Ein Referat von

Christiane Müller und Danny Gräf
(ITS99)

Aktive Netzwerkkomponenten

Einleitung:	**passiv - aktiv, Typen von Zwischensystemen**
Hub:	**Workgroup, Departmental, Enterprise** **Busarchitektur**
Repeater:	**Lokal, optisch, Buffered, Remote, Multiport**
Bridge:	**Merkmale, Kenndaten, Vorteile**
Spanning Tree	
Switch:	**Unterschied zu Multiport-Bridge** **Cut-Through bzw. On The Fly** **Store-and-Forward**
Router:	**Basiskomponenten** **Beispiel** **Vergleichsziehung zu Bridge** **Hop**
Brouter:	**Definition** **Bewertung Bridge gegenüber Router**

Einleitung

Jedes Netzwerk wird grob in zwei Bereiche, einen passiven und einen aktiven unterteilt. Als passiv wird die Infrastruktur bezeichnet. Diese setzt sich zusammen aus Kabel, Anschlussstecker, Patchfelder usw. Netzwerkkomponenten die eine eigene Logik beinhalten werden als aktive Komponenten bezeichnet. Hierzu zählen z.B. Repeater, Brücken, Router, Hubs oder auch die einzelnen Rechner im Netz.

Eine Eigenschaft jedes Netzwerks besteht darin, das sich immer nur ein Bit gleichzeitig auf dem Netzwerkkabel befinden kann. Solange nur zwei Stationen miteinander Daten austauschen stellt dieser Umstand kein Problem dar.

Im Regelfall allerdings gibt es viele Rechner, die gleichzeitig miteinander kommunizieren möchten. Diese Rechner teilen sich dann die Kapazität des Netzwerks auf. Steigt nun die Zahl der sendenden Rechner rapide an, wird die Datenübertragung immer langsamer. Um diesem Umstand aus dem Weg zu gehen teilt man große Netzwerke in Teilnetze, so genannte Subnets auf.

Stelle man sich ein Netzwerk mit 5000 Computern vor, bei dem immer nur einer Daten auf das Netz senden kann. Wird dieses Netz jetzt in 50 Teilnetze mit je 100 Rechnern unterteilt, so können theoretisch bis zu 100 Rechner (in jedem Teilnetz einer) gleichzeitig ihrer Netzwerkkommunikation nachgehen.

Um Netzwerke in einzelne Subnets zu unterteilen bedient man sich Brücken oder Router.

Typen von Zwischensystemen

- Hubs
- Repeaters
- Bridges
- Routers
- Gateways

Das Unterscheidungskriterium bildet diejenige Schicht des ISO/OSI-Referenzmodells, auf der die Zwischensysteme die Netze koppeln. Die Schichten 1 bis 4 im Referenzmodell befassen sich mit dem Datentransfer zwischen Endsystemen und werden deshalb als transportorientierte Schichten bezeichnet. Die meisten Zwischensysteme koppeln Netze in einer dieser Schichten. Die anwendungsorientierten Schichten 5 bis 7 befassen sich mit Aufgaben, die stärker von den eigentlichen Anwendungen abhängen.

Repeater verbinden Netze in der Bitübertragungsschicht, der Schicht 1. Sie ermöglichen die Adaption zwischen verschiedenen Übertragungsmedien (Kupferkabel und Glasfaser). Weiterhin regenerieren sie empfangene Signale, um insgesamt grössere Distanzen überbrücken zu können.

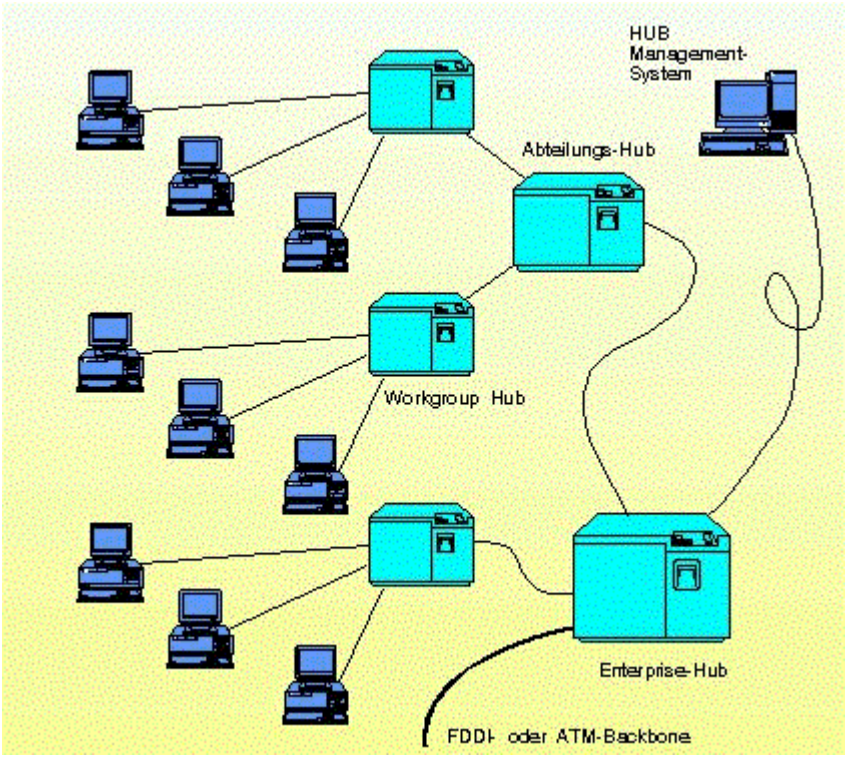
Bridges arbeiten auf der Medienzugangsschicht (MAC-Schicht), einer Teilschicht der Sicherungsschicht. Sie können Netze mit gleichen und unterschiedlichen Medienzugangsverfahren (Ethernet, Token Ring) koppeln. Bridges sind vor allem für den Einsatz in lokalen Netzen vorgesehen. Sie sind in der Lage, den Verkehr zwischen den verschiedenen Teilnetzen durch Filterfunktionen zu separieren und führen so zu einer besseren Lokalisierung des Verkehrs im Netzverbund.

In der Vermittlungsschicht, der Schicht 3, werden **Router** eingesetzt. Sie ermöglichen neben der Separierung des Verkehrs in den einzelnen Teilnetzen auch gegenüber von Bridges verbesserte Sicherheitsvorkehrungen. Router eignen sich darüber hinaus gut zur Kopplung lokaler Netze mit Weitverkehrsnetzen (z.B. Internet).

Als **Gateways** werden Zwischensysteme bezeichnet, die Netze oberhalb der Vermittlungsschicht verbinden. Im allgemeinen geschieht die Kopplung in der Anwendungsschicht, kann aber beispielsweise auch in der Transportschicht erfolgen.

Hub

Ein Hub ist ein hochintelligentes Vermittlungssystem zwischen LAN-Segmenten und Endgeräten. Er bildet den Konzentrationspunkt für eine sternförmige Verkabelung zur Bildung logischer LANs, d.h., der Hub adaptiert unterschiedliche LANs und beliebige Medien. Aus diesem Grund spricht man auch von "Wiring Hubs" oder Kabelkonzentratoren. Man unterscheidet Hubs (Naben) vom Einsatzgebiet her in arbeitsgruppenweite (Workgroup), abteilungsweite (Departmental) und unternehmensweite (Enterprise) Hubs, die sich in Größe und Ausstattung unterscheiden.



Ein **Workgroup-Hub** kann nur einige Dutzend Stationen eines einheitlichen Netztyps versorgen. Man nutzt diese Hubs vorwiegend für den Anschluss von PCs oder anderen Endgeräten an die hierarchisch höhergestellten Abteilungs- oder Unternehmens-Hubs. Beispiele für Workgroup-Hubs wären ein 10Base-T-Hub für Ethernet oder der Ringleitungsverteiler für Token Ring.

Abteilungsweite Hubs werden üblicherweise an die unternehmensweiten Hubs angeschlossen und unterstützten um die 100 anschließbare Stationen, meistens von einer einzigen Netzwerktechnologie. Ein größerer Ethernet-Sternverteiler ist ein Beispiel für einen abteilungsweiten Hub.

Unternehmensweite Hubs sind in modularer Technik aufgebaut und können unterschiedliche LAN-Typen realisieren, also z.B. Token Ring, Ethernet und FDDI miteinander verbinden. Je nach Bestückung der Hub-Module können an einen unternehmensweiten Hub einige hundert Stationen in jedem Netz angeschlossen sein. An Modulen gibt es praktisch eine unbegrenzte Vielzahl; sie bieten die Funktionalitäten von Konzentrator, Brücke, Router oder Management-System und unterstützen dabei das Netzwerkmanagement sowie alle gängigen Übertragungsmedien.

Das Herz des Hub sind die internen Busse, die das sogenannte Backplane bilden. Neben der reinen Anzahl von Slots bestimmt vor allem die Busarchitektur die Leistungsfähigkeit des Hub. Die heutigen Hubs arbeiten praktisch alle mit proprietären Bussen, bei denen die Kapazitätszuordnung (Arbitration) durch das Zugangsverfahren bestimmt wird, das auf dem Bus läuft, also Token, CSMA/CD oder FDDI. Der proprietäre Bus eines Hub transportiert die Signale wie auf einem eigenen Netz. Es gibt vier grundsätzliche Konstruktionen für den Backplane eines unternehmensweiten Hub:

- der **segmentierte proprietäre Bus**:
  ist in bestimmte Bereiche für die Unterstützung von z.B. Ethernet, Token Ring oder FDDI unterteilt. Ein Modul, das auf den segmentierten proprietären Bus gesteckt wird, merkt, ob ein Segment frei ist oder nicht. Wenn das Segment frei ist, kann das Modul versuchen, auf ein anderes Segment auszuweichen oder dem bereits durch die Verbindung anderer Module bestehenden Netz beizutreten. Auf diese Weise können Module für unterschiedliche Netztypen den gleichen Bus benutzen.

- **vielfache proprietäre Busse**:
  unterstützen jeweils einen Netztyp, so dass nur zu diesem Netzwerk passende Module eingesteckt werden können und untereinander kommunizieren.

- **gemultiplexte proprietäre Busse**:
  ein physischer Bus wird in mehrere virtuelle Busse aufgespalten, die dann jeweils zu einem Netztyp gehören. Module müssen sich an dieser Virtualisierung orientieren.

- **Systembusse**:
  Ein Modul hat die Kontrolle über den Bus, adressiert ein anderes Modul und schickt diesem Daten beliebigen Typs zu; unter Umständen kann dann auch die Kontrolle auf ein anderes Modul übergehen.

Unternehmensweite Hubs lassen sich untereinander zu großen Netzen zusammenschalten. Dabei können proprietäre Techniken Anwendung finden oder auch standardisierte Technologien wie FDDI oder ATM.

In bezug auf die maximale Anzahl ist es bei der Auswahl, der Installation und der Konfiguration eines Hub in der Praxis relativ uninteressant und unwichtig, ob es sich dabei um einen "Super-Hub" oder um eine kleine Ausführung handelt. Für sämtliche Konfigurationsmöglichkeiten gilt, dass unbedingt die sogenannte 5-Segmente-Regel eingehalten wird. So muss der Aufbau von Ethernet-LANs mit Hubs (Sternverteilern) stets nach den gleichen Regeln erfolgen. Aus der 5-Segmente-Regel, die in der Literatur auch als 5-4-3-Regel bezeichnet wird, ergibt sich, dass zwischen dem Sender und dem Empfänger maximal fünf Segmente einschließlich Hub-zu-Hub Verbindungen liegen dürfen. Des Weiteren dürfen dabei maximal vier Repeater oder Hubs (Konzentratoren) eingesetzt werden, und zwischen dem Sender und dem Empfänger dürfen maximal drei Segmente mit angeschlossenen Endgeräten liegen.

Repeater

Repeater sind diejenigen Komponenten innerhalb der Netzwerkmaterie, die in der Vergangenheit am schnellsten weiterentwickelt wurden.

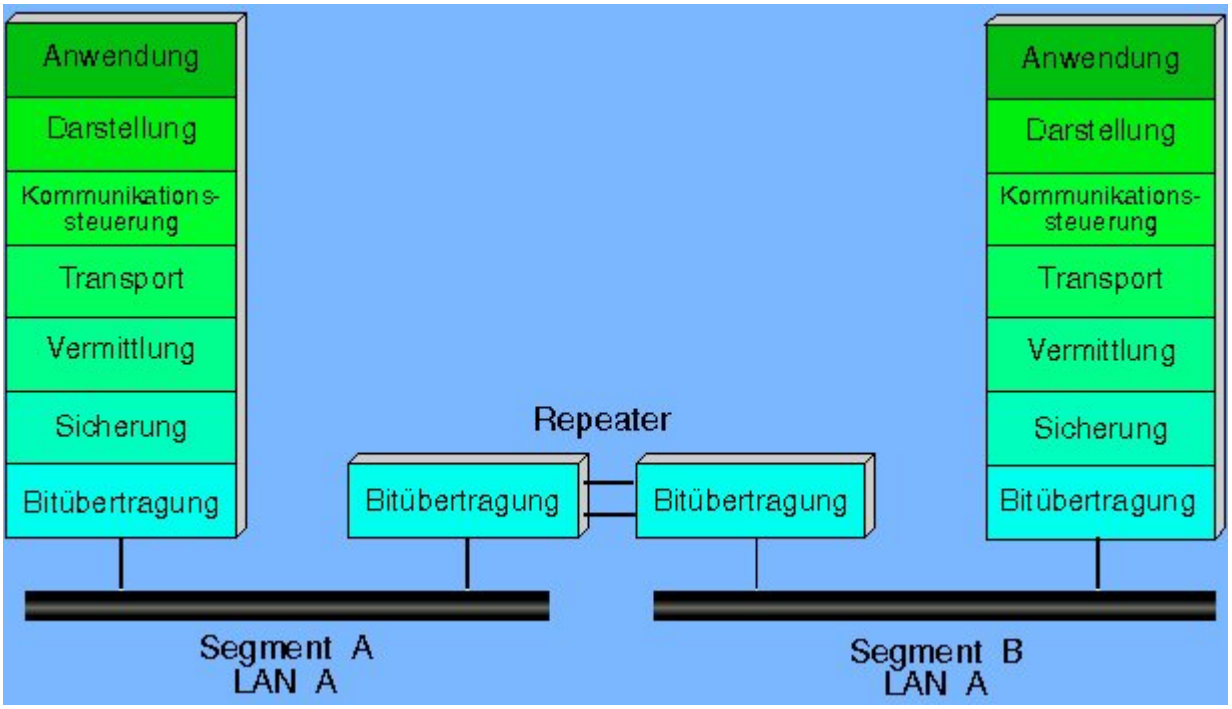
Innerhalb des OSI-Referenzmodells ist die Funktionalität eines Repeaters grundsätzlich auf der ersten Schicht (Physical Layer, Bitübertragungsschicht) anzusiedeln.

Bei einem Repeater (zu denen beispielsweise auch Sternkoppler und Ringleitungsverteiler zählen) handelt es sich - ganz allgemein ausgedrückt - um eine Signalverstärker. Ein Repeater verstärkt das ankommende Signal so, dass es wieder auf den Pegel des Ausgangssignals gesetzt wird, und gibt das Signal dann wieder zurück auf das Übertragungsmedium.

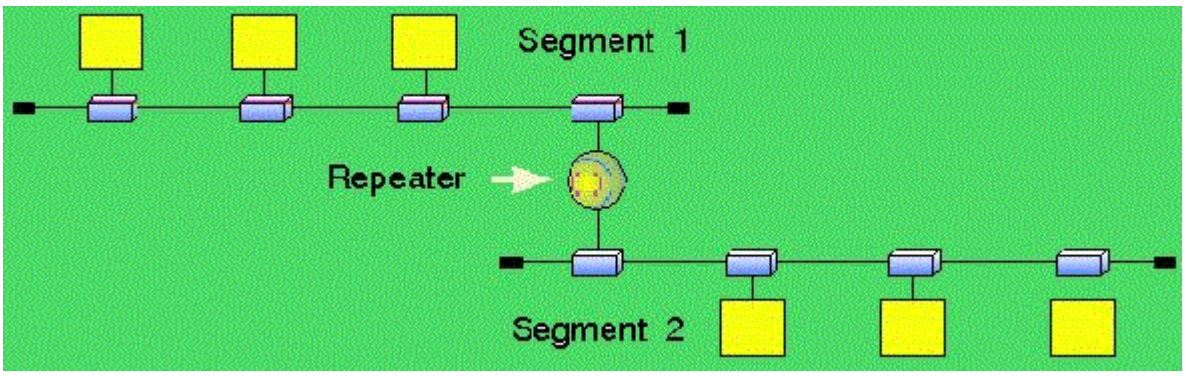
Mit einem Repeater erfolgt die Übertragung der Daten von einem beliebigen Sender zu einem Empfänger, wobei die erwähnte Signalverstärkung zum Einsatz kommt. Auf diese Weise können auch unterschiedliche Netzwerksegmente zu einem einzigen Netzwerk verbunden werden. Repeater stellen in der ursprünglichen Funktionalität grundsätzlich keine Möglichkeit zur Filterung der Daten zur Verfügung. Allerdings gibt es heutzutage auch so genannte "halb-intelligente" Repeater, die teilweise Funktionen einer Brücke übernehmen und so beispielsweise über gewisse Filterfunktionen verfügen.

Heutzutage existiert eine gewisse Diskrepanz in Bezug auf die Bezeichnung und die Funktionalität der Repeater. Während einige Fachleute diese Komponenten als "dumme Geräte" bezeichnen, die in der heutigen strukturierten Verkabelung keine Daseinsberechtigung mehr haben, erweitern wiederum andere Fachleute den Begriff Repeater und dehnen ihn auch auf Sternkoppler und ähnliche Komponenten aus.

Neben den bereits erwähnten Sternkopplern werden dem Bereich der Repeater größtenteils auch Komponenten wie Umsetzer von Koaxial- auf symmetrisches Kupferkabel oder auch von LWL- auf symmetrisches Kupferkabel (Twisted Pair) zugeordnet. Dabei ist jedoch zu beachten, dass es in den Bereichen auch spezielle Komponenten gibt, die als Transceiver bezeichnet werden.



In Lokalen Netzen dient ein Repeater zur Verbindung zweier LAN-Segmente, um die physikalische Topologie über die Ausdehnung eines einzelnen Segmentes hinaus zu erweitern. Local Repeater verbinden zwei Kabelsegmente direkt miteinander.



Bei **lokalen Repeatern** darf die maximale Entfernung zwischen den beiden Kabelsegmenten 100 m betragen, was der doppelten maximalen Länge eines Transceiver-Kabels entspricht. Überschreitet der Abstand zwischen zwei Segmenten eine Entfernung von 100 m, treten **Remote Repeater** anstelle der lokalen Repeater.

Der Repeater regeneriert den Signalverlauf sowie Pegel und Takt. Die meisten Repeater verfügen über eine Selbsttestfunktion und erkennen auch fehlerhafte Signale bzw. Kollisionen auf einem LAN-Segment. Bei einer Kollisionserkennung generiert der Repeater ein Jam-Signal. Fehlerbehaftete Signale werden nicht auf das andere Segment weitergeleitet. Dadurch erreicht man eine gewisse Lokalisierung von Fehlern. Ein Repeater ist völlig protokolltransparent und wird zur Überwindung von Längenrestriktionen einzelner Kabelsegmente eingesetzt, wodurch eine Topologie-Erweiterung des Netzes möglich wird.

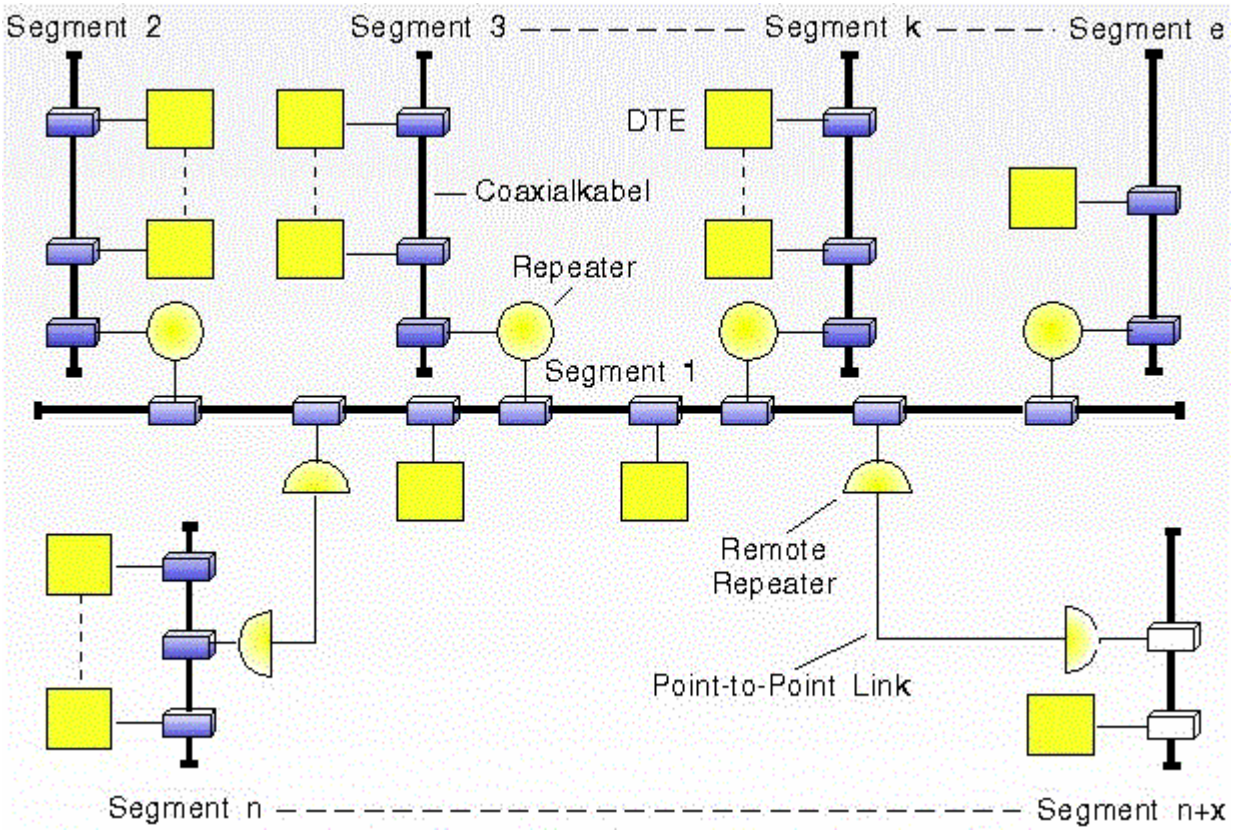
Arbeitet ein Repeater mit Zwischenspeicherung spricht man von einem **Buffered Repeater**. Ein Buffered Repeater arbeitet auf der Sicherungsschicht. Im Gegensatz zu Standard Repeatern beruht das Arbeitsprinzip darauf, dass ein Buffered Repeater nur vollständige Datenpakete empfängt, zwischenspeichert und auf das angeschlossene Netz überträgt. Dieser Vorgang wird auch Store-and-Foreward-Verfahren genannt.

Neben den Repeatern mit Lokal- und Remote-Funktionalität gibt es noch den **Multiport-Repeater**, der sich dadurch auszeichnet, dass er mehrere Ausgänge unterstützt, sowie den optischen Repeater.

Der **optische Repeater** dient dazu, eventuelle Lichtsignaldämpfungen auszugleichen. Obwohl die Reichweite von Lichtwellenleitern, speziell die der Monomodefaser, außerordentlich hoch ist, muss bei sehr langen Strecken das Signal in gewissen Abständen von einem optischen Repeater verstärkt und auch regeneriert werden. Dazu wird das optische Signal verstärkt, die Flankensteilheit der Impulse wiederhergestellt und anschließend wieder in das nächste Glasfaserkabel eingespeist.

In LWL-LANs übernimmt der Repeater die gleichen Funktionen, wobei er das Lichtsignal decodiert, in ein elektrisches Signal umformt und es anschließend über eine LED oder Laserdiode in den Lichtwellenleiter einspeist.

Remote Repeater



Der Remote-Repeater dient dazu, größere Entfernungen (max. 1000m) zwischen den LAN-Segmenten eines Lokalen Netzes zu überbrücken.

Ein Remote-Repeater ist ein Repeater, der aus zwei Teilen besteht (daher auch "Repeater-Paar"), weswegen ein Teil auch als Half-Repeater bezeichnet wird. Beide Teile eines Remote-Repeaters sind über Vollduplex-Leitungen miteinander verbunden und bilden funktional einen Repeater, der koaxiale LAN-Segmente auf der Bitübertragungsschicht verbindet. Diese Verbindung wird auch Link-Segment bezeichnet. Die beiden Half-Repeater erfüllen zusammen mit dem Link-Segment die komplette Repeater-Funktionalität.

Multiport-Repeater

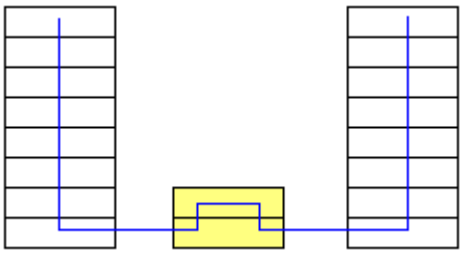
Der Multiport-Repeater bietet die Möglichkeit, mehrere (typischerweise bis zu acht) Cheapernet-Segmente zusammenzuführen und über einen Transceiveranschluß mit dem Standard-Ethernet zu verbinden. Bei zwei oder mehr anzuschließenden Cheapernet-Segmenten ist die Lösung kostengünstiger als der Einsatz von Standard-Repeatern.

In der Praxis wird diese Lösung nicht mehr oft eingesetzt, da man durch Konzentratoren oder Hubs für gleiche Anwendungen eine wesentlich höhere Funktionalität erzielt.

Repeater ermöglichen zwar die Überwindung der Längenbegrenzung, eine Lasttrennung oder gar die Integration von Filterfunktionen, Segmentierung ist jedoch nicht möglich. Für solche Anwendungsfälle müssen spezielle Komponenten wie Brücken oder Router zum Einsatz kommen.

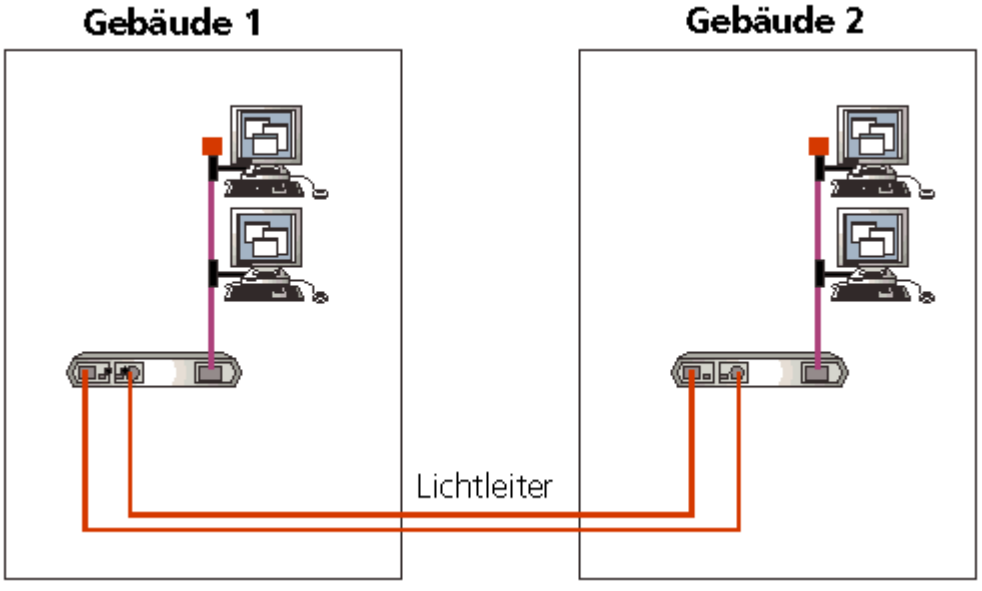
Bridge

Eine Bridge trennt zwei Ethernet-LANs physikalisch, Störungen wie z. B. Kollisionen und fehlerhafte Pakete gelangen nicht über die Bridge hinaus. Die Bridge ist protokolltransparent, d. h. sie überträgt alle auf dem Ethernet laufenden Protokolle. Die beiden beteiligten Netze erscheinen also für eine Station wie ein einziges Netz. Durch den Einsatz einer Bridge können die Längenbeschränkungen des Ethernets überwunden werden. Die Bridge arbeitet mit derselben Übertragungsrate, wie die beteiligten Netze. Die Anzahl der hintereinandergeschalteten Bridges ist auf 7 begrenzt (IEEE 802.1). Normalerweise wird man aber nicht mehr als vier Bridges hintereinanderschalten.



Jede lokale Bridge ist über Transceiver an zwei Ethernet-LANs angeschlossen (Es gibt auch Bridges, die mehrere LANs verbinden können). Die Bridge erstellt für jedes LAN eine Tabelle der Adressen aller Stationen, die Datenpakete aussenden. Ist die Zieladresse eines Paketes in dem LAN, in dem es von der Bridge empfangen wurde, wird es ignoriert. Ist es nicht darin, wird es in das andere LAN gesendet. Es werden somit nur solche Pakete übertragen, die an die jeweils andere Seite adressiert sind. Broadcasts und Multicasts werden immer übertragen. Je nach Typ der Bridge können auch extra Filter gesetzt werden, um etwa den Zugang mancher Stationen zu verhindern oder nur bestimmte Protokolle zuzulassen. Eine Bridge arbeitet auf der Ebene 2 des OSI-Schichtenmodells.

Die Bridge empfängt von beiden Netzsegmenten, mit denen sie wie jede normale Station verbunden ist, alle Blöcke und analysiert die Absender- und Empfängeradressen. Steht die Absenderadresse nicht in der brückeninternen Adresstabelle, so wird sie vermerkt. Die Bridge lernt und speichert so die Information, auf welcher Seite der Bridge der Rechner mit dieser Adresse angeschlossen ist. Ist die Empfängeradresse bekannt und der Empfänger auf derselben Seite wie der Absender, so verwirft die Bridge das Paket (filtert es). Ist der Empfänger auf der anderen Seite oder nicht in der Tabelle, wird das Paket weitergeschickt. Die intelligente Bridge lernt so selbständig, welche Pakete weitergeschickt werden müssen und welche nicht. Bei managebaren Bridges können zusätzliche Adress-Filter gesetzt werden, die regeln an welche Adressen die Bridge Informationen immer weiterschicken muss oder nie weiterschicken darf.



Bridges können Ethernet-Segmente auch über synchrone Standleitungen, Satellitenverbindungen, Funkverbindungen, öffentliche Paketvermittlungsnetze und schnelle Lichtleiternetze (z.B. FDDI) verbinden. In der Regel müssen solche Bridges immer paarweise eingesetzt werden.

Weitere Merkmale/Vorteile einer Bridge sind:

- Ausfallsicherheit
  Störungen gelangen von der einen Seite einer Bridge nicht auf die andere Seite. Sie werden auch in diesem Sinne zum Trennen von sog.Kollisions-Domainen eingesetzt.
- Datensicherheit
  Informationen, die zwischen Knoten auf einer Seite der Bridge ausgetauscht werden, können nicht auf der anderen Seite der Bridge abgehört werden.
- Durchsatzsteigerung
  In den durch Bridges getrennten Netzsegmenten können jeweils unterschiedliche Daten-Blöcke gleichzeitig transferiert werden. Hierdurch wird die Netzperformance erhöht. Allerdings erzeugen Brücken dadurch, dass sie die Blöcke zwischenspeichern eine zusätzliche Verzögerung und können deswegen bei kaum ausgelasteten Netzen die Performance sogar verschlechtern.
- Vermeidung von Netzwerkschleifen
  Eine Bridge unterstützt den sog. Spanning Tree Algorithmus, wodurch es möglich ist, auch Schleifen- oder Ring-Konfigurationen (= redundante Verbindungen) im Netz zu erlauben. Die Bridges im Netz kommunizieren miteinander, im Gegensatz zu "dummen" Repeatern oder Hubs, und stellen über den Algorithmus sicher, dass bei mehreren redundanten Verbindungen immer nur eine gerade aktiv ist.

Weitere Kenndaten einer Bridge sind:

die Größe der Adresstabelle: gibt an, wie viele Adressen (Knoten) insgesamt in der Bridge gespeichert werden können

die Filterrate: gibt an, wie viele Pakete pro Sekunde (packets per second, pps) eine Bridge maximal empfangen kann. Bei voller Last und minimaler Paketlänge können in einem Ethernet-Segment theoretisch bis zu 14.880 Pakete pro Sekunde auftreten. Auf beiden Ports hat eine 2-Port- Bridge also insgesamt maximal 29.760 Pakete pro Sekunde zu filtern. Alle modernen Bridges erreichen diese theoretisch möglichen Maximalwerte.

und die Transferrate: gibt an, wie viel Pakete pro Sekunde die Bridge auf die andere Seite weiterleiten kann. Der Maximalwert ist hier 14.880 pps, da bei dieser Transferrate beide Segmente voll ausgelastet sind.

Für den Anwender bzw. die einzelnen Endgeräte stellt sich der Einsatz einer Brücke so dar, als handle es sich um ein (großes) Netzwerk. Hinweise darauf, dass eine Brücke eingesetzt wird, ergeben sich in der Praxis in der Regel nicht.

Die weitere Entwicklung der Brücken hat dazu geführt, dass mit ihrem Einsatz mittlerweile auch Netzwerke mit unterschiedlichen Zugriffsverfahren miteinander gekoppelt werden können. Während früher mit Hilfe eine Brücke ausschließlich homogene Netzwerke miteinander gekoppelt werden konnten, ist es heutzutage sogar möglich, über eine Brücke ein Ethernet-Netzwerk mit einem Token-Ring-Netzwerk zu verbinden, also durchaus auch Netzwerke mit unterschiedlichen Zugriffsmethoden.

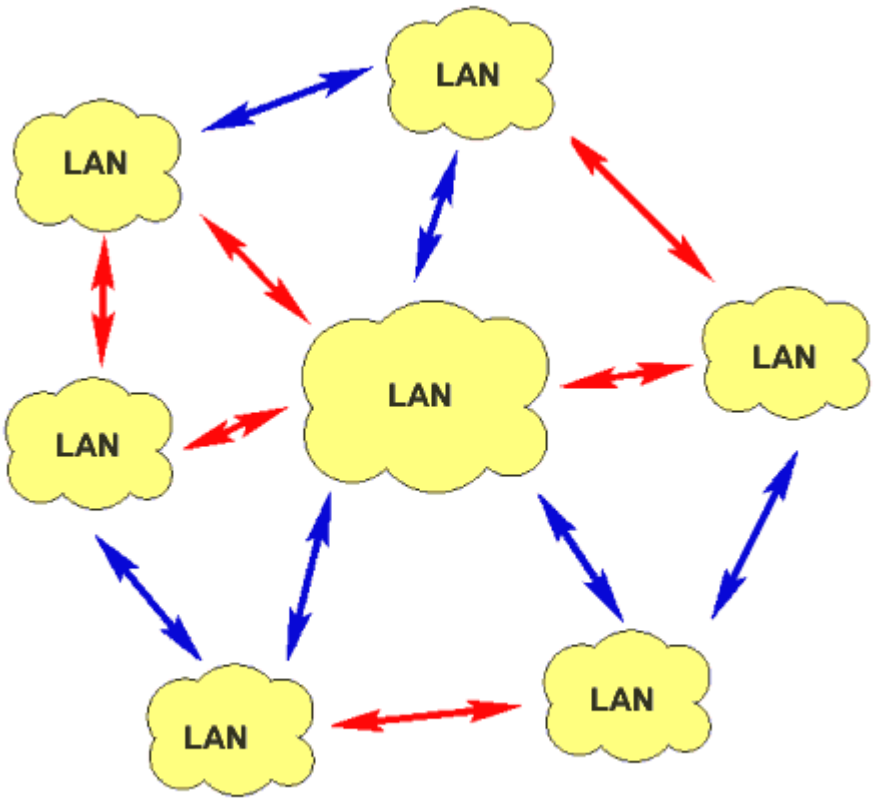
Aufgrund der spezifischen Eigenschaften bietet sich der Einsatz von Brücken überall dort an, wo ein ständiger Austausch großer Datenmengen erfolgt, und zwar zwischen Netzwerkbereichen mit gleichen Zugriffsverfahren.

Spanning Tree - Algorithmus

Das Spanning-Tree-Verfahren ist ein Verfahren zur Schleifenunterdrückung in Brücken-gekoppelten Netzwerken. Bei diesem Verfahren werden physikalisch redundante Netzwerkstrukturen ermittelt und in einer zyklenfreien Struktur abgebildet. Diese Massnahme reduziert die aktiven Verbindungswege einer beliebig vermaschten Netzwerkstruktur einer Baumtopologie (daher der Name Spanning Tree, SPT). Mathematisch betrachtet ist eine Baumstruktur so geartet, dass alle vernetzten Punkte nur durch einen Weg miteinander verbunden sind. Ausserdem sind alle vernetzten Punkte von allen anderen vernetzten Punkten aus erreichbar, zudem gibt es zwischen zwei beliebigen vernetzten Punkten keine Zyklen.

Das Erkennen von Schleifen in der Netztopologie ist zum einen erforderlich, um zu verhindern, dass Dateneinheiten endlos kreisen. Zum anderen kann es vermeiden, das ein Endsystem Dateneinheiten repliziert, das heisst, über verschiedene Wege empfängt. Der Spanning-Tree-Algorithmus baut aufgrund der aktuellen Netztopologie einen logischen Baum auf, entlang welchem die Daten durch das Netz geleitet werden. Die Bridges bilden die Knoten des Baumes. Zwischen je zwei lokalen Netzen wird ein eindeutiger Pfad von Bridges definiert. Sind mehrere Bridges zwischen zwei Netzen konfiguriert, so regelt der Algorithmus eindeutig, welche Bridge die Dateneinheit an das nachfolgende Netz weiterreicht.

Im folgenden Beispiel sind verschiedene LANs durch Bridges miteinander verknüpft, die im Bild durch Pfeile repräsentiert werden.

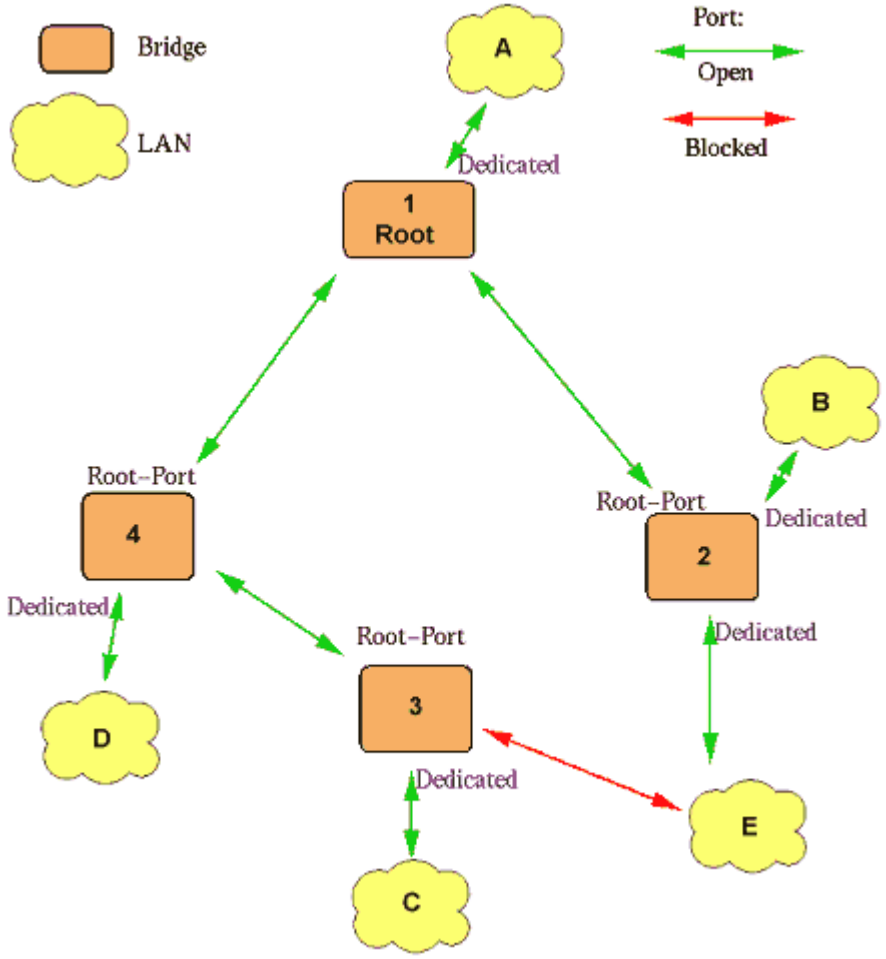


Alle Bridge-Links gemeinsam würden redundante Pfade im Netz ermöglichen, was endlos kreisende Pakete zur Folge hätte. Mit dem **Spanning Tree-Algorithmus** wird einer der möglichen logischen Pfade im Netz ausgewählt, der keine Schleifen enthält. Das Ergebnis wird durch die blauen Pfeile dargestellt die eine baumartige Struktur bilden. Im Extremfall kann hierdurch eine Bridge sogar ganz aus dem Netzverkehr herausfallen.

Die Bridges kommunizieren untereinander mit Hilfe der sog. **Bridge Protocol Data Units (BPDU)** Jede Bridge benötigt eine gewisse Grundkonfiguration, um den Algorithmus einsetzen zu können:

- Bridge: Eindeutige Bridge-ID.
- Port: Eindeutige Port-ID.
- Port: Relative Port-Priorität.
- Port: "Kostenfaktor" für jeden Port (je höher die Netzwerk-Performance im angeschlossenen LAN, desto geringer die Kosten).

In Abhängigkeit dieser Parameter wird der logische Baum folgendermaßen automatisch von allen Bridges zusammen aufgespannt:



1. Auswahl der Root-Bridge
   Die Root-Bridge ist die Bridge mit der kleinsten Bridge-ID. Haben zwei Bridges dieselbe ID, so wird diejenige mit der kleinsten MAC-Adresse ausgewählt.
2. Auswahl eines Root-Ports pro Bridge
   Mit Ausnahme der Root-Bridge, wird bei jeder Bridge einer der Ports als Root-Port festgelegt. Dieser Port wird mit Hilfe der geringsten "Wegkosten" zur Root-Bridge ermittelt.
3. Zuordnung einer Bridge pro LAN
   Diese Zuordnung ist entscheidend, da sonst Schleifen entstehen.
   - Im Falle dass nur eine Bridge an ein bestimmtes LAN angebunden ist, ist die Wahl einfach: jener Port, welcher zu diesem LAN gehöhrt, wird ihm auch global zugeordnet.
   - Haben mehrere Bridges einen direkten Zugang zu einem LAN, wird diejenige ausgewählt, welche betreffend der Wegkosten zur Root-Bridge am günstigsten ist.

Switch

Der Switch ist wie Hub oder Repeater ein Gerät des Osi-Layers 2, d. h. er kann LANs mit verschiedenen physikalischen Eigenschaften verbinden, z. B. Koax- und Twisted-Pair-Netzwerke. Allerdings müssen, ebenso wie bei der Bridge, alle Protokolle höherer Ebenen 3 bis 7 identisch sein!. Ein Switch ist somit protokolltransparent. Er wird oft auch als Multi-Port-Bridge bezeichnet, da dieser ähnliche Eigenschaften wie eine Bridge aufweist. Jeder Port eines Switch bildet ein eigenes Netzsegment. Jedem dieser Segmente steht die gesamte Netzwerk-Bandbreite zu Verfügung. Dadurch erhöht ein Switch nicht nur - wie die Bridge - die Netzwerk-Performance im Gesamtnetz, sondern auch in jedem einzelnen Segment. Der Switch untersucht jedes durchlaufende Paket auf die MAC-Adresse des Zielsegmentes und kann es direkt dorthin weiterleiten. Der große Vorteil eines Switches liegt nun in der Fähigkeit seine Ports direkt miteinander verschalten zu können, d. h. dedizierte Verbindungen aufzubauen.

Was ist nun der Unterschied zwischen einem Switch und einer Multiport-Bridge?

Bei den Produkten der meisten Hersteller gibt es keinen. Switch klingt nach Tempo und Leistung, deswegen haben viele Hersteller ihre Multiport Bridges Switches genannt. Der Begriff Switch für Multiport Bridges wurde von der Firma Kalpana (inzwischen von Cisco aufgekauft) kreiert, da deren Produkte nicht der IEEE-Spezifikation einer Bridge entsprachen, konnte Kalpana die Produkte nicht Bridges nennen und hat den Namen Switch gewählt. Kalpana war nun sehr erfolgreich mit dem Marketing ihrer Switches. Deswegen haben andere Hersteller ihre Bridges auch Switch, Switch mit Bridge-Eigenschaften oder Bridging Switch genannt. Switches brechen die Ethernet-Busstruktur in eine Bus-/Sternstruktur auf. Teilsegmente mit Busstruktur werden sternförmig über je einen Port des Switch gekoppelt. Zwischen den einzelnen Ports können Pakete mit maximaler Ethernet-Geschwindigkeit übertragen werden. Wesentlich ist die Fähigkeit von Switches, mehrere Übertragungen zwischen unterschiedlichen Segmenten gleichzeitig durchzuführen. Dadurch erhöht sich die Bandbreite des gesamten Netzes entsprechend. Die volle Leistungsfähigkeit von Switches kann nur dann genutzt werden, wenn eine geeignete Netzwerktopologie vorhanden ist bzw. geschaffen werden kann. Die Datenlast sollte nach Möglichkeit gleichmäßig über die Ports verteilt werden. Systeme, die viele Daten übertragen, müssen unter Umständen an einen eigenen Switch Port angeschlossen werden. Dies bezeichnet man dann als **Private Ethernet**. Außerdem sollte man versuchen, Systeme die viel miteinander kommunizieren, an einen gemeinsamen Port des Switches anzuschließen, um so die Datenmengen, die mehr als ein Segment durchlaufen müssen, zu reduzieren.

Allgemein haben sich in der Switch-Technologie zwei Gruppen herauskristallisiert:

Cut-Through bzw. On The Fly
Der Ethernet Switch wartet im Gegensatz zu normalen Bridges nicht, bis er das vollständige Paket gelesen hat, sondern er überträgt das ankommende Paket nach Empfang der 6-Byte-Destination-Adresse. Da nicht das gesamte Paket bearbeitet werden muss, tritt eine Zeitverzögerung von nur etwa 40 Mikrosekunden ein. Sollte das Zielsegment bei der Übertragung gerade belegt sein, speichert der Ethernet Switch das Paket entsprechend zwischen. Bei den Switches werden, im Gegensatz zu Bridges, mit Ausnahme von short frames (Pakete, die kleiner als die minimal zulässigen 64 Bytes sind), fehlerhafte Pakete auch auf das andere Segment übertragen. Grund hierfür ist, dass die CRC-Prüfung (Cyclic Redundancy Check) erst bei vollständig gelesenem Paket durchgeführt werden kann. Solange der Prozentsatz von fehlerhaften Paketen im Netz gering ist, entstehen keine Probleme. Sobald aber (z.B. aufgrund eines Konfigurationsfehlers, fehlerhafter Hardware oder extrem hoher Netzlast bei gleichzeitig langen Segmenten mit mehreren Repeatern) der Prozentsatz der Kollisionen steigt, können Switches auch dazu führen, dass die Leistung des Gesamtnetzes deutlich sinkt.

Cut-Through-Switching bietet dann einen Vorteil, wenn man sehr geringe Verzögerungen bei der Übertragung zwischen einzelnen Knoten benötigt. Diese Technologie sollte also eingesetzt werden, wenn es darum geht, in relativ kleinen Netzen eine große Anzahl Daten zwischen wenigen Knoten zu übertragen.

Store-and-Forward
Die Switches dieser Kategorie untersuchen im Gegensatz zu den vorher erwähnten das gesamte Datenpaket. Dazu werden die Pakete kurz zwischengespeichert, auf ihre Korrektheit und Gültigkeit überprüft und anschließend verworfen oder weitergeleitet. Einerseits hat dies den Nachteil der größeren Verzögerung beim Weiterschicken des Paketes, andererseits werden keinerlei fehlerhafte Pakete auf das andere Segment übertragen.

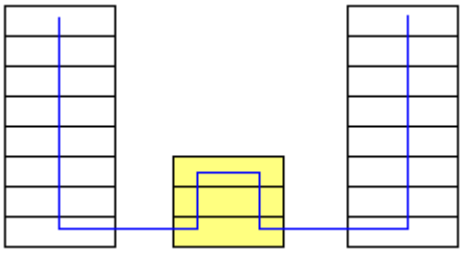
Diese Lösung ist bei größeren Netzen mit vielen Knoten und Kommunikationsbeziehungen besser, weil nicht einzelne fehlerhafte Segmente durch Kollisionen das ganze Netz belasten können. Bei diesen Anwendungen ist die Gesamttransferrate entscheidend, die Verzögerung wirkt sich hier kaum aus.

Inzwischen sind Switching-Produkte (z.B. von 3Com, Cisco oder Allied Telesyn) am Markt, die beide Technologien unterstützen. Dies geschieht entweder per Konfiguration (Software) oder automatisch anhand der CRC-Fehler-Häufigkeit. Wird eine vorgegebene Anzahl von fehlerhaften Paketen überschritten, schaltet der Switch automatisch von "Cut Through" auf "Store and Forward" um.

Router

Router verbinden, im Gegensatz zu Bridges, in OSI-Schicht 3 auch Netze unterschiedlicher Topologien. Sie sind Dreh- und Angelpunkt in strukturiert aufgebauten LAN- und WAN-Netzen. Mit der Fähigkeit, unterschiedliche Netztypen sowie unterschiedliche Protokolle zu routen, ist eine optimale Verkehrslenkung und Netzauslastung möglich. Routing wird erst dann erforderlich, wenn Kommunikation zwischen Stationen in unterschiedlichen Subnetzen erfolgen soll. Sie sind nicht protokolltransparent, sondern müssen in der Lage sein, alle verwendeten Protokolle zu erkennen, da sie Informationsblöcke protokollspezifisch umsetzen.

Bevor der Router ein Paket an ein angeschlossenes LAN oder WAN weiterleitet, untersucht dieser die Adressangaben des Datenpakets, z. B. die IP-Adresse und leitet die Daten abhängig von seiner Routing-Tabelle weiter. Er arbeitet also nicht wie die Bridge oder dem Switch mit den Adressen der MAC-Ebene. Dieses hat den Vorteil, das ein Host nicht die MAC-Adresse des Empfängers wissen muss um diesem eine Nachricht zu übermitteln. Die Adresse der Netzwerk-Protokollebene, z. B. IP genügt.
Dieses Weiterleiten von Daten anhand einer Tabelle heißt **Routen**.



Durch die für das Routen notwendige Untersuchung des Datenpakets, erhöht sich die Verweilzeit der Daten im Router selbst (Latenzzeit). Die eigentliche Stärke von Routern liegt in ihrer Fähigkeit mittels Algorithmen (z. B. Load Balancing Algorithmus) den in der Regel bestmöglichen Weg für ein Datenpaket zum Empfänger aus seiner Routing-Tabelle zu wählen.

Um die Daten "routen" zu können, ist es notwendig, dass der Router alle angeschlossenen Netzwerkprotokolle versteht und diese auch die Fähigkeit des Routens unterstützen. Der Vorteil des Routers gegenüber der Bridge ist die logische Trennung und die Bildung von (Sub-)Netzen bei TCP/IP bzw. von Areas bei DECNET.

Weitere Features von Routern sind ihre Netzwerk-Management- und die Filter-Funktionen. Durch geeignet gewählte Routing-Einstellungen ist es möglich, die Netwerk-Performance je nach Anforderungen ans Netz zu verbessern. Die Filterfunktionen auf Netzwerk-Protokollebene sind ähnlich wie bei der Bridge. Router bieten aber eine generell höhere Isolation da sie z. B. Broadcasts in der Regel nicht weiterleiten. Außerdem können sie zusätzlich als "screening Router" verwendet werden, indem z. B. bestimmten IP-Adressen der Zugriff auf bestimmte Netzteile verwehrt wird. Aus den erwähnten Gründen sind Router in der Regel per Software konfigurierbar.

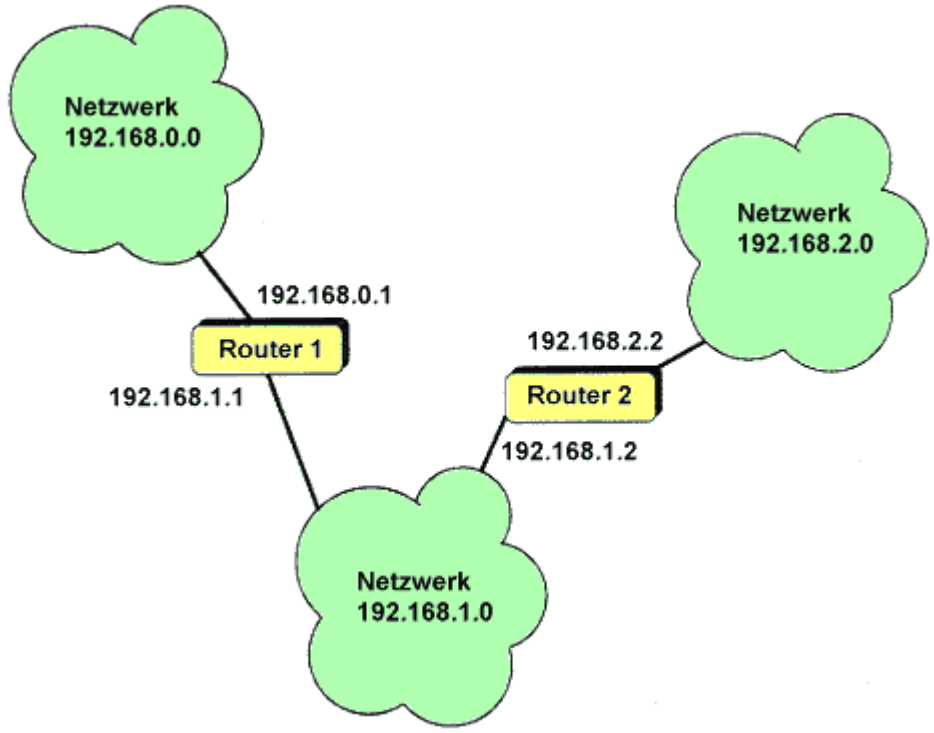
Basiskomponenten des Routing

Zur Durchführung des Routings werden drei Basiskomponenten benötigt:

- Routing-Protokolle: ermöglichen End- und Zwischensystemen Informationen miteinander auszutauschen, die das Routing betreffen.
- Routing -Algorithmen: ermitteln Wege im Netz, zu deren Bewertung sie Routing-Metriken heranziehen.
- Routing-Tabellen: Die Wegewahlinformation halten die einzelnen Systeme jeweils in Routing-Tabellen.

Beispiel für drei IP-Netze mit Routern

Das folgende Netz besteht aus drei IP-Netzen, die über Router verbunden sind. Jeder Router hat zwei Netzwerk-Interfaces, die jeweils in zwei der Netze hängen. Es ist nicht unbedingt erforderlich, für jedes Netz eine eigenen Interface zu verwenden; über sogenannte 'virtuelle Interfaces' kann man mehrere Netze auf ein Hardwareinterface legen.



Die Routing-Tabellen dazu sehen so aus:

Router 1		Router 2	
Empfänger im Netzwerk	Zustellung über	Empfänger im Netzwerk	Zustellung über
192.168.0.0	direkt	192.168.0.0	192.168.1.1
192.168.1.0	direkt	192.168.1.0	direkt
192.168.2.0	192.168.1.2	192.168.2.0	direkt

Während es Brücken egal ist, welche Netzwerk-Pakete (z. B. IP, IPX o. Ä.) transportiert werden, müssen Router alle Netzwerk-Protokolle kennen, die sie befördern sollen.

Die verwendeten Übertragungsprotokolle müssen natürlich grundsätzlich routbar sein, um einen Router einsetzen zu können. Ein klassisches Beispiel für ein nicht routbares Protokoll ist beispielsweise NetBEUI; die Standartprotokolle wie IPX/SPX oder auch TCP/IP sind routbar.

Mit dem Einsatz einer Brücke können zwei oder mehrere Netzwerke (Segmente) zu einem Gesamtnetzwerk zusammengefasst werden; bei einem Router erfolgt zwar ebenfalls eine Verbindung unterschiedlicher Netzwerke (auch heterogener), jedoch bleibt jedes Netz für sich als separates Segment erhalten (Eindeutigkeit der Netzwerkadresse). Ein Router arbeitet auch wesentlich effektiver als eine Brücke. So werden bei einem Router, obwohl er ebenfalls unterschiedliche Netzwerke verbinden kann (Brücken-Funktion), grundsätzlich nicht die Adressen der einzelnen Endgeräte, sondern ausschließlich die Adressen der beteiligten Netzwerke in Form einer so genannten "Routing-Tabelle" angelegt. Im Gegensatz zu Brücken wissen Router auch nicht, ob eine empfangende Station in einem anderen Netzwerk (Segment) auch tatsächlich empfangsbereit ist.

Besteht das gesamte (gekoppelte) Netzwerk nicht nur aus zwei sondern aus mehreren Segmenten, so verfügt grundsätzlich jeder Router über sämtliche Adressen der beteiligten Netzwerke. Somit kann ein Router sehr schnell feststellen, ob ein angesprochenes Netzwerk verfügbar ist. Ist ein angesprochenes Netzwerk vorhanden, kann ein Router dann aufgrund der Routing-Tabellen den kürzesten Weg für den Datenpfad ermitteln. Auf dem Weg vom Sender zum Empfänger wird das "Überspringen" eines Routers als **Hop** (Hüpfer) bezeichnet.

Der Einsatz eines Routers dient vornehmlich dazu, zwei oder mehr Netzwerke (Segmente) miteinander zu koppeln, wobei jedoch jedes einzelne Netzwerk (Segment) für sich bestehen bleibt. Dies wird durch die Auswertung der Netzwerkadressen im Router ermöglicht.

Genau wie bei Brücken, so ist auch beim Routereinsatz der Wechsel des Zugriffsverfahrens möglich, womit beispielsweise jederzeit ein Wechsel zwischen CSMA/CD und Token Passing realisiert werden kann. Dabei bietet sich der Einsatz von Routern dort an, wo kleine Datenmengen über mehrere Netzwerkbereiche mit unterschiedlichen Zugriffsverfahren und Protokollen übertragen werden sollen.

Hop

Ein Hop ist eine Zähleinheit, die auf die Lebensdauer eines Paketes (TTL) eingeht. Das Hop-Verfahren wird im IP-Protokoll angewandt; wobei beim Durchlauf eines Datenpaketes durch einen Router der Wert des Zeitstempels um jeweils eine Zeiteinheit reduziert wird. Eine Entfernung von zwei Hop bedeutet, dass auf dem Weg von der Quelle bis zum Ziel zwei Router durchlaufen werden.

Die Zeiteinheit ist in Sekunden festgelegt. Das bedeutet im Falle einer Datagrammübertragung, dass die maximale Zeit 255 Sekunden beträgt. Bei jedem Übergang über einen Router wird der Wert um eine Sekunde reduziert. Das Datagramm kann also 255 Router durchlaufen, bevor es zerstört wird.

Brouter

Das Wort Brouter ist ein Kunstwort, das sich aus den Anfangsbuchstaben der Bridge und den Endbuchstaben des Routers zusammensetzt. Von der Funktionalität her sind Brouter oberhalb von Brücken anzusiedeln. Sie besitzen Routing-Funktionalitäten als Spanning-tree-Algorithmen und damit die Möglichkeit, redundante Strukturen zu realisieren, Lastverteilungs-Algorithmen und Filtermechanismen. Anstelle des Begriffes Brouter wird für diese Geräte auch die Bezeichnung "Routing Bridge" verwendet.

Eine alternative Hierarchiedarstellung ergibt sich aus der unterschiedlichen Interpretation des Brouter-Begriffs: Aus der Learning Bridge entwickelte sich die Learning Filter Bridge und die Routing Bridge, während sich parallel dazu aus dem Router der Multiprotokoll-Router und der "Brouter" entwickelten. "Brouter" meint hier nicht eine Brücke mit erweiterter Funktionalität, sondern den hybriden Router, der mehrere Protokolle routet und die restlichen Datenpakete im Brückenbetrieb handhabt.

Generell ist zur Zeit die Tendenz zu beobachten, dass Brücken- und Router-Varianten der verschiedenen Produktlinien sich aneinander angleichen, um die Vorteile beider Systeme möglichst weitgehend zu verbinden. Das Angebot an "reinen" Brücken und an "reinen" Routern wird zunehmend geringer, insbesondere im Multiprotokoll-Router-Bereich, da diese Geräte speziell dafür ausgelegt sind, möglichst alle Protokolle eines Netzes parallel bearbeiten zu können - was bedeutet, dass die nicht routbaren Protokolle in diesen Koppelelementen mittels zusätzlicher Brückenfunktionalität handhabbar gemacht werden müssen.

Bewertung von Bridge gegenüber Router

Der Einsatz von Bridges zur Kopplung lokaler Netze hat gegenüber Zwischensystemen höherer Schichten den Vorteil der Effizienz, da weiterzuleitende Pakete nur wenige Protokollschichten durchlaufen müssen.

Bei der Installation von Netzen stellt sich oftmals die Frage, ob Bridges oder Router als Zwischensysteme eingesetzt werden sollen. Zunächst könnte man argumentieren, dass Router wesentlich mehr Möglichkeiten zur Verfügung stellen, allerdings dadurch komplexer und somit in der Regel leistungsschwächer sind. Meist sind sie auch teurer sind als Bridges. Bridges sind dafür nicht in der Lage, die gekoppelten Netze so gut zu separieren wie Router und bieten auch schlechtere Sicherheitsmöglichkeiten.

Eine gezielte Auswahl eines Zwischensystems hängt stark vom angestrebten Einsatzspektrum ab. Über reine Bridges und Router hinaus existieren sogenannte **Brouter** (Bridge-Router). Sie sind in der Lage, sowohl als Bridge als auch als Router zu wirken. Die Selektion zwischen den Funktionalitäten geschieht dynamisch zur Laufzeit, basierend auf den empfangenen Dateneinheiten.

- Quellen:

www.well-com.ch/thema/kopplung.htm
www.infakt.de/Themen/IP04.htm
www.ewetel.net/~marcus.kroeger/netzhard.htm