2.2c OSI-Referenzmodell: Schicht 2c - Vernetzung

PROVISORICH (VERSION 13.7.2002)

- Aufgaben und Funktionen
- Brücken (Bridges), Lokale Brücke, Abgesetzte Brücke
- Transparente Bridging, Spanning Tree Protocol
- Rahmenvermittlung (Frame Relay)

Netzkopplungen

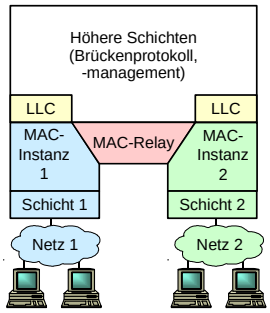
Aus geographischen, historischen, wirtschaftlichen, politischen und organisatorischen Gründen wird die Vernetzung aus Teilnetzen gleicher oder verschiedener Technologien gebildet. Bei Teilnetzen der gleichen Technologie sind mehrheitlich Zuständigkeits- und Sicherheitsfaktoren maßgebend. Sind technologisch ungleiche Netze zu koppeln, so sind zu der physikalischen Anpassung zusätzlich Protokoll- und Datenformat-Umformungen notwendig.

Bridge-Technologien

Viele Unternehmen haben mehrere LANs und möchten diese verbinden. LANs können mit Geräten namens Bridges (Brücken) verbunden werden, die auf der Sicherungsschicht arbeiten. Das bedeutet, dass Bridges den Header auf der Vermittlungsschicht nicht prüfen und Pakete alllerart Protokolle gleichermaßen gut kopieren können.

Es werden sechs Gründe aufgeführt, warum in einem einzelnen Unternehmen mehrere LANs vorhanden sein können.

- Erstens haben viele Universitäts- und Firmenabteilungen ihr eigenes LAN, um damit ihre Personalcomputer, Workstations und Minicomputer zu verbinden. Da sich die Ziele der einzelnen Abteilungen unterscheiden, werden auch verschiedene LANs eingerichtet, ohne die Entscheidung anderer Abteilungen zu berücksichtigen. Früher oder später müssen sie zusammenarbeiten, also wird eine Brücke benötigt. In diesem Beispiel entstanden die verschiedenen LANs aufgrund der Autonomie ihrer Besitzer.
- Zweitens könnte das Unternehmen auf verschiedene geographisch weit voneinander entfernte Gebäude ausgeteilt sein. Hier ist es günstiger, in jedem Gebäude ein LAN einzurichten und diese dann mit Bridges zu versehen, als ein riesiges Koaxialkabel durch das ganze Gebiet zu verlegen.
- Drittens könnte es nötig sein, ein logisches Einzel-LAN in mehrere LANs aufzuteilen, um die Belastung zu verteilen. An vielen Universitäten stehen z.B. für Studenten und Lehrende Tausende von Workstations zur Verfügung. Die Dateien befinden sich normalerweise auf Datei-Servern und werden von den Benutzern an einer Workstation bei Bedarf heruntergeladen. Bei Systemen diesen Umfangs können nicht alle Workstations an ein einzelnes LAN angeschlossen werden. Die insgesamt benötigte Bandbreite wäre zu hoch. Statt dessen werden mehrere LANs über Bridges verbunden. Jedes LAN enthält einen Workstation Cluster mit einem eigenen Datei-Server, so dass der Großteil des Verkehrs auf ein einzelnes LAN beschränkt ist und das Backbone nicht belastet.
- Viertens könnte ein einzelnes LAN zwar die anfallende Arbeit bewältigen, aber die physische Entfernung zwischen den am weitesten voneinander entfernten Maschinen ist zu groß (z.B. mehr als die von 802.3 unterstützten 2,5 km). Auch wenn die Kabelverlegung einfach ist, wird das Netz wegen der extremen Umlaufzeit nicht den Anforderungen gerecht. Die einzige Lösung ist die Unterteilung des LANs und die Installation von Bridges zwischen den einzelnen Segmenten. Das bedeutet, dass die physische Ausdehnung eines Netzes mit Bridges erweitert werden kann.
- Fünftens ist die Zuverlässigkeit zu betrachten. Bei einem einzelnen LAN kann ein defekter Knoten, der andauernd Unsinn sendet, das ganze LAN beeinträchtigen. Bridges können an kritischen Stellen wie Notausgänge eingebaut werden, um den teuflischen Knoten davon abzuhalten, das ganze System lahmzulegen. Im Gegensatz zu einem Repeater, der nur kopiert, was er sieht, kann eine Bridge so programmiert werden, dass nicht alles weitergegeben wird.
- Sechstens können Bridges zur Sicherheit eines Unternehmens beitragen. Die meisten LAN-Schnittstellen haben einen Gemischtmodus: Dem Computer werden alle Pakete übergeben, nicht nur die an ihn adressierten. Werden an verschiedenen Stellen Bridges eingesetzt und empfindliche Daten einfach nicht weitergeleitet, können Teile des Neues so isoliert werden, dass keine Daten mehr entweichen können.



- **Transparente Bridge**
  - Lernen der Lokation von Endsystemen
  - Filtern bzw. Weiterleiten von Dateneinheiten
  - Erkennen von Schleifen in der Netztopologie
- **Source-Routing-Bridges**

Es gibt verschiedene Arten von Bridges.

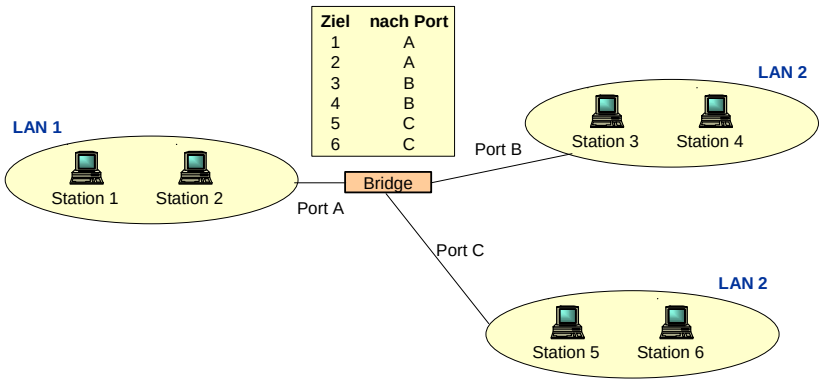
Betrachtet werden:

- Transparent Bridge,
- Source-Routing Bridge,
- Remote Bridge.

Bild: LAN-Kopplung mit Bridges

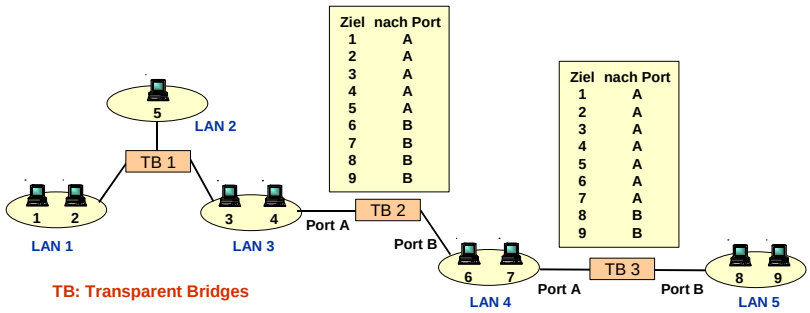
Transparente Bridges

Die erste 802-Bridge ist die transparente Bridge oder Spanning-Tree-Bridge. Das ausschlaggebende Anliegen derjenigen, die diese Auslegung unterstützten, war die völlige Transparenz Aus ihrer Sicht muss es bei einer Anlage mit mehreren LANs möglich sein, eine von IEEE genormte Bridge zu kaufen, sie anzuschließen, und dann soll das Netz sofort laufen. Es sollte nicht nötig sein, die Hardware zu ändern, die Software zu ändern, die Adressierung zu ändern oder die Routing-Tabellen oder Parameter zu laden - nichts dergleichen. Nur die Kabel einstecken und fertig. Die bereits bestehenden LANs sollten nicht in Mitleidenschaft gezogen werden.



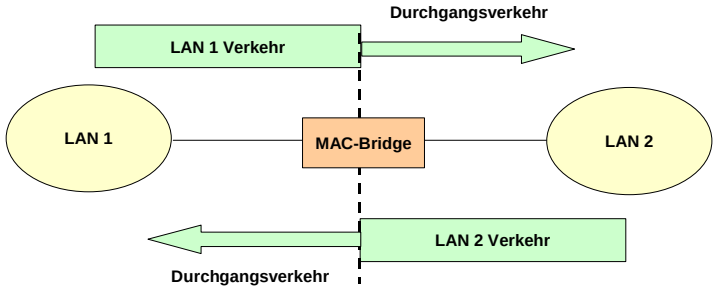
Eine transparente Bridge arbeitet im Gemischtmodus und akzeptiert jeden Rahmen von allen angeschlossenen LANs. Als Beispiel betrachte man ein Bridge mit drei LANs. Durch eine Weiterleitungstabelle können ankommende Rahmen über den richtigen Port an jede Station weitergeleitet werden.

Bild: Transparent Bridges: Weiterleitungstabelle



Bei mehreren Bridges erhalten die Tabellen die Informationen, in welchen LAN-Teilen sich die Stationen befinden.

Bild: Transparent Bridges: Weiterleitungstabelle



Kommt ein Rahmen an, muss sich die Bridge entscheiden, ob er verworfen oder weitergegeben wird, und im letzteren Fall, auf welches LAN er auszugeben ist. Diese Entscheidung wird durch das Nachschlagen der Zieladresse in einer großen Hash-Tabelle innerhalb der Bridge gefällt. Die Tabelle kann jeden möglichen Empfänger und den dazugehörigen Port (das dazugehörige LAN) ausgeben. Ein MAC-Bridge ist somit auch ein Filter.

Bild: Hauptaufgabe einer MAC-Bridge: Filterfunktion

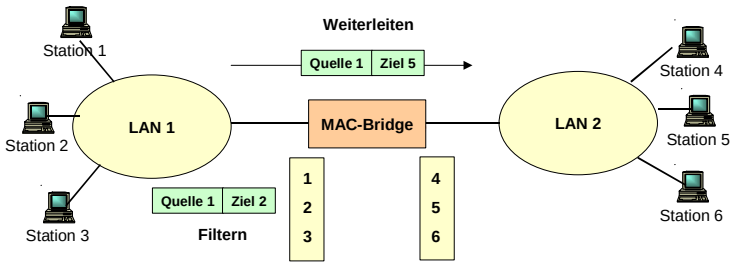
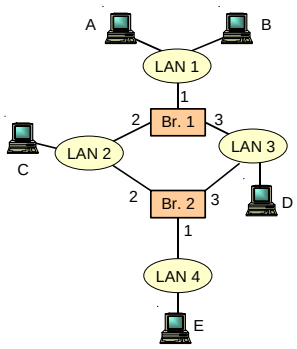


Bild: MAC-Bridge: MAC-Adressen als Filter

Bei der erstmaligen Installation der Bridges sind die Hash-Tabellen leer. Keine der Bridges weiß, wo welches Ziel liegt, so dass der Flooding-Algorithmus angewandt wird. Jeder eintreffende Rahmen für ein unbekanntes Ziel wird auf jedes angeschlossene LAN ausgegeben, außer auf das, von dem er angekommen ist. Mit der Zeit lernt die Bridge, wo die verschiedenen Ziele liegen. Irgend wann sind ihr alle Ziele bekannt und alle Rahmen werden an das jeweils richtige LAN abgegeben, Damit ist auch keine weitere Flooding-Anwendung mehr nötig.

Die Topologie kann sich ändern, wenn Maschinen und Bridges ein- und ausgeschaltet oder verlegt werden. Für die dynamische Topologie wird die Ankunftszeit des Rahmens in den Hash-Tabelleneintrag mit aufgenommen. Jedesmal, wenn ein bereits eingetragener Rahmen ankommt, wird die Zeit des Eintrags aktualisiert. Damit stellt die Zeitangabe im Eintrag den letzten Zeitpunkt dar, an dem ein Rahmen von dieser Maschine gesehen wurde.

In periodischen Abständen überprüft nun ein Prozess die Hash-Tabelle der Bridge und löscht alle Einträge, die älter als ein paar Minuten sind. Wird ein Computer von seinem LAN getrennt, an eine andere Stelle im Gebäude verlegt und dort wieder angeschaltet, ist er innerhalb weniger Minuten wieder lauffähig, ohne dass manuelle Eingaben erforderlich sind. Dieser Algorithmus bedeutet auch, dass der Verkehr zu einer mehrere Minuten lang untätigen Maschine geflutet werden muss, bis sie selbst wieder einen Rahmen versendet.



- Bridge 1 empfängt Paket von A an C
- Bridge 1 lernt, dass A über LAN-Port 1 erreichbar ist
- Kennt Bridge 1 Station C, so leitet sie das Paket über LAN-Port 2 weiter
- Fluten bei unbekannter Zieladresse
- Spanning Tree
- Filterdatenbasis:
  - Zieladresse
  - Ausgangsport
  - Zeitgeber
- Filtern: Pakete mit lokalen Adressen werden nicht über Bridge weitergeleitet (z.B. Daten von A an B)

Die Routing-Prozedur für einen eingehenden Rahmen hängt vom Quell- und vom Ziel-LAN wie folgt ab:

- Sind Ziel- und Quell-LAN identisch, wird der Rahmen verworfen
- Sind Ziel- und Quell-LAN verschieden, wird der Rahmen weitergegeben
- Ist das Ziel-LAN unbekannt, wird die Flooding-Technik angewandt

Immer wenn ein Rahmen ankommt, muss dieser Algorithmus angewandt werden. Es gibt spezielle VLSI-Chips, die die Tabelleneinträge alle paar Mikrosekunden überprüfen und auf den neuesten Stand bringen.

Bild: Transparentes Bridging

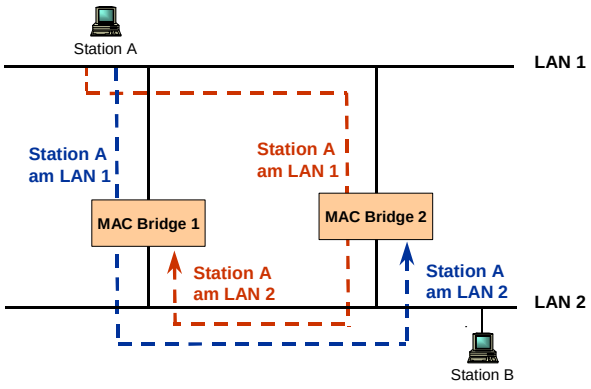


Bild: Transparent Bridges: Schleifenbildung

Um die Zuverlässigkeit noch weiter zu erhöhen, werden bei manchen Anlagen zwei oder mehr Bridges parallel zwischen zwei LANs benutzt. Aber auch diese Anordnung verursacht zusätzliche Probleme, weil in der Topologie Schleifen erzeugt werden.

Ein einfaches Beispiel dieser Problematik kann bei der Behandlung eines Rahmens F von Station A mit unbekanntem Ziel beobachtet werden. Jede Bridge folgt den normalen Regeln für unbekannte Ziele und flutet. In diesem Beispiel bedeutet das lediglich, Rahmen F nach LAN 2 zu kopieren. Kurz danach erkennen Bridges 1 und 2 einen Rahmen mit unbekanntem Ziel und kopieren ihn auf LAN 1. Dieser Kreislauf setzt sich unendlich fort.

Die Lösung für dieses Problem sicht die Kommunikation der Bridges untereinander und die Überlagerung der aktuellen Topologie mit einem überspannenden Baum (Spanning-Tree) vor, der jedes LAN erreicht. Um eine fiktive schleifanlose Topologie aufzubauen, werden einige potentielle Verbindungen zwischen den LANs ignoriert. Im Beipiel 1 gibt es fünf über fünf Bridges zusammengeschlossene LANs. Diese Konfiguration kann in einem Graphen dargestellt werden, in dem die

LANs als Knoten erscheinen. Je zwei durch eine Bridge verbundene LANs werden durch eine Kante verbunden. Der Graph kann auf Grund von wenigen Regeln auf einen überspannenden Baum reduziert werden. Bei diesem überspannenden Baum gibt es genau einen Pfad von jedem LAN zu jedem anderen. Haben die Bridges einmal Übereinkunft über den überspannenden Baum getroffen, erfolgen alle Übertragungen zwischen den LANs über den überspannenden Baum. Da von jeder Quelle zu jedem Ziel ein eindeutiger Pfad führt, sind Schleifen unmöglich.

Um einen überspannenden Baum aufzubauen, sendet jede Bridge alle paar Sekunden ihre Kennung (d.h. eine vom Hersteller installierte und garantiert eindeutige Seriennummer) und eine Liste aller anderen ihr bekannten Bridges zwischen den LANs. Die Bridge mit der niedrigsten Seriennummer bildet die Wunel. Dann wird ein Baum mit kürzeltmöglichen Pfaden von der Wurzel zu jeder Bridge aufgebaut und das LAN zusammengestellt. Dieser Baum ist der sogenannte Spanning-Tree. Fällt eine Bridge oder ein LAN aus, wird ein neuer Baum berechnet.

Aus diesem Algorithmus entsteht ein einheitlicher Weg von jedem LAN zur Wurzel und damit zu jedem anderen LAN. Obwohl der Baum alle LANs umfaßt, müssen nicht unbedingt alle Bridges im Baum enthalten sein (um Schleifen zu vermeiden). Sogar nach der Erstellung des überspannenden Baums läuft der Algorithmus weiter, um Änderungen in der Topologie automatisch zu erfassen und die Konfiguration (den Baum) entsprechend anzupassen.

Bridges können auch zur Verbindung von weit entfernten LANs benutzt werden. In diesem Modell besteht jede Anlage aus einer Reihe von LANs und Brücken, von denen eine mit einem WAN verbunden ist. Rahmen für entfernte LANs werden über das WAN weitergereicht. Hier kann der grundlegende Algorithmus des Spanning-Tree angewandt werden, aber vorzugsweise mit gewissen Optimierungen bzw. der Minimierung des WAN-Verkehrsvolumens

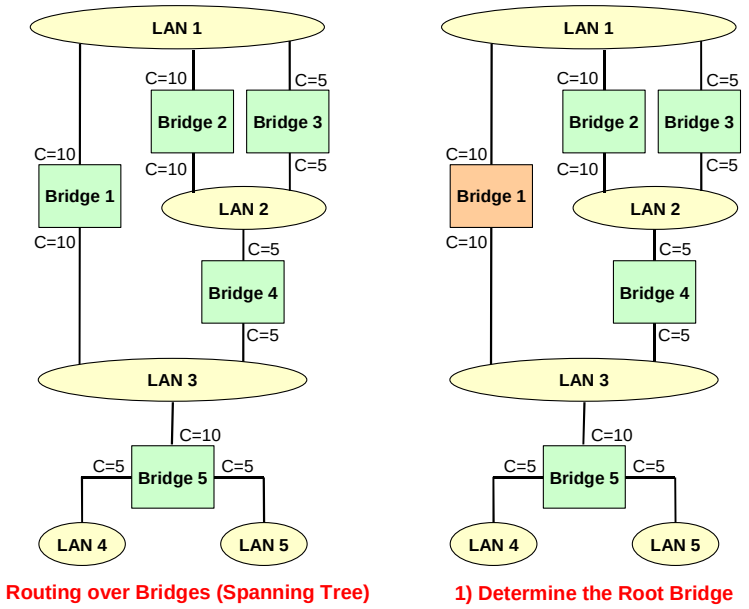


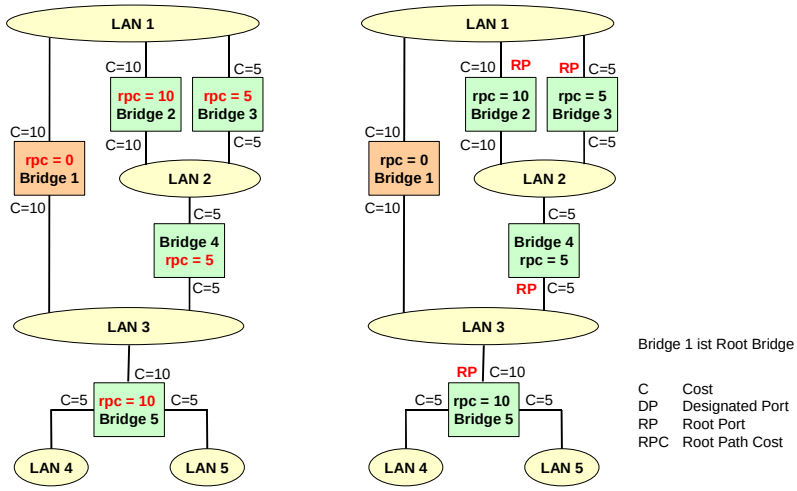
Bild: Beispiel 1: Spanning Tree Algorithmus (1)

Ausgangspunkt:

1) Bridges haben eine eindeutige Identifikationsnummer.
2) Jeder Port eines Bridges wird einen Kostenfaktor zugewiesen

Spanning Tree Algorithmus:

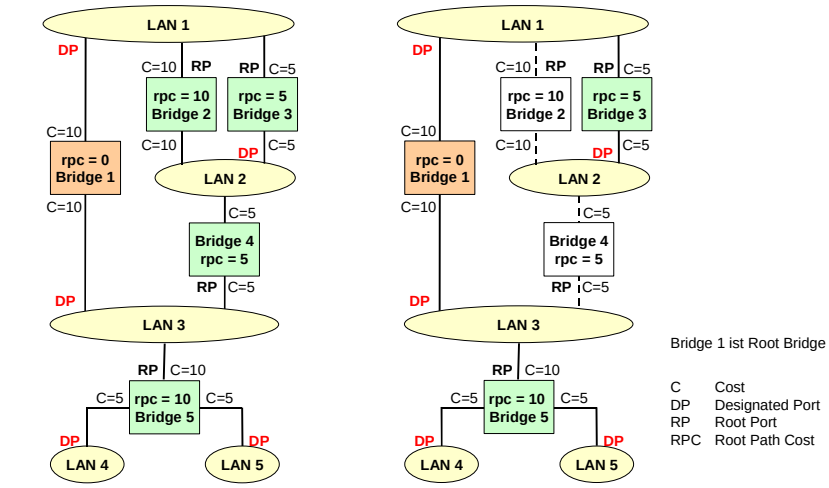
1. Wahl des Root-Bridge als Bridge mit der niedigsten Identifikationsnummer.
2. Berechnung der niedrigsten Wurzelpfadkosten für jeden Bridge.
3. Bestimmung des Root-Bridge Ports für jeden Bridge. Dies ist der Port mit der niedrigsten Wurzelpfadkosten
4. Bestimmung des Designated Ports für jedes LAN. Dies ist der Port eines Bridges, der ein LAN mit den geringsten Kosten mit dem Root-Bridge verbindet.
5. Entfernung von allen Bridges ohne Designated Port



2) Bestimme RPC für jede Bridge

3) Bestimme Route Bridge Port für alle Bridges

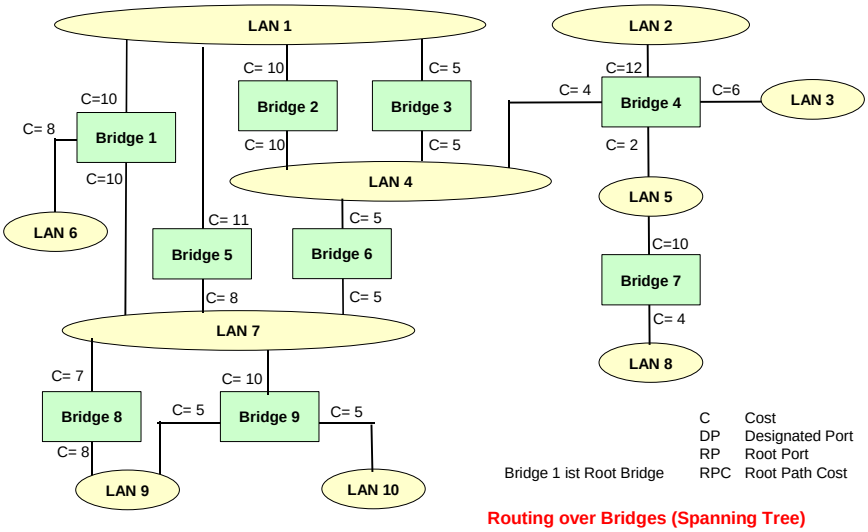
Bild: Beispiel 1:
Spanning Tree Algorithmus (2)



4) Bestimme Designated Port für alle LANs

5) Entferne Bridge falls nicht DP

Bild: Beispiel 1:
Spanning Tree Algorithmus (3)



Routing over Bridges (Spanning Tree)

Bild: Beispiel 2:
Spanning Tree Algorithmus (1)

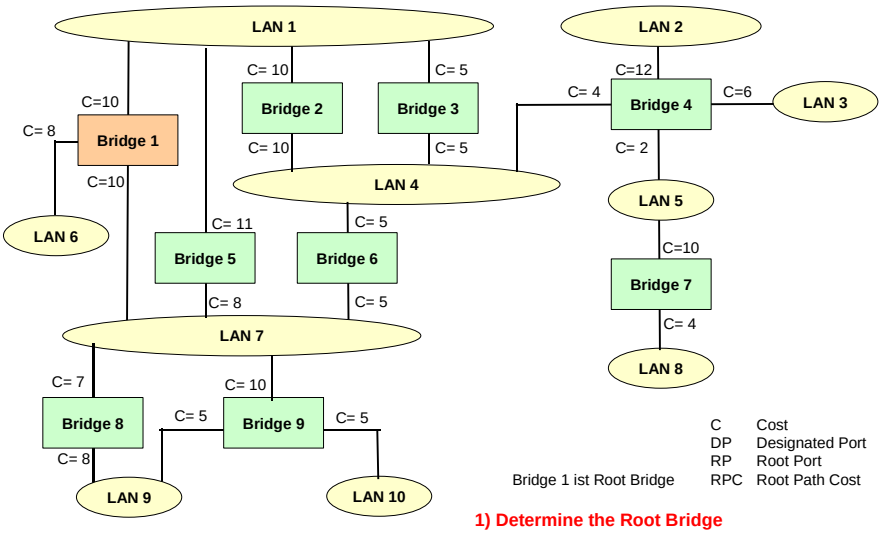


Bild: Beispiel 2:
Spanning Tree Algorithmus (2)

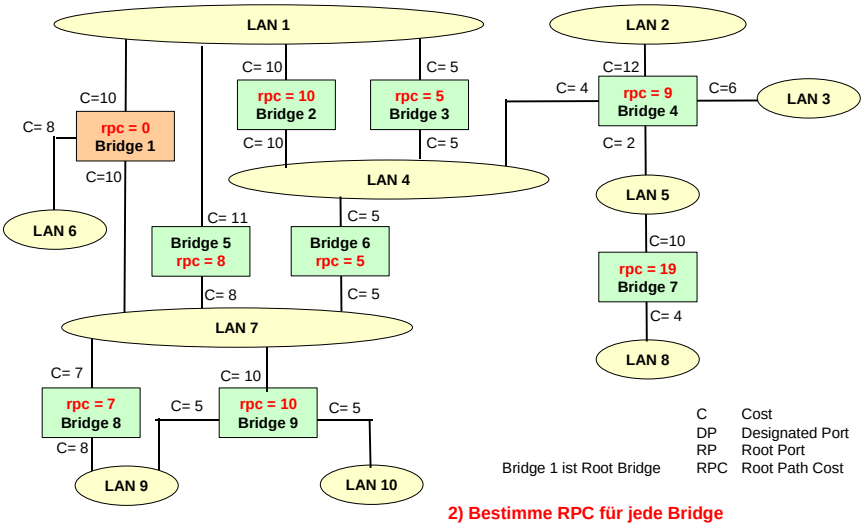


Bild: Beispiel 2:
Spanning Tree Algorithmus (3)

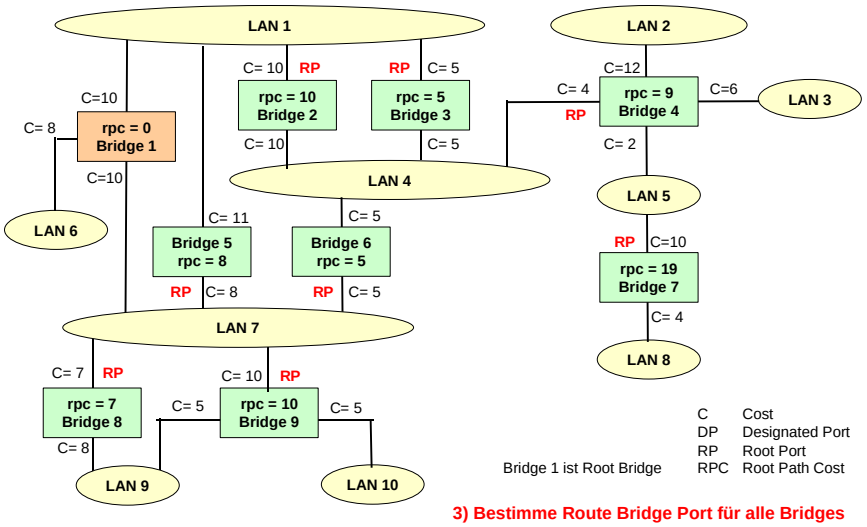
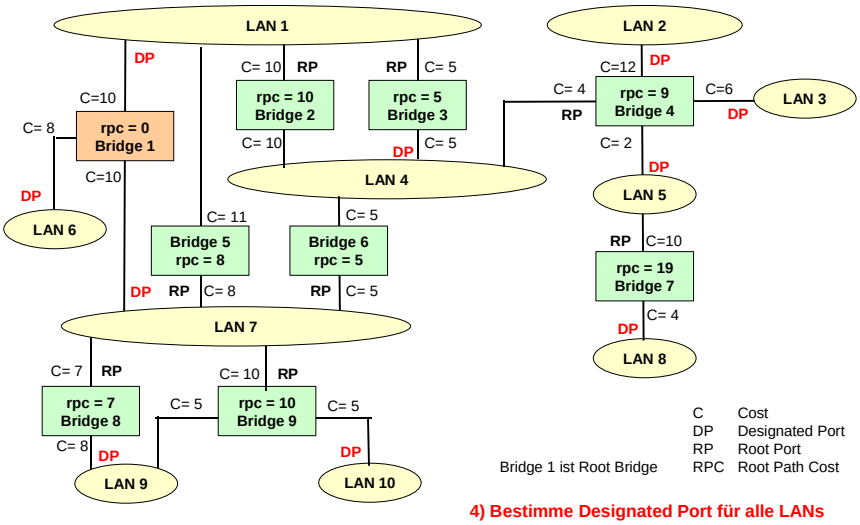
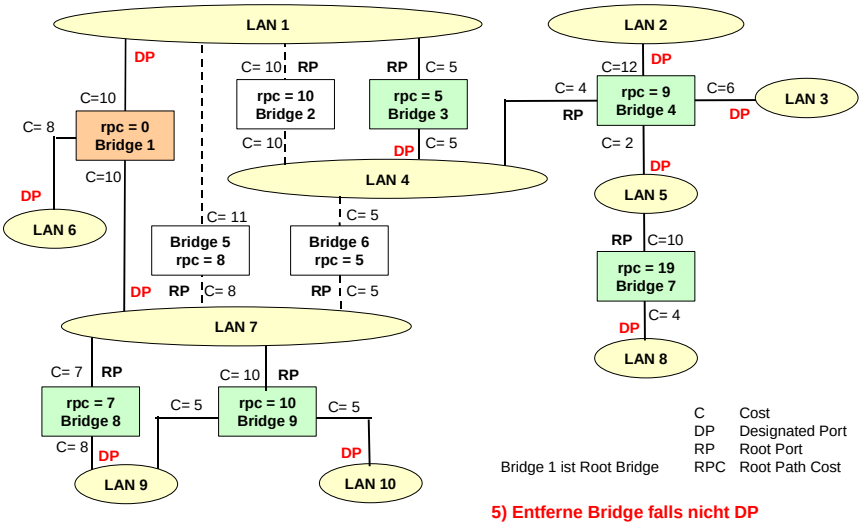


Bild: Beispiel 2:
Spanning Tree Algorithmus (4)



4) Bestimme Designated Port für alle LANs

Bild: Beispiel 2:
Spanning Tree Algorithmus (5)



5) Entferne Bridge falls nicht DP

Bild: Beispiel 2:
Spanning Tree Algorithmus (6)

- Einkapselung von MAC-Dateneinheiten (keine Umsetzung)
- Remote-Bridges treten paarweise auf
- nur zur Kommunikation zwischen LAN 1 und LAN 2
- Transparente Verbindung
- Keine Kommunikation von LAN 1 oder 2 mit dem WAN
- virtuelle Anschlüsse

Bild: Remote Bridges

Remote-Bridges
Bridges werden vorwiegend zum Verbinden von zwei oder mehr entfernten LANs benutzt, z.B. in einem Unternehmen mit Niederlassungen und/oder Fertigungsstätten mit je einem eigenen LAN an verschiedenen Orten. Im Idealfall werden alle LANs miteinander verbunden, um so einen globalen Netzverbund zu realisieren

Dieses Ziel kann erreicht werden, indem man in jedem LAN eine Bridge installiert und die Bridges paarweise über Punkt-zu-Punkt-Leitungen (z.B. Standleitungen des Telefonnetzes) miteinander verbindet. Für die Punkt-zu-Punkt-Leitungen sind verschiedene Protokolle möglich, z. B. ein Standardprotokoll der Sicherungsschicht und das Einfügen kompletter MAC-Rahmen in das Nutzdatenfeld. Diese Strategie Funktioniert am besten, wenn alle LANs identisch sind und die einzige

Aufgabe nur darin besteht, Rahmen zum richtigen LAN zu befördern. Eine andere Alternative wäre das Entfernen des MAC-Headers und -Teilers in der Quell-Bridge, wobei man dann den Rest in das Nutzdatenfeld des Punkt-zu-Punkt-Protokolls einfügt. An der Ziel-Bridge kann dann ein neuer MAC-Header und -Teiler erzeugt werden. Dieser Ansatz hat aber den Nachteil, dass die beim Zielhost ankommende Prüfsumme nicht die ist, die vom Quellhost berechnet wurde. Aus diesem Grund werden eventuell im Bridge-Speicher vorhandene fehlerhafte Bits nicht aufgedeckt.

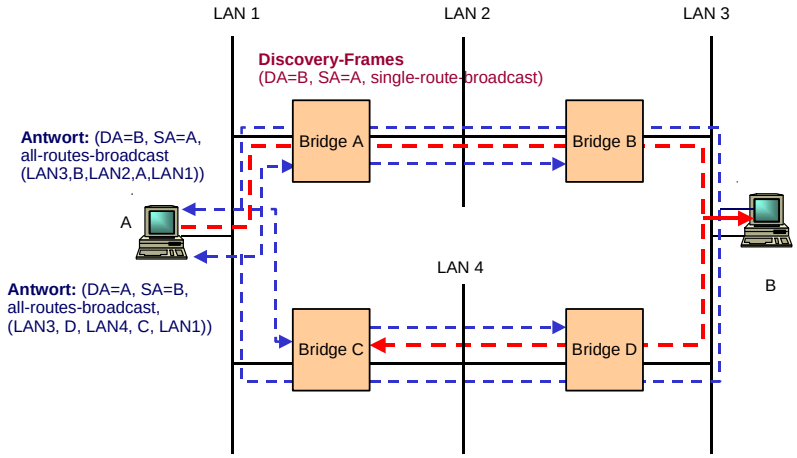


Bild: Source Route Bridging

Source-Routing-Bridges

Transparente Bridges haben den Vorteil der einfachen Installation. Man steckt sie einfach ein. Andererseits nutzen sie die Bandbreite nicht optimal, weil sie nur einen Teil der Topologie (den überspannenden Baum) berücksichtigen. Im wesentlichen basiert Source-Routing auf der Annahme, dass der Sender eines Rahmens weiß, ob sich das Ziel in seinem eigenen LAN befindet. Sendet er einen Rahmen an ein anderes LAN, setzt die Quellmaschine das High-Order-Bit der Quelladresse auf 1. Des weiteren setzt sie in den Rahmen-Header den genauen Pfad, den der Rahmen bereisen muss.

Dieser Pfad wird wie folgt ausgebaut: Jedes LAN hat eine eindeutige, aus 12 Bit bestehende Nummer. Jede Bridge hat eine 4 Bit große Nummer, durch die sie innerhalb ihres LANs eindeutig identifiziert wird. Zwei Bridges, die weit auseinander liegen, können also beide z.B. die Nummer 3 haben, während Bridges im gleichen LAN eindeutig nummeriert werden müssen. Eine Route ist eine Folge von Bridge, LAN, Bridge, LAN, ...Nummern.

Eine Source-Routing-Bridge ist nur an den Rahmen interessiert, bei denen das High-Order-Bit des Ziels auf 1 steht. Erkennt sie einen solchen Rahmen, tastet sie die Route ab und sucht die Nummer des LANs, in dem der Rahmen angekommen ist. Folgt der LAN-Nummer ihre eigene Nummer, gibt die Bridge den Rahmen an das LAN weiter, dessen Nummer nach ihrer Nummer folgt. Folgt der LAN-Nummer die Nummer einer anderen Bridge, leitet sie den Rahmen nicht weiter.

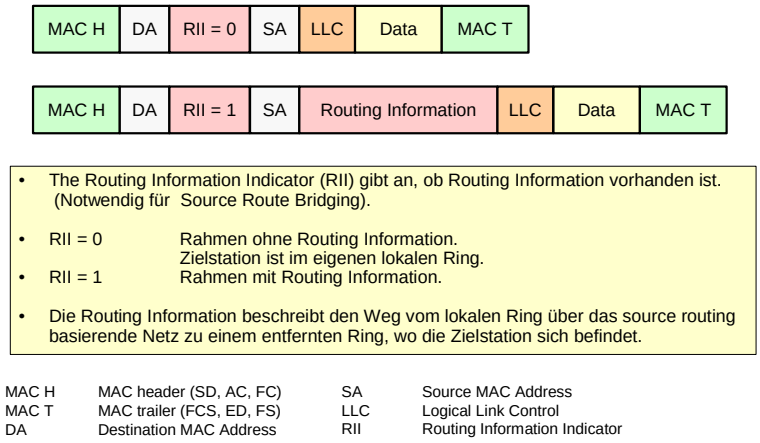
Dieser Algorithmus eignet sich für drei mögliche Implementierungen:

- Software: Die Bridge läuft im Gemischtmodus und kopiert alle Rahmen in ihrem Speicher, um zu sehen, ob das werthöchste Zielbit auf 1 gesetzt wurde. Trifft das zu, wird der Rahmen weiter bearbeitet, andernfalls nicht.
- Hybrid: Die LAN-Schnittstelle der Bridge untersucht das Zielbit und übergibt der Bridge ausschließlich Rahmen mit gesetztem Bit. Diese Schnittstelle kann leicht in die Hardware integriert werden. Sie reduziert die Zahl der von der Bridge zu prüfenden Rahmen.
- Hardware: Die LAN-Schnittstelle untersucht nicht nur das werthöchste Zielbit, sondern sieht auch noch in der Route nach, ob ihre Bridge an der Weitergabe beteiligt ist. Nur Rahmen, die übertragen werden müssen, kommen bei der Bridge an. Diese Implementierung stellt den höchsten Hardware-Aufwand, verringert aber die Anzahl der Durchgänge zwischen CPU und Bridge, da alle irrelevanten Rahmen ausgesondert werden.

Diese drei Implementierungen unterscheiden sich in Preis und Leistung. Bei der ersten entstehen keine zusätzlichen Hardwarekosten für die Schnittstelle, aber es wird eine sehr schnelle CPU für die Bearbeitung aller Rahmen benötigt. Bei der letzten ist ein spezieller VLSI-Chip erforderlich, aber man verlagert so einen Großteil der Rechenarbeit von der Bridge auf den Chip, so dass entweder eine langsamere CPU benutzt werden oder die Bridge mehr LANs bedienen kann.

Beim Source-Routing wird vorausgesetzt, dass jede Maschine des Netzverbunds die Route zu jeder anderen Maschine genau kennt. Wie diese Routen ermittelt werden, ist ein wichtiger Teil des Source-Routing-Algorithmus. Dem Grundkonzept zufolge gibt die Quelle einen Broadcast-Rahmen aus, um herauszufinden, wo sich das Ziel befindet, falls es nicht bekannt ist. Dieser Suchrahmen (Discovery Frame) wird von jeder Bridge gesendet. Er erreicht damit jedes LAN im Netzverbund. Kommt die Antwort zurück, fügen die Bridges ihre Kennung ein, so dass der Sender den zurückgelegten Weg sehen und endgültig die beste Route ermitteln kann.

Hat ein Host einmal einen Weg zu einem bestimmten Ziel gefunden, wird dieser in einem Cache-Speicher abgelegt, so dass der Suchprozeß beim nächsten Mal nicht erneut durchgeführt werden muß. Bei dieser Methode entsteht zwar nicht die oben



beschriebene Rahmenexplosion, sie belastet aber die Hosts mit zusätzlichem Verwaltungsaufwand. Außerdem ist der Algorithmus insgesamt nicht transparent, was ja ursprünglich eines der Hauptziele war.

Der wichtigste Unterschied zwischen den zwei Bridge-Typen ist die Unterscheidung zwischen verbindungsloser und verbindungsorientierter Netztechnik. Die transparente Bridge hat kein Konzept einer virtuellen Verbindung und leitet jeden Rahmen unabhängig von allen übrigen weiter. Demgegenüber ermittelt die Source-Routing-Bridge anhand von Suchrahmen eine geeignete Route und benutzt künftig immer diese Route.

Die transparente Bridge ist für die Hosts völlig unsichtbar und uneingeschränkt mit allen vorhandenen 802-Produkten kompatibel. Die Source-Routing-Bridge ist weder transparent noch kompatibel. Um Source-Routing anwenden zu können, müssen die Hosts das Bridge-Schema kennen und aktiv teilnehmen. Die Aufteilung eines vorhandenen in zwei LANs, die durch eine Source-Routing-Bridge verbunden werden, setzt Änderungen der Host-Software voraus.

Transparente Bridges erfordern kein Netzmanagement. Die Bridges konfigurierten sich selbst automatisch auf die gegebene Topologie. Bei Source-Routing-Bridges muß der Netzmanager die LAN- und Bridge-Nummern manuell konfigurieren. Fehler wie doppelte LAN- oder BridgeNummern lassen sich nur sehr schwer abgrenzen, weil sie verursachen können, dass einige Rahmen in Schleifen kreisen. Zwei vormals getrennte Netze können beim Einsatz von transparenten Bridges beispielsweise direkt miteinander verbunden werden, während beim Source-Routing eventuell viele LAN-Nummern manuell geändert werden müssen.

Einer der wenigen Vorteile der Source-Routing-Bridge ist der, dass sie theoretisch optimales Rouring bietet, während die transparente Bridge auf den Spanning-Tree begrenzt ist. Source-Routing eignet sich auch gut, wenn parallele Bridges eingesetzt werden, um die Belastung auf die LANs aufzuteilen. Die Lokalisierung von Zielen wird bei transparenten Bridges durch das Backward-Learning und bei Source-Routing-Bridges durch Suchrahmen vorgenommen. Backward-Learning hat den Nachteil, dass die Bridge warten muß, bis ein Rahmen von einer bestimmten Station eingeht, um ihre Position zu erfassen. Der Nachteil von Suchrahmen besteht darin, dass sie sich in einem umfangreichen Netzverbund exponentiell vermehren.

Die Handhabung von Störungen unterscheidet sich bei den beiden Verfahren beträchtlich. Transparente Bridges erkennen Störungen auf anderen Bridges und LANs sowie Änderungen der Topologie schnell und automatisch, da sie laufend die Steuerrahmen der verschiedenen Komponenten prüfen. Hosts bekommen diese Änderungen überhaupt nicht mit.

- The Routing Information Indicator (RII) gibt an, ob Routing Information vorhanden ist. (Notwendig für Source Route Bridging).
- RII = 0 Rahmen ohne Routing Information. Zielstation ist im eigenen lokalen Ring.
- RII = 1 Rahmen mit Routing Information.
- Die Routing Information beschreibt den Weg vom lokalen Ring über das source routing basierende Netz zu einem entfernten Ring, wo die Zielstation sich befindet.

MAC H	MAC header (SD, AC, FC)	SA	Source MAC Address
MAC T	MAC trailer (FCS, ED, FS)	LLC	Logical Link Control
DA	Destination MAC Address	RII	Routing Information Indicator

Bild: IEEE 802.5 Rahmenformat mit RII

text text text text text text text text text text text text text text text text text text text text text text text text text text text text text text text

Beim Source-Routing ist die Situation ganz anders. Wenn eine Bridge versagt, nehmen die Stationen, deren Route über sie führt, anfänglich nur wahr, dass ihre Rahmen nicht mehr bestätigt werden. Sie warten das Timeout ab und versuchen es immer wieder. Endlich folgern sie, dass etwas nicht in Ordnung ist. Sie wissen aber immer noch nicht, ob das Problem mit dem Ziel selbst oder mit dem gewählten Weg zusammenhängt. Nur durch die Versendung eines weiteren Suchrahmens erfahren sie, ob das Ziel ansprechbar ist. Wenn unglücklicherweise eine Haupt-Bridge ausfällt, müssen viele Hosts den Ablauf der Timer abwarten und neue Suchrahmen aussenden, bevor das Problem gelöst ist, auch wenn ein alternativer Weg verfügbar ist. Diese höhere Fehleranfälligkeit ist eine der größten Schwächen aller verbindungsorientierten Systeme.

Was die Komplexität und die Kosten anbelangt, bestehen viele Kontroversen. Hat die SourceRouting-Bridge einen VLSI-Chip, der nur die weiterzugebenden Rahmen einliest, hat sie einen etwas niedrigeren Rahmenverarbeitungsaufwand zu bewältigen und bietet im Verhältnis zu den getätigten Hardwareinvestitionen eine bessere Leistung. Ohne diesen Chip schneidet sie schlechter ab, weil dann der Verarbeitungsaufwand pro Rahmen (Ermitteln der Route im Rahmen-Header) wesentlich höher ist.

Source-Routing erhöht auch die Komplexität der Hosts. Sie müssen Routen speichern, Suchrahmen senden und Routeninformationen in jeden Rahmen kopieren. Alle diese Dinge erfordern mehr Speicher und CPU-Leistung. Da eine Installation in der Regel viel mehr Hosts als Bridges umfaßt, erscheint es vorteilhafter, die nötige Komplexität und Mehrkosten in wenigen Bridges als in vielen Hosts zu realisieren.

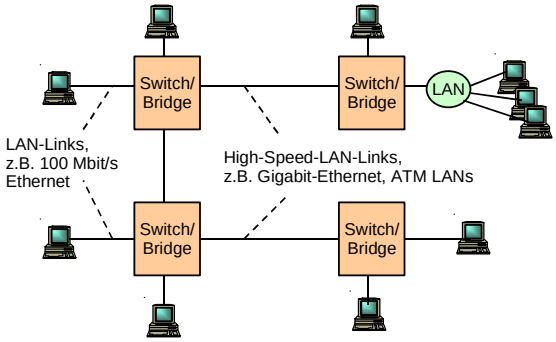


Bild: LAN Switching

Heutige LANs verwenden mehrheitlich Switches an denen dei Rechnerstationen direkt oder Über Ethernet-Kollisionsdomainen angeschlossen sind. Die Swiches sind oft über Gigabit-Ethernet (GbE) Links miteinander verbunden.

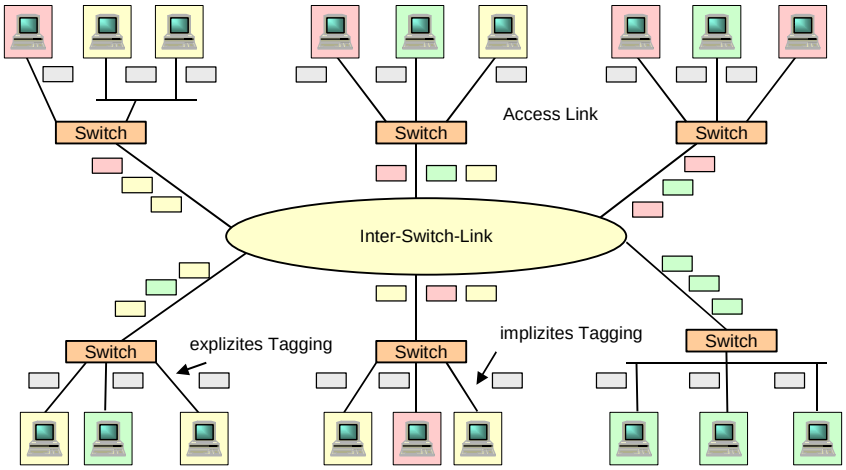


Bild: Virtuelle LANs mit IEEE 802.1Q Tagging

Durch einen sogenannten IEEE 802.1Q Tag können Virtuelle LANs (VLANs) aufgebaut werden. Es gibt verschiedenen Gruppen von Stationen, die zu einem VLAN gehören. Ihre Rahmen werden nur an Stationen innerhalb einer Gruppe weitergeleitet.

- Frame Tagging für Ethernet u. Token Ring
- Paket gehört zu 1 virtuellen LAN (VLAN)
- VLAN = Broadcast-Domäne
- Funktionen zur Konfiguration und Management von VLANs

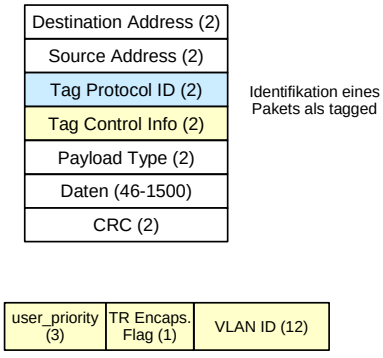
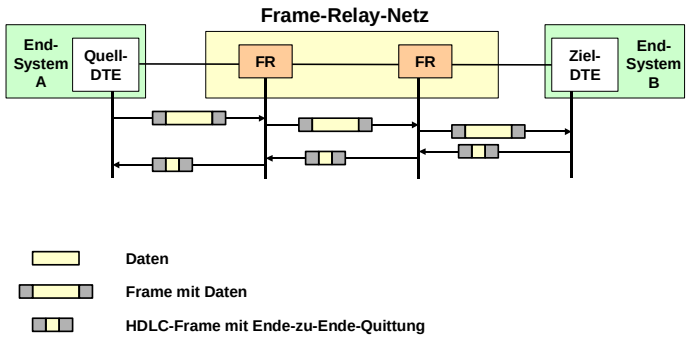


Bild: IEEE 802.1Q

text text text text text text text text text text text text text text text text text text text text text text text text text text text text text text

Frame Relay (FR)



Frame Relay ist ein Rahmenvermittlungsverfahren, das in Schicht 2 abläuft. Rahmen werden nur Ende-zu-Ende quittiert. Rahmen, die in Zwischenknoten als fehlerhaft identifiziert werden, werden verworfen.

Bild: Paketvermittlung in Frame-Relay-Netzen

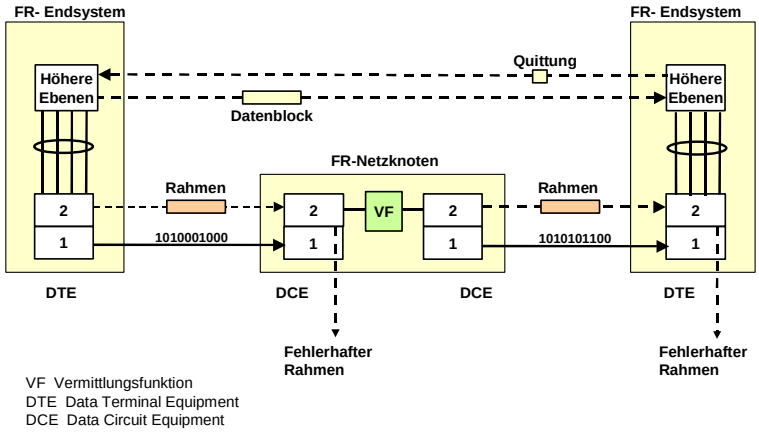
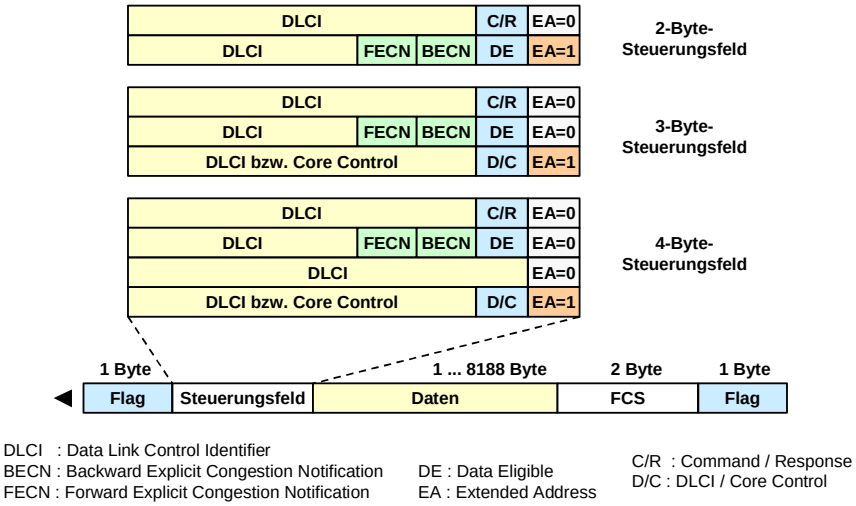


Bild: Paketvermittlung in Frame-Relay-Netzen



Das FR-Protokoll verwendet variabel lange, HDLC-artige Rahmen. Das Adressfeld ist 2 Byte lang (optional auch 3-4 Byte) und enthält neben einigen Bits mit Sonderfunktionen den 10-Bit-DLCI zur Identifikation der virtuellen Verbindung. Damit lassen sich 2^{10} = 1024 logische Kanäle adressieren. Mittels des DLCI wird die Funktion des statistischen Multiplexens auf Schicht 2 durchgeführt. Einige DLCI sind für Sonderaufgaben reserviert, weshalb noch 976 Stück zur Unterscheidung von Benutzerverbindungen bleiben.

Bild: Aufbau des Frame-Relay-Rahmens

FECN: Das FECN-Bit (Forward Explicit Congestion Notification, nach vorn gerichtete Überlastanzeige) kann von einem überlasteten Netz auf 1 gesetzt werden, um dem empfangenden Endgerät anzuzeigen, dass die in seine Richtung übertragenen Rahmen durch überlastete Ressourcen der FR-Netzknoten gelaufen sind. FR-Netzknoten und Endgeräte dürfen das FECN-Bit setzen, kein FR-Netzknoten darf aber ein gesetztes FECN wieder auf 0 zurücksetzen.

BECN: Das BECN-Bit (Backward Explicit Congestion Notification, nach hinten gerichtete Überlastanzeige) kann von einem überlasteten Netz auf 1 gesetzt werden, um dem Endgerät anzuzeigen, dass die von ihm gesendeten Rahmen durch

überlastete Ressourcen gelaufen sind. Wie beim FECN auch, dürfen FR-Netzknoten und Endgeräte das BECN-Bit setzen, kein FR-Netzknoten darf aber ein gesetztes BECN wieder auf 0 zurücksetzen.

DE: Das DE-Bit (Discard Eligibility, Lösch-Priorität) ist im Überlast-Fall von Interesse.

Das DE-Bit wird für zwei verschiedene Zwecke eingesetzt:

- FR-Endgeräte können optional dieses Bit benutzen, um ihre Daten zu priorisieren. Sie zeigen damit den Transitknoten an, welche Daten (DE = 1) diese im Falle einer schweren Überlast bevorzugt verwerfen sollen. Damit wird es wahrscheinlicher, dass wichtigere Daten (DE =0) ihr Ziel erreichen.
- Einige FR-Netzknoten verwenden das DE-Bit, um vom Endgerät empfangene Daten zu markieren, die oberhalb der zwischen Anwender und Netzbetreiber vereinbarten Übertragungskapazität liegen. In diesem Fall setzt der FR-Netzknoten das Bit. Tritt dann irgendwo im Netz akute Überlast auf, so werden zunächst die Rahmen verworfen, die oberhalb der CIR liegen (also DE-markiert sind).

Endgeräte und Netz dürfen also dieses Bit setzen. Das Netz darf jedoch ein vom FR-Endgerät auf 1 gesetztes DE-Bit nicht mehr auf 0 zurücksetzen. Das Netz ist in Überlastsituationen außerdem nicht verpflichtet, nur Frames mit DE = 1 zu verwerfen. In der Praxis bieten die FR-Knoten die Auswertung des DE-Bits als optionale Methode zum selektiven Verwurf an. Ob das Merkmal aktiviert ist oder nicht, muss mit dem jeweiligen Netzbetreiber geklärt werden.

C/R: Das ebenfalls im Adreßfeld stehende C/R-Bit (Command/Response) ist anwendungsspezifisch und wird vom FR-Netz transparent übertragen. Dieses Bit kann von der Applikation dazu verwendet werden, auf ein- und demselben logischen Kanal Steuer- von Benutzer-Informationen zu unterscheiden.

EA: Mittels der EA-Bits (Extended Address) wird die Form des Adreßfelds bestimmt. Neben dem oben dargestellten 2-Byte-Format existieren noch eine 3- und eine 4-Byte-Version, in denen entsprechend mehr DLCI zur Verfügung stehen, die ansonsten aber die gleichen Funktions-Bits enthalten. Da die beim 2-Byte-Adreßfeld möglichen 976 DLCI normalerweise nicht alle benötigt werden, sind die erweiterten Adreßfelder von geringer praktischer Bedeutung.

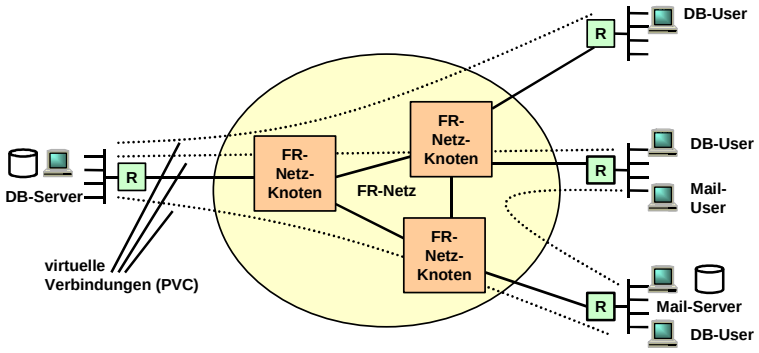


Bild: Endgeräte und FR-Netzknoten

Ein Frame-Relay Netz ermöglicht den dynamischen Auf- und Abbau von logischen Verbindungen.

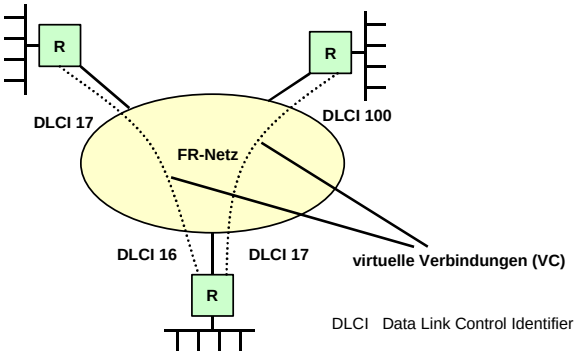


Bild: Bedeutung des DLCI
(Streckenweise Adressierung)

Logische Verbindungen in Frame Relay sind durch eine Reihe von DLCIs (Data Link Control Identifier) gegeben. Jede DLCI hat seine Gültikeit über einen Streckenabschnitt. In jedem FR-Knoten ermöglichen Tabellen den Austausch der Identifier und die entsprechende Weiterleitung der Rahmen zu den richtigen Ausgangsports.

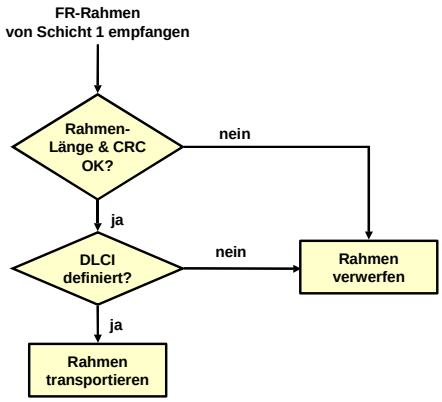
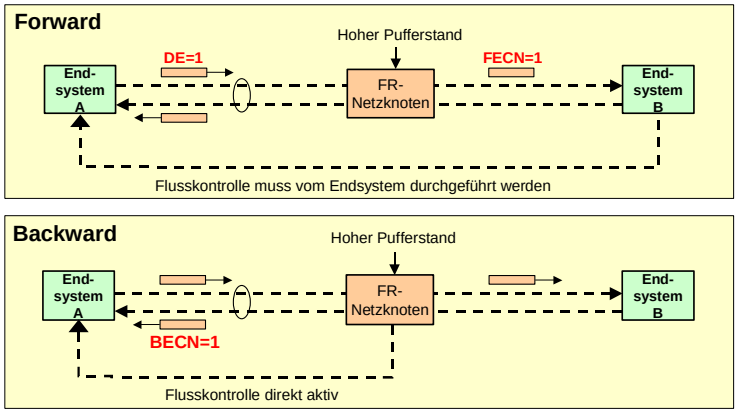


Bild: Flussdiagramm FR-Protokoll

Die Einfachheit der Weiterleitung wird durch ein Flussdiagramm illustriert.

- Prüfung auf Korrektheit der empfangenen Rahmen.
  Verwerfung bei fehlerhaftem Rahmen.
- Prüfung von DLCI des Rahmens.
  Hat der DLCI einen erlaubten (dem Netz bekannten) Wert, so wird der Rahmen gemäß der Routing-Tabelle des Netzknotens weitergeleitet. Bevor der Rahmen dem Empfänger übergeben wird, ändert das FR-Netz noch den DLCI und berechnet den CRC neu.
- Prüfung auf Überlastung des Netzknotens.
  Bei Überlastung können Rahmen verworfen werden

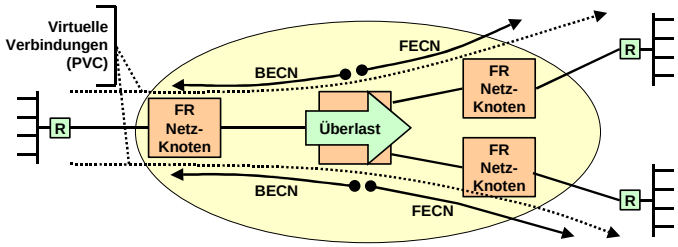
.



BECN : Backward Explicit Congestion Notification
FECN : Forward Explicit Congestion Notification

Bild: Überlastabwehr
Explicit Congestion Notification

Stellt ein FR-Netzknoten die Überschreitung eines bestimmten Auslastungs-Schwellenwerts fest, so wird den betroffenen Endgeräten die möglicherweise bevorstehende Stau-Situation signalisiert. Damit soll diesen die Möglichkeit gegeben werden, den Stau durch die Reduzierung ihrer Datenrate zu verhindern. Es handelt sich nur um eine Überlast-Anzeige, keine Flußsteuerung. Diese Überlast-Anzeige geschieht in beide Richtungen der betroffenen Verbindung mittels zweier Bits des Adressfelds (FECN und BECN).



BECN : Backward Explicit Congestion Notification
FECN : Forward Explicit Congestion Notification

Bild: Überlastabwehr FECN/BECN

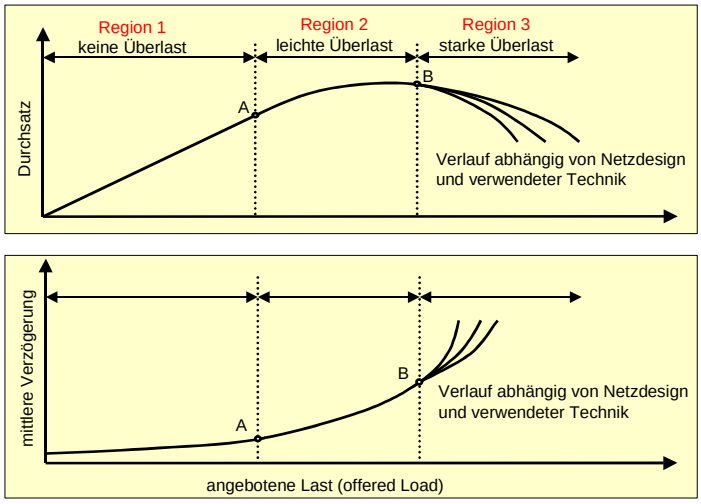


Bild: Durchsatz und Verzögerung bei Überlast

Die Summe des Verkehrs, den alle Endgeräte zu einer bestimmten Zeit ins Netz senden, wird offered Load (angebotene Last) genannt. Bezüglich der Verkehrssituation werden im FR-Netz drei Zustände unterschieden, die mit der angebotenen Last im Zusammenhang stehen.

Im Zustand nicht überlastet ergibt sich bei steigender angebotener Last keine Qualitätsminderung für die Endgeräte. Der Datendurchsatz des Gesamtnetzes erhöht sich linear mit der angebotenen Last.

Ab einem bestimmten Verkehrsaufkommen (Betriebspunkt A) steigt der Gesamtdurchsatz des Netzes jedoch nur noch degressiv. Die Verzögerung der Rahmen im Netz steigt dann überproportional zum Lastwachstum. Die Wahrscheinlichkeit für das Eintreten dieses Zustands kann durch entsprechende Dimensionierung der Übertragungskapazität bei der Netzplanung minimiert werden.

Er kann dennoch in dem seltenen Fall auftreten, dass zufällig viele User gleichzeitig Bursts produzieren. Dann versucht das FR-Netz durch Anwendung der unten beschriebenen Mechanismen zur Überlastbeseitigung (z.B. Setzen von FECN/BECN-Bits) wieder in den nicht überlasteten Bereich zurück zu gelangen.

Steigt die Datenmenge trotzdem weiter, so kann das Netz möglicherweise in den dritten Zustand (schwere Überlast, Betriebspunkt B) eintreten. Hier steigen die Delays der einzelnen Verbindungen weiter an, und der Durchsatz des Gesamtnetzes nimmt trotz steigender Datenmenge ab. Um in den nicht überlasteten Zustand zurückzukehren, müssen etsprechende Überlastabwehrmechanismen eingesetzt werden..

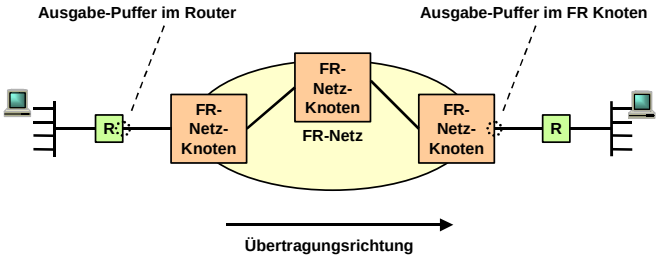


Bild: Staupunkte in Frame-Relay-Netzen