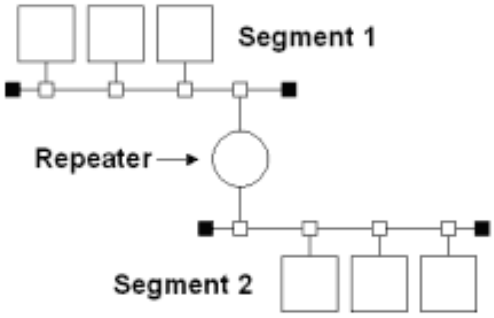
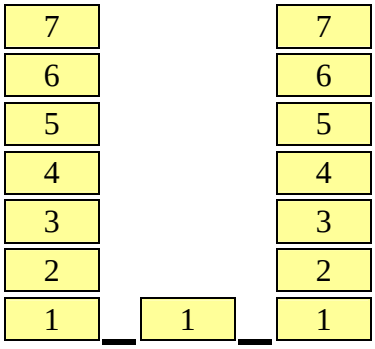
Vermittlungsgeräte (indermediary devices) in Computernetzen: Repeater, Hub, Bridge, Switch, Router, Gateway

Repeater



Verbindung zweier Segmente über einen Repeater



Der Repeater im OSI-Modell

Ein **Repeater** (englisch für „Wiederholer“) ist ein Signalverstärker, der in der Bitübertragungsschicht (Schicht 1) des OSI-Modells ein Signal empfängt, dieses dann elektrisch oder optisch neu aufbereitet und wieder aussendet. Rauschen sowie Verzerrungen der Laufzeit (Jitter) und der Pulsform werden bei dieser Aufbereitung aus dem empfangenen Signal entfernt. Von einfachen Repeatern wird die übertragene Information nicht beeinflusst, sondern nur das elektrische bzw. optische Signal aufbereitet. In Lokalen Netzen werden Repeater verwendet, um Netzsegmente zu erweitern.

Ein Repeater mit mehr als zwei Anschlüssen wird auch als Hub oder Multi-Port-Repeater bezeichnet.

Repeater in der Netztechnik

Der Einsatz von Repeatern bietet sich z. B. bei LANs in Bus-Topologie an, um die maximale Kabellänge von z. B. 185 m bei 10BASE2 (auch „BNC“ oder „Koax“) zu erweitern. Der Repeater teilt das Netz zwar in zwei physische Segmente, die logische Bus-Topologie bleibt aber erhalten. Durch diesen Effekt erhöht der Repeater die Ausfallsicherheit des Netzes, da bei Wegfall eines Teilnetzes das jeweils andere weiter unabhängig agieren kann. In einer "normalen" Bus-Topologie würde es zum Ausfall des gesamten Netzes kommen. Repeater erhöhen nicht die zur Verfügung stehende Bandbreite eines Netzes.

Man unterscheidet in der LAN-Technik zwei Typen von Repeatern:

- **Local-Repeater**, die zwei lokale Netzsegmente miteinander verbinden und
- **Remote-Repeater**, die zwei räumlich getrennte Netzsegmente, über ein so genanntes *Link-Segment* verbinden. Ein *Link-Segment* besteht aus zwei Repeatern, die per Glasfaserkabel miteinander verbunden sind. Dies macht es möglich, größere Distanzen zu überbrücken.

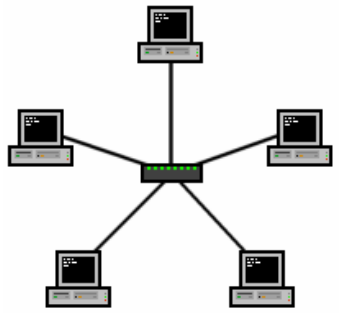
Repeater können in einem Ethernet nicht beliebig kaskadiert werden, um eine größere Netzausdehnung zu erreichen. Da mit Repeatern verbundene Segmente eine Kollisionsdomäne bilden, dürfen zwei Stationen auf Grund der Laufzeiten des Signals nur soweit voneinander entfernt sein, dass die Kollisionserkennung noch eindeutig funktioniert. Dies wird mit der 5-4-3-Regel bewerkstelligt.

Abgrenzung zum Begriff WLAN-Repeater

In der Informationstechnologie können sogenannte WLAN-Repeater zur Ausweitung der Reichweite eines drahtlosen Funknetzes verwendet werden. Hierbei halbiert sich die Datenübertragungsrate des Funknetzes, da der Repeater sowohl mit den Clients als auch mit dem Wireless Access Point kommuniziert. Beim Einrichten eines Repeaters entsteht kein neues WLAN, sondern der Repeater ist unter der SSID-des Root-Accesspoints sichtbar. Damit ist es für den Benutzer unerheblich, ob er sich direkt mit dem Root-AP oder über den Repeater verbindet.

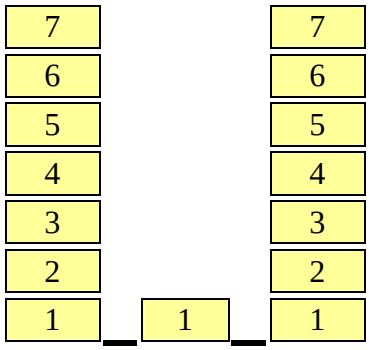
Fast alle modernen, handelsüblichen Wireless Access Points bieten einen Repeatermodus, um größere Gebäude, Grundstücke und Gelände mit einer ausreichenden Netzabdeckung zu versorgen. Mittels Roaming können sich die Clients frei im gesamten Versorgungsgebiet des Netzes bewegen, ohne dass der Datenverkehr durch Verbindungsabbrüche beeinträchtigt wird.

Hub



Stern-Topologie
Die Topologie eines Hubs ist ***physikalisch***.ein Stern

Bus-Topologie
Die Topologie eines Hubs stellt logisch ***eine Art*** Bus dar.



Der Hub im OSI-Modell

Der **Hub** (engl. *hub* ‚Nabe' [technisch], ‚Knotenpunkt') bezeichnet Geräte, die Netzknoten (physisch) sternförmig verbinden. Sie werden verwendet, um Netzknoten oder auch weitere Hubs, z. B. durch ein Ethernet, miteinander zu verbinden.

Ein Hub besitzt nur Anschlüsse (auch *Ports* genannt) mit gleicher Geschwindigkeit. Besitzt ein Hub beispielsweise eine BNC-Kupplung und RJ45-Anschlüsse, so beträgt seine Geschwindigkeit 10 Mbit halbduplex. Zum Anschluss weiterer Hubs oder Switche wird entweder ein spezieller Uplink-Port (auch X-Port oder MDI-X) oder ein gekreuztes Kabel benutzt. Ein Hub arbeitet, genauso wie ein Repeater, auf Ebene 1 des ISO/OSI-Referenzmodells (Bitübertragungsschicht) und wird deswegen auch *Multiport-Repeater* oder *Repeating-Hub* genannt. Das Signal eines Netzteilnehmers wird in keinem Fall analysiert, sondern nur elektronisch aufgebessert (entrauscht und verstärkt) und im Gegensatz zum Switch – der sich zielgerichtet Ports des Empfängers sucht – an **alle anderen** Netzteilnehmer weitergeleitet (Broadcast). Aus diesem Grund kann man an jedem Anschluß eines Hubs (im Gegensatz zu denen eines Switches) auch den Datenverkehr zwischen Netzwerkteilnehmern mit Netzwerksniffern analysieren oder mitschneiden.

Bei Einsatz eines Hubs im Netz wird durch die Verkabelung im physikalischen Sinne eine Stern-Topologie realisiert. Der logische Aufbau ähnelt dem einer Bus-Topologie, weil jede gesendete Information alle Teilnehmer erreicht. Alle Teilnehmer in einem Netzwerk, die an einen Hub angeschlossen sind, befinden sich in derselben Kollisionsdomäne. Durch einen Hub wird die Ausfallsicherheit gegenüber einem Bus-Netz erhöht. Die Störung eines Kabels legt hier nicht das gesamte Netz lahm, sondern beeinträchtigt lediglich einen einzelnen Teilnehmer, der dann nicht mehr erreichbar ist. Außerdem ist der Fehler einfacher zu lokalisieren.

Hubs können in einem Ethernet nicht beliebig kaskadiert werden, um eine größere Netzausdehnung zu erreichen. Wie bei Repeatern muss also die 5-4-3-Regel befolgt werden, damit Probleme mit zu hohen Signallaufzeiten (RTDT) vermieden werden. Aufgrund dieser Probleme werden heute fast überall Switche verwendet. Im Gigabit-Bereich (und höher) wurden daher auch keine Hubs/Repeater mehr spezifiziert.

Da Hubs und Switche rein äußerlich sehr ähnlich aussehen, werden Switche fälschlicherweise auch als Hubs bezeichnet. Tatsächlich gibt es aber wesentliche technische Unterschiede, selbst wenn die Geräte praktisch gleich aussehen. Den Verwechslungen leistet unter anderem auch Vorschub, dass auch Geräte, die auf den OSI/ISO-Schichten zwei bis vier agieren, also keine Hubs sind, ebenfalls unter der Bezeichnung Hub verkauft werden.

5-4-3-Regel

Die **5-4-3-Regel** oder auch **Repeater-Regel** besagt, dass bei einem Ethernet-Netzwerk mit gemeinsamem Zugriff in einer Baumtopologie (10BASE2, 10BASE-T) maximal 5 Segmente mit 4 Repeatern verwendet werden dürfen, wobei nur an 3 Segmenten aktive Endgeräte angeschlossen sind.
Segmente ohne aktive Geräte heißen *Linksegmente* oder *Inter-Repeater-Leitungen*. Ihre Aufgabe besteht lediglich darin, zwei Repeater miteinander zu verbinden, um größere Reichweiten zu überbrücken.

Grund

In einem klassischen Ethernet können durch den Halbduplex-Betrieb Kollisionen auftreten. Diese sollen möglichst vermieden, müssen aber auf jeden Fall zuverlässig erkannt werden (CSMA/CD).
Die Laufzeit eines Signales, und damit die maximale Bandbreite einer Broadcastdomäne, lässt sich durch die Summierung der Laufzeiten je Segment und der Verzögerung der Koppelelemente ermitteln. Dieser muss unterhalb des Round Trip Delays liegen.
Eine für jede Geschwindigkeit spezifische maximale Round-Trip-Delay-Time (RTDT) darf nicht überschritten werden. Die RTDT ist die Zeit, die ein Netzwerkpaket benötigt, um vom einen Ende des Netzes zum weitestentfernten anderen Ende des Netzes zu gelangen - und wieder zurück. Wird das Netz zu groß, also die RTDT zu hoch, werden Kollisionen häufiger, unerkannte Kollisionen möglich und der gesamte Netzverkehr beeinträchtigt. Solche Störungen sind schwierig einzugrenzen, da Übertragungen bei niedriger Netzlast normal funktionieren können.
Da diese Berechnung der RTDT relativ komplex sein kann, wurde mit der Router-Regel eine einfachere Repeater-Methode entwickelt, mit der die Laufzeitbeschränkung eingehalten werden kann.
Zu beachten ist, dass die 5-4-3-Regel nur auf den Bereich einer einzelnen Kollisionsdomäne anwendbar ist. Wird die Kollisionsdomäne durch den Einsatz eines Switch geteilt, beginnt die Zählung neu.

Repeater, Hubs und Switche

Werden bei 10BASE-T zwei Hubs über einen Uplink miteinander verbunden, so zählen sie als zwei halbe Repeater bzw. als ein Repeater. Ein neues Segment entsteht, wenn ein weiterer Hub an einen Port (des Repeaters) für Endgeräte (*kein* Uplink) angeschlossen wird.
Wird anstelle eines Hubs ein Switch verwendet, findet insoweit die 5-4-3-Regel keine Anwendung. Ein Switch ermöglicht einen Vollduplex-Betrieb, in dem keine Kollisionen mehr auftreten können.

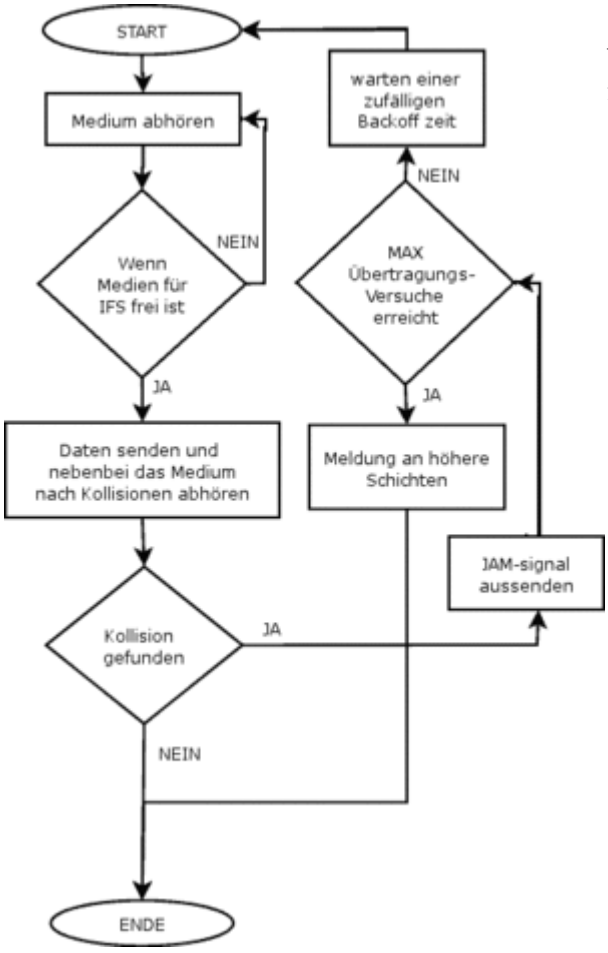
Fast Ethernet

Bei Fast Ethernet können unter Ausnutzung der maximalen Segmentlänge nur noch zwei Repeater kaskadiert werden.

Carrier Sense Multiple Access/Collision Detection

Der englische Begriff **Carrier Sense Multiple Access/Collision Detection** (**CSMA/CD**) (zu Deutsch etwa: „Mehrfachzugriff mit Trägerprüfung und Kollisionserkennung“) bezeichnet ein asynchrones Medienzugriffsverfahren (Protokoll), das den Zugriff verschiedener Stationen auf ein gemeinsames Übertragungsmedium regelt. Es handelt sich um eine Erweiterung von CSMA. Verwendung findet CSMA/CD beispielsweise im Bereich der Computernetze beim Ethernet und ist dort als IEEE 802.3 standardisiert worden. Bei Wireless LANs wird ein ähnlicher Mechanismus namens Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) benutzt.

Funktion bzw. Ablauf



Funktionsdarstellung in einem Programmablaufplan

Wenn ein Gerät Daten senden möchte, hält es sich an folgenden Ablauf:

1. *Horchen*: Zuerst muss das Medium überwacht werden, ob es belegt ist.
→ Frei: Wenn das Medium eine bestimmte Zeit lang (InterFrameSpacing) frei ist, weiter mit Schritt 2.
→ Belegt: Weiter mit Schritt 3.
2. *Senden*: Informationsübertragung, zugleich wird das Medium fortwährend weiter abgehört.
→ Erfolg: Übertragung wird erfolgreich abgeschlossen und eine Erfolgsmeldung an höhere Netzwerkschichten gemeldet, weiter mit Schritt 5.
→ Kollision: Wird eine Kollision entdeckt, beende die Datenübertragung und setze ein definiertes Störsignal *(jam)* auf die Leitung um sicherzustellen, dass alle anderen Transceiver die Kollision ebenfalls erkennen, dann weiter mit Schritt 3.
3. *Leitung ist belegt*: Überprüfung der Anzahl der Übertragungsversuche:
→ Maximum nicht erreicht: Eine zufällige Zeit (*Backoff*, s. u.) abwarten, dann wieder bei Schritt 1 beginnen.
→ Maximum erreicht: Weiter mit Schritt 4.
4. *Fehler*: Maximale Anzahl von Übertragungsversuchen wurde überschritten. Ein Fehler wird an die höheren Netzwerkschichten gemeldet, weiter mit Schritt 5.
5. *Ende*: Übertragungsmodus verlassen

Kollisionen und Kollisionserkennung

Bei Netzübertragungsverfahren wie Ethernet findet eine paketorientierte Datenübertragung in Datagrammen (Datenframes) auf einem gemeinsam genutzten Medium (Funk, Kabel), oder abstrakter, innerhalb einer gemeinsamen Kollisionsdomäne statt. Es wird also weder ein endloser Datenstrom erzeugt noch werden Zugriffe auf das Medium anderweitig deterministisch gesteuert. Daher ist es möglich, dass mehrere Stationen dasselbe Medium (z. B. Koaxialkabel) zeitgleich verwenden wollen. Hierdurch können dann Kollisionen entstehen, welche die übertragenen Signale unbrauchbar machen. Um dies wirkungsvoll zu unterbinden, wird das CSMA/CD-Verfahren eingesetzt. Aufgabe des CSMA/CD-Verfahrens ist es, auftretende Kollisionen aufzuspüren, zu reagieren und zu verhindern, dass sich diese wiederholen.

Von einer Kollision spricht man, wenn sich zwei (oder mehr) Signale gleichzeitig auf einer gemeinsamen Leitung befinden. Dabei überlagern sich die beiden elektrischen Signale zu einem gemeinsamen Spannungspegel. Die Folge ist, dass der Empfänger das elektrische Signal nicht mehr in die einzelnen logischen Signale (Bits) unterscheiden kann.

Das Verfahren ist, verglichen mit Token-Passing-Verfahren (z. B. Token Ring) oder Master-kontrollierten Netzen (z. B. ISDN), relativ einfach, was auch entscheidend zu seiner Verbreitung beigetragen hat. Modernere Ethernetverfahren (z. B. Fast Ethernet) umgehen die Kollisionsbildung ebenfalls. Kollisionen werden dort beispielsweise durch den Einsatz von gepufferten aktiven Verteilern (Switch) in geswitchten Umgebungen ebenfalls wirkungsvoll verhindert.

CSMA/CD und der Duplex-Modus

CSMA/CD ist der Sicherungsschicht des OSI-Modells zuzuordnen. Es wird von der Ethernetschnittstelle (z. B. Netzwerkkarte) durchgeführt, soweit diese im Halbduplex-Modus betrieben wird. Durch Konfiguration der Schnittstelle in den Vollduplex-Modus wird CSMA/CD abgeschaltet. Somit kann die Schnittstelle gleichzeitig senden und empfangen. Kollisionen müssen dabei verhindert werden, indem nur zwei Stationen dasselbe Übertragungsmedium nutzen können. Dies kann z. B. durch den Einsatz eines Switches erreicht werden. Dann können pro Segment oder Kollisionsdomäne zwei Knoten (Stationen) im Duplex-Betrieb aktiv sein, ohne dass es zu Kollisionen kommt.

Auch gibt es gänzlich kollisionsfreie Übertragungsprinzipien wie das Token Passing, es kommt z. B. bei ARCNET oder Token Ring zum Einsatz.

Physische Kollisionserkennung

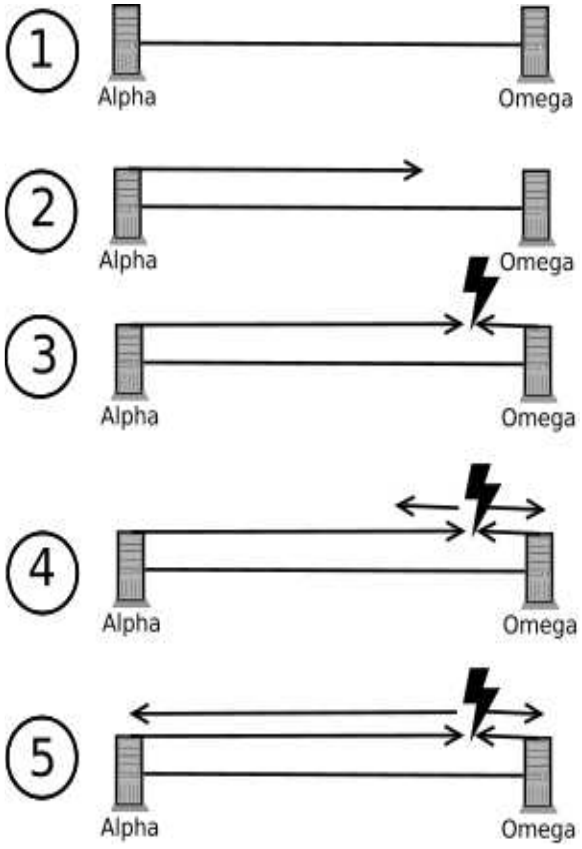
Signale sind als Spannungspegel messbar, wobei eine Überlagerung von Signalen eine Addition der Spannungspegel bedeutet. Eine Kollision von Signalen führt dabei zur Überschreitung eines Schwellwertes der Gleichspannungsanteile. Diese Spannungsüberschreitung kann von allen (auch den momentan unbeteiligten) Rechnern erkannt und als Kollision identifiziert werden.

Zusammenhang: Netzwerkausdehnung und Kollisionserkennung

Eine Kollision muss insbesondere vom Sender erkannt werden, damit er eine Sendewiederholung durchführen kann. Aus diesem Grund ist die minimale Paketlänge (eigentlich Framelänge), bzw. die Sendedauer für einen Frame minimaler Länge, so dimensioniert, dass die maximale RoundTripDelayTime (RTDT) nicht unterschritten wird. Die RTDT ist die Zeit, die ein Datenpaket benötigt, um vom einen Ende des Netzes zum weitestentfernten anderen Ende des Netzes zu gelangen – und wieder zurück. Dadurch wird sichergestellt, dass eine Kollision, die erst kurz vor dem Empfänger auftritt (ungünstigster Fall), sich noch bis zum eigentlichen Sender ausbreiten kann, ohne dass dieser das Senden beendet hat. Somit erkennt der Sender die Kollision, weiß dass sein Frame nicht richtig beim Empfänger angekommen ist und sendet den Frame erneut.

Damit die Kollisionserkennung zuverlässig funktioniert, wurde eine maximal zulässige Netzwerkausdehnung und eine dazu passende minimale Framelänge (64 Byte) für Ethernet festgelegt. Sollen „zu kurze“ Frames übertragen werden, müssen diese dazu nötigenfalls auf eine zulässige minimale Paketlänge verlängert werden. Wären die Pakete zu klein, was die gleiche Wirkung wie ein zu großes Netz (zu hohe RTDT) hätte, könnte es zu vom Sender unerkannten Kollisionen kommen, und der gesamte Netzverkehr könnte beeinträchtigt werden. Solche Störungen sind tückisch, da Übertragungen bei niederer Netzlast oder auch bei bestimmten Paketgrößen normal funktionieren können. Da Repeater und Hubs in die RTDT eingehen, jedoch keine wirklich fassbare Ausdehnung, wenn auch eine messbare Verzögerungszeiten haben, ist es praktikabler, von Zeiten als von Paketlängen zu sprechen.

Beispiel



Zeigt das Senden von Alpha nach Omega

In einem Netz maximaler Ausdehnung (~maximale RoundTripDelayTime) sind Station *Alpha* und *Omega* die beiden am weitesten auseinanderliegenden Stationen. Das Medium ist frei und *Alpha* beginnt mit der Übertragung. Bis *Omega* bemerkt, dass *Alpha* sendet, dauert es genau eine halbe RoundTripDelayTime – die Zeit, welche die Pakete/Signale von *Alpha* brauchen, um bis zur Station *Omega* zu gelangen. Hat nun *Omega* auch etwas zu übertragen und unmittelbar vor dem Eintreffen der Pakete von *Alpha* mit dem Senden begonnen – als aus Sicht von *Omega* die Leitung ja noch frei war – kommt es zunächst bei *Omega* zur Kollision, *Omega* bemerkt die Störung seiner Aussendung und kann entsprechend reagieren. Bis jetzt auch *Alpha* die Kollision bemerkt, dauert es noch mindestens eine weitere halbe RTDT – die Zeit, welche die Signale von *Omega* brauchen, um bis zur Station *Alpha* zu gelangen. Damit *Alpha* die Kollision bemerkt und eine Sendewiederholung initiieren kann, muss *Alpha* also noch solange weiter senden, bis die Pakete von *Omega* eingetroffen sind. Außerdem müssen alle Stationen, die die Pakete von *Alpha* empfangen haben, rechtzeitig über die Kollision informiert werden. Die minimale Sendedauer (~ minimale Paketgröße) muss also stets größer sein als die RTDT (~ doppelte Ausdehnung des Netzes).

Das Backoff-Verfahren bei Ethernet

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

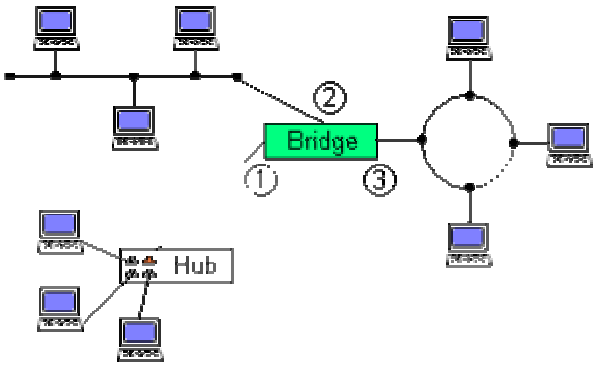
Bei Ethernet wählen die Konfliktparteien hierzu eine zufällige ganze Zahl **z** aus dem Intervall $[0;(2^i) - 1]$ (das sog. Contention Window), wobei `i` für die Anzahl der bereits aufgetretenen Konflikte steht. Die Anzahl der möglichen Sendeslots steigt also exponentiell, daher wird dieses Verfahren Binary Exponential Backoff genannt. Die Sendestation wartet nun den Zeitraum von `z * slot time` (s.o.) ab und sendet danach erneut, falls das Medium frei ist. Hat keine andere Station dasselbe `z` gezogen, gibt es also keinen Konflikt mehr.

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

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

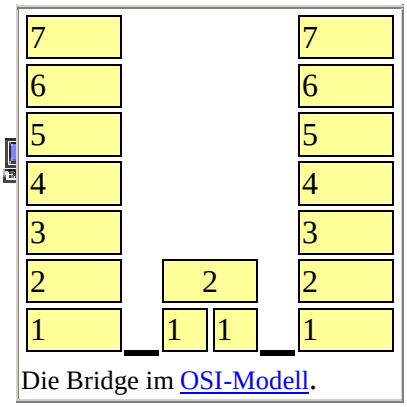
Aufgrund der auftretenden Kollisionen ist es nicht möglich, die theoretische Übertragungskapazität eines Mediums voll auszuschöpfen. In der Praxis kann man davon ausgehen, dass sich im günstigsten Fall etwa 70 % der Nominalleistung erzielen lassen, unter ungünstigeren Bedingungen sind es unter 30 %.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

Bridge



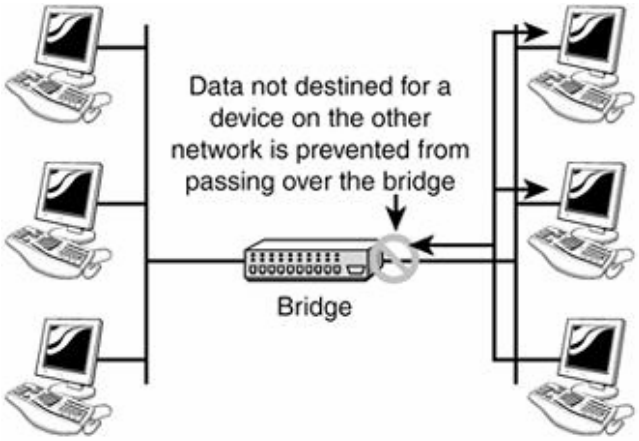
3 Netzsegmente an einer Bridge
Bus-, Ring- und Sternsegment bilden eigene Kollisionsbereiche

http://www.elektroniktutor.de/netze/net_pict/bridge.gif



Die Bridge im OSI-Modell.

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



Eine *MAC-Bridge* (*IEEE 802.1D*) wird hauptsächlich eingesetzt, um ein Netz in verschiedene Kollisionsdomänen aufzuteilen. Somit kann die Last in großen Netzen vermindert werden, da jeder Netzstrang nur die Pakete empfängt, deren Empfänger sich auch in diesem Netz befindet. Eine MAC-Bridge verbindet Netze mit gleichen Zugriffsverfahren.

http://commons.wikimedia.org/wiki/File:Bridge.JPG

Die *LLC-Bridge* (auch Remote-Bridge oder Translation Bridge) wird verwendet, um zwei Teilnetze mit verschiedenen Zugriffsverfahren (z. B. CSMA/CD und Token-Passing) zu koppeln (siehe Bild links oben) und besteht (idealisiert) aus zwei Teilen, die miteinander verbunden sind, wobei das Medium zwischen beiden Teilen hierbei egal ist. Innerhalb der LLC-Bridge findet eine Umsetzung (Translation) statt. Bei dieser Umsetzung werden alle Parameter des Quellnetzes (wie MAC-Adresse, Größe und Aufbau des MAC-Frames) an das Zielnetz angepasst, soweit diese vom Zielnetz unterstützt werden. Eine solche Übersetzung ist nicht immer direkt möglich. Bei Inkompatibilität der Netze muss teilweise der Umweg über Router-Funktionalität gegangen werden.

Eine *Transparente Bridge* lernt, welche MAC-Adressen sich in welchem Teilnetz befinden. Die Bridge *lernt* mögliche Empfänger, indem die Absender von Paketen in den einzelnen Teilnetzen in eine interne Weiterleitungstabelle eingetragen werden. Anhand dieser Informationen kann die Bridge den Weg zum Empfänger bestimmen. Die Absenderadressen werden laufend aktualisiert, um Änderungen sofort zu erkennen.

Eine *Source Routing Bridge* besitzt keine Weiterleitungstabelle. Hier muss der Sender die Informationen zur Weiterleitung zum Ziel bereitstellen.

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

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

Allen Bridge-Arten ist gemeinsam, dass ihre (Netz-)Ports im Promiscuous Mode arbeiten, so werden alle Pakete empfangen, dann erfolgt eine Überprüfung (Checksum), sodass nur korrekte Frames weitergesendet werden. Weiterhin wird im ungelernten Zustand jedes eingehende Paket an alle Ports gesendet (außer an den Port, welcher das Paket gesendet hatte).

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

Bridge vs. Switch

Es gibt in der Fachliteratur keine eindeutige Einteilung der Technik, die Bridges oder Switche definieren. Switche arbeiten als transparente Bridges, haben jedoch eine höhere Durchsatzleistung und mehr Ports. Hinzu kommt, dass moderne Switche auch häufig mit einer *Layer 3 Instance*, einem einfachen Router, ausgestattet werden. Allgemein wurden Bridges etwa ab 1985 zum Segmentieren (Verkleinern der Kollisionsdomäne) von Netzen und zum Verbinden unterschiedlicher Architekturen (z. B. Ethernet – TokenRing) entwickelt und vermarktet. Switche wurden erst viel später (1990) entwickelt. Sie können unter gewissen Umständen Router ersetzen, sogar dann, wenn sie keine eigene *Layer 3 Instance* enthalten. Zum Beispiel wenn der Einsatz eines Switches statt einer Bridge nötig wurde, um eine Kollisionsdomäne zu verkleinern und eine Bridge nicht genug Ports und Durchsatz hatte.

Zur Verkleinerung der Kollisionsdomäne erhält ein Switch möglichst viele Ports, an die jeweils nur wenige Geräte – im Idealfall eines – angeschlossen werden. Zusätzlich stellen ein oder mehrere sogenannte Uplink-Ports Verbindungen zum nächsten Switch bzw. Router her. Oft, aber nicht notwendigerweise sind Uplink-Ports in einer schnelleren oder höherwertigen (Ethernet-) Technik realisiert als die anderen Ports (z. B. Gigabit-Ethernet statt Fast-Ethernet oder Glasfaserkabel anstatt Twistedpair-Kupferkabel). Nicht modulare Switche haben in der Regel mindestens vier bis maximal etwa 48 Ports. Große „modulare“ Switche können je nach Modell zu Einheiten mit mehreren hundert Ports konfiguriert werden. Im Gegensatz zu Bridges können Switche mehrere Pakete zeitgleich zwischen verschiedenen Portpaaren übertragen. Am ehesten entspricht eine Bridge einem Switch im Betriebsmodus *Store and Forward* mit meist nur zwei Ports: *„a switch is a multiport bridge“* (ein Switch ist eine Mehrport-Bridge) lautete noch 1991 ein Lehrspruch der Firma Cisco, seit der Übernahme von Kalpana 1994 geht man bei Cisco differenzierter mit dem Thema um.

In den Anfangszeiten der Switch-Technik waren auch Port-Switche verbreitet, das waren preisgünstigere Geräte, welche über einen dedizierten Uplink-Port verfügten und an den restlichen Ports lediglich eine MAC-Adresse pro Port speichern konnten. Bridges hingegen können stets viele MAC-Adressen in ihrer internen SAT-Tabelle (Source Address Table) speichern. Umgekehrt benötigen Bridges zum Anschluss mehrerer Geräte oft externe Verteiler z. B. Hubs.

In der Regel können Bridges und Switche Netzwerke mit verschiedenen Übertragungsgeschwindigkeiten miteinander verbinden. Bridges können meist sowohl auf MAC- als auch auf LLC-Basis arbeiten, Switche hingegen arbeiten auf MAC-Basis. Switche können

folglich keine unterschiedlichen Architekturen (z. B. Ethernet – Token Ring) überbrücken. Da Ethernet den Markt dominiert, hat die Überbrückung verschiedener LAN-Architekturen nur eine geringe Bedeutung. Nicht zuletzt deshalb sind Bridges mittlerweile Nischenprodukte.

Bei größeren Switchen, genau so wie bei leistungsstarken Bridges, kann für jedes verbundene Netzwerk-Segment eine bestimmte Bandbreite festgelegt werden, auch können bestimmte Dienste priorisiert werden (Flow Control). Daneben unterstützen große moderne Switche eine Vielzahl von Protokollen und Verfahren (z. B. Discovery-Protokolle, VLANs, MANs, QoS, *Layer 3 Instance* mit diversen Routing-Protokollen, Management-Protokolle (SNMP, RMON, Syslog), Infrastruktur-Protokolle (DHCP-Server, BOOTP/TFTP-Server, FTP-Server, SSH-Server), Sonderbehandlung für spezielle Protokolle (DHCP und BOOTP Relay-Agent), Sicherheits-Features (Layer 2 bis 4 ACLs, Gratuitous ARP Protection, DHCP-Enforcement, MAC-Lockdown, Broadcasting-Kontrolle, Ingress-Filter), Redundanz-Protokolle (VRRP), usw.). Dabei verschwimmen auch die Unterschiede zu Routern immer mehr.

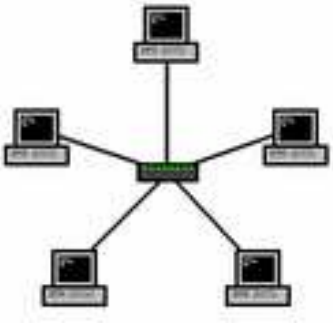
Bridges und Virtualisierung

Bridges, die innerhalb eines Betriebssystems eingerichtet werden, spielen eine große Rolle beim Thema Virtualisierung. Hierbei wird ein sogenanntes Bridgedevice eingerichtet, welches eine reelle Netzwerkkarte um virtuelle Netzwerkkarten erweitert und diese wie eine Bridge verbindet. Diese Schnittstellen werden dem virtualisierten Gastsystem als (virtuelle) Netzwerkkarten zur Verfügung gestellt. Erst über diese Netzwerkkarten wird die externe Netzwerkkommunikation eines Gastsystems über die reelle Netzwerkschnittstelle des Hostsystems auch nach außen möglich.

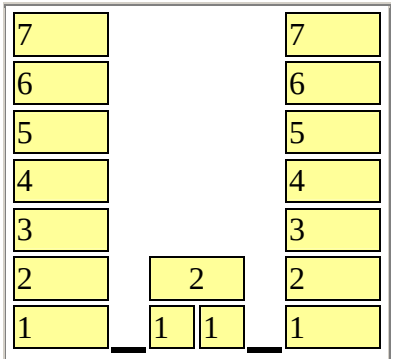
Software-Bridges

Neben dedizierter Hardware kann man auch Computer auf Apple-Mac-OS-, BSD-, DOS-, Linux- oder Windows-XP-Basis als Bridge-Lösungen einsetzen. Eine spezielle Hardware arbeitet zwar überwiegend robuster und durch die spezielle Architektur auch schneller; dennoch bestechen gerade Linux- und BSD-Versionen durch eine umfangreiche Unterstützung verschiedenster Netzwerkkarten und Protokolle. Leistungsbegrenzend wirken aber die geringen Datendurchsatzraten und die relativ hohen Latenzzeiten der bei PCs gängigen Bus-Systeme. Niemals erreichen PCs die Durchsatzraten von Switchen und nur selten die von Bridges. Allgemein haben Software-Router auf PC- oder Workstationbasis oft einen weiteren Nachteil: den relativ hohen Stromverbrauch. Bereits nach einem Jahr können die Stromkosten höher sein als der Preis für ein kleines Kompaktgerät. Manche Bridges nennen sich zwar Hardware-Bridge, bestehen aber tatsächlich aus PC-Komponenten. Lediglich das Gehäuse oder die zum Teil mechanisch veränderten PCI-Steckplätze und das Betriebssystem erwecken den Anschein eines Spezialsystems. Zwar arbeiten diese Systeme meist sehr robust und zuverlässig; dennoch wird auch hier das Bridging per Software und ohne spezielle Hardwareunterstützung durchgeführt.

Switch



Ein Netzwerk mit zentralem Switch ist eine Stern-Topologie.



Der Switch im OSI-Modell (Grundfunktion eines Switches).

Ein **Switch** (engl. *Schalter*; auch *Weiche*) ist ein Kopplungselement, das Netzwerksegmente miteinander verbindet. Der Begriff bezieht sich allgemein auf eine Weiterentwicklung einer Netzwerk-Bridge – ein aktives Netzwerkgerät – das Datenpakete auf dem Data Link Layer (Layer 2) des OSI-Modells weiterleitet. Switche, die zusätzlich Daten auf der Netzwerkebene (Layer 3 und höher) verarbeiten, werden oft als Layer-3-Switche oder Multilayer-Switche bezeichnet. Der erste Ethernet-Switch wurde von Kalpana im Jahr 1990 eingeführt. Das dem Switch vergleichbare Gerät auf Layer-1-Ebene wird als Hub bezeichnet.

Eigenschaften und Funktionen

Einfache Switche arbeiten auf der Schicht 2 (Sicherungsschicht) des OSI-Modells. Der Switch verarbeitet bei Erhalt eines Pakets die 48 Bit lange MAC-Adresse (z. B. 08:00:20:ae:fd:7e) und legt dazu einen Eintrag in der SAT (Source-Address-Table) an, in der neben der MAC-Adresse auch der physikalische Port, an dem diese empfangen wurde, gespeichert wird. Im Unterschied zum Hub werden Netzwerkpakete jetzt nur noch an den Port weitergeleitet, der für die entsprechende Zieladresse in der SAT gelistet ist. Ist der Weg zur Zieladresse allerdings noch unbekannt (Lernphase), leitet der Switch das betreffende Paket an alle aktiven Ports. Ein Unterschied zwischen Bridge und Switch ist die Anzahl der Ports beziehungsweise die Portdichte: Bridges haben typischerweise nur zwei Ports, selten drei oder mehr, Switche hingegen haben als Einzelgeräte meist zwischen vier (bei SOHO-Installationen), 12 (bei kommerziellen Installationen) oder 48 und mehr (in Rechenzentren oder großen Gebäudeinstallationen) Ports und können mehrere Ports unabhängig voneinander zeitgleich verbinden (non Blocking). Ein anderer möglicher Unterschied zu Bridges ist, dass manche Switch-Typen die Cut-Through-Technik und andere Erweiterungen (s.u.) beherrschen. So verringern sich die Bitzeiten (Zeitdauer für die Verarbeitung eines Bits). Switche können natürlich auch mit Broadcasts umgehen. Bis auf wenige Ausnahmen gilt: Ein Switch ist eine Bridge, aber nicht jede Bridge ist ein Switch. Eine Ausnahme bilden Bridges, die verschiedene Protokolle wie Token Ring und Ethernet (MAC-Bridge oder LLC-Bridge) verbinden können. Eine solche Funktionalität ist bei Switchen nicht anzutreffen.

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

Man unterscheidet auch zwischen Layer-2- und Layer-3- bzw. höheren Switchen. Layer-2-Geräte sind die älteren Modelle und verfügen nur über grundsätzliche Funktionen. Sie

beherrschen meist keine Management-Funktionen (sind allerdings „Plug-and-Play“-fähig), oder wenn doch, dann nur einen geringen Funktionsumfang wie Portsperren oder Statistiken. Professionelle Layer-3- bzw. höhere Switche verfügen in der Regel über Management-Funktionen; neben den grundlegenden Switch-Funktionen verfügen sie zusätzlich über Steuer- und Überwachungsfunktionen, die auch auf Informationen aus höheren Schichten als Layer 2 beruhen können, wie z. B. IP-Filterung, VLAN, Priorisierung für Quality of Service, Routing und andere Funktionen, die für die Überwachung und Steuerung eines Netzes hilfreich sind. Die Steuerung dieser Switche geschieht je nach Hersteller über die Kommandozeile, eine Weboberfläche, eine spezielle Steuerungssoftware oder über eine Kombination dieser drei Möglichkeiten. Bei den aktuellen nicht gemanageten (Plug-and-Play-)Switchen beherrschen die höherwertigen Geräte ebenfalls Layer-3-Funktionen wie tagged VLAN oder Priorisierung und verzichten dennoch auf eine Konsole oder ein sonstiges Management-Interface.

Funktionsweise

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

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

Wird die Zieladresse in der SAT gefunden, so befindet sich der Empfänger an der zugehörigen Schnittstelle angeschlossenen Segment. Das Paket wird dann an diese Schnittstelle weitergeleitet. Sind Empfangs- und Zielsegment identisch, muss das Paket nicht weitergeleitet werden, da die Kommunikation ohne Switch im Segment selbst stattfinden kann. Falls die Zieladresse (noch) nicht in der SAT ist, muss das Paket an alle anderen Schnittstellen weitergeleitet werden. In einem IPv4-Netz wird der SAT-Eintrag meist während der sowieso nötigen ARP-Adressenanfragen vorgenommen. Zunächst wird aus der ARP-Adressenanfrage eine Zuordnung der Absender-MAC-Adresse möglich, aus dem Antwortpaket erhält man dann die Empfänger-MAC-Adresse. Da es sich bei den ARP-Anfragen um Broadcasts handelt und die Antworten immer an bereits erlernte MAC-Adressen gehen, wird kein unnötiger Verkehr erzeugt. Broadcast-Adressen werden niemals in die SAT eingetragen und daher stets an alle Segmente weitergeleitet. Pakete an Multicast-Adressen werden von einfachen Geräten wie Broadcasts verarbeitet. Höher entwickelte Switche beherrschen häufig den Umgang mit sowie die Verarbeitung von Multicasts und senden Multicast-Pakete dann nur an die registrierten Multicast-Adress-Empfänger.

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

Unterschiedliche Arbeitsweisen

Ein Ethernet-Paket enthält die Zieladresse in den ersten 48 Bits (6 Bytes) nach der so genannten Datenpräambel. Mit der Weiterleitung an das Zielsegment kann also schon nach Empfang der ersten sechs Bytes begonnen werden, noch während das Paket empfangen wird. Ein Paket ist 64 bis 1518 Bytes lang, in den letzten vier Bytes befindet sich zur Erkennung von fehlerhaften Paketen eine CRC-Prüfsumme (*zyklische Redundanzprüfung*). Datenfehler in Paketen können also erst erkannt werden, nachdem das gesamte Paket eingelesen wurde.

Je nach den Anforderungen an die Verzögerungszeit und Fehlererkennung kann man daher Switche unterschiedlich betreiben:

- **Cut-Through** – Eine sehr schnelle Methode, wird hauptsächlich von besseren Switches implementiert. Hierbei schaut der Switch beim eingetroffenen Paket nur auf die Ziel-MAC-Adresse, trifft eine Weiterleitungsentscheidung und schickt das Paket entsprechend weiter. Um Zeit zu sparen wird das Paket nicht auf Fehlerfreiheit geprüft. Der Switch leitet deshalb auch beschädigte Pakete weiter, diese müssen dann durch andere Schicht-2-Geräte oder höhere Netzwerkschichten aufgefangen werden. Die Latenzzeit in Bit beträgt hier 112. Sie setzt sich aus der Präambel (8 Byte) und der Ziel-MAC-Adresse (6 Byte) zusammen.
- **Store-and-Forward** – Die grundlegendste, aber auch langsamste Switch-Methode mit der größten Latenzzeit. Sie wird von jedem Switch beherrscht. Der Switch empfängt zunächst das ganze Paket (speichert dieses; „Store“), trifft wie gehabt seine Weiterleitungsentscheidung anhand der Ziel-MAC-Adresse und berechnet dann eine Prüfsumme über das Paket, das er mit dem am Ende des Paketes gespeicherten CRC-Wert vergleicht. Sollten sich Differenzen ergeben, wird das Paket verworfen. Auf diese Weise verbreiten sich keine fehlerhaften Pakete im lokalen Netzwerk. Store-and-Forward war lange die einzig mögliche Arbeitsweise, wenn Sender und Empfänger mit verschiedenen Übertragungsgeschwindigkeiten oder Duplex-Modi arbeiteten oder verschiedene Übertragungsmedien nutzen. Die Latenzzeit in Bit ist hier identisch mit der Paketlänge, bei Ethernet und Fast Ethernet sind es folglich mindestens 512 Bit, bei Gigabit Ethernet mindestens 4096 Bit, Obergrenze ist die MTU in Bit (~ 12.000 Bit). Heute gibt es auch Switche, die einen Cut-and-Store-Hybridmodus beherrschen, der vor allem beim Switchen von schnell nach langsam beschleunigend wirkt.
- **Fragment-Free** – Schneller als Store-and-Forward, aber langsamer als Cut-Through. Anzutreffen vor allem bei besseren Switches. Prüft, ob ein Paket die im Ethernet-Standard geforderte minimale Länge von 64 Bytes (512 Bit) erreicht und schickt es dann sofort auf den Zielport, ohne eine CRC-Prüfung durchzuführen. Fragmente unter 64 Byte sind meist Trümmer einer Kollision, die kein sinnvolles Paket mehr ergeben.
- **Error-Free-Cut-Through/Adaptive Switching** – Eine Mischung aus mehreren der obigen Methoden. Wird ebenfalls meist nur von teureren Switchen implementiert. Der Switch arbeitet zunächst im „Cut through“-Modus und schickt das Paket auf dem korrekten Port weiter ins LAN. Es wird jedoch eine Kopie des Paketes im Speicher behalten, über die dann eine Prüfsumme berechnet wird. Stimmt sie nicht mit der im Paket überein, so kann der Switch dem defekten Paket zwar nicht mehr hinterhersignalisieren, dass es falsch ist, aber er kann einen internen Zähler mit der Fehlerrate pro Zeiteinheit hochzählen. Wenn zu viele Fehler in kurzer Zeit auftreten, fällt der Switch in den Store-and-Forward-Modus zurück. Wenn die Fehlerrate wieder niedrig genug ist, schaltet er in den Cut-through-Modus um. Ebenso kann der Switch temporär in den Fragment-Free-Modus schalten, wenn zuviele Fragmente mit weniger als 64 Byte Länge ankommen. Besitzen Sender und Empfänger unterschiedliche Übertragungsgeschwindigkeiten oder Duplex-Modi bzw. nutzen andere Übertragungsmedien (Glasfaser auf Kupfer), so muss ebenfalls mit Store-and-Forward Technik geswitcht werden.

Heutige nach dem Client-/Server-Prinzip arbeitende Netzwerke unterscheiden zwei Architekturen: das symmetrische und asymmetrische Switching gemäß der Gleichförmigkeit der Anschlussgeschwindigkeit der Ports. Im Falle eines asymmetrischen Switchings, d.h. wenn Sende- und Empfangsports unterschiedliche Geschwindigkeiten aufweisen, kommt das Store-and-Forward-Prinzip zum Einsatz. Bei symmetrischem Switching also der Kopplung gleicher Ethernetgeschwindigkeiten wird nach dem Cut-Through-Konzept verfahren.

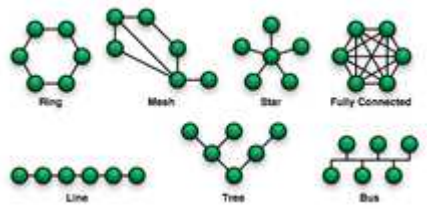
Port-Switching, Segment-Switching

In den Anfangszeiten der Switching-Technologie gab es die zwei Varianten *Port-* und *Segment-Switching*. Diese Differenzierung spielt in modernen Netzwerke nur noch eine untergeordnete Rolle, da an den Ports der Switche heutzutage üblicherweise nur ein Endgerät angeschlossen wird.

- Ein **Port-Switch** verfügt pro Port über nur einen SAT-Eintrag für eine MAC-Adresse. An solch einem Anschluss dürfen folglich nur Endgeräte (Server, Router, Workstation) und keine weiteren Segmente, also keine Bridges, Hubs oder Switches (hinter denen sich mehrere MAC-Adressen befinden) angeschlossen werden. Siehe MAC-Flooding. Zusätzlich gab es oft einen Uplink-Port, für den diese Einschränkung nicht galt. Dieser Port hatte oft keine SAT, sondern wurde einfach für alle MAC-Adressen benutzt, die nicht einem anderen lokalen Port zugeordnet waren. Solche Switches arbeiteten in der Regel nach dem Cut-Through-Verfahren. Trotz dieser scheinbar nachteiligen Einschränkungen existierten auch Vorteile: Die Switches kamen mit extrem wenig Speicher aus (geringere Kosten) und auf Grund der Minimalgröße der SAT konnte auch die *Switching-Entscheidung* sehr schnell getroffen werden.
- Alle neueren Switche sind **Segment-Switche** und können an jedem Port zahlreiche MAC-Adressen verwalten, d. h. weitere Netz-Segmente anschließen. Hierbei gibt es zwei unterschiedliche SAT-Anordnungen: Entweder jeder Port hat eine eigene Tabelle von beispielsweise max. 250 Adressen, oder es gibt eine gemeinsame SAT für alle Ports – mit beispielsweise maximal 2000 Einträgen. Vorsicht: Manche Hersteller geben 2000 Adresseinträge an, meinen aber 8 Ports mit jeweils maximal 250 Einträgen pro Port.

Mehrere Switch in einem Netzwerk

Bis zur Einführung von Gigabit-Ethernet (1000BaseTX) erfolgte die Verbindung mehrerer Switche entweder über einen speziellen Uplinkport oder über ein gekreuztes Kabel (crossover cable), neuere Switche wie auch alle Gigabit-Ethernet Switche beherrschen Auto-MDI(X), sodass diese auch ohne spezielle Kabel miteinander gekoppelt werden können. Oft, aber nicht notwendigerweise, sind Uplink-Ports in einer schnelleren oder höherwertigen (Ethernet-) Technologie realisiert als die anderen Ports (z. B. Gigabit-Ethernet statt Fast Ethernet oder Glasfaserkabel anstatt Twistedpair-Kupferkabel). Im Unterschied zu Hubs können nahezu beliebig viele Switche miteinander verbunden werden. Die Obergrenze hat hier nichts mit einer maximalen Kabellänge zu tun, sondern hängt von der Größe der Adresstabelle (SAT) ab. Bei aktuellen Geräten der Einstiegsklasse sind oft 500 Einträge (oder mehr) möglich, das begrenzt die maximale Anzahl von Knoten (~Rechnern) auf ebendiese 500. Kommen mehrere Switche zum Einsatz, so begrenzt das Gerät mit der kleinsten SAT die maximale Knotenanzahl. Hochwertige Geräte können leicht mit mehreren tausend Adressen umgehen. Wird die maximale Zahl überschritten, so passiert das gleiche wie beim MAC-Flooding, folglich bricht die Performance drastisch ein.



Topologien

Zur Steigerung der Ausfallsicherheit können Verbindungen redundant aufgebaut werden. Dabei werden der doppelte Transport von Paketen und Switching-Schleifen durch die vorherige Ausführung des Spanning Tree Protocol (STP) verhindert. Eine andere Möglichkeit, ein Netz mit Schleifen redundant zu machen und gleichzeitig die Leistung zu steigern, ist das Meshing. Hier dürfen beliebige Schleifen zwischen meshingfähigen Geräten gebildet werden; zur

Leistungssteigerung können dann für Unicast-Datenverkehr (ähnlich wie beim Trunking) alle Schleifen (auch Teilschleifen) weiter genutzt werden (es wird kein Spannbaum gebildet). Multicast und Broadcast müssen vom Meshing-Switch gesondert behandelt werden und dürfen nur auf einer der zur Verfügung stehenden vermaschten Verbindungen weitergeschickt werden. Ethernet-Switche, die Meshing unterstützen, kommen unter anderem von Avaya/Nortel oder HP.

Eine bessere Nutzung von doppelt ausgeführten Verbindungen ist die Port-Bündelung (engl.: trunking, bonding, etherchannel – je nach Hersteller), wodurch bis zu acht [2009] gleichartige Verbindungen parallel geschaltet werden können, um die Geschwindigkeit zu steigern. Diese Technologie beherrschen professionelle Switches, die auf diese Weise untereinander, von Switch zu Switch, oder aber von Switch zu Server verbunden werden können. Der Standard ist mittlerweile verabschiedet IEEE 802.1AX-2008, nur ist [2009] nach wie vor das Zusammenschalten von Switches verschiedener Hersteller problematisch.

Stacking ist im Switching-Umfeld eine Technik, mit der aus mehreren unabhängigen, stacking-fähigen Switchen ein gemeinsamer logischer Switch mit höherer Portanzahl und gemeinsamem Management konfiguriert wird. Stacking-fähige Switche verfügen über besondere Ports, die sogenannten Stacking-Ports, welche üblicherweise mit besonders hoher Übertragungsrate und geringer Latenzzeit arbeiten. Beim Stacking werden die Switche, die in der Regel vom gleichen Hersteller und aus der gleichen Modellreihe stammen müssen, mit einem speziellen Stack-Kabel miteinander verbunden. Eine Stacking-Verbindung ist normalerweise die schnellste Verbindung zwischen mehreren Switchen und überträgt neben Daten auch Managementinformationen. Solche Schnittstellen können durchaus teurer sein als Standard-HighSpeed-Ports, die natürlich ebenfalls als Uplinks genutzt werden können; Uplinks sind immer möglich, aber: nicht alle Switche unterstützen das Stacking.

Architekturen

Den Kern eines Switches bildet die Switching-Fabric, durch die die Pakete vom Eingangs- zum Ausgangsport transferiert werden. Die Switching Fabric ist vollständig in Hardware implementiert, um geringe Latenzzeiten und hohen Durchsatz zu gewährleisten. Zusätzlich zur reinen Verarbeitungsaufgabe, sammelt sie statistische Daten, wie transferierte Paketzahl, Durchsatz oder Fehler. Die Vermittlungstätigkeit lässt sich auf drei Arten durchführen:

- Shared Memory Switching: Dieses Konzept lehnt sich an die Vorstellung an, dass Rechner und Switch in ähnlicher Weise arbeiten. Sie erhalten Daten über Eingangsschnittstellen, bearbeiten diese und geben sie über Ausgangsports weiter. Analog dazu signalisiert ein empfangenes Paket dem Switchprozessor über einen Interrupt seine Ankunft. Der Prozessor extrahiert die Zieladresse, sucht den entsprechenden Ausgangsport und kopiert das Paket in den Puffer. Als Folge ergibt sich eine Geschwindigkeitsabschätzung aus der Überlegung, dass wenn N Pakete/s in den und aus dem Speicher ein- und ausgelesen werden können, die Vermittlungsrate N/2 Pakete/s nicht übersteigen kann.
- Bus Switching: Bei diesem Ansatz überträgt der Empfangsport ein Paket ohne Eingriff des Prozessors über einen gemeinsamen Bus an den Ausgangsport. Den Engpass bildet der Bus, über den jeweils nur ein Paket zur Zeit transferiert werden kann. Ein Paket, das am Eingangsport eintrifft und den Bus besetzt vorfindet, wird daher in die Warteschlange des Eingangsports gestellt. Da jedes Paket den Bus separat durchqueren muss, ist die Switchinggeschwindigkeit auf den Busdurchsatz beschränkt.
- Matrix Switching: Das Matrixprinzip ist eine Möglichkeit die Durchsatzbegrenzung des gemeinsam genutzten Busses aufzuheben. Ein Switch dieses Typs besteht aus einem Schaltnetzwerk, das N Eingangs- mit N Ausgangsports über 2N Leitungen verbindet. Ein Paket, das an einem Eingangsport eintrifft, wird auf den horizontalen Bus übertragen bis es sich mit dem vertikalen Bus schneidet, der zum gewünschten Ausgangsport führt. Ist diese Leitung durch die Übertragung eines anderen Paketes blockiert, muss das Paket in die Warteschlange des Eingangsports gestellt werden.

Vorteile

Switche haben folgende Vorteile:

- Wenn zwei Netzteilnehmer gleichzeitig senden, gibt es keine Datenkollision (vgl. CSMA/CD), da der Switch intern über die Backplane beide Sendungen gleichzeitig übermitteln kann. Sollten an einem Port die Daten schneller ankommen, als sie über das Netz weitergesendet werden können, werden die Daten gepuffert. Wenn möglich, wird Flow Control benutzt, um den/die Sender zu einem langsameren Verschicken der Daten aufzufordern. Hat man 8 Rechner über einen 8-Port-Switch verbunden, und jeweils zwei senden untereinander mit voller Geschwindigkeit Daten, sodass vier Full-Duplex-Verbindungen zustande kommen, so hat man rechnerisch die 8-fache Geschwindigkeit eines entsprechenden Hubs, bei dem sich alle Geräte die maximale Bandbreite teilen. Nämlich 4 × 200 Mbit/s im Gegensatz zu 100 Mbit/s. Zwei Aspekte sprechen jedoch gegen diese Rechnung: Zum einen sind die internen Prozessoren besonders im Low-Cost-Segment nicht immer darauf ausgelegt, alle Ports mit voller Geschwindigkeit zu bedienen, zum anderen wird auch ein Hub mit mehreren Rechnern nie 100 Mbit/s erreichen, da umso mehr Kollisionen entstehen, je mehr das Netz ausgelastet ist, was die nutzbare Bandbreite wiederum drosselt. Je nach Hersteller und Modell liegen die tatsächlich erzielbaren Durchsatzraten mehr oder minder deutlich unter den theoretisch erzielbaren 100 %, bei preiswerten Low-Cost Geräten sind Datenraten zwischen 60 % und 90 % durchaus üblich.
- Der Switch zeichnet in einer Tabelle auf, welche Station über welchen Port erreicht werden kann. Hierzu werden im laufenden Betrieb die Absender-MAC-Adressen der durchgeleiteten Pakete gespeichert. So werden Daten nur an den Port weitergeleitet, an dem sich tatsächlich der Empfänger befindet. Pakete mit unbekannter Ziel-MAC-Adresse werden wie Broadcasts behandelt und an alle Ports mit Ausnahme des Quellports weitergeleitet.
- Der Voll-Duplex-Modus kann benutzt werden, so dass an einem Port gleichzeitig Daten gesendet und empfangen werden können, wodurch die Übertragungsrate verdoppelt wird. Da in diesem Fall auch Kollisionen nicht mehr möglich sind, wird die Übertragungsrate nochmals erhöht.
- An jedem Port kann unabhängig die Geschwindigkeit und der Duplex-Modus ausgehandelt werden.
- Zwei oder mehr physikalische Ports können zu einem logischen Port (HP: Bündelung, Cisco: Etherchannel) zusammengefasst werden, um die Bandbreite zu steigern; dies kann über statische oder dynamische Verfahren, z. B. LACP oder PAgP, erfolgen.
- Ein physikalischer Switch kann durch VLANs in mehrere logische Switche unterteilt werden. VLANs können über mehrere Switche hinweg aufgespannt werden (IEEE 802.1q).

Nachteile

- Ein Nachteil von Switchen ist, dass sich die Fehlersuche in einem solchen Netz unter Umständen schwieriger gestaltet. Pakete sind nicht mehr auf allen Strängen im Netz sichtbar, sondern im Idealfall nur auf denjenigen, die tatsächlich zum Ziel führen. Um dem Administrator trotzdem die Beobachtung von Netzwerkverkehr zu ermöglichen, beherrschen manche Switche *Port-Mirroring*. Der Administrator teilt dem (verwaltbaren) Switch mit, welche Ports er beobachten möchte. Der Switch schickt dann Kopien von Paketen der beobachteten Ports an einen dafür ausgewählten Port, wo sie z.B. von einem Sniffer aufgezeichnet werden können. Um das Port-Mirroring zu standardisieren, wurde das SMON-Protokoll entwickelt, das in RFC 2613 beschrieben ist.
- Ein weiterer Nachteil liegt in der Latenzzeit, die bei Switchen höher ist (100BaseTX: 8–20 µs) als bei Hubs (100BaseTX: < 0,7 µs). Da es beim CSMA-Verfahren sowieso keine

garantierten Zugriffszeiten gibt und es sich um Unterschiede im Millionstelsekundenbereich handelt (µs, nicht ms), hat dies in der Praxis kaum Bedeutung. Wo bei einem Hub ein einkommendes Signal einfach an alle Netzteilnehmer weitergeleitet wird, muss der Switch erst anhand seiner MAC-Adresstabelle den richtigen Ausgangsport finden; dies spart zwar Bandbreite, kostet aber Zeit. Dennoch ist in der Praxis der Switch im Vorteil, da die absoluten Latenzzeiten in einem ungeswitchten Netz aufgrund der unvermeidbaren Kollisionen eines bereits gering ausgelasteten Netzes die Latenzzeit eines vollduplexfähigen (fast kollisionslosen) Switches leicht übersteigen. (Die höchste Geschwindigkeit erzielt man weder mit Hubs noch mit Switchen, sondern indem man gekreuzte Kabel einsetzt, um zwei Netzwerk-Endgeräte direkt miteinander zu verbinden. Dieses Verfahren beschränkt jedoch, bei Rechnern mit je einer Netzwerkkarte, die Anzahl der Netzwerkteilnehmer auf 2.)
- Switche sind Sternverteiler mit einer sternförmigen Netzwerktopologie und bringen bei Ethernet (ohne Portbündelung, STP oder Meshing) keine Redundanzen mit. Fällt ein Switch aus, ist die Kommunikation zwischen allen Teilnehmern im (Sub-) Netz unterbrochen. Der Switch ist dann der Single Point of Failure. Abhilfe schafft die Portbündelung (FailOver), bei der jeder Rechner über mindestens zwei LAN-Karten verfügt und an zwei Switche angeschlossen ist. Zur Portbündelung mit FailOver benötigt man allerdings LAN-Karten und Switche mit entsprechender Software (Firmware).

Sicherheit

Beim klassischen Ethernet mit Thin- oder Thickwire genau so wie bei Netzen, die Hubs verwenden, war das Abhören des gesamten Netzwerkverkehrs noch vergleichsweise einfach. Switche galten zunächst als wesentlich sicherer. Es gibt jedoch Methoden, um auch in geswitchten Netzen den Datenverkehr anderer Leute mitzuschneiden, ohne dass der Switch kooperiert:

- MAC-Flooding – Der Speicherplatz, in dem sich der Switch die am jeweiligen Port hängenden MAC-Adressen merkt, ist begrenzt. Dies macht man sich beim MAC-Flooding zu Nutze, indem man den Switch mit gefälschten MAC-Adressen überlädt, bis dessen Speicher voll ist. In diesem Fall schaltet der Switch in einen *Failopen-Modus*, wobei er sich wieder wie ein Hub verhält und alle Pakete an alle Ports weiterleitet. Verschiedene Hersteller haben – wieder fast ausschließlich bei Switchen der mittleren bis hohen Preisklasse – Schutzmaßnahmen gegen MAC-Flooding implementiert. Als weitere Sicherheitsmaßnahme kann bei den meisten managed Switchen für einen Port eine Liste mit zugelassenen Absender-MAC-Adressen angelegt werden. Protokolldateneinheiten (hier: Frames) mit nicht zugelassener Absender-MAC-Adresse werden nicht weitergeleitet und können das Abschalten des betreffenden Ports bewirken (Port Security).
- MAC-Spoofing – Hier sendet der Angreifer Pakete mit einer fremden MAC-Adresse als Absender. Dadurch wird deren Eintrag in der Source-Address-Table überschrieben, und der Switch sendet im Folgenden allen Datenverkehr zu dieser MAC an den Switchport des Angreifers. Abhilfe wie im obigen Fall durch feste Zuordnung der MACs zu den Switchports.
- ARP-Spoofing – Hierbei macht sich der Angreifer eine Schwäche im Design des ARP zu Nutze, welches zur Auflösung von IP-Adressen zu Ethernet-Adressen verwendet wird. Ein Rechner, der ein Paket via Ethernet versenden möchte, muss die Ziel-MAC-Adresse kennen. Diese wird mittels ARP erfragt (ARP-Request Broadcast). Antwortet der Angreifer nun mit seiner eigenen MAC-Adresse zur erfragten IP (nicht seiner eigenen IP, daher die Bezeichnung *Spoofing*) und ist dabei schneller als der eigentliche Inhaber der IP, so wird das Opfer seine Pakete an den Angreifer senden, welcher sie nun lesen und gegebenenfalls an die ursprüngliche Zielstation weiterleiten kann. Hierbei handelt es sich nicht um einen Fehler des Switches. Ein Layer-2-Switch kennt gar keine höheren Protokolle als Ethernet und kann seine Entscheidung zur Weiterleitung nur anhand der MAC-Adressen treffen. Ein Layer-3-Switch muss sich, wenn er autokonfigurierend sein

soll, auf die von ihm mitgelesenen ARP-Nachrichten verlassen und lernt daher auch die gefälschte Adresse, allerdings kann man einen managed Layer-3-Switch so konfigurieren, dass die Zuordnung von Switchport zu IP-Adresse fest und nicht mehr von ARP beeinflussbar ist.

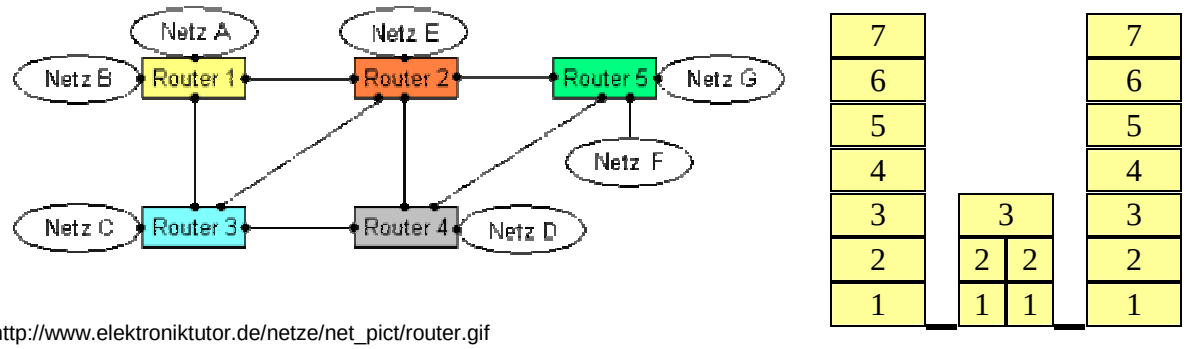
Kenngrößen

- Forwarding Rate (Durchleitrate): gibt an, wie viele Pakete pro Sekunde eingelesen, bearbeitet und weitergeleitet werden können
- Filter Rate (Filterrate): Anzahl der Pakete, die pro Sekunde bearbeitet werden
- Anzahl der verwaltbaren MAC-Adressen (Aufbau und max. Größe der Source-Address-Table)
- Backplanedurchsatz (Switching fabric): Kapazität der Busse (auch Crossbar) innerhalb des Switches
- VLAN-Fähigkeit oder Flusskontrolle.
- Managementoptionen wie Fehlerüberwachung und -signalisierung, Port-basierte VLANs, Tagged-VLANs, VLAN Uplinks, Link Aggregation, Meshing, Spanning Tree Protocol (Spannbaumbildung), Bandbreitenmanagement usw.

Router

Router (['ruːtə(r)] oder ['raʊ̯tə(r)]) sind Netzwerkgeräte, die mehrere Rechnernetze – je nach Sichtweise – koppeln oder trennen. Dabei analysiert der Router die ankommenden Datenpakete nach ihrer Zieladresse und blockt diese oder leitet sie weiter. Geroutete, d. h. weitergeleitete, Pakete gelangen so entweder in ein direkt am Router angeschlossenes Zielnetz (auch Ziel-Subnetz) oder werden zu einem anderen im Netz erreichbaren Router weitergeleitet.

Arbeitsweise



http://www.elektroniktutor.de/netze/net_pict/router.gif

Router arbeiten auf Schicht 3 (Vermittlungsschicht/Network Layer) des OSI-Referenzmodells. Ein Router besitzt mehrere *Schnittstellen* (engl. Interfaces), über die Netze erreichbar sind. Diese Schnittstellen können auch virtuell sein. Beim Eintreffen von Datenpaketen muss ein Router den besten Weg zum Ziel und damit die passende Schnittstelle bestimmen, über welche die Daten weiterzuleiten sind. Dazu bedient er sich einer lokal vorhandenen Routingtabelle, die angibt, über welchen Anschluss des Routers (bzw. welche Zwischenstation) welches Netz erreichbar ist.

Router können Wege auf drei verschiedene Arten lernen und mit diesem Wissen dann die Routingtabelleneinträge erzeugen:

- direkt verbundene Netze: Sie werden automatisch in eine Routingtabelle übernommen, wenn ein Interface mit einer IP-Adresse konfiguriert wird.
- statische Routen: Diese Wege werden durch einen Administrator eingetragen. Sie dienen zum einen der Sicherheit, sind andererseits aber nur verwaltbar, wenn ihre Zahl begrenzt ist, d.h. die Skalierbarkeit ist für diese Methode ein limitierender Faktor.
- dynamische Routen: In diesem Fall lernen Router erreichbare Netze durch ein Routingprotokoll, das Informationen über das Netzwerk und seine Teilnehmer sammelt und an die Mitglieder verteilt.

Die Routingtabelle ist in ihrer Funktion einem Adressbuch vergleichbar, in dem nachgeschlagen wird, ob eine Ziel-IP-Adresse bekannt ist, d. h. ein Weg zu diesem Netz existiert. Da ein Router nicht für alle IP-Adressen hierfür eine Antwort weiß, muss es eine Standardvorgabe geben.

Da Routingtabellen bei den meisten Systemen nach der Genauigkeit sortiert werden, also zuerst spezifische Einträge und später weniger spezifische, kommt die Default-Route, als unspezifische, am Ende und wird für alle Ziele benutzt, die über keinen besser passenden, spezifischeren Eintrag in der Routingtabelle verfügen.

Einige Router beherrschen auch ein sogenanntes *Policy Based Routing*; dabei wird die Routingentscheidung nicht nur auf Basis der Zieladresse (Layer-3) getroffen, sondern es werden zusätzlich andere Angaben berücksichtigt, beispielsweise die Quelladresse, Qualitätsanforderungen oder Parameter aus höheren Schichten wie TCP oder UDP. So können dann zum Beispiel Pakete, die HTTP (Web) transportieren, einen anderen Weg nehmen als Pakete mit SMTP-Inhalten (Mail).

Router können nur für Routing geeignete Datenpakete, also von routingfähigen Protokollen, wie z. B. IP (IPv4 oder IPv6) oder IPX/SPX, verarbeiten. Andere Protokolle, wie z. B. das ursprünglich von MS-DOS und MS-Windows benutzte NetBIOS bzw. NetBEUI, die nur für kleine Netze gedacht waren und von ihrem Design her nicht routingfähig sind, werden von einem Router nicht weitergeleitet. Pakete aus diesen Protokollfamilien werden in aller Regel durch Systeme, die auf Schicht 2 arbeiten, also Bridges oder Switches, verarbeitet. Viele professionelle Router können bei Bedarf auch diese Bridge-Funktionen wahrnehmen und werden dann Layer-3-Switch genannt. Als Schicht-3-System enden am Router alle Schicht-2-Funktionen, darunter auch die Broadcastdomäne. Dies ist insbesondere in großen lokalen Netzen wichtig, um das Broadcast-Aufkommen für die einzelnen Stationen gering zu halten. Sollen allerdings Broadcast-basierte Dienste über den Router hinweg funktionieren, dann werden spezielle Router benötigt, die diese Broadcasts empfangen, auswerten und gezielt einem anderen System zur Verarbeitung zuführen können.

Außerdem sind Ein- und Mehrprotokoll-Router (auch Multiprotokoll-Router) zu unterscheiden. Einprotokoll-Router sind nur für ein Netzwerkprotokoll z. B. IPv4 geeignet und können daher nur in homogenen Umgebungen eingesetzt werden. Multiprotokoll-Router beherrschen den gleichzeitigen Umgang mit mehreren Protokollfamilien wie DECnet, IPX/SPX, SNA, IP und anderen. Heute dominieren IP-Router das Feld, da praktisch alle anderen Netzwerkprotokolle nur noch eine untergeordnete Bedeutung haben, und, falls sie doch zum Einsatz kommen, oft auch gekapselt werden können (NetBIOS over TCP/IP, IP-encapsulated IPX). Früher hatten Mehrprotokoll-Router in größeren Umgebungen eine wesentliche Bedeutung, damals verwendeten viele Hersteller unterschiedliche Protokollfamilien, daher kam es unbedingt darauf an, dass vom Router mehrere Protokoll-Stacks unterstützt wurden. Multiprotokoll-Router findet man heute fast ausschließlich in Weitverkehrs- oder ATM-Netzen.

Wichtig ist hierbei auch die Unterscheidung zwischen den *gerouteten Protokollen* (z. B. IP oder IPX) und *Routing-Protokollen*. Routing-Protokolle dienen der Verwaltung des Routing-Vorgangs und der Kommunikation zwischen den Routern, die z. B. so ihre Routing-Tabellen austauschen (z. B. BGP, RIP oder OSPF). Geroutete Protokolle hingegen sind die Protokolle die den Datenpaketen, die der Router transportiert, zugrunde liegen (z. B. IP oder IPX).

Typen (Bauformen)

Backbone-Router, Hardware-Router

Die Hochgeschwindigkeitsrouter (auch Carrier-Class-Router) im Internet (oder bei großen Unternehmen) sind heute hochgradig auf das Weiterleiten von Paketen optimierte Geräte, die viele Gigabit Datendurchsatz pro Sekunde in Hardware routen können, d. h. die benötigte Rechenleistung wird zu einem beträchtlichen Teil durch spezielle Netzwerkinterfaces dezentral erbracht, ein zentraler Prozessor (falls überhaupt vorhanden) wird hierdurch nicht oder nur sehr wenig belastet. Die einzelnen Ports oder Interfaces können unabhängig voneinander Daten empfangen und senden. Sie sind entweder über einen internen Hochgeschwindigkeitsbus (Backplane) oder kreuzweise miteinander verbunden (Matrix). In der Regel sind solche Geräte für den Dauerbetrieb ausgelegt (Verfügbarkeit von 99,999 % oder höher) und besitzen redundante Hardware (Netzteile usw.), um Ausfälle zu vermeiden. Auch ist es üblich, alle Teilkomponenten im laufenden Betrieb austauschen oder erweitern zu können (hot plug). In den frühen Tagen der Rechnervernetzung war es dagegen üblich, handelsübliche Workstations als Router zu benutzen, bei denen das Routing per Software implementiert war.

High-End-Switche

Bei manchen Herstellern (z. B. bei Hewlett-Packard) findet man die Hochgeschwindigkeitsrouter (auch Carrier-Class-Router, Backbone-Router oder Hardware-Router) nicht unter einer eigenen Rubrik *Router*. Router werden dort gemeinsam mit den High-End-Switchen (Layer-3-Switch und höher, Enterprise Class) vermarktet. Das ist insoweit logisch, als Switche aus dem High-End-Bereich heute praktisch auch immer die Routingfunktionalität beherrschen. Technisch sind dies Systeme, die, ebenso wie die als Router bezeichneten Geräte, hochgradig auf das Weiterleiten von Paketen optimiert sind und viele Gigabit Datendurchsatz pro Sekunde bieten. Sie werden per Managementinterface konfiguriert und können wahlweise als Router, Switch und natürlich auch im Mischbetrieb arbeiten. In diesem Bereich verschwimmen die Grenzen zwischen beiden Geräteklassen mehr und mehr – auch finanziell.

Software-Router

Neben Hardware kann man beispielsweise auch UNIX-Workstations, -Server oder auch PCs als Router einsetzen. Alle unixbasierten Systeme beherrschen Routing von Haus aus. PCs kann man mit entsprechenden Programmen zum Router machen (z. B. KA9Q für MS-DOS-Systeme) oder durch eine entsprechende Betriebssystem-Distribution (z. B. auf Linux basierend Smoothwall, IPCop und Fli4l, wobei letzteres ein Ein-Disketten-ISDN/DSL-Router ist, oder auch m0n0wall auf BSD-Basis). Das freie Betriebssystem OpenBSD (eine UNIX-Variante) bietet neben den eingebauten, grundlegenden Routingfunktionen auch mehrere erweiterte Routingdienste, wie unter anderem OpenBGPD und OpenOSPFD, die auch in kommerziellen Produkten zu finden sind. Ähnliche Erweiterungen sind aber auch für die kommerziellen UNIX sowie für Linux verfügbar. Microsoft Windows bietet in allen NT-basierten Workstation- und Server-Varianten (NT, 2000, XP, 2003, Vista, 7) ebenfalls Routing-Dienste. Auch die Serverversion von Apples Mac OS X enthält eine konfigurierbare Router-Funktion.

Als entscheidender Nachteil von Software-Routern auf PC- oder Workstationbases gilt der im Verhältnis zur Leistung hohe Stromverbrauch. Gerade im SoHo-Bereich können die Stromkosten innerhalb eines Jahres höher liegen als der Preis für ein kleines Kompaktgerät. Ein Vorteil dieser Geräteklasse hingegen ist die hohe Flexibilität, daher werden solche Systeme oft gleich als kostengünstiges kombiniertes System mit integrierter Firewall-, Proxy-, und Antivirus-Software betrieben (z. B. mit Endian Firewall, IPCop, Microsoft Internet Security and Acceleration Server, pfSense, uvm.).

DSL-Router, WLAN-Router

Diese Geräte sind Kombinationen aus verschiedenen Komponenten.

So wird die Kombination aus DSL-Modem (xDSL jeglicher Bauart), Switch und Router als *DSL-Router* bezeichnet. Je nach eingebautem Modem unter anderem als ADSL- oder SDSL-Router. Oft sind es aber keine vollständigen Router, da diese Geräte ausschließlich als Internetzugangs-Systeme dienen und nur mit aktiviertem PPPoE (oder PPPoA) sowie NAT-Routing (oder IP-Masquerading) eingesetzt werden können. Manche Hersteller nennen Router mit implementierten PPPoE/PPPoA und NAT/Masquerading auch dann bereits DSL-Router, wenn diese nur über ein externes Modem per DSL mit dem Internet verbinden können.

Die Kombination aus Access Point und Router wird häufig als *WLAN-Router* bezeichnet. Das ist solange korrekt, soweit es einen WAN-Port gibt. Das Routing findet dann zwischen WLAN und WAN (und falls vorhanden auch zwischen LAN und WAN) statt. Fehlt dieser WAN-Port, handelt es sich hier lediglich um Marketing-Begriffe, da reine Access Points auf OSI-Ebene 2 arbeiten und somit Bridges und keine Router sind. Häufig sind auch WLAN-Router keine vollwertigen Router, sie haben oft die gleichen Einschränkungen wie DSL-Router (PPPoE, NAT – siehe oben). Bei IPv6 entfällt bei diesen Geräten in der Regel NAT. Lediglich in der Übergangsphase muss der Router ggf. noch zusätzlich Tunnelprotokolle z. B. 6to4 beherrschen.

Firewall-Funktionalität in DSL-Routern

Fast alle DSL-Router sind heute NAT-fähig, d. h. in der Lage, Netzadressen zu übersetzen. Weil ein Verbindungsaufbau aus dem Internet auf das Netz hinter dem NAT-Router nicht ohne weiteres möglich ist, wird diese Funktionalität von manchen Herstellern bereits als NAT-Firewall bezeichnet, obwohl nicht das Schutzniveau eines Paketfilters erreicht wird.[1] Die Sperre lässt sich durch die Konfiguration eines Port Forwarding umgehen, was z. B. für manche VPN- oder Peer-to-Peer-Verbindungen notwendig ist. Zusätzlich verfügen die meisten DSL-Router für die Privatnutzung auch über einen rudimentären Paketfilter, teilweise auch stateful. Diese Paketfilter kommen auch bei IPv6 zum Einsatz. Wegen des Wegfalls von NAT wird Port Forwarding wieder zu einer einfachen Freigabe des Ports. Als Betriebssystem kommt auf vielen Routern dieser Klasse Linux und als Firewall meist iptables zum Einsatz. Einen Content-Filter enthalten solche Produkte zumeist nicht.

Software- oder Hardware-Router

Generell leisten heute Software-Router wertvolle und umfangreiche Dienste – allerdings überwiegend im nicht professionellen Umfeld. Allgemein gibt es für Software-Router zwei unterschiedliche Implementierungsarten, zum Einen dedizierte Router, hierbei wird ein PC, eine Workstation oder ein Server so gut wie ausschließlich als Router eingesetzt (häufig auch noch als DHCP-, DNS-Server oder Firewall); zum Anderen nicht dedizierte Router, hier übernimmt ein Server zu seinen bestehenden Aufgaben zusätzlich noch das Routing. Beide Systeme sind für den performance-unkritischen Bereich gut geeignet und können mit professionellen Lösungen, vor allem was die Kosten angeht, konkurrieren, in der Leistungsfähigkeit sind sie aber meist unterlegen.

Das liegt unter anderem daran, dass solche Systeme bislang häufig noch auf einem klassischen PCI-Bus mit 32-Bit Busbreite und 33-MHz-Taktung (PCI/32/33) beruhten. Über einen solchen Bus lassen sich theoretisch ca. 1 GBit/s (1000 MBit/s, entspricht etwa 133 MByte/s) im Halb-Duplex-Modus (HDX) leiten; da die Netzwerkpakete den PCI-Bus allerdings in diesem Fall zweimal passieren, (Karte–PCI–Arbeitsspeicher–CPU–Arbeitsspeicher–PCI–Karte) reduziert sich der max. routbare Datenstrom eines hierauf basierenden Software-Routers auf etwa 0,5 GBit/s. Ethernet wird heute fast immer geswitcht und im Voll-Duplex-Modus FDX betrieben, damit kann beispielsweise Gigabit-Ethernet, obwohl es Namen wie *1 GBit/s Ethernet*, *1GbE* oder *1000Base-TX* anders vermuten lassen, bereits 2 GBit/s (je 1GbE in jede Richtung)

übertragen. Hieraus folgt, dass ein System auf PCI/32/33-Basis die netzwerkseitig theoretisch mögliche maximale Übertragungsrate von 2 GBit/s keinesfalls erreichen kann. Systeme mit einem PCI/64/66-Bus können busseitig etwa 4 GBit/s leisten, gerade ausreichend die Spitzenlast zweier 1GbE-Schnittstellen im FDX-Modus. Noch höherwertige klassische (legacy) Server-Systeme verfügen über noch schnellere Schnittstellen (PCI-X 266 oder besser), sowie über mehrere unabhängige PCI-Busse und können daher auch ohne Probleme höhere Durchsatzraten erzielen - wobei man sich hier auf Grund des typischerweise hohen Energieverbrauchs solcher Server, besonders im dedizierten Routerbetrieb, die Kosten-Nutzen-Frage stellen muss - Hardware-Router mit spezialisierten CPUs und anwendungsspezifisch arbeitenden Chipsätzen (Anwendungsspezifische Integrierte Schaltung kurz ASIC) schaffen das weitaus energieeffizienter.

Erst durch die Einführung von PCI-Express (mit 2 GBit/s bei Version 1.x und 4 GBit/s pro Lane bei Version 2.x im FDX-Modus - und mehr), steht auch bei Standard-PCs eine ausreichende Peripherie-Transferleistung für mehrere 1GbE-Verbindungen (auch 10GbE) zur Verfügung, sodass sich energieeffiziente, durchsatzstarke Software-Router so auch aus preiswerter Standardhardware bauen lassen. Da bislang aber alle Werte theoretischer Art sind und in der Praxis nicht nur Daten durch den Bus geleitet werden, sondern auch Routing-Entscheidungen getroffen werden müssen, wird ein Software-Router möglicherweise weiter an Leistung einbüßen. Vorsichtigerweise sollte man in der Praxis nur von der Hälfte des theoretisch möglichen Datendurchsatzes ausgehen. Wer mit solchen Datenraten leben kann, ist mit einem Software-Router, zumindest was die Kosten und die Leistung angeht, gut bedient.

Hardware-Router aus dem High-End Bereich sind, da sie über spezielle Hochleistungsbusse oder „cross bars“ verfügen können, in der Leistung deutlich überlegen – was sich allerdings auch im Preis widerspiegelt. Zusätzlich sind diese Systeme für den ausfallsicheren Dauerbetrieb ausgelegt (Verfügbarkeit von 99,999 % und höher). Einfache PCs können da nicht mithalten, hochwertige Server und Workstations verfügen aber ebenfalls über redundante Komponenten und eine für viele Anwendungsfälle ausreichend hohe Ausfallsicherheit.

Übrigens bestehen manche so genannte Hardware-Router tatsächlich aus PC-Komponenten. Lediglich das Gehäuse oder die zum Teil mechanisch veränderten PCI-Steckplätze und das „kryptische“ Betriebssystem erwecken den Anschein, es seien Spezialsysteme. Zwar arbeiten auch diese Systeme meist sehr robust und zuverlässig, dennoch wird auch hier das Routing per Software durchgeführt.

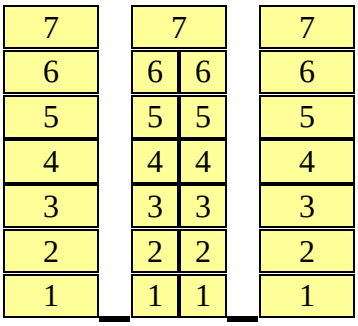
Routing-Cluster

Um z. B. 1GbE- oder 10GbE-Netze performant routen zu können, benötigt man nicht unbedingt einen hochpreisigen Hardware-Router. Wer geringe Einbußen bei der Übertragungs-Geschwindigkeit in Kauf nimmt, kann hierfür auch einen *Routing-Cluster* einsetzen. Dieser kann aus je einem Software-Router (z. B. Workstation mit zwei 10GbE-LAN-Karten PCI-Express) pro Ethernet-Strang aufgebaut sein. Die Software-Router werden über einen professionellen Switch mit genügend vielen Ports und entsprechend hoher Durchsatzrate (einige Hundert GBit/s) miteinander verbunden. Im Unterschied zu Netzen mit zentralem Backbone entspricht die maximale Datendurchsatzrate des gesamten *Routing-Clusters* der maximalen Durchsatzrate des zentralen Switches (einige Hundert GBit/s). Optional können die Cluster auch redundant (z. B. per High-Availability-Unix oder HA-Linux) ausgelegt sein. Solche Cluster-Systeme benötigen zwar relativ viel Platz und erreichen nicht die Leistung und Zuverlässigkeit von Hochgeschwindigkeitsroutern, dafür sind sie aber höchst modular, gut skalierbar, vergleichsweise performant und dennoch kostengünstig; daher findet man sie dort, wo Kosten höher als Performance bewertet werden, beispielsweise in Schulen oder Universitäten.

Gateway

Ein **Gateway** [□geɪtweɪ] (englisch *gateway*, deutsch auch *Protokollumsetzer*) erlaubt es Netzwerken, die auf völlig unterschiedlichen Protokollen basieren, miteinander zu kommunizieren. Als Beispiel könnte ein Gateway das IP-Protokoll nach IPX konvertieren, sobald die Pakete durch das Netz hindurch auf ihrem Weg zum Ziel das Gatewaygerät passieren, um eine Kommunikation zwischen derartigen Netzen zu realisieren. Wobei auch eine dienstbasierte Umsetzung der Protokolle möglich ist, wie beispielsweise E-Mail zu SMS oder E-Mail zu Fax.

Arbeitsweise



Ein Gateway im OSI-Schichtenmodell
zwischen zwei kommunizierenden Geräten.

Zu diesem Zweck nimmt ein Gateway eine Protokollumsetzung vor. Dem Gateway ist dabei alles erlaubt, was zur Konvertierung der Daten notwendig ist, auch das Weglassen von Informationen, wenn diese im Zielnetz nicht transportiert werden können. Im Detail werden sämtliche Protokollinformationen, die an ein Datenpaket angehängt werden (zum Beispiel IPX/SPX), entfernt und durch andere (zum Beispiel aus der Internetprotokollfamilie) ersetzt. Daneben gibt es auch Gateways für zahlreiche andere Verwendungszwecke, etwa SMS-Gateways (E-Mail u. a. zu Short Message Service), Fax zu E-Mail, E-Mail zu Sprache etc.

Abgrenzung zum Standardgateway als Router (default Gateway)

In der Anfangszeit von IP war man nicht selten gezwungen, Netzwerke unterschiedlichen Typs miteinander zu verbinden und damit zwangsläufig deren Protokolle zu konvertieren. Denn IP wurde mit Protokollen wie DECnet, SNA und Novells IPX/SPX konfrontiert. Der Begriff **default Gateway** aus der IP-Netzwerkkonfiguration sollte dem Administrator verdeutlichen, dass er hier ein Gateway eintragen kann. Doch was dort tatsächlich eingesetzt wird, hängt von der jeweiligen Netzwerkarchitektur ab.

Mit der Vorherrschaft des IP-Protokolls zog der Router immer öfter an die Stelle des Gateways. Mittlerweile gibt es in diesem Segment kaum noch Gateways, da die Netze fast ausschließlich über das IP-Protokoll kommunizieren. Eine Protokollumsetzung ist also nicht mehr erforderlich.

Statt Protokolle zu konvertieren, leitet das *default Gateway* einer IP-Konfiguration heute also lediglich alle nicht zu einem Subnetz gehörenden Netzwerkanfragen in ein anderes Subnetz weiter und erfüllt damit schlicht die Funktionen eines Routers, weshalb die Bezeichnung „default Router“ heutzutage treffender wäre. Gateways werden daher im allgemeinen Sprachgebrauch oftmals mit Routern gleichgesetzt, obwohl Router keine Gateways sind.

Router arbeiten auf der dritten Schicht (Vermittlungsschicht) des OSI-Referenzmodells, ein Gateway kann dagegen auf den Schichten vier bis sieben implementiert werden.

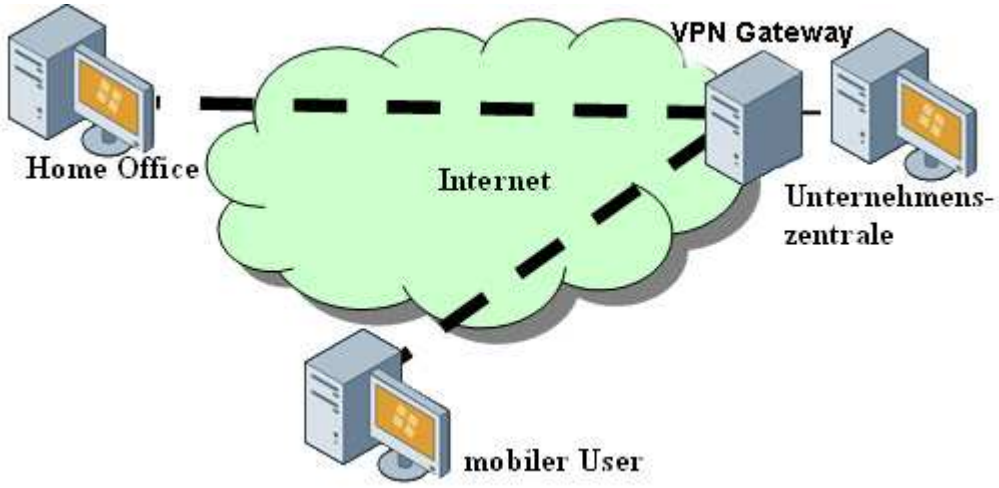
Internet-Gateway

Teilweise wird im Heimbereich ein Kombigerät aus DSL-Router und DSL-Modem als Internet-Gateway bezeichnet. Diese Geräte vereinen, vereinfacht ausgedrückt, die Funktion, Netzwerke miteinander zu verbinden (Routing), mit der Fähigkeit, hierfür unterschiedliche Protokolle zu benutzen (Gateway). So werden IP-Pakete aus dem Heimnetzwerk bei DSL-Verwendung zumeist über das PPPoE-Protokoll in das Netz des Providers übersandt.

Die Protokollbenennung eines Standardgateways ist dabei auf der Implementierungsebene als mehrschichtig zu bezeichnen, weil im Gegensatz zum einfachen Router die Fähigkeit einer eigenständigen, temporär von einem Hauptsystem unabhängigen Inbetriebnahme besteht. Dies bezieht sich nicht nur auf WAN-Aktivitäten, sondern auch auf alle Prozesse, welche auf Betriebssystemen heute möglich sind.

Andererseits kann das Internet-Gateway eine andere Bezeichnung für das Herstellen einer VPN-Verbindung über einen gesicherten Tunnel sein.

VPN-Gateway



http://www.virenschutz.info/images/tutorialbilder/vpn/vpn-gateway-big.jpg

Ein VPN-Gateway ermöglicht über ein öffentliches Netz, wie das Internet, beispielsweise den sicheren Zugriff auf ein entferntes Firmennetzwerk, das normalerweise nicht öffentlich zugänglich ist. Somit können verschiedene Dienste, wie z. B. E-Mail, Intranet oder Laufwerksfreigaben, die eigentlich nur LAN-intern zur Verfügung stehen, über eine getunnelte Verbindung genutzt werden.

http://de.wikipedia.org/wiki/Repeater
http://de.wikipedia.org/wiki/Hub(Netzwerk)
http://de.wikipedia.org/wiki/5-4-3-Regel
http://de.wikipedia.org/wiki/Bridge_(Netzwerk)
http://de.wikipedia.org/wiki/Switch_(Computertechnik)
http://de.wikipedia.org/wiki/Router
http://de.wikipedia.org/wiki/Gateway_(Informatik)