Internetworking

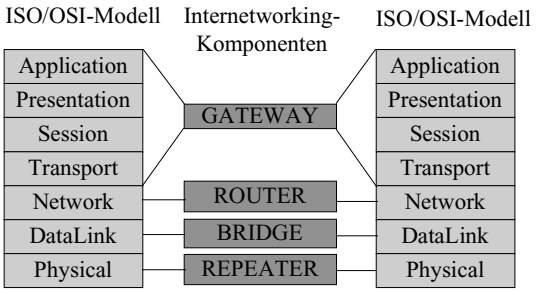
Einleitung

Mit ***Internetworking*** bezeichnet man den ***Zusammenschluß von Rechnernetzen***. Ein solches Netzwerk besteht aus einer Anzahl geographisch verteilter Recheneinheiten, die durch ein Übertragungsmedium miteinander verbunden sind und gemeinsam ihren Benutzern einen Dienst zur Verfügung stellen. Das vermehrte Zusammenwachsen von LANs und WANs mit häufig verschiedenen Protokollwelten erfordert flexible und leistungsstarke ***Kopplungs-elemente.***

Kopplungselemente

Repeater, Bridges, Router und Gateways sind die entscheidenden Komponenten des Internetworking. Jüngstes Koppelelement sind die ***Switches***. Sie sind nach OSI-Modell auf der gleichen Stufe wie Bridges anzuordnen, haben jedoch einen speziellen Vermittlungsansatz. Es gibt unterschiedliche Möglichkeiten, LANs miteinander zu verbinden. Die Internetworking-Komponenten unterscheiden sich im wesentlichen konstruktiv und von der abzudeckenden Funktionalität, die in Relation zu den entsprechenden Schichten des OSI-Referenzmodells ausgedrückt werden kann.

Beziehung zwischen dem OSI-Modell und den Internetworking-Komponenten



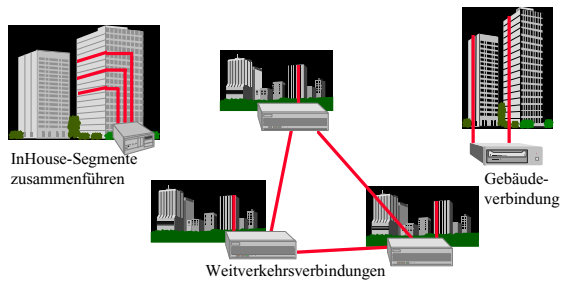
Ueberblick

- Bei den vier grundsätzlichen Internetworking-Komponenten gibt es eine Vielzahl von Untergruppen. Hier ein kleiner Ueberblick:

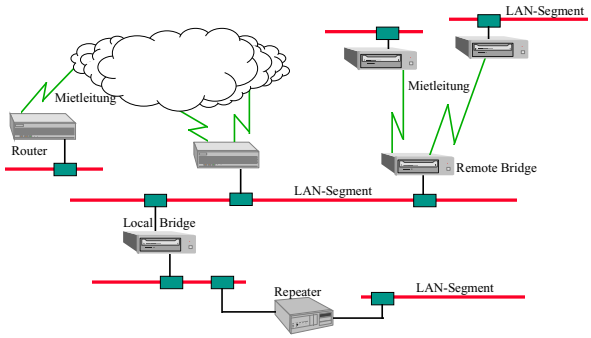
Repeater	Bridge	Router	Gateway
Local Repeater Remote Repeater Multiport Rep. Hub ...	Local Bridge Remote Bridge Filter Bridge Self Learning B. Switch ...	Local Router Remote Router Multiprotokol R. Brouter ...	Mail Gateway Host Gateway Applikations G. ...

Ueberblick (2)

- Das nachfolgende Bild soll den grundsätzlichen Einsatz der verschiedenen Internetworking-Komponenten aufzeigen:



Ueberblick (3)

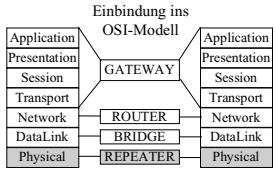


Repeater

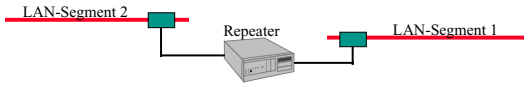
Ein Repeater ist eine aktive Komponente, die Regenerierungsfunktionen übernimmt. In lokalen Netzen dient ein Repeater zur Verbindung zweier Kabelsegmente, um die physikalische Topologie über die Ausdehnung eines einzelnen Segmentes hinaus zu erweitern. ***Der Repeater regeneriert den Signalverlauf sowie Pegel und Takt.*** Die meisten Repeater verfügen über eine Selbsttestfunktion und erkennen auch fehlerhafte Signale auf einem Segment. Diese werden dann nicht auf das andere Segment weitergeleitet. Dadurch erreicht man eine gewisse Lokalisierung von Fehlern. Ein Repeater ist völlig transparent und wird zur Überwindung von Längenrestriktionen einzelner Kabelsegmente eingesetzt, wodurch eine Topologieerweiterung des Netzes möglich wird. In Ethernet-LANs werden Repeater in zwei Realisierungen vorgesehen, als ***Local Repeater*** und als ***Remote Repeater***. ***Multiport Repeater*** sind solche, die mehrere Ausgänge haben. In LWL-LANs übernimmt der Repeater die gleichen Funktionen, wobei er das Lichtsignal dekodiert, in ein elektrisches Signal umformt und es anschließend über eine LED oder Laserdiode in den Lichtwellenleiter einspeist.

Repeater

- Repeater dienen hauptsächlich zur Topologieerweiterung des LAN's.
- Repeater regenerieren bitserielle Datenströme, d.h. alle empfangenen Signale werden verstärkt und regeneriert auf das andere angeschlossene Segment weitergeleitet.



- Local Repeater werden zur Kopplung von 2 oder mehr Netzsegmenten eingesetzt, die bis 100m voneinander entfernt sind (max. Ethernet Anschlusskabel-Länge).
- Remote Repeater können mittels Glasfaserinterface Segmente über eine Distanz von maximal 1000m (pro Segmentseite) miteinander verbinden.



Remote Repeater

Ein Remote Repeater ist ein Repeater, der aus zwei Teilen besteht, - deswegen auch die Bezeichnung Half-Repeater - die untereinander durch eine Leitung verbunden sind. Er dient dazu, größere Entfernungen (z.B. 2 km) zwischen den Segmenten zu überbrücken.

Multiport-Repeater

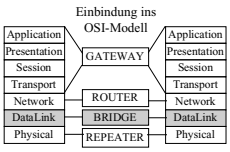
Ein Multiport-Repeater erfüllt Repeaterfunktionen und besitzt mehrere Ports. Durch ihn können z.B. typischerweise bis zu acht Cheapernet-Segmente mit einem Ethernet-LAN verbunden werden. Hubs, zusammen mit einer strukturierten Verkabelung im Einsatz, sind typische Multiport-'Twisted-Pair-Ethernet' (resp. LWL-) -Repeater.

Bridge

Bridges verbinden gemäß ihrer OSI-Definition Subnetze protokollmäßig auf der ***Schicht 2*** (LLC, IEEE 802.2) und 2a (MAC layer) des ***OSI-Referenzmodells***. Brücken sind in der Lage, die Grenzen eines Netzwerkes hinsichtlich der Stationszahl und der Längenausdehnung zu erweitern. Wird ein Netzwerk durch eine Brückenkopplung in zwei Subnetze strukturiert, so kann jedes Subnetz wieder die volle Stationszahl und Längenausdehnung entsprechend dem definierten Standard (z.B. Ethernet, Token Ring etc.) erhalten. Darüber hinaus leisten Brücken eine einfache Fehlerbegrenzungsfunktionalität. Fehlerhafte Layer-2-Pakete werden nicht transportiert. Außerdem schaffen Brücken eine Begrenzung des lokalen Verkehrs auf das Subnetz seines Entstehens; d.h., wenn ein Paket an eine Station im Subnetz des Absenders geschickt wird, transportiert die Brücke dieses Paket nicht. Dieses Merkmal trägt entscheidend zur Lastreduktion in großen Netzen bei. Die ***Arbeitsweise von Brücken wird durch den Informationsinhalt der Schicht 2 geprägt***. Dabei ist die zentrale Information der Schicht 2 die ***physikalische Adresse, auch MAC-Adresse*** genannt. Mit Hilfe der MAC-Adressen wird der Datenstrom durch die Brücken gesteuert. Da MAC-Adressen in allen IEEE- und ISO-Normen identisch aufgebaut sind, sind Brücken flexible Koppelelemente; auch zwischen Subnetzen unterschiedlichen Typs. Zentrales Wesensmerkmal von Brücken ist die ***transparente Netzwerkkopplung bezogen auf höhere Protokolle***. Daher hört man oft auch die Bezeichnung ***'Transparent Bridge' (TB)***. Das bedeutet für den Anwendungsfall, daß sämtliche Protokolle, die auf einer bestimmten MAC- oder LLC-Schicht aufsetzen, transparent, d.h. uninterpretiert von der Brücke weitergeleitet werden. So wird durch ein einziges Koppelelement die Verbindung der verschiedenen höheren Protokollwelten sichergestellt (z.B. AppleTalk, DECnet, LAT, IPX, TCP/IP, OSI, XNS etc.). Die Kopplung wird ohne spezielle Konfiguration in den Endgeräten der angebundenen Subnetze durchgeführt. Wenn auch die grundsätzliche Funktionalität (Kopplung auf Ebene 2) bei allen Brücken identisch ist, so gibt es doch verschiedene Ausprägungen dieser Art von Koppelelementen, die unterschiedliche Eigenarten haben. Prinzipiell unterscheidet man ***local Bridges*** und ***remote Bridges***.

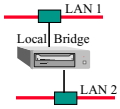
Bridge

- Brücken verbinden LANs
- Sie entflechten (entlasten) den Datenverkehr
- Sie entscheiden anhand der Hardware-Adr., ob ankommende Pakete übertragen oder lokal gehalten werden.
- Sie speichern Pakete, bis die Empfangsseite bereit ist (Buffering).
- Brücken passen die Uebertragungsgeschwindigkeiten (LAN <-> Mietleitung) an.
- Bei Bufferüberlauf und Verkehrsüberlast werden Datenpakete 'gelöscht'!
- Brücken können Daten filtern (frei wählbare Bedingungen; Layer 2 Adressen!).



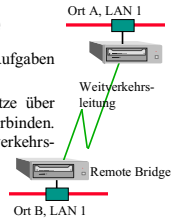
Local Bridge

- Kopplung der physikalischen Subnetze zu einem logischen Gesamtnetz (echter Datenrefresh durch CRC-Kontrolle)
- Netzlastentkopplung (Der lokale Datenverkehr wird nicht auf das angeschlossene Segment übertragen.)
- Datenfilter (Frei wählbare Kriterien auf Stufe MAC-Adresse).



Remote Bridge

- Die Remote Bridge erfüllt grundsätzlich die gleichen Aufgaben wie eine Local Bridge.
- Zusätzlich kann eine Remote Bridge entfernte Subnetze über öffentliche Netze zu einem logischen Gesamtnetz verbinden. Dazu hat sie neben dem LAN-Interface auch eine weitverkehrstaugliche Schnittstelle (V.24, V.35, etc.).



Local Bridge

Lokale Brücken verbinden LAN-Segmente direkt, als Subnetzkopplung innerhalb eines Unternehmens- oder Campus-Netzes. Die Verbindung wird über die LAN-Eingangsports und -Ausgangsports der Brücke hergestellt, d.h. mit Ein- und Ausgangsgeschwindigkeiten der LAN-Bandbreite. Handelt es sich um LANs gleichen Typs, erfolgt die Verbindung relativ problemlos. Handelt es sich um verschiedene MAC-Protokolle an den Ein- und Ausgangsports, muß zur Umsetzung vom 'schnelleren' LAN zum 'langsameren' LAN ausreichend Pufferplatz für eine Zwischenspeicherung der Pakete vorhanden sein.

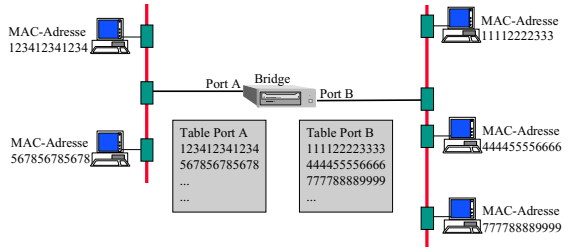
Remote Bridge

Die Remote Bridge verbindet Subnetze über Weitverkehrsstrecken, blosse Backbone-Strecken ohne eigene angebundene Endstationen; sie muß zumindest paarweise eingesetzt werden. An beiden Endpunkten einer Weitverkehrsstrecke zwischen zwei LAN-Subnetzen wird jeweils eine Remote Brücke installiert, was zu der manchmal verwendeten Bezeichnung 'Half Bridge' geführt hat. Eine Remote Bridge kann einen oder mehrere LAN-Ports sowie einen oder mehrere Remote Ports haben. Da Remote Bridges je nach Kapazität der Weitverkehrsverbindungs-Leistungen sehr große Kapazitätsunterschiede vom LAN zum Weitverkehrsnetz (Port-Speed) ausgleichen müssen, spielen der Pufferplatz und die Pufferorganisation eine große Rolle.

Funktionsweise von Bridges (Bridging)

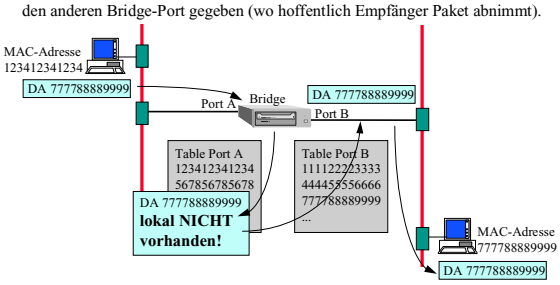
Wie erfüllen Brücken ihre Aufgabe ?

- Brücken brauchen Entscheidungshilfen, ob ein Paket im lokalen Segment bleibt, oder ob das Paket auf das andere Segment geschickt werden muss.
- Zur Entscheidung bauen sich Brücken Port-Tabellen mit den an diesem Segment angeschlossenen Stationen (MAC-Adresse) auf (dynamisch oder statisch).



Wie erfüllen Brücken ihre Aufgabe ? (2)

- Station '123412341234' will Station '777788889999' (DA = Destination Address) ein Paket senden.
- Bridge findet DA nicht auf ihrer eigenen Port A-Seite; somit wird das Paket auf den anderen Bridge-Port gegeben (wo hoffentlich Empfänger Paket abnimmt).

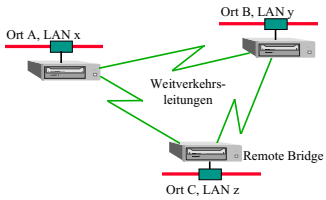


Wie erfüllen Brücken ihre Aufgabe ? (3)

- Vorteile / Wirkungsweise von Brücken:
  - Die ausschliessliche Uebertragung von Datenpaketen mit nicht-lokaler Zieladresse auf das benachbart angeschlossene Segment.
  - Sehr einfach zu installieren (plug und play).
  - Ermöglichen einen transparenten Datentransport (Transparent Bridge; TB).
  - Mittels des Selbstlernmechanismus werden portabhängige Tabellen erstellt.
  - Aufgrund von Vergleichen der Zieladresse eines Datenpaketes mit den Einträgen der Adress-Tabellen wird entschieden, ob Pakete übertragen (auch wenn Ziel nicht bekannt ist) oder verworfen werden.
  - Echte Lasttrennung (segmentweise Abblockung von Paketen).
  - Durch zusätzliche Datenfilter können einfache Filter oder komplexe Filtermasken erstellt werden. Diese Filter sperren den Datentransport für bestimmte Daten oder Ereignisse.
  - gebräuchliche Filterarten: - Source- / Destination-Address
    - Typ-Feld (nur bei Ethernet, nicht 802.3)
    - Daten / Ereignisfelder

Wie erfüllen Brücken ihre Aufgabe ? (4)

- Nachteile beim Bridging-Prinzip (gegenüber Routing)



  - Pakete werden über alle abgehenden Leitungen gesendet
  - Broadcast werden übers ganze Netz (LAN und WAN) verbreitet
  - Redundante Leitungen werden nicht aktiv genutzt (hot standby; realisiert durch IEEE 802.1d - spanning tree algorithm)

Spanning-tree-algorithm (SPT)

Spanning-tree ist ein Verfahren zur Schleifenunterdrückung in Brücken-gekoppelten Netzwerken (siehe dazu auch ‘IEEE 802.1d’). Bei diesem Verfahren werden physikalisch redundante Netzstrukturen ermittelt und in einer zyklenfreien Struktur abgebildet. Diese Maßnahme reduziert die aktiven Verbindungswege einer beliebig vermaschten Netzstruktur auf die einer Baumstruktur (daher der Name Spanning Tree, SPT - Die Baumstruktur ist dadurch gekennt-zeichnet, daß ausgehend von einer Wurzel (Root) eine Menge von Verzweigungen zu weiteren Knoten existiert, die bis auf die letzte Stufe (‘Blätter’) wiederum die gleiche grundsätzliche Struktur mit weiteren Verzweigungen aufbauen.). Eine Baumstruktur ist 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.
Der Algorithmus ist in entsprechenden Brückentypen implementiert, wobei jede Brücke im Rahmen bestimmter Optimalitätskriterien den Weg hin zur Wurzel (‘Root’; Ursprung des

Baumes) der Baumstruktur berechnet. Als Berechnungsparameter können Entfernungen, Kapazitäten, Kosten (virtuell, selbst wählbar) oder Verkehrsbelastungen herangezogen werden.
Die Spanning-Tree-Berechnung findet statt, wenn eine Bridge aufstartet oder wenn eine Aenderung der Topologie detektiert wird. Der ganze Prozess erfordert einen Informationsaustausch zwischen den Brücken. Der Austausch von Konfigurations-Nachrichten findet in Intervallen von etwa 1 bis 4 Sekunden statt. Wenn eine Bridge ausfällt (was eine Aenderung der Topologie bewirkt) werden die Nachbar-Bridges sehr bald feststellen, dass keine Konfig-Daten mehr kommen, und eine erneute Spanning-tree-Berechnung initiieren!
Alle Topologie-Entscheidungen werden lokal gemacht. Die Konfigurationsnachrichten werden zwischen benachbarten Bridges ausgetauscht. Es gibt keine zentrale Stelle, die die Topologie bestimmt oder Verwaltungsaufgaben ausführt.

Source-route-bridging-algorithm (SRB)

Der Source-route-bridging-algorithm ist das Gegenstück zum Spanning-tree-algorithm. Der SRB-Algorithm wurde von IBM entwickelt und im IEEE 802.5 Token Ring Standard festgehalten. Der Name Source-route-bridging kommt daher, dass die ***komplette Source-zu-Destination-Wegleitung (Route) in einem inter-LAN-Frame*** von der Source-Station (Absender-) eingetragen wird.
Ablauf: Wenn ein Host X einen Frame zu Host Y senden will, weiss X noch nicht, ob Y am selben Ring angeschlossen ist. Um dies zu bestimmen, schickt X einen Test-Frame auf den lokalen Ring. Kommt der Frame zurück und zeigt damit das Nichtvorhandensein von Y am selben Ring an, geht X davon aus, dass Y an einem entfernten Ring angeschlossen ist. Um die genaue Lage von Y zu finden, sendet X einen ***Explorer-Frame*** aus. Jede Bridge, die diesen Explorer-Frame sieht, kopiert ihn auf alle Ausgänge und addiert weitere Routing-Infos (Ring-/Bridgenummern-Paare). Ein Explorer-Frame besitzt damit die Information, auf welchem Weg er durch das Netzwerk zu Y gekommen ist. So kann Y jeden der ankommenden Explorer-Frames beantworten, in dem er die angesammelte Routing-Information verwendet. Hat Host X alle Antworten bekommen, kann er einen Weg aussuchen. Wenn von X ein Weg nach Y gefunden wurde, wird dieser in die Frames für Y im ***Routing Information Field (RIF)*** eingetragen. Die Präsenz eines RIF in einem 802.5 Frame wird durch das Setzen des U-Bits in der Source-Address angezeigt (siehe dazu auch IEEE 802.5). Das Feld wird dann ***Routing Information Indicator*** genannt.

Der wichtigste Unterschied von SRB im Gegensatz zu Transparent Bridging (SPT) besteht darin, dass die Endstationen für die Wegleitung ihrer Frames durch den LAN-Verbund zuständig sind. SRB belastet dadurch die LANs zusätzlich mit einem nicht vernachlässigbaren Datenverkehr, da es Explorer-Frame-Typen gibt, die von jeder Bridge erneut als Broadcast gesendet werden müssen.

Source-route-transparent-algorithm (SRT)

Das Source-route-transparent-Verfahren wurde entwickelt, damit SRB- und SPT-Systeme im gleichen Netz zusammenarbeiten können. Eine SRT-Bridge stellt Source-Routing-Funktionen für solche Pakete bereit, die Routing-Infos enthalten, und arbeitet als Transparent-Bridge für Pakete ohne Routing-Information. Bridges mit dem SRT-Verfahren stellen die Interoperabilität zwischen allen Komponenten im Netz sicher, gleich welchen Bridging-Mechanismus die einzelnen Internetworking-Elemente verwenden, resp. unterstützen!

Switch

Shared Media versus non shared media (switched path) - Verfahren

Shared Media, also ein geteiltes Übertragungsmedium, ist die Übertragungsbasis traditioneller Netzwerktechnologien wie Ethernet, Token Ring und FDDI. Alle Netzwerkstationen haben Zugriff auf das Übertragungsmedium und teilen sich dieses. Neben dem Nachteil, die vorhandene ***Übertragungsbandbreite unter allen aktiven Stationen aufteilen*** zu müssen, kommt dabei aufgrund der Shared-Media-Topologie der Nachteil hinzu, daß defekte Stationen die Funktionsfähigkeit aller anderer Netzstationen beeinträchtigen können.
Hinzu kommt, daß alle Stationen die Möglichkeit haben, auch auf Datenpakete zugreifen zu können, die nicht an sie adressiert sind, was die Datensicherheit von LANs erheblich reduziert.
Aufgrund dieser Nachteile wird mit der ***Switching-Technologie*** das ***Prinzip des nicht geteilten Übertragungsmediums (non shared media)*** realisiert.

Switching

Switching ist ein Prinzip der Datenkommunikation, bei dem die zu übertragenden Datenpakete innerhalb von sogenannten ***Switching-Systemen*** (Schalteinheiten) mit Hilfe aufwendiger Hardware ***sehr schnell von den Eingangsports direkt zu den gewünschten Ausgangsports vermittelt*** werden können. Ursprünglich in der Telefonie (TVA) und in großen Weitverkehrsvermittlungsanlagen eingesetzt, revolutioniert dieses Prinzip seit einiger Zeit auch die LAN-Infrastrukturen. Mit dem Segment-Switching kann in LAN-Verbunden eine wesentliche Durchsatzsteigerung erzielt werden. Dabei werden die verschiedenen Segmente eines Netzwerks nicht durch herkömmliche Brücken oder Router miteinander verbunden, sondern durch leistungsfähigere Segment-Switching-Systeme. Wird ***an jedem Switching-Port nur eine einzige LAN-Station*** angeschlossen, so spricht man von ***Mikrosegmentierung***. Die Switches sind in der Lage, mehrere Pakete gleichzeitig und ohne nennenswerte Verzögerung zu vermitteln (Duplex-Betrieb). In LANs kann so der Gesamtdurchsatz zwischen den Segmenten auf ein Vielfaches der bei shared media gewohnten Übertragungskapazität gesteigert werden.
Hauptschwierigkeit bei der Realisierung von Systemen mit dediziert zugeordneten (geswitchten) Bandbreiten ist die enorm hohe Verarbeitungsgeschwindigkeit, die in den entsprechenden Switching-Systemen erforderlich ist.

Ethernet-Switching

Ethernet-Switching ist eine Implementierung der oben erläuterten Switching-Technik um die volle Netzkapazität an das Endgerät zu bringen. Bei dieser Technik wird das Netz zum Zwecke der Lasttrennung in Mikrosegmente geteilt. Ist an jedem Port nur jeweils ein LAN-Node angeschlossen, so steht (wenn der Switch genügend schnell ist) allen Rechnern die nominelle Ethernet-LAN-Bandbreite zur Verfügung (10-, resp. 100 MB/s)! Vom Prinzip her arbeiten Ethernet-Switches wie 1-zu-1-Brücken; sie verwenden also als Entscheidungsgrösse ebenfalls die Layer 2 MAC-Adressen. Alle ankommenden Pakete werden nur an den Port weitergeleitet, an dem die Zieladresse angebunden ist. Ethernet-Switches sind vergleichbar mit traditionellen Hubs, haben jedoch an Stelle des Kollisions-Busses eine sehr schnelle Schaltzentrale (Cross-Connect) implementiert. Dies bedeutet auch, dass Ethernet -Switching nicht mit der Koaxial-Busverkabelung realisiert werden kann, sondern nur mit strukturierter Twisted-Pair- oder LWL-Verkabelung!
Switches verhalten sich im Netzwerk genau so transparent wie Bridges. Die Clients müssen also nicht wie bspw. bei Routern bei einem Standortwechsel mit neuen Netzwerkadressen konfiguriert werden. Switches ersetzen jedoch Router nicht. Diese werden gebraucht, um die 'Switching-Inseln' auf höheren OSI-Layern (Protokollen) miteinander zu koppeln.

Router

Router werden entsprechend ihren Möglichkeiten in verschiedene Typen unterteilt:

Einzelprotokoll-Router (single protocol router)

Der Einzelprotokoll-Router verbindet LAN-Subnetze auf der Basis eines einzelnen LAN-Protokolls, daher rührt auch sein Name. Die Verbindung kann eine LAN-LAN-Verbindung oder eine LAN-WAN-Verbindung (Mietleitung, X.25, ISDN) sein. Das klassische Beispiel für einen Einzelprotokoll-Router ist ein X.25-Vermittlungsknoten, da ja das Routing seinen Ursprung deutlich mehr im Weitverkehrsbereich als im LAN-Bereich hat.

Multiprotokoll-Router (multiple protocol router)

Sie sind in der Lage, im Gegensatz zu Single-protocol-Routern, mehrere Protokolle parallel zu handhaben. Über verschiedene Protokoll-Stacks (Implementierung mehrerer Schicht-3-Protokolle), die in einem Gerät realisiert sind, werden verschiedene logische Netzwerke jeweils untereinander verbunden. Dadurch werden Mehrfach-Backbones (je Protokoll ein logischer Backbone mit einem eigenen Single-protocol-Router-Typ) eliminiert - ein einziger Gerätetyp im Backbone reicht zur Kopplung aller Protokollwelten aus.

Brouter (bridge-router)

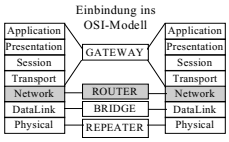
Das Wort Brouter ist ein Kunstwort, das sich aus den Anfangsbuchstaben der Bridge und den Endbuchstaben des Routers zusammensetzt. Von der Funktionalität her sind Brouter oberhalb von Brücken anzusiedeln. Sie besitzen Routing-Funktionalitäten als auch Spanning-tree-Algorithmen und damit die Möglichkeit, 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 Pakete im Brückenbetrieb handhabt. Generell ist die Tendenz, 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.

Um die geforderte Verbindung von Endgeräten in verschiedenen Subnetzen auf Netzwerkebene zu leisten, müssen Router eine Reihe von Basiskomponenten realisieren:

- Ein Verfahren für die Stationen, sich dem Router gegenüber zu identifizieren (und umgekehrt).
- Einen Algorithmus für 'nichtlokale' Pakete, um den nächsten Router auszuwählen, der das Paket empfangen soll (der Algorithmus nennt sich 'Routing' nach der zentralen Funktion eines Routers).
- Einen header für Informationen wie Zieladresse der Endstation, life time (Zeitstempel), Fragmentierung und Reassemblierung.

Router

- Router verbinden LANs (auch über WAN)
- Sie verbinden zwei (oder mehrere) physikalisch und logisch getrennte Netzwerke.
- Sie arbeiten auf dem OSI-Layer 3 (Network).
- Sie sind gegenüber den unteren Schichten (bspw. MAC-Adresse) unabhängig.
- Fragmentieren und reassemblieren Pakete.
- Sie ermitteln in komplexen Netzwerken für Datenpakete eine geeignete Route.
- Stellen für die Wegwahl einen Adressabbildungsmechanismus zur Verfügung.
- Steuern den Datenfluss durch Windows-Mechanismen.
- Haben neben den LAN-Interfaces auch WAN-Schnittstellen für den Weitverkehr.
- Router sind bei grossen und vermaschten Netzen effizienter als Brücken.



Routing

Unter Routing versteht man eine Wegwahl-Funktion zur Vermittlung von Nachrichten zwischen mehreren lokalen Netzen. ***Das Routing-Problem kann folgendermaßen charakterisiert werden: Wie läßt sich die von einem Knoten zu einem zweiten Knoten zu transportierende Nachrichtenmenge unter Verwendung der Ressourcen des Netzes optimal transportieren?*** Routing-Verfahren lassen sich grob klassifizieren in: - Zentralisierte und verteilte Verfahren, bei denen entweder eine Zentralstation die notwendigen Wegwahlinformationen hat und die Wegwahlentscheidung trifft, oder, bei der verteilten Technik, die einzelnen Knoten (IMPs; Individual Managment Ports) ihre Entscheidung selbst treffen. - Bei den statischen Verfahren (siehe ***statisches Routing***) wird die optimale Wegwahl einmalig berechnet und es wird immer der gleiche Weg über die IMPs benutzt. Das wirkt sich bei Änderung der Randbedingungen nachteilig aus. - Dagegen stehen die dynamischen Verfahren (siehe ***dynamisches Routing***), die die Wegwahl aufgrund aktueller Zustandsparameter des Netzwerkes treffen. Dies stellt bei großen Netzwerken ein Problem dar, da sich der Netzzustand ständig ändert. - Bei den lokalen und globalen Verfahren wird einerseits der Netzzustand in der unmittelbaren Umgebung, andererseits der gesamte Netzzustand berücksichtigt. - Die Leitwegbestimmung wird über deterministische und stochastische (auf der Wahrscheinlichkeit beruhende) Verfahren bzw. Entscheidungsregeln getroffen.
Router verbinden Subnetze gemäß der Schicht 3 des ISO/OSI-Referenzmodells. Da die Schicht 3 für alle aktuell etablierten Industriestandards unterschiedlich ist, ist die ***Router-Kopplung*** hinsichtlich der höheren Schichten ***protokollabhängig***, d.h., ein Router muß alle Protokolle 'verstehen', die er bearbeiten soll. Durch die Kopplung auf Schicht 3 können unterschiedliche Schicht-2-Protokolle sehr gut ausgetauscht werden. Aufgrund der implementierten Routing-Protokolle stellt eine Router-Kopplung im Vergleich zur Brückenkopplung komplexere und unter Umständen effizientere Möglichkeiten zur Verfügung, redundante Netzstrukturen hinsichtlich dynamischer Wegwahl und alternativer Routen auszunutzen. Durch den Einsatz von Netzwerkadressen lassen sich hierarchische Netzstrukturen (Unterteilung in verschiedene Klassen von Subnetzen) realisieren. ***Im Gegensatz zu Bridges interpretieren Router nur die Pakete, die direkt an sie adressiert sind, defaultmäßig erfolgt kein Pakettransport. Nur wenn das Zielnetz bekannt ist, wird ein Paket entsprechend weitergeleitet.*** Broadcasts werden nicht weitergeleitet, sondern bei routingfähigen Protokollen vom Router bearbeitet. Aufgrund der komplexeren Wegwahl-Funktionalität und der Unterbindung von Default-Transport eignen sich Router insbesondere zur LAN-interconnection über Weitverkehrsnetze. Router haben mindestens ein existierendes Protokoll oberhalb des LLC-Protokolls (IEEE 802.2) implementiert. Bekannte Protokolle sind z.B. - IP, OSPF (TCP/IP-Familie, internet protocol, open shortest path first), - IPX (Novell NetWare), - IS-IS, (ISO routing), - XNS, IDP, RIP, EP (Xerox networks system, internet datagram protocol, routing information protocol, error protocol), - X.25, CCITT-Empfehlung für öffentliche WAN-Verbindungen.

statisches Routing

Statisches Routing basiert, wie der Name schon sagt, auf einer ***festen Vorgabe des Weges*** zwischen zwei beliebigen Endsystemen. Diese Vorgabe wird bei der Einrichtung, d.h. Installation des Netzwerkes getroffen und ***in der Regel als feste Tabelle im Router abgespeichert***. Die Endgeräte sind jeweils einem Router zugeordnet, über den sie erreichbar sind und andere Ziele erreichen können. Die genaue Konfiguration des Netzes, Anzahl und Lage der Router, eingesetzte Leitungen und deren Übertragungskapazität muß bei Festlegung der Routen bekannt sein. Dann lassen sich als Konfigurationsparameter berücksichtigen: - Anzahl und Lage der Endsysteme und Router, - vorhandene Leitungen und deren Kapazität, - Annahmen über das zu erwartende Lastaufkommen, - Prioritäten unter den Netzteilnehmern. Im Änderungsfall muß eine statische Route manuell umkonfiguriert werden (Fehler, Erweiterung, Umzüge etc.), woran der Nachteil des Verfahrens deutlich sichtbar wird.

dynamisches Routing

Ein wesentlicher Vorteil von Routern ist die Möglichkeit, ***Routen dynamisch***, d.h. bei laufendem Netzbetrieb, ***je nach Netzerweiterung*** neu einzurichten ***oder je nach Lastsituation*** zu ändern. Diese Verfahren werden auch ***adaptives Routing*** genannt, da die Wegwahl an die aktuelle Netzsituation ‘adaptiert’ werden kann. Die optimale Wegwahl wird nach einer anfänglichen Parametersetzung allein durch das Routing-Protokoll bestimmt und ist so für den Benutzer transparent. Solche dynamischen Routing-Protokolle realisieren eine zentrale Funktion des Netzwerkes und berücksichtigen im Vergleich zum statischen Routing zusätzliche Faktoren: - Leitungs- und Knotenausfall; hier können Redundanzkonzepte mit alternativen Routen zum Tragen kommen. - Kenntnis alternativer Wege, um bestimmte Netzteile zu umgehen, z.B. bei Hochlastsituationen in Form von - Leitungsüberlastung oder - Überlastung der Verarbeitungswarteschlange (des Interfaces) im Router. Ein dynamisches Verfahren besticht durch seine Flexibilität. Aber: Um die Flexibilität zu erreichen, müssen die beteiligten Router ständig Kontrollinformationen über die aktuell verfügbare Konfiguration und Topologie austauschen. Dies bedeutet zusätzlichen Overhead, der sich direkt als zusätzliche Netzlast niederschlägt - insbesondere bei relativ langsamen oder geschaltenen (Wähl-, ISDN-) remote Leitungen, aber auch bei entsprechender Intensität in LANs ein nicht zu vernachlässigender Faktor, der machmal wieder ein (teilweise) statisches Routing nötig macht!

Routing - Tabellen

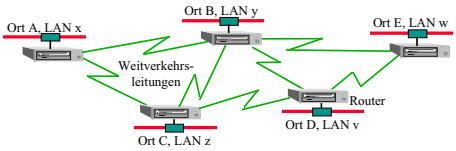
Um eine Ende-zu-Ende-Verbindung zwischen kommunikationswilligen Endgeräten herzustellen, d.h. den Pakettransport vom Sender bis zum Empfänger durchzuführen, müssen zwei Endstationen (Sendestation, Empfängerstation) über ihre Netzadressen eindeutig identifizierbar sein. Dann können die zwischen diesen Endgeräten liegenden Router gemäß ihren Routing-Tabellen das Paket von der Sendestation über den ersten Router zum zweiten, von dort zum dritten usw. weiterleiten, bis schließlich der 'letzte' Router auf dem Weg durch verschiedene Subnetze es an die Empfängerstation weiterleitet. Die Routing-Tabellen (in jedem Router) beinhalten für den jeweiligen Router die Information, in welche Richtung ein Paket mit dem vorgefundenen Zielnetzwerk weiterzuleiten ist.

Router - Terminologie

Die OSI-Terminologie unterscheidet zwischen ***intermediate systems (IS)*** und relay systems. Erstere können beliebige Router oder Hosts mit Routing-Intelligenz sein, letztere sind reine 'Verbindungselemente', also nur Router. Ein Gesamtnetz ist unterteilt in Subnetze; der Dienst, den der Router / das intermediate system erbringt, ist der entsprechende Subnetzdienst für die Endsysteme. Eine Routing-domain ist eine Menge von Endsystemen, die eine gemeinsame Sprache sprechen, d.h. das selbe Routing-Protokoll benutzen***. Ein Hop ist der Durchlauf eines Paketes durch einen Router / intermediate system auf dem Weg von der Sende- zur Empfangsstation.*** Eine Entfernung von zwei Hop bedeutet, daß auf dem Weg von der Quelle bis zum Ziel zwei Router (außer dem direkt an das Subnetz der Quellstation angeschlossenen Router) durchlaufen werden. Ein ***ES-IS-Protokoll (End System to Intermediate System)***, wie z.B. IP oder XNS oder IPX, ist ein Protokoll, mit dem sich Endgeräte dem Router mitteilen (und umgekehrt). ES-IS-Protokolle werden auch als 'routbare' Protokolle bezeichnet. Ein ***IS-IS-Protokoll*** (***Intermediate System to Intermediate System)*** ist ein Protokoll, das Router untereinander benutzen, um Routing-Informationen, Fehlermeldungen etc. auszutauschen. IS-IS-Protokolle (bspw. RIP oder OSPF) können auch als 'Router-Protokolle' bezeichnet werden.

Funktionsweise von Routern (Routing)

Wie arbeiten Router ?

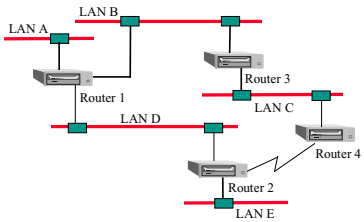


- Ermitteln für die Datenpakete den geeignetsten Weg. Entscheiden anhand von Netzwerkadressen wo die Pakete durchgeleitet werden.
- Finden die geeigneten Partner-Router durchs Netzwerk (selbständig, dynamisch)
- Behandeln nur Pakete, die explizit an den Router adressiert sind.
- Netzwerkadress-Systeme sind protokollabhängig (TCP/IP, DECnet, IPX, XNS,...)
- Die zu übertragenden Protokolle müssen verstanden und konfiguriert sein.
- Router erlauben ein (zusätzliches) detailliertes Filtern nach verschiedenen Kriterien.

Wie arbeiten Router ? (2)

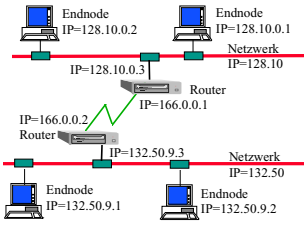
- Router brauchen Entscheidungshilfen, ob ein Paket im lokalen Segment bleibt, oder ob und wie das Paket auf ein anderes Segment geschickt werden muss.
- Zur Entscheidung bauen sich Router Tabellen auf, anhand derer sie entscheiden können, wie ein Ziel erreicht werden kann (dynamisch oder statisch).

Router-Table Router 1		
Ziel	via	Variante
LAN A	direkt	-
LAN B	direkt	LAN D
LAN C	LAN B	LAN D
LAN D	direkt	LAN B
LAN E	LAN D	LAN B
...		
...		



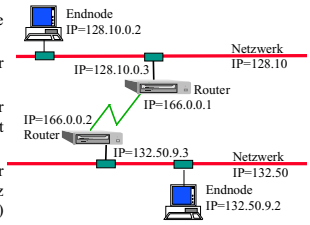
Wie arbeiten Router ? (3)

- Funktionsweise eines Netzwerkes; hier am Beispiel einer TCP/IP-Protokoll-Umgebung. (Das IP; Internet Protokoll resp. die Internet-Adresse ist für den Netzwerk-Teil verantwortlich.)
- Die Netzwerk-, Router- und Node-adressen müssen übereinstimmen - d.h. entsprechend konfiguriert sein!
- Die Router haben für jeden Port (d.h. für jedes Netz) eine eigene Adresse.
- Die Bekanntmachung der Netze zwischen den Routern erfolgt automatisch (dynamisch) mit speziellen Router-Informations-Protokollen. Beispiele: RIP, OSPF, IS-IS



Wie arbeiten Router ? (4)

- Erster IP-Adressteil (Net-Id) ist pro Netzsegment immer gleich (hier: 128.10, resp. 132.50). Zweiter Teil (Node-Id) muss pro Netz eindeutig (unterscheidbar) sein (bspw. 0.2 oder 9.2). Die Aufteilung erfolgt durch eine Netzmaske (IP-Netmask).
- Beispiel: Node 128.10.0.2 will Node 132.50.9.2 ein Paket senden.
- Paket gelangt zu seinem Net-Router (gleiches Netz -> 128.10-Router)
- Der lokale Router routet Paket über WAN-Port (166.0.0.1) zu Router mit Zielnetzwerk (Port -> 166.0.0.2.)
- Zeil-Router findet Zielnetz in seiner Portliste -> legt das Paket auf Netz 132.50 wo dieses zu Node (132.50.) 9.2 gelangt.



Nachfolgend wichtige Router-Protokolle im Internetworking-Umfeld (IP und OSI):
(Nicht eingegangen wird auf das proprietäre ***Interior Gateway Routing Protocol (IGRP)*** von Cisco, das OSI ***Connectionless Network Protocol (CLNP)*** sowie auf die ***Interdomain-Routing-Protokolle Exterior Gateway Protocol (EGP)*** und ***Border Gateway Protocol (BGP)***, das eine Weiterentwicklung von EGP ist.)

Routing Information Protocol (RIP)

RIP wurde auf der Basis des XNS RIP entwickelt und hat sich als Standardmodul des BSD Unix 4.3 sehr stark etabliert. Viele Internet-Netze haben es übernommen.
Bei RIP schicken alle Router in Intervallen (Standard-mässig alle 30 Sekunden) ihre eigenen ***Routing-Tabellen als Broadcast an die Router*** am gemeinsamen LAN oder an einer Punkt-Punkt-Verbindung. (Wenn innerhalb von 6 solchen Updates (180 Sekunden) für eine erreichbare Route vom entsprechenden Router kein Update kommt, markiert er diese Route als unerreichbar.) Die Entfernung zu anderen Netzwerken wird dabei in Relation, d.h. aus der Sichtweise der eigenen Routing-Tabelle angegeben. Auf der Basis der empfangenen Tabellen berechnen die Router die kürzesten übermittelten Entfernungen zu jedem Zielnetz und nehmen den Nachbar-Router, der diese Entfernung bekanntgegeben hat, als Ziel-Router zur Weiterleitung. Die ***maximale Entfernung*** darf ***15 Hops*** betragen, wird der Wert 16 mitgeteilt, steht dies für 'nicht erreichbar'.

RIP-Updates werden als UDP-Pakete (User Datagram Protocol; siehe TCP/IP) im IP verschickt. In einem ***RIP-Paket*** sind folgende Felder enthalten:
- ***Command***: Definiert die Art des RIP-Paketes. Dies kann entweder ***Request oder Response*** sein. Ein Request kann von einem soeben aufgestarteten Router geschickt werden, um die Routing-Tabellen der andern Router zu erfahren.
- ***Version***: (heute) auf '1' gesetzt.
- ***Address Family Identifier***: ist immer auf '2' gesetzt. Die Vorkehrung diese Feldes zeigt, dass RIP ursprünglich für verschiedene Protokolle gedacht war.
- ***IP Address***: Die IP-Adr. des Netzes oder Hosts, die der Absender-Router erreichen kann.
- ***Hop Count***: Definiert die Metrik, welche der Absender-Router aufweist, um das Ziel-IP-Netzwerk zu erreichen.

Es ist sehr schwierig eine Aussage zu machen, ***wie schnell Aenderungen in einem Netzwerk konvergieren***. Wenn eine Verbindung ausfällt, ist dies logischerweise nicht sofort jedem Router im Netz klar, somit ist es eine gewisse Zeit lang möglich, dass Loops bestehen oder nicht auf Alternativ-Wege umgeschaltet wird. Um die Netz-Leistung in solchen Phasen nicht zu stark zu belasten und die Konvergenz zu verkürzen, sind Zusätze nötig:
- Das ***split Horizon*** genannte Verfahren verhindert, dass ein Router eine Route über das gleiche LAN propagiert, über welches er den Weg selber gelernt hat.
- Eine Erweiterung wird mit sogenannten ***triggered Updates*** gemacht. Dies erfordert, dass ein Router bei einer Aenderung in der Metrik einer Route sofort einen Update aussendet.
- Normalerweise befindet sich eine Route im ***Up-State***. Der ***Hold-Down-State*** ist erforderlich, um zu vermeiden, dass ein Router seine richtige Erkenntnis von einem Route-Ausfall durch einen falschen Update eines andern Routers revidiert. Der ***Garbage-Collection-State*** ist erforderlich, dass der Router die nicht-erreichbare Route den andern Routern mitteilen kann.

Eigenheiten (Limitationen) von RIP:
- Der maximale Hop-Count ist 15, d.h. im Netz maximal 16 in Serie geschaltete Router.
- Der Hop-Count alleine ist keine sehr differenzierte Metric. Es kann sein, dass zwar eine Route einen Hop mehr besitzt, jedoch sehr schnelle Verbindungen verwendet. Dann ist diese Route unter Umständen effizienter, als eine mit weniger Hops!
- Die Updates beinhalten die gesamte Routing-Tabelle und sind daher sehr datenintensiv. Da ein RIP-Paket maximal 25 Routing-Tabellen-Zeilen enthalten kann, müssen viele Pakete geschickt werden, um eine längere Tabelle zu propagieren.
- Die Konvergenz ist, bedingt durch das Update-Intervall, relativ lang.

Open Shortest Path First (OSPF) - Protocol

OSPF ist ein seit 1989 existierendes Routing-Protokoll, das RIP kurz- bis mittelfristig gänzlich ablösen soll. Es ist im ***RFC (Request for Comment) 1131 spezifiziert.*** OSPF gilt heute neben RIP als Defacto-Standard.

OSPF bietet folgende Qualitäten:
- Rasche Konvergenz und Resistenz gegen Routing-Loops
- Updates mit geringer Netz-Belastung. OSPF verwendet Multicast- statt Broadcast-Verfahren. Somit bekommen nur diejenigen Router OSPF-Pakete, die auch mit OSPF arbeiten.
- Authentifizierung der Routing-Pakete, womit eine gewisse Sicherheit geboten werden kann.
- Erlaubt (beispielsweise gegenüber RIP) effizientere IP-Adressplatz-Verwendung durch variable Subnetzmaskenlängen.
- Bietet ein Area-(Domain)Konzept, um den netzweiten Datenverkehr zu limitieren.
- Kann Type of Service (TOS) routing. OSPF verwendet das TOS-Feld des IP-Paketes und erlaubt, dass verschiedenen TOS-Werten verschiedene Costs zugewiesen werden können.
- OSPF verwendet direkt IP und unterstützt Multipath-Routing (parallel verschiedene Routen).

Die Grundoperationen von OSPF sind:
- Jeder Router sendet periodisch ein ***Link-State-Advertisment (LSA)*** an seine Nachbarn. Im LSA sind die LANs und die Nachbar-Router (die der Router kennt) enthalten. Router sind Nachbarn, wenn sie über ein gemeinsames Netz (gleiches LAN oder über Pkt-Pkt Link) miteinander verbunden sind.
- Um die Nachbarn zu finden, werden periodisch von jedem Router 'Hello'-Pakete auf die Broadcast-Adresse verschickt.
- LSAs werden durch den sogenannten ***Flooding-Mechanismus*** durch die gesamte Routing-Domain verteilt, indem jeder Router das LSA an all seine Nachbarn weiterleitet, ausser denjenigen, von welchem das LSA kam, oder wenn das LSA zu alt ist (um Loops zu beenden).
- Jeder Router bildet durch die Interpretation der LSA eine ***Link-State-Database***.

Intermediate System to Intermediate System (IS-IS) - Routingprotocol

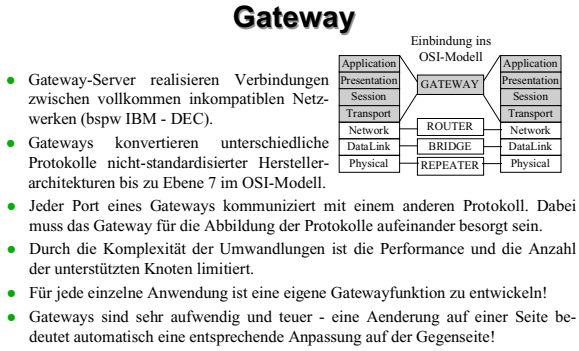
Das ***IS-IS-Protokoll ist ein Router-Protokoll im OSI-Umfeld*** (ISO 10589). Das Protokoll arbeitet nach einem ähnlichen Konzept wie OSPF (hierarchy und link state algorithm), nur ist es für OSI-Adressierung ausgelegt. Das IS-IS-Protokoll basiert auf einem Domain-Konzept und ermöglicht dadurch globale, flexible und hierarchische Modellierung. Wichtiges Merkmal einer domain ist, daß sie sich weiter untergliedern läßt, in subdomains, sub-subdomains etc. Der Routing-Algorithmus für ***IS-IS ist Digitals Phase V (DECnet/OSI) entlehnt***. Der Algorithmus ist sowohl für kleine als auch für große Netze geeignet (bis zu 10'000 Router und bis zu 100'000 Endknoten). IS-IS unterstützt vier verschiedene Metriken (nur die Default-Metrik verpflichtend): - Leitungskapazität (default), - Verarbeitungszeit (transit delay, optional), - Kosten (optional), - Fehlerrate der Verbindung (optional). Ein intermediate system kann eine beliebige Kombination dieser Metriken unterstützen; für jede Metrik berechnet es einen eigenen SPF-Baum (Shortest Path First) und erstellt eine eigene Routing-Tabelle. Der Einsatz verschiedener Metriken macht aufgrund der verschiedenen möglichen Netze (Ethernet, Token Ring, FDDI, X.25, Satellit) durchaus Sinn, da in einem Fall die Auslastung, im anderen die Kosten das wichtigere Kriterium sein können.
Im Gegensatz zu IP-Routing ist bei OSI ein Routing-Protokoll definiert, dass zwischen einem Router (IS) und einer End-Station (ES) operiert. Durch das ***Intermediate System to End System (IS-ES)*** Protokoll lernen die ES, wer und wo die IS sind, die es erreichen kann.

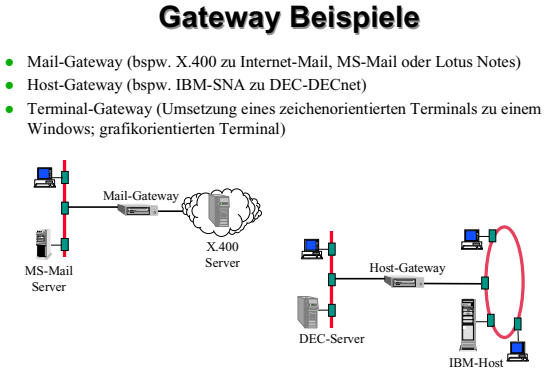
Gateway

Ein Gateway ist die Hard- und Software, um verschiedene Netze miteinander zu verbinden oder an andere Netze durch Protokollumsetzung anzuschließen. Ein Gateway hat die Aufgabe, Nachrichten von einem Rechnernetz in ein anderes zu übermitteln, wofür vor allem die Übersetzung der Kommunikationsprotokolle notwendig ist. Es wird durch einen speziell dafür eingesetzten Rechner realisiert. Dies bezieht sich auch auf die Verknüpfung von nicht-normkonformen Netzen wie SNA, DECnet usw. ***Ein Gateway ist jeweils auf der kleinsten gemeinsamen Schicht der miteinander zu verbindenden Netze angesiedelt; das kann im Extremfall Schicht 7 sein (OSI-Referenzmodell).*** Das Gateway 'versteht' beide Protokolle vollständig und ist in beiden Welten ein adressierbarer Netzknoten. Die vollständige Umwandlung beinhaltet:

- Umsetzung der Adressen
- Umsetzung der Formate
- Code-Konvertierung
- Zwischenpufferung der Pakete
- Paketbestätigung
- Flußkontrolle / Geschwindigkeitsanpassung

Ein Gateway realisiert aufgrund der vollständigen Bearbeitung aller Kommunikationsschichten für die verbundenen Protokollwelten oft eine höhere Funktionalität hinsichtlich Terminal-Emulation, Grafikfähigkeit, Programm-zu-Programm-Kommunikation, Filetransfer und Anzahl parallel möglicher Sessions als gemeinsam benutzbare Standardprotokolle. Nachteilig ist die Beschränkung auf jeweils zwei verschiedene Protokolle, was beim Einsatz von n Protokollen n x (n-1)/2 Gateways erfordert (quadratische Steigerung!) und entsprechenden Betreuungsaufwand und Unübersichtlichtkeit der logischen Netzstruktur erzeugt.





Gateway-Server

Ein Gateway-Server ist ein Rechner, der den angeschlossenen Netzen oder Geräten eine Kommunikationsleistung zur Verfügung stellt. So kann beispielsweise ein Mainframe als Gateway-Server den angeschlossenen PCs einen zentralen Zugang zu Datenbanken und anderen Netzen ermöglichen. Diese Funktion kommt immer dann zur Anwendung, wenn teure, aber relativ selten benötigte Zugriffe auf Datenbank oder andere Netze notwendig sind.