staat und die Wirtschaft sich gemeinsam darum bemühen. Dazu sind gegenseitiges Verstehen und gemeinsame Anstrengungen nötig.

INHALTSVERZEICHNIS

Neueste und aktuelle Informationen
finden Sie immer unter:

www.dievers.de

Auch diesen Leitfaden und
alle weiteren Orientierungshilfen können
Sie im Web bestellen.

A. VORSTELLUNG

Das im Oktober 1999 auf dem Stand „Computer und Schule“ des bayerischen Kultusministeriums auf der SYSTEMS in München vorgestellte Projekt „Die vernetzte Schule“, ist mittlerweile ein gemeinnütziger Verein.

Neben den Sponsoren der „ersten Stunde“, ELSA AG und SMC Networks GmbH, konnten inzwischen weitere Firmen als Sponsoren gewonnen werden. Eine Auflistung finden Sie unter www.dievers.de

Ziel der Initiative ist es, möglichst viele Schulen mit einem Netzwerk und einem Internet-Zugang auszustatten und so die technischen Voraussetzungen für den sinnvollen Einsatz der Informationstechnologie an Schulen zu schaffen.

Der Internet-Zugang für Schulen ist bereits seit einigen Jahren in aller Munde und in einigen Fällen auch bereits realisiert. Aber um ihn für alle Schüler gewinnbringend einsetzen zu können, sollte es möglich sein, von sämtlichen PCs aus, die in einer Schule installiert sind, gleichzeitig darauf zuzugreifen. Dies kann aber nur mit einem funktionsfähigen Netzwerk, das alle vorhandenen Schulrechner miteinander verbindet, in die Tat umgesetzt werden.

Ein Netzwerk der Schulrechner ermöglicht zusätzlich zu der gemeinsamen Nutzung des Internet-Zuganges auch den sinnvollen und realistischen Einsatz von rechnergestütztem und multimedialem Unterricht. Denn nun können zentral verwaltete Server eingesetzt werden, auf denen die erforderlichen Programme abgelegt werden. Das bedeutet, dass die Programme bei Bedarf aus allen Klassenräumen, die mit PCs ausgestattet und an das Netzwerk angeschlossen sind, ohne Installationsaufwand für die einzelnen Schüler-PCs sofort abgerufen werden können. Die Rechner, an denen die Schüler arbeiten, verfügen nur noch über die notwendigste Software. Dadurch minimiert sich der Verwaltungsaufwand, um diese Rechner funktionsfähig zu halten.

Die vorliegende Information stellt eine Planungshilfe für die Schulen bei der Konzeption und der Umsetzung eines Schulnetzwerks dar. Schritt für Schritt wird an Hand von Beispielen aufgeführt, welche Komponenten für eine Vernetzung notwendig sind. Die Beispiele beginnen mit der Vernetzung der PCs in einem einzigen Klassenraum. Sie zeigen weiterhin, wie nach und nach andere Klassenräume angeschlossen werden bis hin zur Vernetzung der gesamten Schule. Sonderfälle wie z. B. weit entfernt liegende Klassenräume oder drahtlose Vernetzung sind ebenfalls abgehandelt. Auch für den Anschluss an das Internet, sei es für nur einen Klassenraum oder die gesamte Schule, sind Beispiele enthalten.

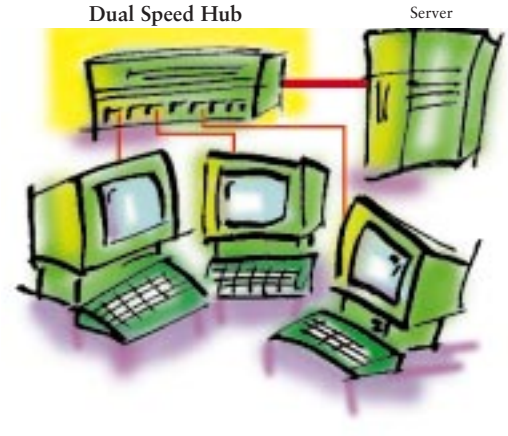
Es ist ein standardisierter und erweiterungsfähiger Baukasten mit allen Elementen zusammengestellt worden, die für ein Netzwerk, sei es groß oder klein, benötigt werden. Diese Elemente sind einem umfassenden Portfolio namhafter Hersteller entnommen. Dadurch können auch in Zukunft neue Entwicklungen und Technologien integriert werden und der Investitionsschutz ist so gesichert.

Die vorliegende Planungshilfe enthält auch im Anhang einen umfassenden technischen Leitfaden, der die Grundlagen der Netzwerktechnologien vermittelt, die für die Vernetzung der Schule eine Rolle spielen. Dazu gehören die LAN-Technologien, mit deren Hilfe innerhalb der Schule die Verbindung der einzelnen PCs realisiert wird. Auch die wesentlichen Informationen für den Internet-Zugang sind enthalten.

„Die vernetzte Schule e.V.“

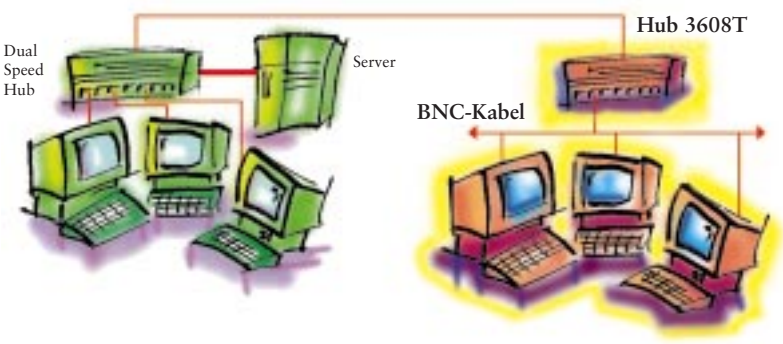
B. SZENARIEN

Beispiel 1: Rechner in einem Klassenraum vernetzt



Es soll ein Klassenraum mit 12 Rechnern ausgestattet werden. Da in diesem Klassenraum auch rechnergestützter Unterricht abgehalten werden soll, wird ein Rechner als Server eingesetzt, auf dem die Programme abgelegt werden. Damit alle Schüler auf diese Programme zugreifen können, müssen alle Rechner miteinander vernetzt werden. Die Rechner sind bereits mit Ethernet-Twisted-Pair-Karten ausgestattet. Es wird ein Hub eingesetzt, mit dem alle Rechner über ein Twisted Pair Kabel verbunden werden. Da die Rechner sich ihre Programme vom Server holen, benötigt dieser einen wesentlich höheren Datendurchsatz. Daher wird der Server mit einer Fast Ethernet-Karte ausgerüstet. Um die Verbindung zwischen den Ethernet-Rechnern und dem Fast Ethernet Server einfach herstellen zu können, wird ein Dual Speed Hub mit 16 Ports wie der 5216DS von SMC gewählt. Dieser Hub ist selbstständig in der Lage, auf allen Ports die maximal mögliche Geschwindigkeit einzustellen.

Beispiel 2: Anschluss eines existierenden BNC-Klassenraums

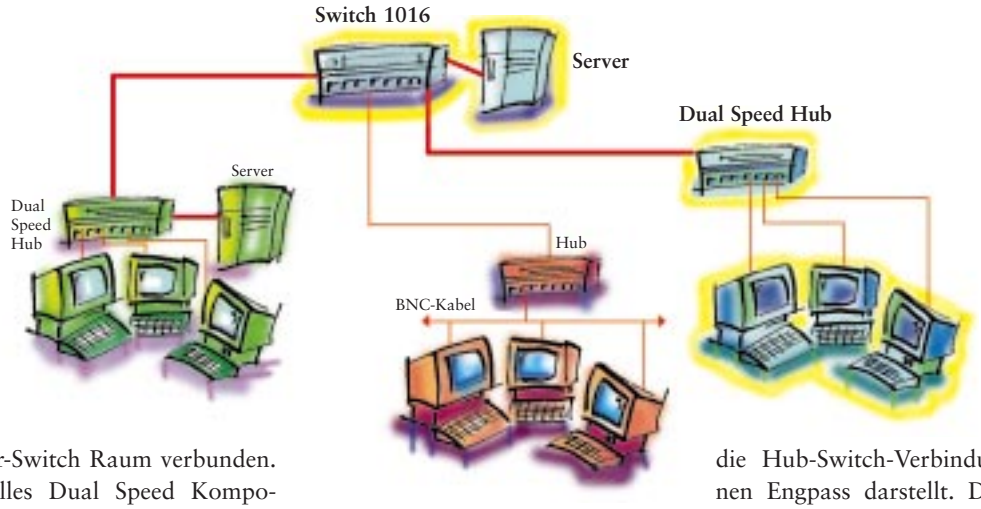


Schon vor einigen Jahren ist ein Rechner-Klassenraum eingerichtet worden. Der Einfachheit halber wurden die Rechner damals mit Thin Ethernet und BNC-Steckern vernetzt. Der Klassenraum bildet eine Insel, er hat keine Verbindung zu dem neuen Netzwerk, das in der Zwischenzeit eingerichtet wurde. Aber auch dieser Klassenraum soll auf den jetzt existierenden Server mit den neuen Unterrichtsprogrammen zugreifen können. Aber dafür wird eine Verbindung zwischen den beiden Netzwerken benötigt. Der eingesetzte Hub, an den auch der Server angeschlossen ist, verfügt noch über einen freien Port. Um das BNC-Netzwerk nicht umkonfigurieren zu müssen, wird der Hub 3608T von SMC eingesetzt. Dieser hat auf der einen Seite eine Verbindung zum BNC-Netzwerk, auf der anderen Seite eine Verbindung über ein Twisted Pair Kabel mit dem existierenden Hub. So wird das gesamte BNC-Netzwerk an das restliche Netzwerk angeschlossen.

Beispiel 3: Mehrere Klassenräume werden vernetzt

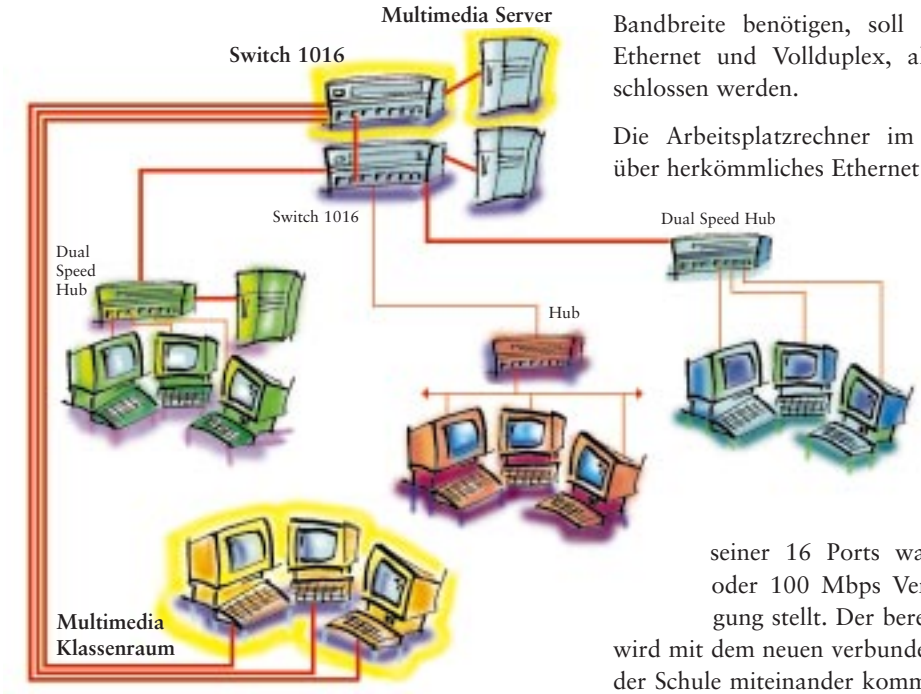
Die neue Art des Unterrichts trifft auf große Akzeptanz. Immer mehr Lehrer und Schüler möchten davon profitieren, immer mehr Klassenräume sollen mit Rechnern ausgestattet werden. Um den Verwaltungsaufwand gering zu halten, entscheidet man sich für einen zentralen Server, auf dem die benötigten Programme abgelegt werden. Dieser Server sollte in einem separaten Raum installiert werden.

Zusätzlich zu dem Server wird in diesem Raum auch der 10/100 Mbps Switch 1016DT von SMC installiert, an den der Server angeschlossen wird. In den Klassenräumen wird jeweils ein Hub eingesetzt, an den die Arbeitsplatzrechner angeschlossen werden. Dies kann ein 8-Port Dual Speed Hub wie der 5208DS von SMC sein oder ein Hub mit 16 Ports wie der 5216DS. Jeder Hub wird mit dem Switch im



Server-Switch Raum verbunden. Da alles Dual Speed Komponenten sind, stellt sich die Hub-Switch-Verbindung automatisch auf 100 Mbps ein. Der Switch bietet zusätzlich den Vorteil, dass er jedem Hub eine eigene, dedizierte 100 Mbps-Verbindung zur Verfügung stellt, sodass bei Zugriffen von mehreren Schülern einer Klasse auf den Server die Hub-Switch-Verbindung keinen Engpass darstellt. Desweiteren wird der Zustand, sowie die Geschwindigkeit der einzelnen Verbindungen, zu PCs, Server und Switch-Hub durch verschiedenfarbige LED's angezeigt, was eine eventuelle Fehlersuche erheblich vereinfacht.

Beispiel 4: Einrichtung eines Multimedia-Klassenraums

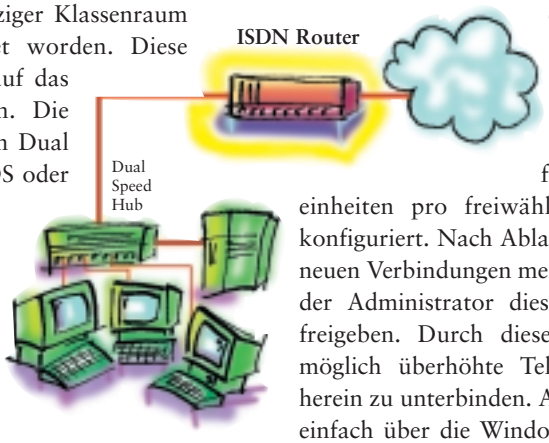


Es soll nun ein eigener Multimedia-Klassenraum eingerichtet werden, um zusätzliche Unterrichtsunterstützung einsetzen zu können. Für die Multimedia-Anwendungen wird ein eigener Server eingerichtet, der auch im Serverraum stehen soll. Da diese Anwendungen bis zum Arbeitsplatzrechner hin, recht viel Bandbreite benötigen, soll der Server über Fast Ethernet und Vollduplex, also 200 Mbps, angeschlossen werden.

Die Arbeitsplatzrechner im Klassenraum werden über herkömmliches Ethernet oder Fast Ethernet angeschlossen, aber jedem Rechner soll eine eigene, dedizierte 10/100 Mbps Verbindung zur Verfügung gestellt werden. Um dies zu erreichen, wird ein weiterer 10/100 Switch eingesetzt, wie der 1016DT von SMC, der auf jedem seiner 16 Ports wahlweise dedizierte 10 oder 100 Mbps Verbindungen zur Verfügung stellt. Der bereits existierende Switch wird mit dem neuen verbunden, sodass alle Rechner der Schule miteinander kommunizieren können. Ein wesentlicher Vorteil liegt hier in der Einfachheit der Konfiguration, denn alle Komponenten erkennen selbstständig die Gegenstelle und damit auch die maximal mögliche Übertragungsgeschwindigkeit, somit ist keinerlei Konfiguration nötig.

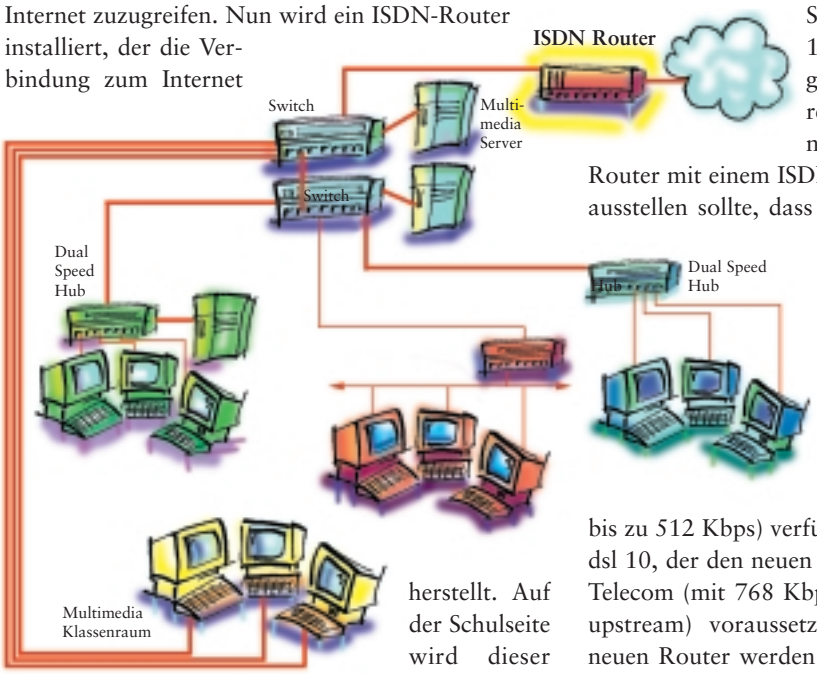
Beispiel 5: Zugang vom EDV-Raum zum Internet

In einer Schule ist ein einziger Klassenraum mit Rechnern ausgestattet worden. Diese Rechner sollen auch alle auf das Internet zugreifen können. Die Rechner werden über einen Dual Speed Hub wie den 52xxDS oder 56xxDS von SMC miteinander vernetzt. An diesen Hub wird über 10 Mbps ein ISDN-Router wie der ELSA LANCOM 1000 angeschlossen. Dieser Router verfügt zusätzlich über einen ISDN-Port, der die Verbindung in das Internet realisiert. Er sichert so allen Schülern, die an den Arbeitsplatzrechnern arbeiten, einen gleichzeitigen Zugang zum Internet. Außerdem stellt er alle notwendigen Sicherheitsfunktionen wie NAT/PAT und Firewall zur Verfügung um das lokale Schulnetz vor Eindringlingen effektiv zu schützen. Gleichzeitig ermöglicht er auch eine Kontrolle der Gebühren, d. h. am Router werden die maximal zur Verfügung stehenden Gebühreneinheiten pro freiwählbarer Zeiteinheit (Budget) konfiguriert. Nach Ablauf des Budgets werden keine neuen Verbindungen mehr aufgebaut, natürlich kann der Administrator dieses Budget vorzeitig wieder freigeben. Durch diese Gebührenkontrolle ist es möglich überhöhte Telefonrechnungen von vornherein zu unterbinden. Alle diese Funktionen werden einfach über die Windows Tools ELSA LANConfig und LANMonitor, das auch über einen Internet SetupWizard verfügt, verwaltet. Werden später innerhalb der Schule weitere Klassenräume vernetzt, kann der Router als Verbindung ins Internet beibehalten werden.



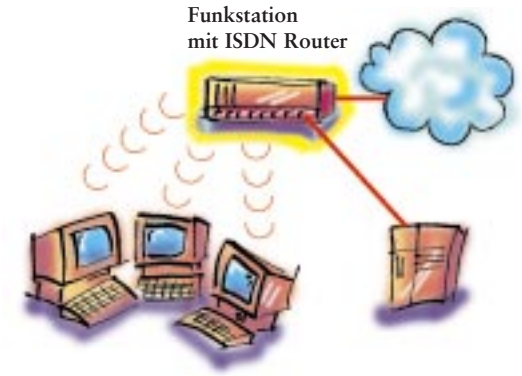
Beispiel 6: Anschluss des Schulnetzwerks an das Internet

Um die Kooperation der Schule mit anderen Schulen zu fördern und um den Schülern die Möglichkeit zu geben, weitreichende Recherchen vorzunehmen, soll nun auch ein Anschluss an das Internet realisiert werden. Da bereits ein Schulnetzwerk besteht, soll dies vollständig angebunden werden, sodass von jedem PC aus die theoretische Möglichkeit besteht, auf das Internet zuzugreifen. Nun wird ein ISDN-Router installiert, der die Verbindung zum Internet herstellt. Auf der Schulseite wird dieser Router mit einem 10/100 Mbps-Port eines Switches oder Hubs verbunden. Ist ein Switch vorhanden, sollte der Router aus Performance-Gründen an diesen angeschlossen werden. Der Router verfügt über Möglichkeiten wie NAT, um die bereits benutzten, nicht offiziellen IP-Adressen beizubehalten. Eine Firewall für die notwendigen Sicherheitsstrukturen sowie eine Gebührenkontrolle sind vorhanden (siehe Beispiel 5). Es wird ein Router eingesetzt, der auf der LAN-Seite über eine 10 Mbps Ethernet-Schnittstelle, wie z. B. der ELSA LANCOM 1000 oder eine Fast Ethernet Schnittstelle wie der LANCOM 1100 verfügt. Da davon ausgegangen wird, dass nicht mehrere Klassen gleichzeitig im Internet surfen, wird zunächst ein Router mit einem ISDN-Port gewählt. Falls sich herausstellen sollte, dass der Durchsatz der ISDN-Verbindung nicht ausreicht, können zunächst beide ISDN B-Kanäle aktiviert werden, um so den doppelten Durchsatz zu erhalten. Reicht auch dies nicht, kann er entweder gegen den ELSA LANCOM Business 4100, der über vier ISDN-Ports (8 B-Kanäle mit bis zu 512 Kbps) verfügt, oder den ELSA LANCOM dsl 10, der den neuen xdsl Service „T-ISDN dsl“ der Telecom (mit 768 Kbps downstream und 128 Kbps upstream) voraussetzt, ausgetauscht werden. Die neuen Router werden mit Hilfe desselben Windows Tools ELSA LANConfig bzw. ELSA LANMonitor verwaltet und konfiguriert, was die Umstellung erheblich vereinfacht.



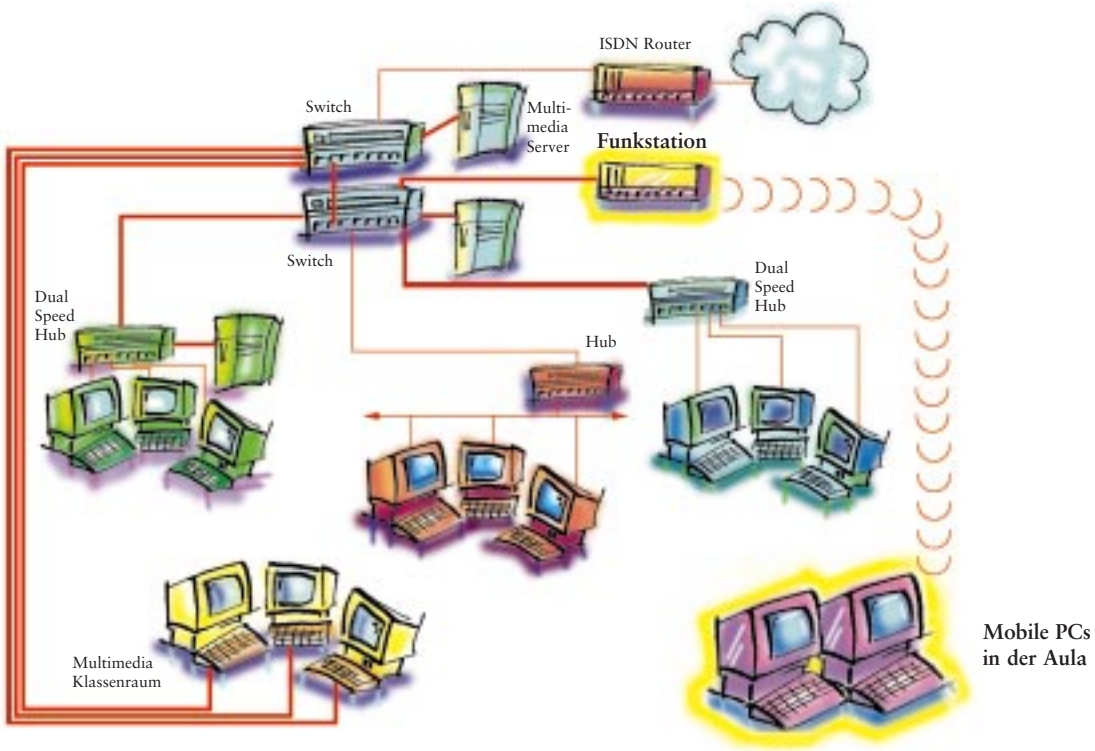
Beispiel 7: Drahtlose Vernetzung eines Klassenraums mit Anschluss an das Internet

Eine Schule ist in einem Gebäude untergebracht, das unter Denkmalschutz steht. Es soll ein Klassenraum mit Rechnern eingerichtet werden, aber es können keine Kabel verlegt werden. Dadurch ist nur eine drahtlose Vernetzung über Funktechnologie möglich. Alle PCs werden mit entsprechenden Plug&Play Schnittstellen-Karten von ELSA ausgerüstet und können über Funk miteinander bzw. mit dem Server, der direkt an die 10/100 Mbps Ethernet Schnittstelle der ELSA Funkstation angeschlossen ist, kommunizieren. Die Funkstation ELSA LANCOM IL2 Wireless ISDN verfügt zusätzlich über einen eingebauten ISDN Router, über den der Internetzugang einfach realisiert werden kann. Desweiteren verfügt der Router natürlich über die gleichen Funktionen



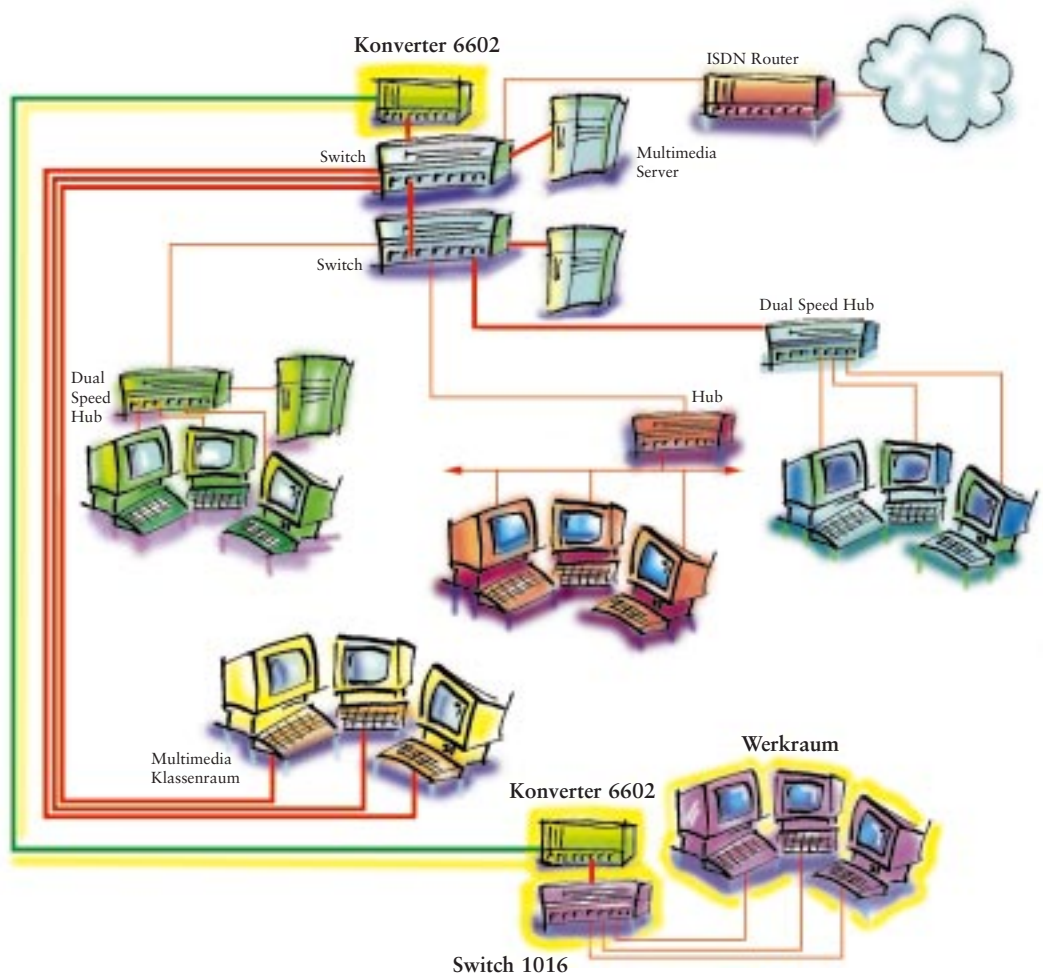
und Möglichkeiten, wie alle Router der ELSA LANCOM Serie (Firewall, Gebührenkontrolle, LANCAPI etc.). Siehe Beispiel 5 und 6.

Beispiel 8: Drahtloser Anschluss der Aula an das Netzwerk



Ein Schuljubiläum steht bevor, dass groß gefeiert werden soll. Für die Feierlichkeiten wird die Aula ausgewählt. Es sollen auch die Möglichkeiten der neuen Unterrichtsformen vorgestellt und demonstriert werden. Dafür werden aber einige PCs in der Aula benötigt, die an das Schulnetzwerk angeschlossen sind und darüber auch einen Zugang zum Internet haben. Da die Aula etwas abseits liegt, kann aber kein Kabel verlegen werden. Es wird die drahtlose Station ELSA LANCOM Wireless eingesetzt, die auf der einen Seite mit einem Hub verbunden wird und auf der anderen Seite über Funk die PCs in der Aula an das Netzwerk anbindet. Die PCs sind mit einer Interfacekarte von ELSA ausgestattet. Dieses Verfahren ist immer dann sinnvoll, wenn kurzfristig ein Raum wie Aula oder Turnhalle an das Netzwerk angeschlossen werden soll und sich der Verkabelungsaufwand nicht lohnt. Da der Empfangsradius sehr stark von den baulichen Gegebenheiten abhängt (max. 30 m im Gebäude, ca. 300 m außerhalb von Gebäuden), ist auf eine optimale Platzierung der Basisstation zu achten.

Beispiel 9: Externe Anbindung mit Lichtleiterkabel



Der Werkraum der Schule ist in einem eigenen Gebäude untergebracht. Auch in diesem Raum sollen nun PCs installiert werden, die mit dem restlichen Schulnetz verbunden werden sollen. Auf Grund der Entfernung (mehr als 100 m) können diese Rechner aber nicht direkt über Twisted Pair an das Schulnetz angeschlossen werden. Daher entscheidet man sich für den 8-Port Dual Speed Hub 5608 von SMC, um die Rechner im Werkraum miteinander zu vernetzen.

Der Anschluss an das Schulnetzwerk wird über zwei 6602FX-Konverter von SMC realisiert. Dieser Konverter verfügt über einen 10/100 Mbit Twisted-Pair und einen 100 Mbit Glasfaser-Anschluss, mit dessen Hilfe größere Entfernungen (bis zu 2 km im Vollduplex-Modus, der sich bei SMC Produkten automatisch einstellt) überbrückt werden können. Im Werkraum wird er über Twisted Pair mit dem Werkraum-Hub verbunden und das Lichtleiterkabel wird an den 6602FX im Server-Switch-Raum der Schule angeschlossen, wo der Konverter mit dem Switch 1016DT verbunden wird.

C. NETZWERK-LEITFADEN

1. EINLEITUNG

Die vorliegende Ausführung stellt einen technischen Leitfaden dar und gibt eine Einführung in Netzwerktechnologien. Ziel ist es, Verständnis über die Abläufe und prinzipiellen Strukturen zu vermitteln. Denn nur mit diesem Wissen ist es möglich, ein effektives Netzwerk zu konzipieren, das auch in der Zukunft Bestand hat.

Ein Schwerpunkt liegt auf der Vernetzung im lokalen Bereich bzw. innerhalb der Schule. Es werden die verschiedenen LAN-Technologien mit ihren Regeln vorgestellt, einschließlich Switching und Funk-LANs.

Ein weiterer Schwerpunkt ist das Internet bzw. das Hintergrundwissen, das benötigt wird, um ein TCP/IP-Netzwerk mit einem Zugang zum Internet aufzubauen. Hierzu gehören Informationen über die IP-Adressierung, ohne die kein TCP/IP-Netzwerk arbeiten kann, wichtige Applikationen wie DHCP und DNS und nicht zuletzt Informationen, die den direkten Zugang zum Internet betreffen.

2. DAS ETHERNET

Für die Vernetzung von Rechnern im lokalen Bereich (local area network = LAN) wird heute häufig Ethernet eingesetzt. Neben dem „alten“ 10 Mbps Ethernet gibt es inzwischen auch die schnelleren Varianten Fast Ethernet mit 100 Mbps und Gigabit Ethernet mit 1000 Mbps. Gerade Fast Ethernet ist auf Grund des Preisverfalls bei den benötigten Netzwerkkomponenten heute eine echte Alternative. Bei neu anzuschaffenden Netzwerkkomponenten sollte man immer darauf achten, dass man sich die Option für Fast Ethernet offen hält.

Neben der Ethernet-Welt findet man im LAN-Bereich auch noch Token Ring, FDDI und inzwischen ATM-Netzwerke.

Auf Grund der problemlosen Installation und Inbetriebnahme sowie der günstigen Preise soll hier nur auf die Ethernet-Varianten eingegangen werden.

2.1 Zugriffsverfahren

Ethernet ist eine Methode, Rechner miteinander zu verbinden, sodass alle angeschlossenen Stationen im Prinzip gleichberechtigt auf ein Kabel als Übertragungsmedium zugreifen können. Damit dies nicht in einem undefinierbaren Chaos endet, ist in dem IEEE 802.3 oder ISO8802-3 Standard die Zugriffsmethode CSMA/CD definiert, die, ähnlich wie Strassenverkehrsregeln, den Zugriff der einzelnen Stationen regelt.

CSMA/CD steht für „Carrier sense, multiple Access with Collision detect“ und arbeitet wie folgt:

- Eine am Ethernet angeschlossene Station will Daten übertragen
- Sie überprüft, ob das Übertragungmedium frei ist, bzw. keine andere Station sendet
- Ist dies der Fall, kann sie die Datenübertragung beginnen
- Ist dies nicht der Fall, wartet sie und versucht es später noch einmal
- Parallel dazu hört jede Netzwerkstation permanent das Übertragungskabel ab, ob Daten gesendet werden, die für diese Station bestimmt sind
- Theoretisch kann es passieren, dass zwei Stationen gleichzeitig mit einer Datenübertragung beginnen. Daher müssen Kollisionen erkannt werden. Dies geschieht dadurch, dass eine sendende Station während des Sendevorgangs gleichzeitig das Kabel abhört, ob eine Kollision auftritt. Ist dies der Fall, unterbricht sie die Datenübertragung und beginnt später wieder von Neuem.

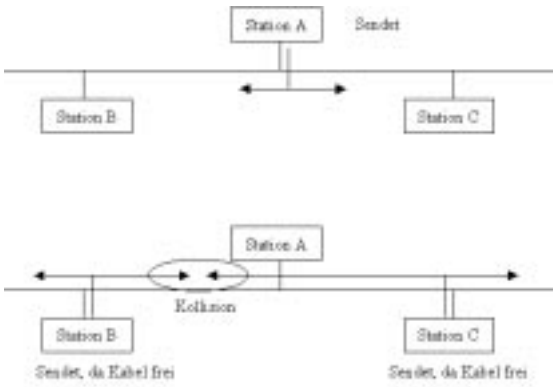


Abbildung 1: CSMA/CD

Wie aber adressiert eine Station im Ethernet einen anderen Rechner (oder Drucker, Server, ...)?

Dies geschieht über MAC-(Media Access Control) Adressen, die vom Hersteller in die Netzwerk-Karte fest eingespeichert wird. Da diese Adressen weltweit eindeutig sind, stellen sie am Ethernet eine eindeutige Identifikation dar. Beim Laden der Netzwerksoftware lernt jede Station ihre eigene Adresse.

Damit dieses Verfahren für die Erkennung von Kollisionen, die am Ethernet einen vollkommen normalen Zustand darstellen, auch funktioniert, müssen bestimmte Regeln eingehalten werden:

- Am Ethernet werden 10 Millionen Bits pro Sekunde, oder 10 Mbps, übertragen.
- Eine Station kann aber nicht eine beliebige Anzahl von Bits pro Übertragungvorgang senden, sondern muss die zu übertragenden Daten zu Paketen zusammenfassen. Diese Pakete haben eine minimale Länge von 64 Bytes und eine maximale Länge von 1500 Bytes.

Die vorher genannten Vorgaben sind fest. Als Kabel können für das Ethernet verschiedene Typen eingesetzt werden, die entsprechende elektrische Bedingungen erfüllen. Damit der CSMA/CD-Mechanismus funktionieren kann, ergeben sich unterschiedliche maximale Längen für die verschiedenen Kabeltypen.

2.2 Verkabelung

Es gibt theoretisch vier verschiedene Typen von Kabeln, um ein Ethernet-Netzwerk aufzubauen:

- **Koax-Kabel oder Thick Koax (10BASE5)**
- **Thin Koax oder BNC (10BASE2)**
- **Shielded Twisted Pair (10BASE –T)**
- **Glasfaser (10BASE-F)**

Die dicken, gelben Koax-Kabel werden heute kaum noch eingesetzt, da diese nicht ganz einfach zu installieren sind.

Glasfaser-Kabel wird man in der Regel nur da einsetzen, wo große Entfernungen (siehe Abschnitt Längenbeschränkungen) zu überbrücken sind oder in einer stark störanfälligen Umgebung (wie z. B. in manchen Industriebetrieben in der Produktion).

Thin Koax Verkabelung wird heute hauptsächlich in kleinen vernetzten Umgebungen eingesetzt. Allerdings findet man sie häufig noch in historisch gewachsenen Netzwerkumgebungen, da es früher die einfachste Methode war, Rechner schnell miteinander zu vernetzen. Falls eine Thin-Koax Verkabelung eingesetzt werden soll, muss darauf geachtet werden, dass alle Netzwerk-Interface-Karten der anzuschließenden PCs oder anderer Netzwerkgeräte einen BNC-Stecker besitzen. Die Netzwerkstationen werden über den BNC-Stecker direkt an das Kabel angeschlossen und stellen damit eine Bus-Topologie dar.

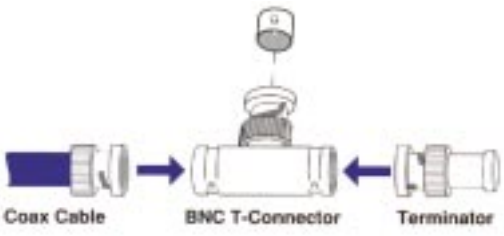


Abbildung 2: BNC-Verkabelung

Shielded Twisted Pair (STP)-Verkabelung wurde in den letzten Jahren zunehmend häufig für den Aufbau eines Netzwerks eingesetzt, nicht zuletzt auch deswegen, weil man sich damit den Weg für zukünftige Technologien offen hält. STP-Kabel gibt es in verschiedenen „Gütestufen“: Kategorie 1 bis Kategorie 6. Je höher die Kategorie, um so stärker der Schutz des Kabels vor äußeren elektrischen Störungen. Auf der anderen Seite sind Kabel höherer Kategorie auch teurer. Für eine 10 Mbps Ethernet-Vernetzung wird mindestens Kategorie 3 benötigt. Kabel ab Kategorie 5 können auch für Fast Ethernet benutzt werden. In STP-Netzwerken wird immer ein Hub benötigt, um die PCs miteinander zu verbinden. Der Anschluss der einzelnen Netzwerkstationen an den Hub erfolgt über einen RJ-45 Stecker, wie z. B. auch bei der Telefon-Verkabelung. STP-Netzwerke stellen damit eine Stern-Topologie dar.

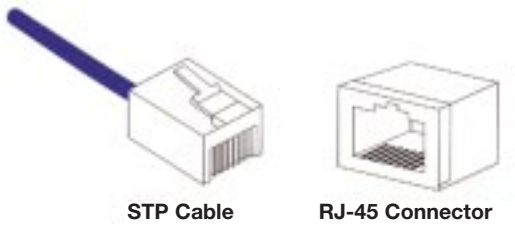


Abbildung 3: STP-Verkabelung

Der große Vorteil von STP-Netzwerken ist die geringere Störanfälligkeit des gesamten Netzwerks, falls an einer Station ein Problem auftritt. Der Hub sollte in der Lage sein, ein Problem einer Station zu erkennen und den Port, an dem diese Station angeschlossen ist, zu schließen. In einem BNC-Netzwerk würde in diesem Fall das gesamte Netzwerk und damit alle angeschlossenen Station gestört. Auch die Fehlersuche gestaltet sich in einem Twisted Pair Netzwerk einfacher, da durch das Abschalten einzelner Ports am Hub die Fehlerquelle eingegrenzt werden kann. (Weitere Infos über http://www.dievers.de)

2.3 Konfigurationsregeln bei 10 Mbps Ethernet

Damit der oben beschriebene Zugriffsmechanismus CSMA/CD mit den Rahmenbedingungen der Paketgröße und 10 Mbps Ethernet funktionieren kann, gibt es abhängig vom Kabeltyp verschiedene Längenbeschränkungen.

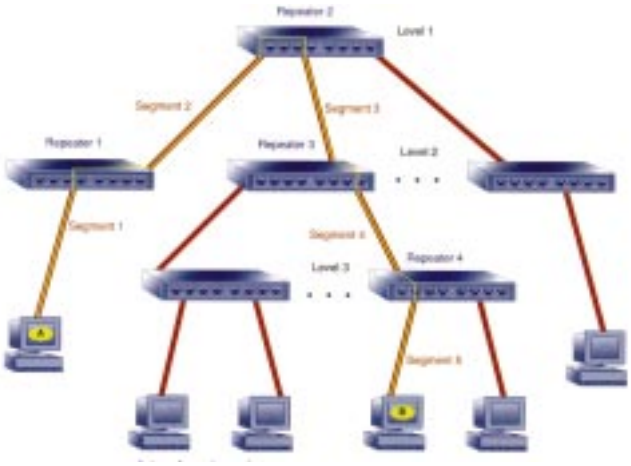
Prinzipiell kann ein Netzwerk dann über Repeater weiter verlängert werden. Die Verlängerung darf aber nicht unbeschränkt vorgenommen werden, sondern es gilt folgende Regel:

Zwischen zwei verschiedenen Netzwerk-Stationen dürfen sich maximal befinden:

- 5 Kabel-Abschnitte hintereinander
- 4 Repeater (oder Hubs)
- 3 Abschnitte, an denen zwei oder mehr PCs oder andere Netzwerkstationen angeschlossen sind

Der letzte Punkt trifft nur in Koax-Netzwerken zu, da in Twisted Pair Netzwerken der Hub oder Repeater benötigt wird, um die PCs miteinander zu verbinden.

Abbildung 4: Ethernet-Regeln



Für die einzelnen Kabeltypen ergeben sich folgende Vorschriften:

2.3.1 BNC

Ein Thin Koax-Abschnitt darf höchstens 185 Meter lang sein mit maximal 30 Stationen. Muss dieser Abschnitt verlängert werden, wird ein Repeater benötigt. Dies kann ein 2-Port Repeater sein, der zwei Abschnitte verbinden kann, oder ein Multiport Repeater, der mehrere Thin-Koax-Segmente zur Verfügung stellen kann. Jedes Segment mit einer maximalen Länge von 185 Metern und maximal 30 Stationen.

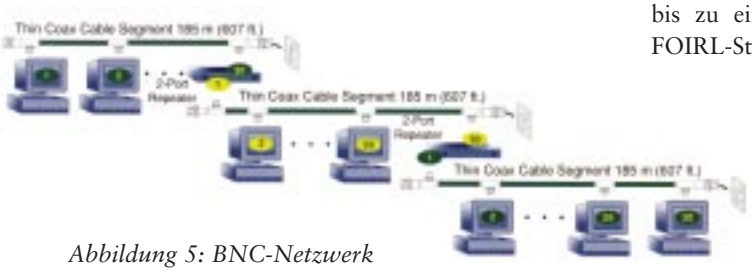


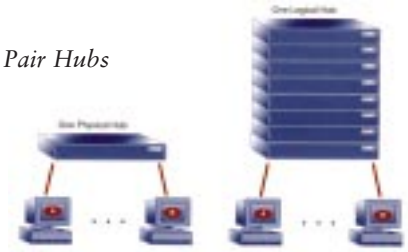
Abbildung 5: BNC-Netzwerk

2.3.2 Twisted Pair

In einem Ethernet Twisted Pair Netzwerk wird der PC über ein Twisted Pair Kabel und den RJ-45 Stecker direkt mit dem Ethernet Hub verbunden. Dieses Kabel darf maximal 100 Meter lang sein. Für eine Vergrößerung des Netzwerks können mehrere Hubs über ein Twisted Pair Kabel miteinander verbunden werden. Diese Verbindung muss auf einem Hub auf einen „Cross-over"-Port (MDI-Port) laufen, der in der Regel entsprechend gekennzeichnet ist. Es ist darauf zu achten, dass keine doppelten Verbindungen (LOOPS) eingebaut werden.

Auch hier gilt es die Regeln für die maximale Anzahl von Repeatern zwischen zwei Netzwerk-Stationen einzuhalten.

Abbildung 6:
Stapelbare Twisted Pair Hubs



An dieser Stelle unterscheiden sich stapelbare Hubs. Da sie mit Hilfe eines ganz speziellen Kabels über einen dedizierten Port miteinander verbunden werden, zählt ein Stapel aus mehreren Hubs, die über das entsprechende Kabel miteinander verbunden sind, für das Ethernet wie ein einziger Hub. Stapelbare Hubs stellen daher eine hervorragende Möglichkeit dar, die Anzahl der Ports in einem Netzwerk zu vergrößern, ohne die Konzeption verändern zu müssen. Man kann mit einem Hub beginnen und bei steigendem Bedarf weitere Hubs zu dem Stapel hinzufügen.

So verbindet ein 24-Port Hub maximal 24 Rechner, während ein Stapel von 8 x 24 Port Hubs 192 Rechner unterstützen kann. Und alle 192 Rechner sind nach den Ethernet-Regeln an einem Hub angeschlossen.

2.3.3 Glasfaser

Ein Ethernet Glasfaser-Netzwerk ist, wie ein Twisted-Pair Netzwerk, immer als eine Stern-Topologie aufgesetzt. Die Netzwerk-Stationen werden über einen Glasfaser-Hub verbunden. Das Glasfaser-Kabel kann bis zu einem Kilometer lang sein, wenn es dem FOIRL-Standard entspricht und sogar bis zu 2 Kilometern, wenn es dem 10BASE-FL Standard entspricht. Da Glasfaser zum einen recht teuer und zum anderen etwas schwierig zu installieren ist, setzt man diese Art der Verkabelung in der Regel nur dort ein, wo sie auch wirklich gebraucht wird. Glasfaser zeichnet sich durch höhere Sicherheit, größere Stabilität in schwierigen Umgebungen und Unempfindlichkeit gegen elektromagnetische Störungen aus.

Glasfaser wird auf Grund der großen Entfernungen, die es überbrücken kann, auch häufig eingesetzt, um Twisted Pair Hubs miteinander zu verbinden.

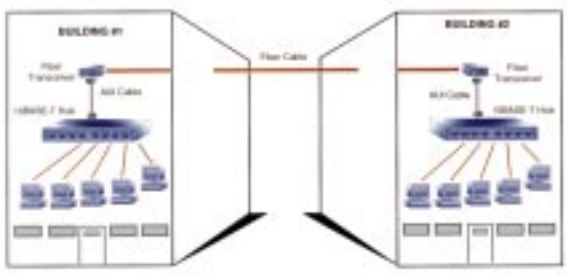


Abbildung 7: Glasfaser Netzwerk

2.3.4 Übersicht Längenbeschränkungen

Mit den obigen Ausführungen ergeben sich folgende Längen-Beschränkungen für Ethernet-basierende Netzwerke:

Kabel Typ	Maximal Kabellänge (pro Segment)	Maximale Ausdehnung (Repeater-Regel)
Twisted Pair (10BASE-T)	100 Meter	500 Meter
Thin Koax (10BASE2)	185 Meter	925 Meter
Glasfaser (FOIRL)	1 Kilometer	5 Kilometer
Glasfaser (FL)	2 Kilometer	10 Kilometer

2.4 Fast Ethernet

Fast Ethernet ist Ethernet, aber mit einer Übertragungsrate von 100Mbps. Das bedeutet, dass auch Fast Ethernet mit dem CSMA/CD Mechanismus und vorgegebenen Paketlängen arbeitet. Als Übertragungsmedium kommen Shielded Twisted Pair Kabel in Frage, aber hier nur in der Kabelgüte Kategorie 5 und höher (100BASE-TX) und Glasfaser (100BASE-FX). Bei Twisted Pair bzw. 100BASE-TX ist darauf zu achten, dass das Kabel aus zwei Drahtpaaren besteht. Bei Fast Ethernet wird ein Drahtpaar zum Senden und ein Drahtpaar zum Empfangen benutzt. Es gibt auch noch den 100BASE-T4-Standard, der aber zumindest in Deutschland so gut wie nie eingesetzt wird und daher hier in dieser Ausführung vernachlässigt wird.

2.4.1 Vorteile

Die Vorteile von Fast Ethernet liegen auf der Hand: höhere Übertragungsraten und damit größere Geschwindigkeit im Netzwerk.

Häufig wird Fast Ethernet im ersten Ansatz dazu eingesetzt, einen Server anzuschließen. Da die heutigen 10 Mbps-Hubs in der Regel zumindest einen 100 Mbps-Port haben, ist dies eine gute Übergangslösung, um Engpässe zu beseitigen, die daraus resultieren, dass auf Server von vielen Anwendern gleichzeitig zugegriffen wird.

Auf Grund des rapiden Preisverfalls bei den Fast Ethernet-Komponenten macht es in der Regel heute Sinn, einen neuen PC, der ans Netz angeschlossen werden soll, gleich mit einer Fast Ethernet Netzwerkkarte auszustatten.

Damit so nicht getrennte Netzwerkwelten geschaffen werden, die auf der einen Seite aus den alten 10 Mbps Geräten bestehen und auf der anderen Seite aus den neuen 100 Mbps-Geräten, gibt es Dual-Speed Hubs. Dual-Speed Hubs haben eine integrierte Intelligenz, sodass sie auf jedem Port erkennen können, ob die auf der anderen Seite angeschlossene Karte 10 Mbps oder 100 Mbps zur Verfügung stellen kann. Sie stellen den entsprechenden Port automatisch auf die höchst mögliche Geschwindigkeit ein und sind gleichzeitig in der Lage, Daten zwischen den 10 Mbps und 100 Mbps Netzwerken zu übertragen. Die Dual-Speed Hubs sind für der Migrationsphase ein unschätzbares Hilfsmittel.

2.4.2 Längenbeschränkungen und Repeater

Wie bei 10 Mbps Ethernet gibt es auch für Fast Ethernet Regeln, die Längenbeschränkungen für die verschiedenen Kabeltypen vorgeben. Auch hier ist es möglich, die vorgegebenen Längen mit Hilfe von Repeatern oder Hubs auszudehnen.

Der Fast Ethernet Standard unterscheidet zwei verschiedene Typen von Repeatern: Class I und Class II.

Ein Class I Repeater hat eine größere Zeitverzögerung bei der Übertragung der Daten von einem Port zu einem anderen. Er übersetzt die hereinkommenden Daten zunächst in die digitalisierte Fassung und sendet sie nach einer weiteren Übersetzung auf die anderen Ports. Dies ermöglicht, verschiedene Medien wie 100BASE-TX und 100BASE-FX in einem Hub zu mischen. Auf der anderen Seite ist aber durch die größere Zeitverzögerung nur ein Class I Hub zwischen zwei Stationen erlaubt.

Der Class II Hub arbeitet schneller, in dem die Daten, die auf einem Port hereinkommen, direkt an die anderen Ports weitergegeben werden. Daher kann ein Class II Hub entweder nur 100BASE-TX- Ports oder nur 100BASE-FX-Ports bedienen. Dafür sind aber maximal zwei Class II-Hubs zwischen zwei Stationen erlaubt.

Zwei Class II Hubs dürfen über ein Kabel von maximal ½ Meter verbunden werden. Wird eine größere Reichweite benötigt, muss man zu einer anderen Technologie, nämlich Switching, übergehen.

Auch hier sei auf die stapelbaren Hubs hingewiesen, die auf Grund der dedizierten Verbindung untereinander nach den Ethernet-Regeln wie ein Hub zählen.

Ansonsten gelten folgende Längenbeschränkungen:

- STP Twisted Pair: maximal 100 Meter zwischen der Netzwerkstation und dem Hub
- Glasfaser: maximal 412 Meter zwischen der Netzwerkstation und dem Hub. Wird ein Hub eingesetzt, um zwei Glasfaser-Abschnitte zu

verbinden, verkürzt sich die maximale Länge. Bei einem Class II Repeater dürfen zwischen den Netzwerk-Stationen maximal 320 Meter liegen, bei einem Class I Hub maximal 272 und bei zwei Class II Hubs maximal 228 Meter.

Daher ergibt sich folgende Tabelle:

Längenbeschränkung Fast Ethernet

Kabel Typ / Hub Typ	Maximaler Netzwerkdurchmesser bei		
	Twisted Pair 100BASE-TX	Glasfaser 100BASE-FX	Twisted Pair + Glasfaser gemischt, 100BASE-TX/FX
Ein Class I Hub	200 Meter	272 Meter	261 Meter
Ein Class II Hub	200 Meter	320 Meter	309 Meter
Zwei Class II Hubs	205 Meter	228 Meter	216 Meter

Abbildung 8: Fast Ethernet

3. SWITCHING

Ein Switch ist ein Netzwerkgerät, das benutzt wird, um ein Ethernet/Fast Ethernet-Netzwerk in verschiedene Segmente zu unterteilen und so die Leistung und Bandbreite des Netzwerks heraufzusetzen, ohne an der Verkabelung Änderungen vornehmen zu müssen.

Bem.: Im Folgenden steht Ethernet immer auch gleichzeitig für Fast Ethernet

3.1 Funktionsweise des Switches

Bei den obigen Ausführungen über Ethernet teilen sich alle Stationen, die am Netz angeschlossen sind, die vorhandenen 10 oder 100 Mbps. Das bedeutet aber auch, dass sich mit zunehmender Benutzeranzahl die Bandbreite, die für den Einzelnen zur Verfügung steht, verringert.

Mit der Unterteilung in verschiedene Collision Domains wird das Netzwerk ebenfalls in verschiedene Ethernet-Segmente unterteilt. Jeder Port eines Switches stellt ein dediziertes Ethernet-Segment zur Verfügung und nur noch alle an diesem Port angeschlossenen Benutzer teilen sich die vorhandene Bandbreite.

Wird also ein vorhandener Hub, z. B. mit 16 Ports, durch einen Switch ausgetauscht, stehen dem Netzwerk sofort 16 x 10 bzw. 100 Mbps zur Verfügung. Dennoch sind die einzelnen Segmente über den Switch miteinander verbunden, sodass die Kommunikation ungestört weiterlaufen kann. Ein Switch ist also eine Möglichkeit, ein Ethernet aus mehreren Segmenten aufzubauen und dem Netzwerk damit ein Vielfaches an Bandbreite zur Verfügung zu stellen.

Die in den vorherigen Kapiteln beschriebenen Konfigurationsregeln beziehen sich immer auf ein Ethernet-Netzwerk bzw. eine Collision Domain. Sie haben keine Bedeutung für den Zusammenschluss von mehreren Ethernet-Netzwerken mit Hilfe von Switches. Solange jede einzelne Collision Domain in sich richtig konfiguriert ist (Längenbeschränkungen, Anzahl von Repeatern), können beliebig viele Netzwerke über Switches zusammengefasst werden. Allerdings muss bei der Verbindung des Switches mit dem Hub oder den einzelnen Rechnern die maximale Kabellänge beachtet werden. Desweiteren dürfen keine doppelten Verbindungen zwischen den Hubs, bzw. Switches, sog. LOOPS, eingebaut werden, siehe auch Punkt 2. Durch den Einsatz eines Switches erweitert sich auch automatisch der Radius des Netzwerks. Dies ist vor allem bei Fast Ethernet interessant, da dort die Längenbeschränkungen doch schnell an ihre Grenzen stoßen.

Ein Switch leitet Datenpakete ausschließlich im Bedarfsfall an andere Ports des Switches weiter, also nur dann, wenn sie gezielt an eine Station adressiert sind, die mit einem anderen Port des Switches verbunden ist. Das bedeutet aber, dass ein Switch in der Lage sein muss, die Adressen der Stationen, die mit einem Port verbunden sind, zu lernen und zu speichern. Bei der Auswahl der Switches sollte daher darauf geachtet werden, dass sie in der Lage sind, möglichst viele Ethernet-Adressen zu speichern.

Abbildung 9: Switching

3.2 Einsatzgebiete

Beim Einsatz eines Switches sollte auf einige Dinge geachtet werden:

- In einer Arbeitsumgebung mit ca. 30 Anwendern und einem gemeinsamen Dateiserver bieten sich zwei Lösungsansätze an.
  - Der Einsatz eines preisgünstigen DualSpeed Hubs. Der Nachteil der Hub-Technologie ist, dass sich alle Stationen die Bandbreite 10 oder 100 Mbps des Hubs teilen müssen.
  - Optimaler aber auch teuerer ist der Einsatz eines Switches. Die Switching-Technologie stellt allen Stationen die volle Bandbreite von 10 oder 100 Mbps bereit. Der Dateiserver sollte hier auf alle Fälle über 100 Mbps angebunden werden.
- In einer Schulumgebung kann man sich vorstellen, dass jeder Klassenraum, der mit PCs ausgestattet ist, auch seinen eigenen Server installiert hat. Der Klassenraum wird über einen Dual-Speed-Hub vernetzt. Nun macht es Sinn, die verschiedenen Klassenräume über einen Switch zu verbinden. So ist die Kommunikation zwischen den Klassenräumen möglich, ohne eine Leistungseinbuße bei den einzelnen „Klassenraum-Netzwerken“ in Kauf nehmen zu müssen.
- Anders sieht die Situation in einem Multimedia-Klassenraum aus. Hier haben alle PCs eine hohe Datenübertragungsrate. Es kann durchaus Sinn machen, die Rechner hier direkt über einen 10/100 Mbps Switch zu vernetzen, um jeder angeschlossenen Station dedizierte 10 Mbps oder 100 Mbps zur Verfügung zu stellen. Allerdings sollte darauf geachtet werden, dass bei dem gleichzeitigen Einsatz eines Servers dieser mit einer höheren Geschwindigkeit, z.B. mit Fast Ethernet und Vollduplex, an den Switch angeschlossen wird, um einen Engpass zu vermeiden.

4. FUNK-LANs

In der Vergangenheit stellte die Einbindung drahtloser Netzwerke eine Nischenanwendung dar, die nur in vereinzelten Fällen eingesetzt wurde. Dies lag zum einen an fehlenden Standards, aber auch an den hohen Investitionskosten, die der Aufbau eines drahtlosen Netzwerks erforderte. Mit der Entwicklung des IEEE 802.11-Standards wird sich dies schnell ändern. Auch gab es in der Vergangenheit Befürchtungen bzgl. der Abhörsicherheit, Störung anderer drahtloser Übertragungen wie Funktelefon und vor allem bzgl. gesundheitlicher Störungen. Diese Befürchtungen können heute weitgehend beruhigt werden.

4.1 Funktionsweise

Im IEEE 802.11-Standard wird als Zugriffsmechanismus CSMA/CA (Carrier Sense, Multiple Access, Collision Avoidance) definiert. Er ist dem Ethernet-Zugriffsmechanismus CSMA/CD ähnlich. Aber in einem drahtlosen LAN kann nicht gewährleistet werden, dass alle Stationen einander „hören“. Dies ist aber Voraussetzung für die Erkennung von Kollisionen. Bei CSMA/CA wird daher vor Beginn der Datenübertragung zuverlässig geklärt, ob ein Kanal frei ist. Ein weiterer Bestandteil der Standards sind Sicherheitsfunktionen. Diese sorgen unter anderem dafür, dass der Zugang zum Netz nur durch eine Systemidentifikation möglich ist. Zusätzlich werden die zu übertragenden Daten „zerhackt“ und über mehrere Sendekanäle „gespreizt“ übertragen, der Empfänger kann mit einem nur ihm bekannten Schlüssel die für ihn relevanten Daten herausfiltern. Diese Technik DSSS (Direct Sequence Spread Spectrum), ursprünglich für das Militär entwickelt, macht ein Abhören für Unbefugte nahezu unmöglich. Desweiteren beinhaltet der Standard eine zusätzliche 40- oder 128-Bit WEP Datenverschlüsselung.
Die meisten Funk-LANs arbeiten im Frequenzbereich von 2,4 GHz. Dies verhindert die Beeinflussung der üblichen kabellosen Telefone. Auch erhöhte Gesundheitsrisiken konnten bisher beim Umgang mit Funk-LANs in diesem Frequenzbereich nicht festgestellt werden.

4.2 Vorteile und Einsatzbereiche

Die Vorteile von Funk-LANs liegen auf der Hand: Der Wegfall der Verkabelung sorgt für eine größere Mobilität und Wahlfreiheit beim Aufbau des Netzwerks. Die trifft z. B. in folgenden Situationen zu:

- In allen Umgebungen, in denen ein Netzwerk aufgebaut werden soll, aber die Installation von Netzwerkleitungen zu kostspielig oder aufwendig (z. B. Altbau) ist.
- In Umgebungen, in denen kurzfristig eine weitere Station in das Netzwerk integriert werden soll, z. B. wenn die Aula einer Schule an das Netzwerk angeschlossen werden soll, um bei einer Veranstaltung eine PC-Demonstration vorzunehmen.
- In Umgebungen, in denen es wichtig ist, den Ort des Arbeitsplatzrechners mobil und frei wählen zu können, ohne auf die Netzwerkanschlüsse Rücksicht nehmen zu müssen. Da der Empfangsradius sehr stark von den baulichen Gegebenheiten abhängt (max. 30-50 m im Gebäude, ca. 300 m außerhalb von Gebäuden), ist auf eine optimale Plazierung der Basisstation zu achten.

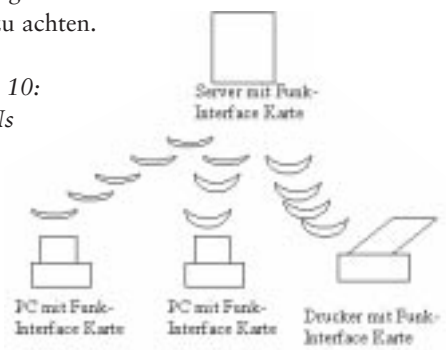


Abbildung 10: Funk-LANs

5. NETZWERKSOFTWARE

Zu einem Netzwerk gehört neben der physikalischen Verkabelung der Rechner auch Software, die es den einzelnen Rechnern erlauben, miteinander Informationen auszutauschen oder auf gemeinsame Ressourcen wie Dateien, Drucker, CDs, Zip-Drives zuzugreifen.

Hier sind vor allem im LAN-Bereich Netzwerk-Betriebssysteme wie Novell mit dem Kommunikationsprotokoll IPX/SPX, Windows-NT mit NetBEUI oder das reine Kommunikationsprotokoll TCP/IP zu nennen. TCP/IP (Transmission Control Protocol/Internet Protocol) hat sich in der Netzwerkwelt heute durchgesetzt. Spätestens mit dem Vordringen des Internets bis in den privaten Bereich ist TCP/IP zu einem Quasi-Standard geworden. Lange Zeit wurde TCP/IP hauptsächlich im Zusammenhang mit UNIX eingesetzt, aber inzwischen ist es in vielen Unternehmensnetzen und auch im PC-Bereich weit verbreitet. So setzt heute Windows NT in vielen Fällen bereits auf TCP/IP an Stelle von NetBEUI auf. Zumal TCP/IP, im Gegensatz zu den anderen Protokollen, nicht nur für das LAN, sondern auch für den Weitverkehrsbetrieb konzipiert wurde.

Hier soll nur eine grundlegende Einführung in TCP/IP gegeben werden.

Prinzipiell spielt Adressierung bei jeder Netzwerksoftware eine entscheidende Rolle. Denn nur wenn es möglich ist, jedem Rechner im Netzwerk eine eindeutige Adresse zuzuweisen, kann dieser Rechner auch gezielt angesprochen werden. Solange wir uns in einem Ethernet-LAN befinden, in dem jeder Rechner eine MAC-Adresse hat und permanent das Ethernet abhört, (ob Daten für diesen Rechner übertragen werden) ist dies noch relativ einfach zu lösen.

In komplexen Netzen, wenn mehrere LANs über Weitverkehrsstrecken (Standleitung, Telefonleitung, Antenne...) miteinander verbunden sind, müssen Router eine Verbindung herstellen vom Ursprungsrechner, der die Information abschickt, zum Zielrechner, für den die Information bestimmt ist. Diese Router arbeiten auf Basis der Netzwerkadressen, um den besten Weg zu finden. Sie sind auch in der Lage, bei Ausfall einer Verbindung einen anderen Weg zwischen den beiden Rechnern festzulegen.

5.1 IP-Adressierung

Jedem TCP/IP-Rechner bzw. jeder Netzwerkschnittstelle eines TCP/IP-Rechners wird eine eindeutige IP-Adresse, bestehend aus 32 Bit, zugewiesen. Diese Adresse setzt sich zusammen aus einer Network-ID und einer Host-ID. Hat ein Rechner mehr als eine Verbindung zum Netzwerk, z. B. einen Zugang zum Ethernet und eine ISDN-Schnittstelle, bekommt jede der zwei Schnittstellen eine eigene Adresse.

Eine korrekte Adressierung ist wichtig, um die Kommunikation zwischen den Rechnern zu gewährleisten. Bei der Kommunikation zwischen zwei Rechnern wird zuerst die Network-ID des Zielrechners mit der eigenen Network-ID verglichen. Ist sie identisch, wird die Information direkt an den Zielrechner weitergeleitet. Bei unterschiedlichen IDs wird die Information an den Default-Router (auch Gateway genannt) weitergeleitet. Die IP-Adresse des Default-Routers muß auf der Absenderstation konfiguriert sein. Der Router leitet nun die Information an den Zielrechner.

Als Network wird jedes physikalische Netzwerk angesehen. Dieses muss über die Network-ID gezielt adressiert werden. So bekommen z. B. alle Rechner, die an einem physikalischen Ethernet-LAN angeschlossen sind, auf dem Ethernet-Interface die gleiche Network-ID, aber jeder Rechner braucht in diesem Network eine eigene Host-ID. Genauso bekommen die zwei Netzwerk-Stationen, die an den beiden Enden einer Standleitung angeschlossen sind, eine gemeinsame Network-ID und jeder eine eigene Host-ID. In dem vorher genannten Beispiel gehört die Ethernet-Schnittstelle des Rechners zu einem anderen Network als die ISDN-Schnittstelle.

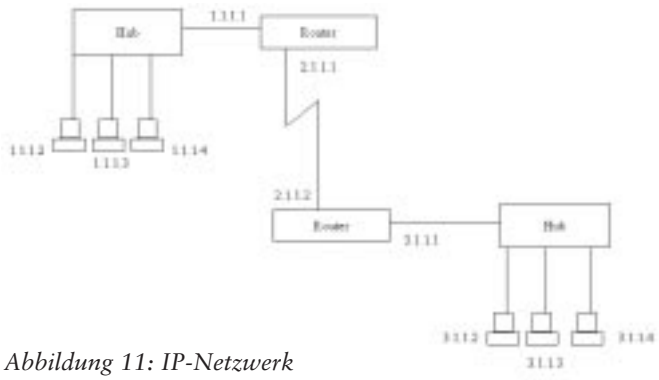


Abbildung 11: IP-Netzwerk

Dieses Beispiel macht das Problem deutlich. An einem Ethernet-Netzwerk sind viele Rechner angeschlossen, es werden also von den 32 Bit der IP-Adresse viele Bits für die eindeutige Adressierung der einzelnen Hosts benötigt.

Auf der anderen Seite müssen bei dem Standleitungs-Netzwerk nur zwei Rechner eine Host-ID bekommen, d. h. es werden nur wenige der vorhandenen 32 Bits für die Host-Adressierung benötigt.

Diesem Umstand wird durch die Aufteilung in Class A, Class B und Class C-Netzwerke Rechnung getragen.

In einem Class A-Netzwerk werden die ersten 8 Bit für die Netzwerk-Adressierung benutzt, die verbleibenden 24 Bits stehen daher für die Adressierung der einzelnen Rechner innerhalb des Netzwerks zur Verfügung.

In einem Class B-Netzwerk gehören die ersten 16 Bit zur Network-ID, die restlichen 16 Bit zur Host-ID.

In einem Class C-Netzwerk schließlich werden mit den ersten 24 Bits die Netzwerke adressiert, es können also viele verschiedene Netzwerke gebildet werden. Dafür bleiben nur 8 Bits für die Host-Adressierung übrig.

Zur besseren Lesbarkeit erfolgt die Darstellung der Adresse 4-stellig dezimal, d. h. jeweils 8 Bit werden dezimal durch Zahlen zwischen 1 und 255 abgebildet, mit einem Punkt als Trennzeichen.

IP-Adressierung

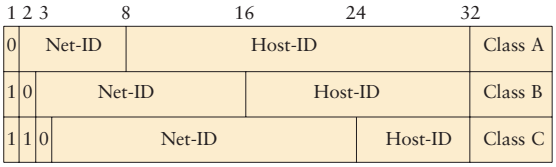
Beispiel:

32-Bit Adresse
00000011 00000111 00001111 10000100

Darstellung
3.7.15.132

Damit aber gleich erkennbar ist, um welches Netzwerk es sich handelt, werden für die verschiedenen Netzwerke die ersten Bits vorbelegt:

Klassifizierung von Netzwerken



Da die Adresse 0 verboten ist und das Setzen aller Bits auf 1 für Broadcast-Meldungen (Host-ID) oder die Netmask (Net-ID) reserviert ist, sieht eine typische Internet-Adresse folgendermaßen aus:

n.m.o.p. mit 0 < n,m,o,p < 255.

In der Netmask werden alle Bits auf 1 gesetzt, die für die Netzwerk-Adressierung benutzt werden. Dies ist, unabhängig von dem Wertebereich, eine weitere Kennzeichnung der Netzwerkklasse.

Mit den obigen Vorschriften für die Kennzeichnung von Class A-, Class B- und Class C-Adressen ergeben sich folgende Bereiche für die Netzwerk-Adressierung:

Adressbereich der Netzwerke

	Adressbereich	Netmask
Class A	1-127.m.o.p	255.0.0.0
Class B	128-191.1-254.o.p	255.255.0.0
Class C	192-223.1-254.1-254.p	255.255.255.0

Innerhalb eines privaten IP Netzwerks ist es möglich, beliebige IP Adressen zu vergeben und das vorhandene physikalische Netzwerk abzubilden. Solange man keine Verbindung zum Internet herstellt, braucht man sich nicht um offiziell zugewiesene Adressen zu kümmern, sondern muss nur die Eindeutigkeit einer Adresse im eigenen Netzwerk sicherstellen.

Betrachtet man aber das Internet, müssen innerhalb des gesamten Internets die Adressen eindeutig sein. Daher gibt es eine Organisation, die offizielle Internet-Adressen vergibt: das Network Information Center NIC (es sind auch einige andere Unternehmen lizensiert, offizielle Internet-Adressen zu vergeben). Hier bekommen Unternehmen oder Schulen, die einen direkten Anschluss an das Internet realisieren möchten, ihre Netzwerkadresse zugewiesen.

Da aber die Netzwerke heute in der Regel aus mehreren physikalischen Netzen bestehen, würden mehrere Network-IDs benötigt, um die verschiedenen Netzwerke abzubilden. Da aber nicht mehr so viele Network-IDs zur Verfügung stehen, bekommt man in der Regel nur eine Network-ID zugewiesen. Hier muss nun von dem Bereich, der eigentlich für die Host-ID gedacht ist, eine Anzahl Bits intern für die Network-ID benutzt werden, um so eine Unterteilung in verschiedene Subnetze vornehmen zu können. Dies wird in der Subnet-Mask definiert.

Subnet-Mask

Class B Adressbereich	Zugehörige Class B Netmask	Subnet-Mask mit zusätzlichen 8 Bit für Netzwerk-Adressierung	Binäre Darstellung der Subnet-Mask
132.150.x.x	255.255.0.0	255.255.255.0	11111111 11111111 11111111 00000000

Bei der Konfiguration von TCP/IP auf dem Rechner muss nun eine IP-Adresse und eine Netmask eingetragen werden. Mit der Netmask wird die Länge der Host-ID und der Net-ID festgelegt.

Wendet man sich an einen Internet-Provider, um über ihn den Zugang zum Internet zu realisieren, bekommt man von ihm die für die Adressierung notwendigen Informationen.

5.2 DHCP (Dynamic Host Configuration Protocol)

Das DHCP-Protokoll erlaubt die dynamische Zuweisung von TCP/IP-Parametern an einen Rechner. Der DHCP-Server schickt dem DHCP-Client alle TCP/IP relevanten Informationen wie IP-Adresse, Gateway etc. Die wesentliche Aufgabe von DHCP besteht darin einem Rechner, auf dem TCP/IP aktiviert wird, dynamisch eine IP-Adresse zuzuweisen.

Dies kann immer die gleiche Adresse sein, die diesem Rechner zugewiesen wird.

Dies kann aber auch eine dynamische Adresse sein, die aus einem Pool von Adressen ausgewählt wird. Fährt der Rechner seine TCP/IP-Software herunter

(oder wird er ausgeschaltet), wird die Adresse wieder zur weiteren Benutzung durch andere Clients freigegeben.

Zusätzlich zur IP-Adresse können per DHCP noch andere Informationen weitergeleitet werden. Dazu gehören:

- Netmask
- Broadcast-Adresse
- DNS-Server (siehe Kapitel DNS)
- Standard-Gateway, das benötigt wird, wenn die Kommunikation zu einem Rechner in einem anderen Netzwerk aufgenommen werden soll. Die Information über ein Standard-Gateway oder einen Router muss jeder Rechner in einem Netzwerk haben, wenn mit mehr als einer Network-ID gearbeitet wird. Wird diese Information nicht über DHCP bezogen, muss sie von Hand eingegeben werden.

DHCP verhindert Konfigurationsfehler (unabsichtlich oder absichtlich) wie z. B. die doppelte Vergabe einer IP-Adresse. Es vereinfacht das IP-Adressmanagement und gewährleistet so einen stabilen und sicheren Netzwerkbetrieb.

Abbildung 12: DHCP

Da DHCP ein LAN-Protokoll ist, können Internet-Provider nicht damit arbeiten. Sie setzen in der Regel ein ähnliches Protokoll ein, PPP (Point-to-Point-Protocol), das auch in der Lage ist, aus einem Pool dynamisch IP-Adressen zuzuweisen. Denn gerade Internet-Provider stehen vor der Situation, dass in der Regel nicht alle Anwender, die über diesen Internet-Provider den Zugang ins Internet bekommen, gleichzeitig im Netz arbeiten. So müssen sie nicht für jeden potentiellen Benutzer eine eigene Internet-Adresse vorhalten, sondern kommen mit einem geringeren Pool von Adressen aus.

5.3 DNS (Domain Name Service)

Vorher wurde beschrieben, wie Rechner über die eindeutige IP-Adresse identifiziert werden. Um sie sich besser merken und eingeben zu können, werden die Adressen nicht in der binären Darstellung angegeben, sondern durch den 4-stelligen, dezimalen Wert.

Aber es ist selbst bei dieser Darstellung nicht einfach, sich die IP-Adressen von Rechnern zu merken. Daher gibt es zusätzlich die Möglichkeit, Rechnern einen Namen zu geben, mit denen sie angesprochen werden können. Die Software selber arbeitet aber nicht mit den Namen, sondern immer über die Adresse. Daher wird ein Übersetzungsmechanismus benötigt, der die Namen in die eigentlichen Adressen übersetzt.

Um möglichst viele verschiedene Namen zur Verfügung zu haben, sind die Namen hierarchisch strukturiert. Dieses hierarchische Schema wird bezeichnet als „Domain Name Service“. Ein Domain Name besteht aus verschiedenen Unternamen, wobei die einzelnen Elemente durch einen Punkt abgetrennt werden. Das letzte Element des Namens gibt die Zugehörigkeit zu einer Organisation oder einem Land an.

Auch die im Internet verwendeten Namen werden von der NIC verwaltet. Dort ist festgelegt, was das letzte Element des Namens bedeutet:

Domain-Bezeichnungen

Domain Name	**Bedeutung**
COM	Kommerzielles Unternehmen
EDU	Schule, Universität oder ähnliche Einrichtung
ORG	Organisation, die in keine andere Kategorie fällt
Länder-kennzeichen	Für Länder außerhalb der USA

So zeigt z. B. der Name **www.zs-augsburg.de** auf die World Wide Web Seite der Zentralstelle für Computer und Unterricht in Augsburg. An der Endung „de“ kann man erkennen, dass es sich um eine Adresse in Deutschland handelt. Viele internationale Unternehmen beantragen eine länderspezifische Domain mit einer deutschen Einstiegsseite, die aber dann weiter verweist auf die Domain mit den entsprechenden Internetseiten der Mutterfirma, die vielleicht in den USA beheimatet ist.

Die Adresse **www.ietf.org** zeigt auf die World Wide Web Seite der IETF, wo z. B. auch die RFCs, die Request-for-Comments, abgerufen werden können, in denen die Beschreibungen der in der TCP/IP-Welt wichtigen Dinge niedergelegt sind.

Früher kostete das Beantragen und Betreiben einer Domain mehr als tausend Mark pro Jahr. Diese Preise sind in den letzten Jahren rapide gefallen. Das führt dazu, dass immer mehr Unternehmen, Institutionen und auch Privatpersonen eine eigene Domain beantragen, auch wenn sie sie im Moment noch nicht betreiben. So sichern sie sich „ihren eigenen Internet-Namen“.

Um die Domain-Namen in echte Netzwerk-Adressen auflösen zu können, braucht man einen oder mehrere Server, auf denen die „Übersetzung“ gespeichert ist. DNS ist intern so strukturiert, dass es für eine Übersetzungsanfrage ausreichend ist, einen ersten DNS-Server zu kontaktieren. Kennt er die Auflösung nicht, wird an einen nächsten Server weitergeleitet, evtl. an noch einen weiteren Server usw. bis die gewünschte Information zur Verfügung gestellt werden kann.

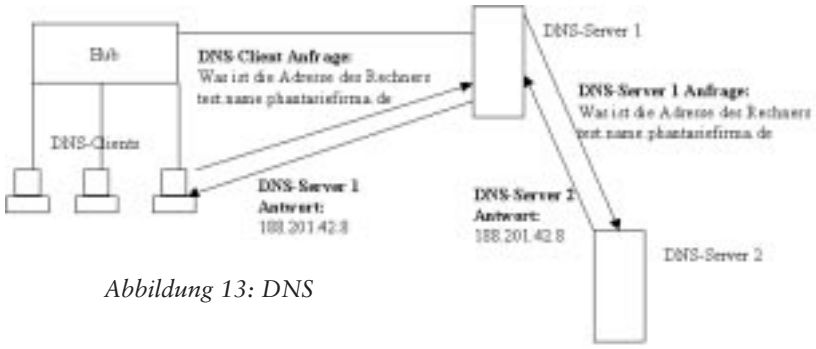


Abbildung 13: DNS

Dies bedeutet, dass bei der Konfiguration von TCP/IP ein DNS-Server angegeben werden muss, wenn mit Namen anstatt Adressen gearbeitet werden soll (falls dieser nicht über DHCP bezogen wird).

6. DAS INTERNET

Das Internet ist ein weltweites Netzwerk, basierend auf TCP/IP-Protokollen und steht heute für:
- 150.000.000 Webseiten
- ca. 65.000 Newsgroups
- Viele verschiedene FTP- oder sonstige Server
- Verschiedene Browser, um die HTML-Seiten zu lesen

Somit ist das Internet ein riesiger Informationsträger, der täglich wächst. In diesem Abschnitt soll nun der technische Hintergrund des Internet betrachtet werden.

6.1 Die Provider-Wahl

Über den Provider wird der Zugang ins Internet angeboten. Internetprovider sind an das weltweite Datennetzwerk angeschlossen und liefern neben dem Zugang über eine Telefonleitung auch die für den Zugang zum Internet wesentlichen Informationen wie:
- IP-Adresse, wenn diese nicht über PPP bezogen wird.
- Benutzername mit Passwort
- E-Mail-Adresse
- IP-Adresse eines DNS-Servers und anderer Server, die für die Benutzung des Internets wichtig sind

Es gibt verschiedene Typen von Internetprovidern:
- Internet Service Provider (ISP) wie z. B. die örtlichen Bürgernetz-Vereine, Online Regions usw. bieten den Zugang zum Internet an. Dazu gehören World Wide Web, E-Mail, Newsgroups und meistens auch der Speicherplatz für eine eigene Homepage.
- Online-Dienste wie T-Online, AOL oder CompuServe bieten zusätzlich ein eigenes redaktionelles Angebot an.

Auf der Schulseite sollte der Anschluss an das Internet durch einen Router realisiert werden. Mit diesem Router wählt man sich beim Provider ein. In der Regel fallen hierfür Telefongebühren an. Daher macht es Sinn, einen Provider auszusuchen, der den Einwahlknoten in der Nahzone anbietet.

Zusätzlich fallen auch die Kosten für den Internetzugang selber an. In der Vergangenheit wurden diese Kosten prinzipiell getrennt abgerechnet: die Kosten für den Internetzugang berechnete der Provider, die Telefongebühren die Telekom. Durch die Liberalisierung des Telefonmarktes änderte sich dieses. Immer mehr Internetprovider bieten Pauschaltarife an, die beide Kosten beinhalten.

Welcher Provider am günstigsten und am besten ist, ist heute generell nicht mehr so einfach zu beantworten. Nahezu monatlich erscheinen in verschiedenen Zeitschriften, angefangen mit Stiftung Warentest bis zu Fachzeitschriften, Vergleiche der verschiedenen Provider. Auch muss bei den verschiedenen Tarifen unterschieden werden, ob über einen langen Zeitraum im Internet „gesurft“ wird, oder der Internetzugang eher seltener benutzt wird. Und zu welcher Tageszeit hauptsächlich im Internet gearbeitet wird, denn häufig sind die Abend- oder Nachttarife wesentlich günstiger.

Auf einige Punkte sollte dennoch geachtet werden:
- Anzahl der möglichen Zugänge und Auslastung. Die Internetprovider bieten mehr Kunden den Zugang zum Internet an, als sie eigene Zugänge besitzen. Denn nicht alle Kunden wählen sich gleichzeitig ein. Aber ist die Auslastung zu groß, besteht die Gefahr, dass gerade dann alle Zugänge belegt sind, wenn im Unterricht der Umgang mit dem Internet demonstriert werden soll.
- Durchsatz der Leitung, die der Internetprovider selber zum Internet unterhält. Denn was nützen z. B. 128 KByte Durchsatz vom eigenen Router zum Provider, wenn dieser dann nicht in der Lage ist, diesen Durchsatz weiterzugeben.
- Werden Standards verwendet? Denn die Funktionalität, über die der eigene Router verfügt, sollte auch vom Provider angeboten werden. So z. B. die Verwendung des PPP-Protokolls (siehe entsprechendes Kapitel).

- Unterstützung bei Problemen. Auch wenn gerade in einer Schule vielleicht vieles im Rahmen von Projekten selber gemacht werden kann, können immer Probleme auftreten, die vor Ort nicht gelöst werden können. Und dann sollte eine Hotline zur Verfügung stehen, die kompetent beraten kann.

6.2 Standalone-Router contra PC mit ISDN-Karte

Ein Netzwerk benötigt ein Gerät das die Verbindung (sog. Gateways oder Router) zum Provider herstellt und regelt. Hierfür gibt es zwei prinzipielle Möglichkeiten:

- Ein Standalone-Router, der nur die Verbindung zum Internet-Provider und zum Internet selber bedient.
- Ein PC mit einer ISDN-Karte. Dies könnte ein PC mit LINUX oder ein Novell-Server mit Multiprotokoll-Router sein.

Während der Einsatz eines PCs im Heimbereich sinnvoll und praktikabel ist, bringt dies in Umgebungen, in denen mehreren Benutzern gleichzeitig der Zugang ins Internet geboten werden soll, aber einige Nachteile mit sich.

Entweder wird ein PC mit Software und eine ISDN-Karte benötigt, der nur die Verbindung zum Internet abhandelt. Dann sind die Kosten höher als für einen dedizierten Router.

Oder ein existierender PC wird mit einer ISDN-Karte ausgestattet. Aller Wahrscheinlichkeit nach wird dies z. B. ein File-Server sein. Das bedeutet aber gleichzeitig, dass der File-Server direkt ins Internet gestellt wird und kaum noch vor dem Zugriff durch Außenstehende zu schützen ist. Zumal dieser Rechner sinnvollerweise nur dann ausgeschaltet werden sollte, wenn kein Anwender mehr einen Zugang zum Internet braucht.

In der Regel sinkt die Stabilität des PCs mit der Übernahme zusätzlicher Funktionen. Und gerade der Zugang zum Internet sollte doch permanent zur Verfügung stehen.

Außerdem müssen Software-Router an die verwendete Hardware angepasst werden, was bei der Vielfalt von unterschiedlichen Geräten oft zu Problemen führt.

Ein dedizierter Router verfügt über erweiterte Funktionen, die den Zugang zum Internet einfach und sicher machen. Hierzu gehören NAT, PAT, Firewall und Gebührenkontrolle (siehe entsprechende Kapitel).

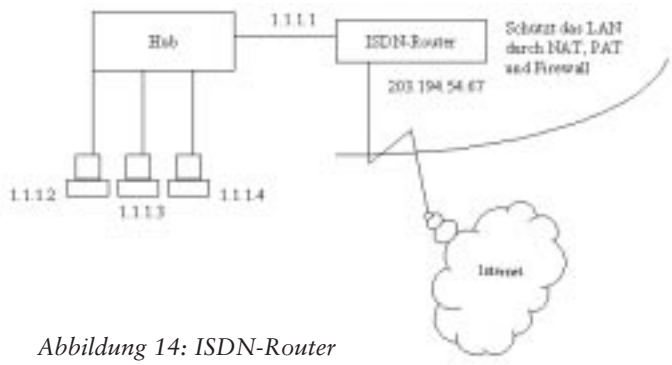


Abbildung 14: ISDN-Router

6.3 ISDN

Der Router, der für die Verbindung zum Internet eingesetzt wird, sollte sinnvollerweise ein ISDN-Router sein. Mit einem ISDN-S0-Anschluss stehen für die Datenübertragung zwei B-Kanäle mit jeweils 64 Kbps Bandbreite zur Verfügung. Diese 128 Kbps sind ein deutlich höherer Durchsatz, als mit herkömmlichen Modems zu realisieren ist. Außerdem basiert ISDN auf digitaler Technik, was für die digitale Übertragung von Daten sinnvoller ist als die Übersetzung und Rückübersetzung in analoge Telefontechnik.

Damit zwei Geräte über eine ISDN-Leitung Daten übertragen können, müssen sie sich mit Hilfe von Protokollen auf eine gemeinsame Sprache einigen. Nur wenn beide das gleiche Protokoll verwenden, können sie sich auch verstehen. Das ISDN verwendet immer zwei Protokolle für die Verbindung:
ein D-Kanal- und ein B-Kanal-Protokoll.

- Der D-Kanal überträgt in der Regel nur die Steuerinformationen, die zum Aufbau und zur Verwaltung der Verbindung benötigt werden. In Deutschland gibt es die Varianten DSS1 (Euro-ISDN), 1TR6 (das ältere, nationale ISDN in Deutschland) und Festverbindungen.
- Der B-Kanal überträgt die eigentlichen Nutzdaten der Verbindung. Auf drei Ebenen (Layern) wird beim B-Kanal-Protokoll in der Layer-Liste festgelegt, wie die Datenübertragung ablaufen soll. So hat man z. B. auf Layer 3 die Auswahlmöglichkeiten transparent, synchrones PPP und asynchrones PPP. Zusätzlich kann mit der Auswahl des Protokolls eine Script-Vearbeitung gestartet werden.

Der ISDN-Router, der für die Verbindung zum Internet-Provider eingesetzt wird, sollte in der Lage sein, entweder im Standleitungsbetrieb (bzw. als Festverbindung) oder im Wählverfahren arbeiten zu können. Welches Verfahren kostengünstiger ist, hängt von der Nutzungsdauer der Leitung ab.

- Wenn der Zugang zum Internet eher sporadisch benötigt wird, reicht eine Wählverbindung meist aus. Die ISDN-Router sind in der Regel in der Lage, die Wählverbindung selbstständig zu verwalten, d. h. bei Bedarf wird die Leitung automatisch aufgebaut und nach Ablauf der Datenübertragung bzw. nach einer vordefinierten Haltezeit wieder beendet.
- Die Festverbindung oder Standleitung verbindet vor allem Netzwerke, zwischen denen ein permanenter Datenaustausch stattfindet. Ab einer bestimmten Verbindungsdauer ist eine Standleitung kostengünstiger als eine Wählverbindung und durch den Wegfall der Anwahlvorgänge auch schneller. Der eingesetzte Router sollte Festverbindungen mit einem oder zwei B-Kanälen unterstützen. Entscheidet man sich für eine Standleitung, ist es in der Regel auch sinnvoll, eine Backup-Leitung aufzusetzen, die dann automatisch freigeschaltet wird, wenn die Hauptleitung zum Provider gestört sein sollte.

6.4 Kostenreduzierung und Gebührenkonto

Zu den reinen Investitionskosten für den Router werden auch die Gebühren für die Datenübertragung via ISDN kommen. Wie können die Kosten in Grenzen gehalten werden?

- Es sollten nur die Daten übertragen werden, die auch wirklich wichtig und notwendig sind. So kann z. B. mit Hilfe von Routing-Tabellen bestimmt werden, welche Daten übertragen werden. Andere Filter können ganze Datengruppen von der teuren ISDN-Leitung ausschließen. „Spoofing-Mechanismen“ helfen, bestimmte Anfragen an ein entferntes Netz lokal im eigenen Netz zubeantworten.
- Um das Datenvolumen bei der Übertragung über die ISDN-Leitung möglichst gering zu halten, werden die Daten komprimiert.
- Außerdem soll die Leitung nur dann offen sein, wenn auch Daten übertragen werden. Intelligentes Line-Management baut die notwendigen Verbindungen selbstständig auf und anschließend nach erfolgreicher Übertragung wieder ab. Werden dabei über das ISDN-Netz die Gebühreninformationen während der Verbindung übermittelt (nach AOCD), nutzen einige Router eine angefangene Gebühreneinheit vollständig aus und beenden die Verbindung erst kurz vor Beginn der nächsten Einheit.
- Die Gebühreneinheiten, die bezahlt werden, sollen natürlich möglichst günstig sein. Der durch die Liberalisierung des Telefonmarktes eingetretene Wettbewerb hat dazu geführt, dass die preiswertesten Telefonverbindungen je nach Tageszeit und Entfernung bei unterschiedlichen Providern (Telefongesellschaften) gefunden werden können. Der Router sucht idealerweise in einer vordefinierten Tabelle automatisch für jede Verbindung die günstigsten Tarife aus.
- Über ein Gebührenkonto im Router, kann eine Anzahl von Gebühreneinheiten festgelegt werden, die maximal in einem bestimmten Zeitraum gebraucht werden darf. So kann z. B. für eine Woche die maximale Anzahl der Einheiten auf 500 begrenzt werden. Wird dieser Wert vor Ablauf einer Woche erreicht, ist ein weiterer Zugriff auf die ISDN-Leitung nicht mehr möglich.

6.5 PPP (Point-to-Point Protocol)

Das Point-to-Point Protocol (PPP) wurde speziell für Netzwerkverbindungen über serielle Kanäle entwickelt und hat sich als Standard für Verbindungen zwischen ISDN-Routern entwickelt. Es realisiert folgende Funktionen:

- Festlegung der zu benutzenden Protokolle. Dazu gehören auch für diese Protokolle notwendigen Parameter wie z. B. IP-Adressen.
- Passwortschutz nach PAP (Password Authentication Protocol) oder CHAP (Challenge Handshake Authentication Protocol). Dies ermöglicht beim Verbindungsaufbau den Austausch von Passwörtern.
- Rückruffunktion (Call Back) - bei dieser Funktion übermittelt die Außenstelle der Zentrale den Wunsch zum Verbindungsaufbau zur Datenübertragung. Der eigentliche Verbindungsaufbau wird dann über die Rückruffunktion von der Zentrale vorgenommen.
- Überprüfung der Verbindung mit dem LCP (Link Control Protocol)
- Bündelung von mehreren Kanälen (Multilink PPP)

Für Router-Verbindungen über WAN-Strecken wie ISDN ist PPP das Standard-Übertragungsprotokoll. Die meisten Router-Hersteller unterstützen PPP, somit ist eine Datenübertragung auch in heterogenen Netzwerken möglich.

6.6 NAT (Network Address Translation) und PAT (Port Address Translation)

Der Zugang zum Internet eröffnet neben dem riesigen Angebot an Informationen auch ein zusätzliches Risiko. Um das LAN vor Angriffen von außen zu schützen, gibt es verschiedene Sicherheitsmechanismen. Ein sehr effektiver „Sicherheits“-Mechanismus ist unter IP-Masquerading oder NAT/PAT bekannt.

Kurz gesagt, bedeutet dies, dass alle Workstations im LAN hinter einer einzigen IP-Adresse versteckt werden. Dies liefert zum einen Sicherheit, da zunächst kein Rechner von außen über seine eigentliche IP-Adresse erreichbar ist. Zum anderen spart dies auch den Kauf von teuren IP-Adressen, da intern im LAN weiterhin mit beliebigen IP-Adressen gearbeitet werden kann, denn diese bleiben im Internet unsichtbar.

Wie funktioniert Network Address Translation?
Zunächst einmal braucht der Router, der die Verbindung zum Internet herstellt, zwei Adressen und zwei Netmasks. Eine Adresse und Netmask für die LAN-Seite und eine für die Internet-Seite. Zusätzlich muss ihm mitgeteilt werden, welche Adresse er nach außen, in das Internet, weitergeben darf.

Bei einem Kommunikationsaufbau wird immer die Zieladresse und Ursprungsadresse der beteiligten Rechner angegeben. Nimmt nun ein Rechner aus dem LAN die Verbindung zum Internet auf, überschreibt der Router die interne Adresse des LAN-Rechners mit seiner offiziellen Internet-Adresse. Es geht also nur diese registrierte Adresse wirklich ins Internet. Der Router muss aber die LAN-Adresse weiterhin der Verbindung oder Session zuordnen können, denn die Informationen, die zurückkommen, sollen ja wieder an den richtigen Rechner weitergeleitet werden.

Beispiel:
Zwei Rechner aus dem LAN machen eine WWW-Abfrage auf verschiedene Web-Seiten. Der Router ersetzt die IP-Adressen der Absenderstationen mit seiner eigenen IP-Adresse. Die Anworten aus dem Web werden nun vom Router wieder den internen Adressen zugeordnet und an die entsprechenden Stationen im LAN weitergeleitet.

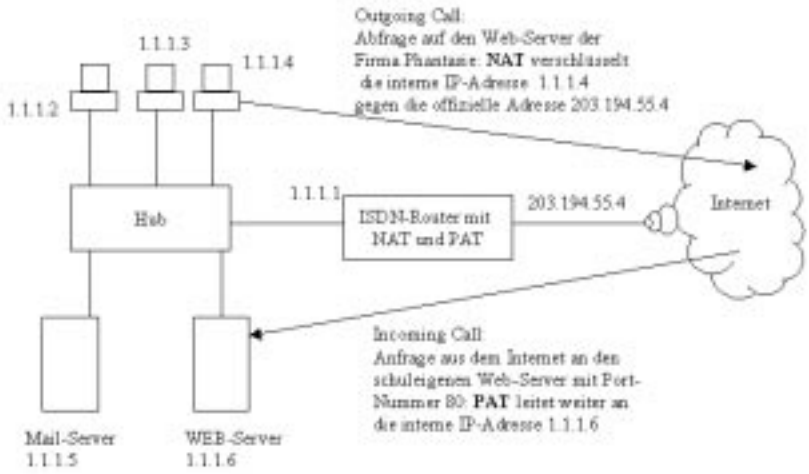
Dieses Verfahren funktioniert aber nur für ausgehende Verbindungen, also Verbindungen, die von der LAN-Seite aus initiiert werden. Nur dann hat der Router die notwendigen Informationen, um die zurückkommenden Informationen richtig weiterzuleiten.

Bedeutet das, dass kein eigener Web- oder FTP-Server aufgestellt werden kann?

Ja, aber nur in Verbindung mit Port Address Translation (PAT). Unter TCP/IP werden allen Applikationen, also z. B. FTP, Web usw. eigene Ports zugewiesen. Soll eine Datei per FTP kopiert werden, wird intern die Adresse des Rechners angegeben, von dem kopiert werden soll. Und die Tatsache, dass dies ein FTP-Zugriff ist, wird in der Port-Nummer 20 bzw. 21 verschlüsselt. Oder ein World Wide Web HTTP-Zugriff bekommt die Port-Nummer 80.

Schickt nun ein Rechner aus dem Internet ein Paket z. B. an einen FTP-Server im Intranet, so sieht es für diesen Internet-Rechner so aus, als wäre der Router der FTP-Server. Der Router kennt über einen Eintrag in einer entsprechenden Tabelle die IP-LAN-Adresse des Servers. Das Paket wird an diesen Rechner weitergeleitet. Alle Pakete, die vom FTP-Server im lokalen Netz kommen (Antworten des Servers), werden hinter der IP-Adresse des Routers versteckt.

Abbildung 15: NAT/PAT

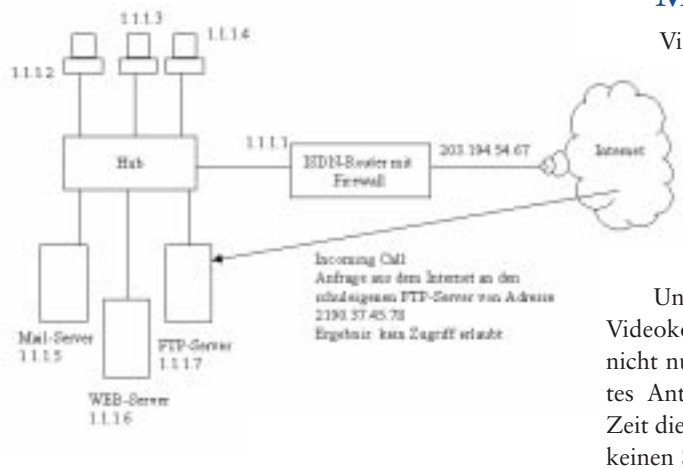


6.7 Firewall

Diese „Feuerwand“ ist ein weiterer Mechanismus, um das Intranet (die LAN-Seite) vor Angriffen aus dem Internet zu schützen. Eine Firewall ist in der Regel eine Kombination von Hard- und Software und bildet eine Grenze zwischen dem Intranet (dem internen LAN) und dem Internet.

Auf dem Router (Firewall) wird definiert welche Daten aus dem Intranet ins Internet transportiert werden dürfen und umgekehrt. Über Filter am Router werden Informationen wie IP-Adresse und Port-IDs untersucht und entsprechende Aktionen eingeleitet. So kann über die Zieladresse der Zugriff auf bestimmte externe Rechner gesperrt werden. Eingehende Informationen können mittels der Absender-Adresse gefiltert werden. Über die Port-ID können Filter auf Anwendungen gesetzt werden. So kann z. B. eine FTP-Verbindung zu einem Rechner erlaubt, eine Telnet-Verbindung zu dem selben Rechner aber gesperrt sein.

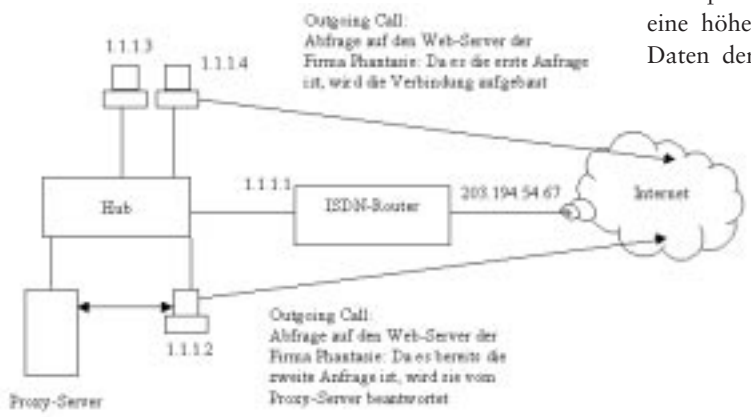
Abbildung 16: Firewall



6.8 Proxy

Zugriffe auf das Internet können auch zunächst auf Proxy-Server (Proxy = Stellvertreter bzw. Bevollmächtigter) umgeleitet werden. Dies kann unter Sicherheitsaspekten geschehen, indem nur Zugriffe auf „vertrauenswürdige“ Internet-Server zugelassen werden. Darüber hinaus können die Proxy-Server aber auch als großer Cache benutzt werden, auf denen zunächst nachgeschaut wird, ob der Zugriffswunsch des Anwenders bereits abgehandelt werden kann. Je mehr Anwender über den Proxy auf das Netzwerk zugreifen, desto größer ist die Wahrscheinlichkeit, dass ein Zugriff aus dem Proxy-Cache befriedigt werden kann. Und das Auslesen des Caches geht wesentlich schneller als der direkte Zugriff auf das Internet.

Abbildung 17: Proxy



7. QUALITY OF SERVICES, MULTIMEDIADIENSTE

Videokonferenzen oder Unterricht über das Netz, Zugang zum Internet, Herunterladen von Musik, Filmen oder interaktiven Lernprogrammen, Fotobearbeitung, all dies ist technisch möglich und verbirgt sich neben anderen Anwendungen hinter dem Begriff Multimedia. Aber immer mehr Anwendungen brauchen immer mehr Bandbreite. Und nicht nur das. Schauen wir uns eine Videokonferenz über das Netz an. Diese braucht nicht nur viel Bandbreite, sondern auch ein definiertes Antwortzeitverhalten. Wenn nicht in kürzester Zeit die Antwort kommt, macht die ganze Konferenz keinen Sinn.

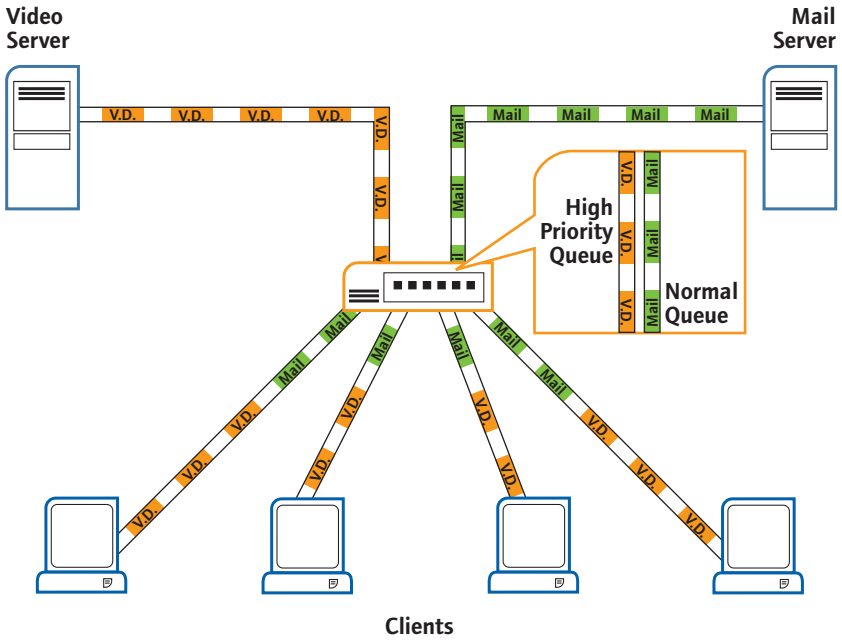
In den ersten Kapiteln haben wir von Ethernet, Fast Ethernet und Gigabit Ethernet gehört. Mit Switching kann die Bandbreite des Netzwerks um ein vielfaches erhöht werden. Also ist die Lösung für die oben beschriebenen Multimedia-Anwendungen Gigabit Ethernet? Gibt es noch eine weitere Möglichkeit, Multimedia-Anwendungen in einer bestehenden Netzwerk-Infrastruktur ohne Gigabit Ethernet zu betreiben?

Die Lösung kann auch in der Priorisierung des Datenstroms liegen, vor allem, wenn diese hohen Durchsatzraten nicht permanent benötigt werden. Denn in der Regel brauchen nicht alle Anwendungen die schnellen Antwortzeiten wie die oben erwähnte Videokonferenz, die zudem nicht täglich stattfindet. Für die alltäglichen Applikationen, wie z. B. das Herunterladen einer Datei, spielt es keine große Rolle, ob es manchmal ein paar Sekunden länger dauert.

Priorisierung gibt nun über den Standard IEEE 802.1p die Möglichkeit, bestimmten Applikationen eine höhere Priorität zuzuweisen als anderen. Die Daten der höher priorisierten Anwendung werden bevorzugt behandelt. IEEE 802.1p definiert ein 3-Bit langes Feld für die Kennzeichnung der Prioritätsklasse. Dies erlaubt einer Unterteilung in 8 verschiedene Prioritätsklassen.

So ist es möglich, zum Beispiel der Videokonferenz über eine höhere Priorität im Netz eine reservierte Bandbreite zur Verfügung zu stellen, unabhängig davon, wie ausgelastet das Netz im Moment ist. Die verbleibende Bandbreite teilen sich alle anderen Anwendungen, sodass sie ungestört weiterarbeiten können, wenn auch vielleicht etwas langsamer.

Abbildung 18: Priorisierung



8. ALLGEMEINE LITERATUR

1. Dr. Franz-Joachim Kauffels:
   Einführung in die Datenkommunikation

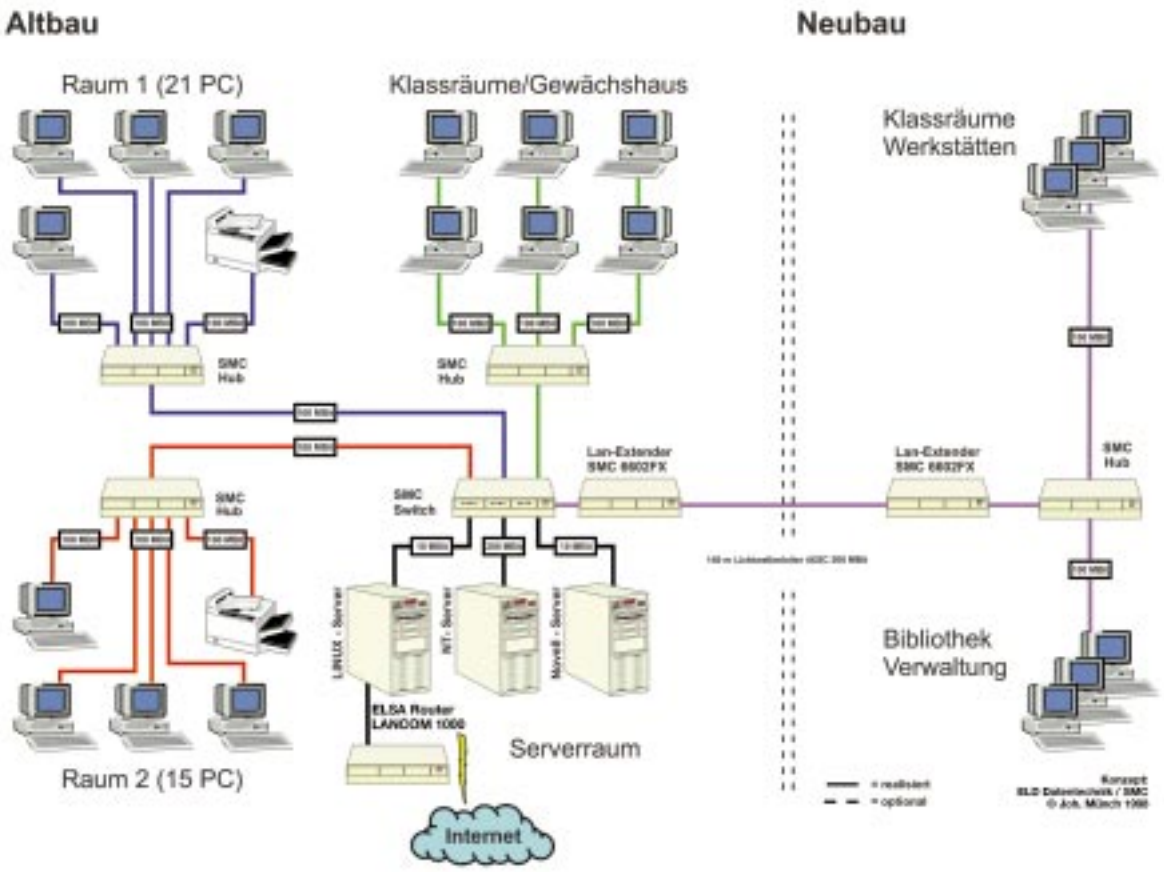
2. Andrew S. Tannenbaum: Computer Networks
   (Auch auf Deutsch verfügbar)

3. John E. McNamara:
   Local Area Networks

4. James Martin:
   Local Area Networks

5. Douglas Comer:
   Internetworking with TCP/IP

6. Douglas Comer:
   Computernetzwerke und Internet



9. BEISPIEL EINER ERFOLGREICHEN INSTALLATION (Berufliche Schulen Neusäß)

Das Beispiel zeigt, wie mit Hilfe eines Daten-Netzwerks (es besteht aus einem LAN = Local Area Network und einem WAN = Wide Area Network) in den einzelnen Unterrichtsräumen Daten untereinander ausgetauscht werden können. In jedem Raum befindet sich eine Verteilerstation (Hub), an die alle PCs angeschlossen sind. Im Server-Raum laufen über eine Hochgeschwindigkeits-Komponente (sog. Switch) die Datenströme zusammen. Dort steht auch der „Router", über den die Verbindung zu anderen Schulen bzw. zum Internet hergestellt wird.

Eine Besonderheit dieses Netzwerks ist die Anbindung des 140 m entfernten Neubaus, wo neben Klassenräumen auch Bibliothek und Schulverwaltung untergebracht sind. Um zwischen beiden Netzwerk-Segmenten die gleich hohe Leistung sicher zu stellen, wurde ein Lichtwellen-Leiter installiert, der beidseitig an je einen sog. „Lan-Extender" angeschlossen ist. Lehrer und Schüler können in diesem Netzwerk zeitnah u. a. auf Lernprogramme im Netzwerk oder auf das Internet zugreifen bzw. mit anderen Schulen kommunizieren.

Die vernetzte Schule e.V. wird von folgenden Unternehmen unterstützt:

co.Tec – Computergestütztes lernen
www.coTec.de

Dätwyler – Kabel und Systeme GmbH
www.daetwyler.de

ELSA AG
www.elsa.de

Fujitsu-Siemens AG
www.fujitsu-siemens.de

Nasdo AG
www.nasdo.de

Rittal GmbH
www.rittal.de

SMC Networks GmbH
www.smc.de

Sony Deutschland AG
www.sony.de

topik Communication GmbH
www.topik.de

Zentralstelle für Computer
im Unterricht Augsburg
www.zs-augsburg.de

Die vernetzte Schule e.V.

Truderinger Str. 217 · 81825 München
Tel: 089/45 45 90-45 · Fax: 089/45 45 90-46
E-Mail: info@dievers.de · www.dievers.de