Zusammenfassung M117

Informatik- und Netzinfrastruktur für ein kleines Unternehmen realisieren

2008-11-12

Emanuel Duss

Über

Autor	Emanuel Duss
Erstellt	2008-07-21
Bearbeitet	2008-11-12
Heute	2011-11-28
Bearbeitungszeit	23:57:43
Lehrjahr des Moduls	1. Lehjahr 2006/2007
Pfad	/ home/emanuel/discordia/Daten/Lehre/Zwischenprüfungen/Zusammenfassungen_von_mir/M117/M117_Zusammenfassung.odt
CC-Lizenz	 Creative Commons Namensnennung-Keine kommerzielle Nutzung-Weitergabe unter gleichen Bedingungen 2.5 Schweiz http://creativecommons.org/licenses/by-nc-sa/2.5/ch/
Powered by	

Bearbeitungsprotokoll

Datum	Änderung(en)
2008-07-21	Erstellt
2008-08-13	Was noch fehlte ergänzt.
2008-09-02	Fertigstellung der Zusammenfassung

Inhaltsverzeichnis

Modulbaukasten

Modulidentifikation

Modulnummer	117
Titel	Informatik- und Netzinfrastruktur für ein kleines Unternehmen realisieren
Kompetenz	Peer to Peer Netzwerk mit bis zu 10 Anschlüssen installieren.
Handlungsziele	1. Mit dem Auftraggeber die Anforderungen an das zu installierende Netzwerk aufnehmen und die gewünschten Dienste/Services bestimmen (File, Print, Internet). 2. Logischen und physischen Aufbau des Netzwerks gemäss betrieblichen Anforderungen und räumlichen Verhältnissen definieren und in einem Netzwerkschema und einem Verkabelungsplan abbilden. 3. Arbeitsschritte für die Installation und Konfiguration planen, die den Aufbau des Netzwerks und die baulichen Verhältnisse berücksichtigen. 4. Physisches Netzwerk aufbauen und die Netzwerkkomponenten gemäss Herstellerdokumentationen installieren und konfigurieren. 5. Ressourcenverwaltung (Gruppen, Shares) und File-/ Printsharing definieren und dabei die Vorgaben hinsichtlich Datensicherheit und Verfügbarkeit berücksichtigen. 6. Netzwerk und angeschlossene Systeme testen und die Testergebnisse dokumentieren.
Kompetenzfeld	Network Management
Objekt	Peer to Peer Netz mit Internetanschluss, das Computer und Drucker in verschiedenen Räumen des gleichen Gebäudes miteinander verbindet.
Niveau	1
Voraussetzungen	Personalcomputer in Betrieb nehmen
Anzahl Lektionen	40
Anerkennung	Eidg. Fähigkeitszeugnis Informatiker/Informatikerin
Modulversion	1.1
MBK Release	R3
Harmonisiert am	04.10.2004

Handlungsnotwendige Kenntnisse

Handlungsnotwendige Kenntnisse beschreiben Wissenselemente, die das Erreichen einzelner Handlungsziele eines Moduls unterstützen. Die Beschreibung dient zur Orientierung und hat empfehlenden Charakter. Die Konkretisierung der Lernziele und des Lernwegs für den Kompetenzerwerb sind Sache der Bildungsanbieter.

Modulnummer	117
Titel	Informatik- und Netzinfrastruktur für ein kleines Unternehmen realisieren
Kompetenzfeld	Network Management
Modulversion	1.1
MBK Release	R3

Handlungsziel	Handlungsnotwendige Kenntnisse
1.	1. Kennt die verbreiteten Netzwerkdienste und kann aufzeigen, welche Anforderungen an ein Netzwerk sich daraus ergeben.
2.	1. Kennt die grundsätzlichen Informationen, die aus einem einfachen Netzwerkschema hervorgehen müssen und kann aufzeigen, wie diese in einem Diagramm abgebildet werden können. 2. Kennt die wichtigsten Regeln für eine korrekte IP Adressierung (Format, Subnetmaske, Klassen, private Adressen) und kann diese anhand von Beispielen erläutern. 3. Kennt die prinzipiellen Aufgaben der Netzwerkkomponenten Switch und Router und kann aufzeigen, wo und zu welchem Zweck diese in einem Netzwerk eingesetzt werden. 4. Kennt die verbreiteten technologischen Möglichkeiten zur Erstellung eines Internetzugangs und kann erläutern, welche Konsequenzen diese für die Nutzung des Internets und die daraus resultierenden Kosten haben. 5. Kennt gängige Kabeltypen, Steckertypen und Ethernet-Varianten (Twisted Pair, UTP, STP, Glasfaser, RJ45, 100BaseTX, 100BaseFX, 1000BaseTX etc.) und kann aufzeigen, bei welche Anforderungen hinsichtlich Leistung und bei welchen räumlichen Gegebenheiten diese zum Einsatz kommen.
3.	1. Kennt relevante bauliche Gegebenheiten und Installationsmöglichkeiten hinsichtlich der Netzwerk-Verkabelung und kann deren Auswirkungen auf Installationsaufwand, Zugänglichkeit für den Unterhalt und Kosten aufzeigen.
4.	1. Kennt die notwendigen Einstellungen der Netzwerkkonfiguration und kann aufzeigen, welchen Beitrag diese zur Sicherstellung der Kommunikation im Netzwerk leisten.
5.	1. Kennt die prinzipiellen Vorkehrungen, die Netzwerkbetriebssysteme für die Ressourcenzuteilung bieten (Lese-, Schreibrecht, Benutzer, Benutzergruppen, Shares) und kann aufzeigen, wie diese die Sicherheit von Daten gewährleisten. 2. Kennt Möglichkeiten, die Vergabe von Rechten zu dokumentieren (z.B. Matrix der Beziehungen zwischen Benutzergruppen und Shares) und kann aufzeigen, wie damit eine korrekte Vergabe der Rechte erleichtert wird.
6.	1. Kennt die Symptome der wichtigsten Fehler in einem Netzwerk und kann mögliche Ursachen (Konfigurationsfehler, Fehler bei der Verkabelung etc.) dafür beschreiben. 2. Kennt die wichtigsten Informationen in der Dokumentation eines einfachen Netzwerks und kann erläutern, wie diese für die Wartung und den Betrieb benötigt werden. 3. Kennt den Zweck und die Funktionen des OSI Schichtenmodells und kann Protokolle sowie Netzwerkkomponenten den entsprechenden Schichten zuordnen.

1 OSI-Referenzmodell

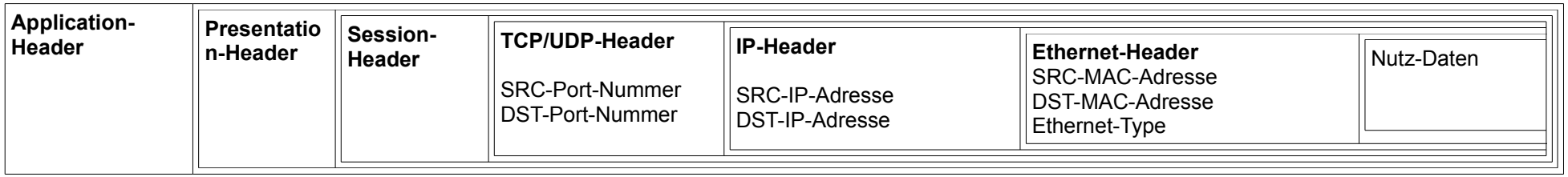
1.1 Zweck

- Mit dem ISO/OSI-Modell kann man in einem Netzwerk systematisch nach Fehlern suchen. Dabei beginnt man von unten und arbeitet sich nach oben.
- Die Schichten werden durch genau definierte Schnittstellen abgegrenzt.
- Jede Schicht bietet der darunter liegenden Schicht bestimmte Dienste an.
- Eine Schicht kann das Daten der darunter liegenden Schicht empfangen oder der darunter liegenden Schicht weiterleiten.

1.2 Übersicht über das OSI-Referenzmodell

#	Layer EN	Layer DE	Einordnung	Funktion	Abhängig	Adressierung	Protokolle	HW
7	Application Layer	Applikationsschicht	Anwendungsorientiert	Netzwerktransparenz für User. Netwerkmanagement. Bereitstellung von Diensten.	Hardware unabhängig		HTTP, FTP, DNS, SMTP, POP3, ...	
6	Persentation Layer	Darstellungsschicht		Konvertierung der ausgetauschten Daten in eine systemunabhängige Form (Umsetzung der Syntax) zur Sicherstellung der wechselseitig richtigen Interpretation. Datenkompression			HTML / XML	
5	Session-Layer	Sitzungsschicht		Auf- und Abbau einer Dialogverbindung (Login auf Webpage). Steuerung des Dialogs: wer wann wie lange sendet. Setzen von Synchronisationspunkten			SMB	
4	Transport Layer	Transportschicht	Transportorientiert	Unterstützung einer zuverlässigen Ende-zu-Ende-Verbindung zwischen Prozessen (Transportdienstbenutzer) auf den Endsystemen. Formelle Aushandlung der Verbindungsbeziehung zwischen Client und Server (über Port). Fehlerkontrolle bei TCP.		Portnummer	TCP / UDP	Firewall
3	Network Layer	Vermittlungsschicht		Weiterleitung der Datenpakete zwischen den einzelnen Netzwerken (WAN, Internet). Adressierung von Computern mit IP-Adressen. Routing von Daten. Adressierung von PCs mit IP-Adressen. Umsetzung von HW-Adressen in IP-Adressen.		IP-Adresse	IP-Protocol ARP	Router, Layer-3-Switch
2	Data Link Layer	Sicherungsschicht		Aufteilung der Bitströme in Frames. Behandlung von Übertragungsfehlern. Regelung des Zugriffs auf das gemeinsam genutzte Übertragungsmedium. Sublayer: LLC und MAC	Hardwareabhängig	MAC-Adresse	z.B. IEEE 802.3 für Ethernet	Switch, Bridge
1	Physical Layer	Bitübertragungsschicht		Übertragung von Bitströmen; Festlegung einer Übertragungsrate für die Bitsynchronisation; Darstellung der Bits mit Leitungscodes (elektrische oder optische Signale)			Kabeltypen, Übertragungsraten	Hub, Repeater

1.3 Datagrammbildung



2 Layer 1: Physical Layer

2.1 Signalausbreitung

Übertragungsrate

- Die Übertragungsrate gibt an, wie viele Bits pro Sekunde übertragen werden können.
- Masseinheit: Bits / Sekunde = bps; Kbits / Sekunde = kbps; Mbits / Sekunde = Mbps; etc...
- Übertragungsrate ist nicht das selbe wie die Bandbreite!

Signalbandbreite

- Je mehr Informationen pro Sekunde übertragen werden soll, desto kürzer sind die Signalimpulse und desto grösser ist die Bandbreite!

Kanalbandbreite

- Frequenzbereich, der das Übertragungsmedium unterstützt.
- Die Kabelkategorien geben den Frequenzbereich an.
- Ist die Frequenz zu gross, können die Daten nicht übertragen werden.

2.1.1 Beeinträchtigung der Signalausbreitung

Dämpfung der Signale

- Die maximale Länge eines Twisted Pair Kabels darf nicht überschritten werden, weil dann ein stabiles Funktionieren nicht garantiert werden kann. Die Netzwerkkomponenten werden dann ausserhalb der Spezifikation betrieben.
- Bei WAN-Strecken ist dies auch so. Man muss dafür sorgen, dass der Signalpegel incht unterschritten wird.
- In den Datenblättern der Kupfer- oder Glasfaserkabel entnimmt man die Dämpfungswerte. Diese ist für eine bestimmte Längenheinheit in Dezibel angegeben.

Dispersion der Signale

- Wenn sich mehrere Frequenzen überlagern, spricht man von Dispersion.
- Das kann vorkommen, wenn sich zwei unterschiedlich schnelle Frequenzen im Übertragungsmedium überschneiden.

Reflektion an Leitungsabschlüssen

- Diese Störung ist nur bei der Bustechnologie anzutreffen (mehrere Computer an einem Kabel)

- Am Ende des Kabels wird das Signal reflektiert und zurückgegeben. Dabei stört es andere Signale.
- Das kann mit Abschlusswiederstände verhindert werden.

Stand der Technik

- Die Qualität steigt von Jahr zu Jahr.
- Twisted Pair Kabel werden in Kategorien eingeteilt

2.1.2 Basisband- und Breitbandübertragung

Basisbandübertragung

- Gesamte Kanalbreite eines Übertragungsmediums wird für eine einzige bitserielle Übertragung eingesetzt.
- Twisted Pair funktioniert auf Basisbandübertragung. Daher die Bezeichnung „Base“.
- IEEE 802.3 ist eine typische Basisbandübertragung.

Breitbandübertragung

- Die verfügbare Kanalbreite wird auf mehrere separate bitserielle Datenströme aufgeteilt.
- Ein einziger Datenstrom kann nur einen Teil der verfügbaren Kanalbandbreite nutzen.
- Die Breitbandübertragung wird in WANs eingesetzt.
- ADSL läuft über die Breitbandübertragung. Die Daten werden auf mehrere, bitserielle Datenströme aufgeteilt.
- Die Kanalbandbreite von Glasfaserkabeln ist riesig. Daher wird die Kanalbandbreite in viele Datenströme aufgeteilt. Es werden Lichtimpulse mit unterschiedlichen Wellenlängen eingespiesen.

2.2 Signalisierung von Bitströmen im Kabel

2.2.1 Verschiedene Kodierungen

NRZ-Kodierung

- NRZ = Non Return to Zero (kein Signal bei 0)
- Einfache Binärkodierung
- Immer im selben Takt wird bei 1 ein Signal gesendet.
- Nur schlecht einsetzbar, da der Empfänger den Takt kennen muss.
- Auf Systemplatinen gut einsetzbar
- In der Netzwerktechnik nicht einsetzbar.

Manchester Kodierung

- Die Manchester-Kodierung wurde bei Ethernet-LANs auf Koaxialkabeln eingesetzt.
- Empfangs-Netzwerk-Karte kann den Sendetakt zurückrechnen.
- Kanalbandbreite steigt auf das doppelte der NRZ-Kodierung
- 0 Bit → fallende Signalflanke
- 1 Bit → steigende Signalflanke

MLT-3 Kodierung

- Multilevel Transmission Encoding – 3 Levels (Mehrere Stufen Kodierung – 3 Stufen)
- Wird beim heutigen weit verbreiteten Ethernet-Standard 100BaseTX verwendet.
- Benötigt drei Spannungspegel (+ / 0 / -) → ternäres Signal
- Bei 1 ändert im Datenstrom der Signalpegel. Bei 0 geschieht nichts. Es geht dabei immer rauf und runter.
- Wenn nur Nullen übertragen werden, ändert sich auf der Leitung logischerweise gar nichts.

4B5B Kodierung

- Bei dieser Kodierung werden lange „0“- oder „1“-Folgen vermieden, die die Taktrückgewinnung erschweren könnten.
- Es werden 4 Daten-Bit in 5 Signal-Bit codiert. Dabei darf es nicht mehr als eine führende 0 und nicht mehr als zwei abschliessende 0 geben.
- Nibble wird auch Halbbyte genannt.
- Bedingt durch das Einfügen von Redundanz erreicht man nur eine Effizienz von 80% (4/5).

Klardaten (4-Bit Nibble)	Kodierte Daten (5-Bit Codon)
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111

1100	11010
1101	11011
1110	11100
1111	11101

In der Tabelle kann man erkennen, dass nun nur noch zwei 0-Bit Werte hintereinander übertragen werden müssen. Diese Codebits werden nicht direkt übertragen, sondern weitercodiert und mit z.B. MLT-3 übertragen.

2.2.2 Übersicht der Codes und grafische Darstellung

Codenamen	0	1
Non Return to Zero (NRZ) Code	elektrisch: Pegel tief; optisch: kein Licht	elektrisch: Pegel hoch; optisch: Licht
Non Return to Zero Inverted (NRZI) Code	elektrisch: kein Pegelwechsel; optisch: kein Zustandswechsel	elektrisch: Pegelwechsel zum Taktbeginn; optisch: Zustand ändern (Licht / kein Licht)
Multi-Level Transition (MLT-3) Code	elektrisch: kein Pegelwechsel	elektrisch: Pegelwechsel von negativ nach 0 oder von 0 nach positiv (falls zuvor negativ); Pegelwechsel von positiv nach 0 oder von 0 nach negativ (falls zuvor positiv)
Manchester Code	elektrisch: Pegel positiv und Polaritätswechsel von positiv nach negativ in der Taktmitte	elektrisch: Pegel negativ und Polaritätswechsel von negativ nach positiv in der Taktmitte

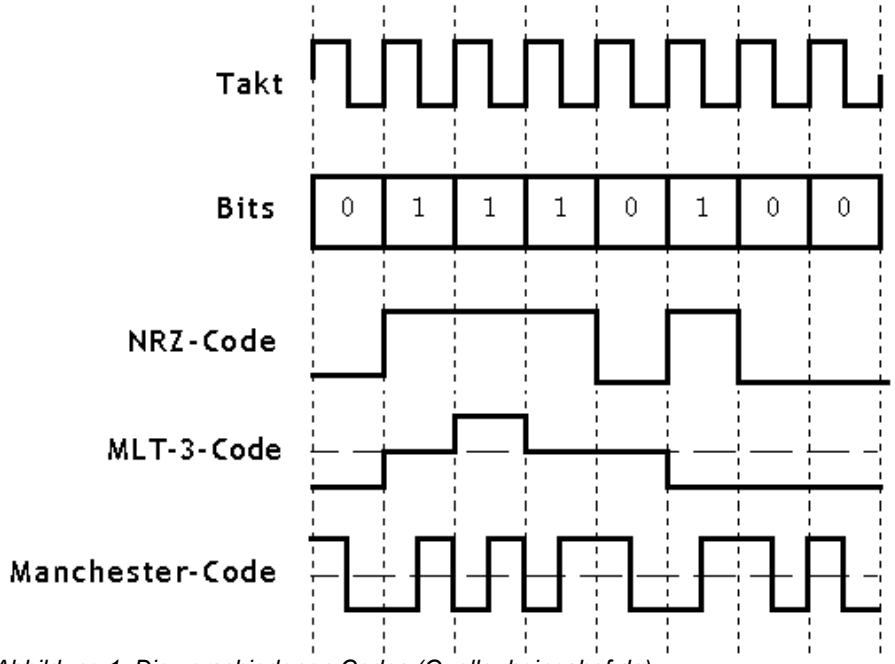


Abbildung 1: Die verschiedenen Codes (Quelle: heineshof.de)

2.3 Autonegotation

2.3.1 Funktion

- Zur Konfiguration von Netzwerkkarten

- Automatische Aushandlung von:
  - höchst mögliche Übertragungsrate
  - das Duplex-Verfahren
  - Möglichkeit der Flusskontrolle
- Arbeitet auf OSI-Layer 1
- Arbeitet mit speziellen Pulsen (Autonegotations-Signale)

Übertragungsraten

- Ethernet arbeitet mit den Übertragungsraten 10 Mbps, 100 Mbps oder 1000 Mbps (1 Gbps)

Halbduplex

- Von einer Netzwerkkarte kann gleichzeitig nur ein Ethernet-Frame empfangen oder nur eines gesendet werden.

Vollduplex

- Eine Netzwerkkarte kann gleichzeitig ein Ethernet-Frame empfangen und ein anderes senden.
- Vollduplex erfordert Software auf dem Layer 2.

Flusskontrolle

- Durch aussenden und empfangen von Pause-Frames kann man den Datenfluss steuern.
- Ein Überlauf des internen Puffers wird verhindert
- Erfordert Software auf dem Layer 2.

2.3.2 Generieren von Autonegotations-Signale

Lormal Link Pulse

- Informationsaustausch der Autonegotation findet über NLP statt.
- In 10BaseT werden periodisch Pulse ausgesendet.
- Stellt fest, ob die Verbindung aktiv ist und ob Daten fliessen können.
- Alle 16 ms wird ein NLP ausgesendet.
- Empfängt die gegenüberliegende Karte währende 50 ms bis 150 ms keinen NLP, gilt die Verbindung als unterbrochen.
- Erhält der Empfänger wieder 2 bis 10 NLPs, ist die Verbindung wieder aktiviert.

Fast Link Pulse

- Für Twisted Pair Netzwerke
- Erweiterte Form von NLP.
- Erkennt automatisch Ethernet-Variante und Geschwindigkeit.

Link Code Word

- Enthält erforderliche Informationen um Übertragungsrate & Duplex-Modus einzustellen.

> Viel genauere Infos zu Autonegotation findet man im Skript vom Lehrer auf Seite 18 – 22.

2.4 Verkabelung

Ein Netzwerkkabel ist ein leitungsgebundenes Übertragungsmedium, bei dem Daten in Form von elektrischen Impulsen oder Lichtsignale übertragen werden.

2.4.1 Koaxialkabel

- Bei Koaxialkabel verwendet man die BUS-Topologie.
- Es kamen zwei Typen von Koaxialkabel zum Einsatz.

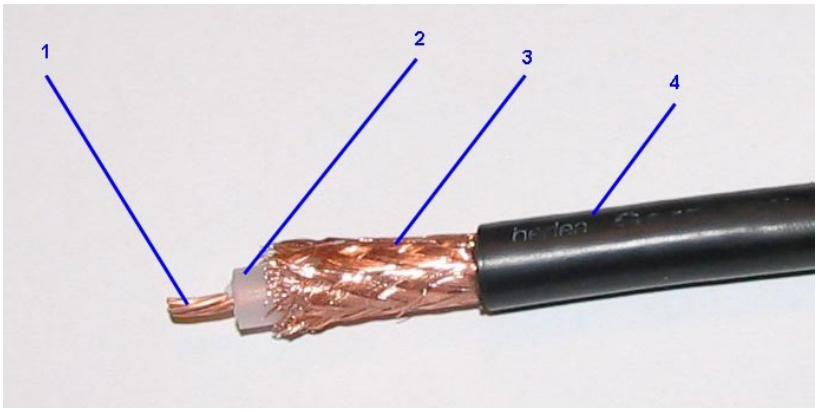


Abbildung 2: Koaxialkabel

1. Seele beziehungsweise Innenleiter
2. Isolation beziehungsweise Dielektrikum zwischen Innenleiter und Kabelschirm
3. Außenleiter (hier einmal ausgeführt)
4. Schutzmantel

Thick Ethernet – 10Base5

- 10Base5: (**10** Mbit/s, **Base**band (Basisband), **5**00 Meter Reichweite)
- Auch bekannt unter Yellow Cable, Thicknet oder Thickwire.
- Eine der ersten Ethernet Netwerktechnologien.
- 10mm dickes Koaxialkabel (RG8) mit einem Wellenwiederstand von 50 Ohm verwendet.
- Zum Anschluss an das Kabel muss ein Loch in das Kabel gebohrt werden. Dieses wird dann mit einer Spezialklemme des Transceivers eingeführt und fest geklammert.
- Der Computer wird am Transceiver angeschlossen.

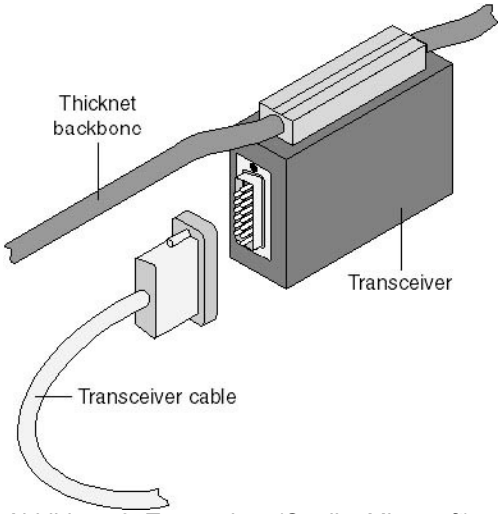


Abbildung 3: Transceiver (Quelle: Microsoft)

Thin Ethernet – 10Base2

- Auch Cheapernet genannt
- Weiterentwicklung von ThickEthernet
- Dünnes Koaxialkabel
- Zum Verbinden werden T-Verbindungsstecker verwendet.
- Deutlich flexibler zum Verkabeln.
- Daher konnte es sich z.B. gegen TokenRing von IBM durchsetzen.

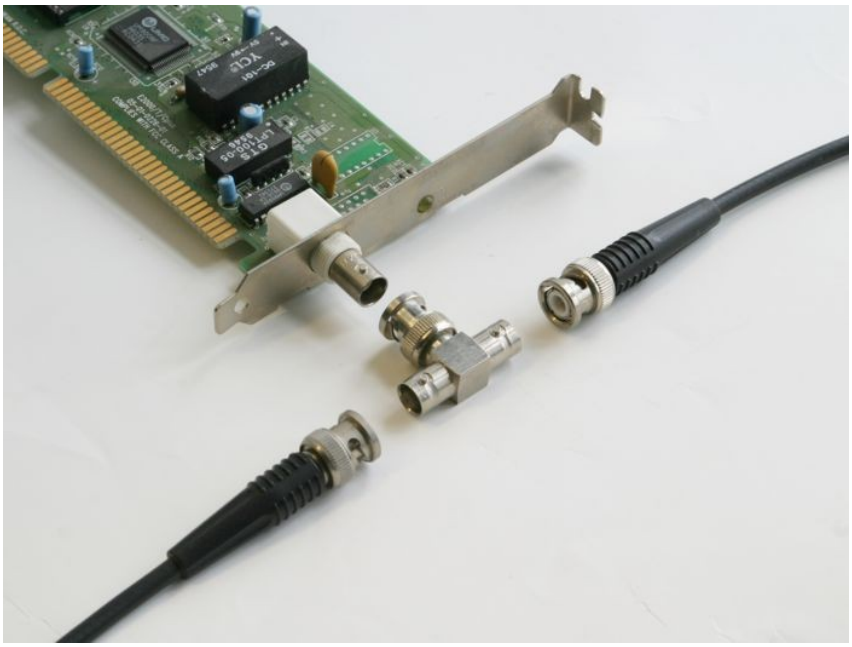


Abbildung 4: Thin Ethernet (Quelle: www.hbernstaedt.de)

2.4.2 Twisted Pair

Kategorien

Cat1	Frequenz: bis 100 kHz für die Datenübertragung ungeeignet. Verwendung: Sprachübertragung (Telefon).
Cat2	Frequenz bis 1 oder 1.5 MHz Verwendung: Hausverkabelung beim ISDN-Primärmultiplexanschluss
Cat3	Frequenz: bis 16 MHz Übertragungskapazität: bis 16 Mbit/s Häufig in den USA eingesetzt, nicht abgeschirmt, wird nicht mehr verkauft
Cat4	Häufig in den USA; nur kleinen Fortschritt zu Cat-3. Übertragungskapazität: 20Mbit/s
Cat5	Am meisten verbreitet; für Signalübertragung mit hohen Datenübertragungsraten bei strukturierten Verkabelungen von Computernetzwerken z.B. für Fast- oder Gigabit-Ethernet. Hat Verbreitung von 1000Base-T (Gigabit-Ethernet) gefördert.
Cat5e	Genauer spezifiziert von Cat-5. Wird im deutschen Raum eingesetzt. Für Langstrecken-100Base-T-Netzwerke. Die meisten Cat-5 Installationen erfüllen auch die Norm Cat-5e.
Cat6	Frequenz: bis 250 MHz Bei grösseren Längen leidet die Übertragungsgeschwindigkeit. Verwendung: für Sprach- und Datenübertragung und Multimedia und ATM-Netze Leistungsfähiger sind: Cat6e (500 MHz) und Cat6a (625 MHz)
Cat7	Frequenz: 600 MHz Vier einzeln abgeschirmte Adernpare (S/STP). Norm IEEE 802.3an (ist für 10 Gigabit geeignet). Die Stecker GG-45 sind abwärtskompatibel, dann wird aber höchstens Cat-6 erreicht.

Durch die Kodierung ist es möglich ein Gigabit Ethernet über ein Cat5e-Kabel zu übertragen.

Datenübertragungsrate bei den Kategorien

Cat-1	Alarmsysteme, analoge Sprachübertragung	UTP-Kabel
Cat-2	Sprache und serielle Schnittstellen	UTP-Kabel
Cat-3	10 Mbps	UTP- und STP-Kabel
Cat-4	16 Mbps	UTP- und STP-Kabel
Cat-5	100 Mbps	UTP- und STP-Kabel
Cat-6	250 Mbps	STP-Kabel

Aufbau von Twisted Pair

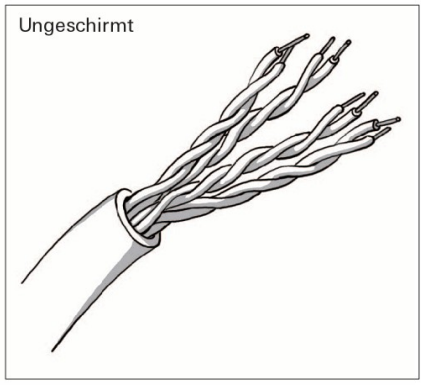
Warum sind die Kabel verdreht? → Um die elektromagnetischen Felder aufzuheben.

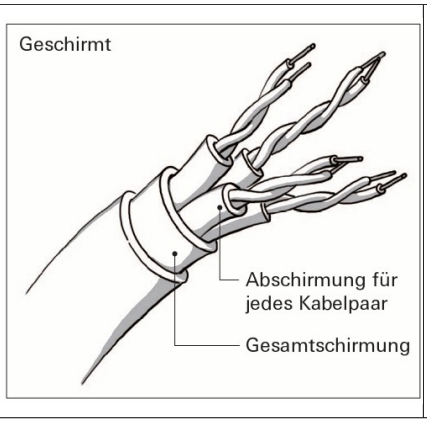
Die verschiedenen Kabeltypen unterscheiden sich vor allem in der Art der Schirmung.

XX/YTP	Die Norm ISO/IEC-11801 (2002) beschreibt die Bezeichnung mit dem Schema.
XX für die Gesamtschirmung	U = Ungeschirmt

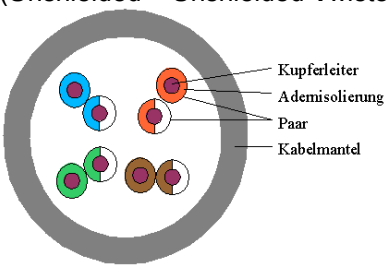
	F = Foliengeschirmt S = Geflechtschirm SF = Geflecht- und Folienschirm
Y für Aderpaarschirmung	U = Ungeschirmt F = Foliengeschirmt S = Geflechtschirm
TP	TP = Immer für Twisted Pair

Beispiele

<table>
<tr>
<td> 

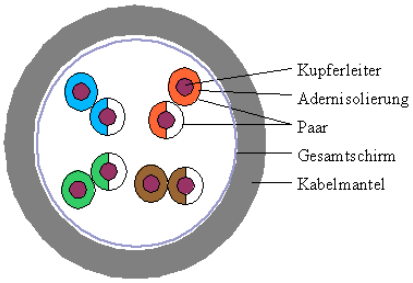

</td>
<td>4 x 2 Kupferdrähte
Paarweise verdrillt
ungeschirmt oder geschirmt
0.5 oder 0.6 mm dick
Distanz: 0.6 bis 100 m
(zwischen 2 Arbeitsstationen)</td>
</tr>
</table>

U/UTP
(**U**nshielded – **U**nshielded **T**wisted **P**air)



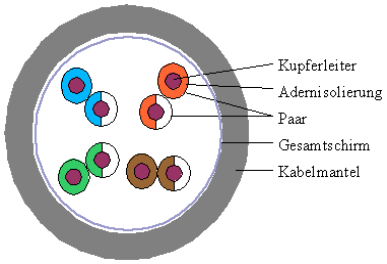
2 Kupferadern, paarweise ohne Abschirmung verdreht

S/UTP
(**S**creened – **U**nshielded **T**wisted **P**air)



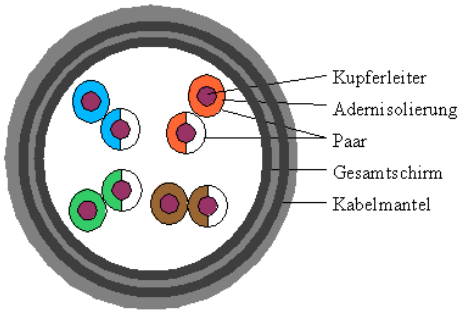
Gesamtschirm aus Kupfergeflecht

F/UTP
(**F**olshielded - **U**nshielded **T**wisted **P**air)



Gesamtschirm aus alukaschierter Kunststoff-Folie

SF/UTP
(**S**creened, **F**olshielded – **U**nshielded **T**wisted **P**air)

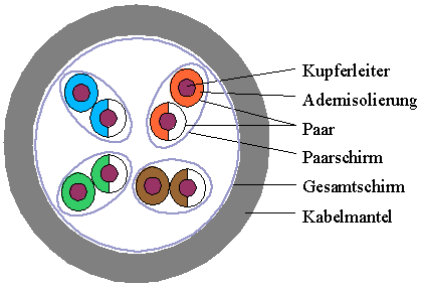


Gesamtschirm aus alukaschierter Polyesterfolie mit darüberliegendem Kupfergeflecht

S/STP
(**S**creened – **S**hielded **T**wisted **P**air)

PiMF-Kabel

Kabel bei dem die Adern paarweise in Metallfolie

 Abschirmung für jedes Kabelpaar sowie Gesamtabschirmung. Störeinflüsse werden optimal unterdrückt und Störungen zwischen den Adernpaaren gegenseitig verhindert.	geschirmt sind. PiMf-Kabel kann als Datenkabel und als Kabel in der Telekommunikation eingesetzt werden. Es ist als Verlegekabel und Patchkabel erhältlich. PiMf-Kabel wird mitunter auch Screened/Shielded Twisted Pair (S/STP) oder Screened/Foiled Twisted Pair (S/FTP) bezeichnet.

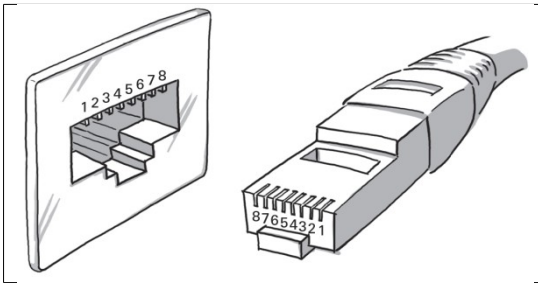
Patchkabel vs. Verlegekabel

Patchkabel	Verlegekabel
● Leiter bestehen aus dünnen Einzeldrähten (Litze) ● Kabel ist flexibel ● Verbindung zwischen Bodendose und Endgerät ● Stecker werden mittels Crimpzange mit dem Kabel verbunden.	● Leiter ist ein einzelner Draht. ● Kabel ist recht starr ● Kabel wird mittels Schneidklemmtechnik auf die Dosen bzw. Buchsen aufgelegt. Das Werkzeug dazu heisst Knacke.

2.4.3 Etagenverkabelung

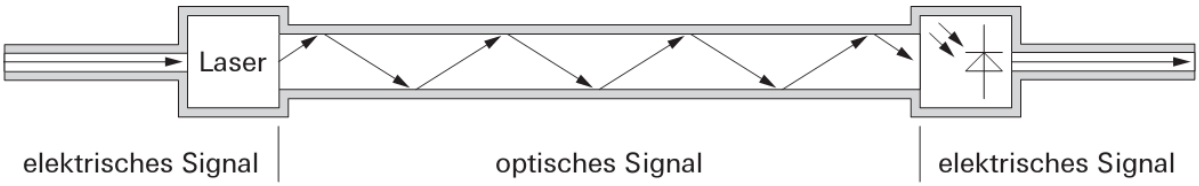
Server → Switch → Patchpanel → Switch → Workstation

2.4.4 Steckerbelegung und Aderfarben

	Die Verbindungsart nennt man **RJ-45** 1)Sendesignal + 2) Sendesignal – 3) Empfangssignal + 4) Empfangssignal –n

2.4.5 Lichtwellenreiter / Glasfaserkabeln

Durch elektrische Impulse werden optische Signale übertragen. Deshalb haben diese Glasfaserkabel eine sehr gute Übertragungseigenschaft (mehrere Gbps) und eine grosse Reichweite. Ausserdem werden sie kaum durch elektromagnetische Felder beeinflusst. Sie sind jedoch sehr teuer. Bezeichnung könnte etwa so sein: 1000BaseFX. Das ist die Zukunft.
Bill Gates hat so sein ganzes Anwesen verkabelt. Ist doch nett, wenn man so viel Geld, Kabel, Freude und Spass hat.



Aufbau

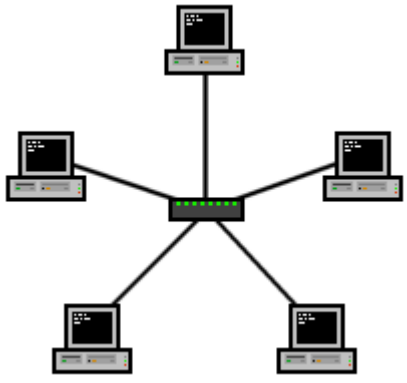
Im Innern ist ein Glaskern, der von einem Glasmantel umgeben ist. Diese sind durch einen Kunststoffmantel geschützt, welcher für die Abschirmung und die Bruchfestigkeit sorgt. Der Glaskern besteht aus vielen kleinen Glasfasern.

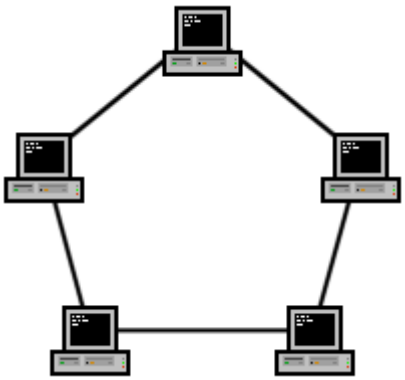
2.5 Netzwerkkomponenten: Repeater und Hub

- Ein Hub ist ein Multiport-Repeater
- Signale auffrischen
- Räumliche Ausdehnung von LANs.
- Ein Hub hat keine MAC-Adresse
- Kein Vollduplex
- Keine Flusskontrolle
- Keine gezielte weiterleitung
- Jedes Ethernet-Frame, das eintrifft wird an alle Ports weitergeleitet.
- Somit kann jeder Computer alles mithören, wenn er will. (Sniffing)
- Die gesamte an den Hub angeschlossene Netzwerkinfrastruktur bildet ein einziges Übertragungsmedium.
- Falls gleichzeitig mehrere Frames durch ein Kabel wollen, entsteht eine Kollision. (Diese könnten auf Layer 2 verhindert werden.)
- Alle angeschlossenen Geräte stehen in der selben Kollisionsdomäne.
- Werden nicht mehr im produktiven Bereich eingesetzt.

2.6 Topologien

Stern-Topologie
Alle Geräte sind mit dem selben Hub/Switch miteinander verbunden.
+) Geräte können während dem Betrieb hinzugefügt werden
-) Beim Ausfall von Hub/Switch geht gar nichts mehr



Ring-Topologie Alle Computer sind gleichberechtigt. Übertragung funktioniert von Knoten zu Knoten (Nur in Spezialfällen angewandt, spezielle Netzwerkkarte nötig +) Nicht in Betrieb befindliche Geräte können schnell überbrückt werden -) Beim Ausfall einer Verbindungsstrecke sind alle Kommunikationen unterbrochen	
Bus-Topologie Es gibt keinen zentralen Knoten, die Verbindung erfolgt über eine gemeinsame Übertragungsleitung (=Bus) +) Bei einem Computerausfall bleibt die Kommunikation aufrechterhalten -) Man kann nur immer eine Nachricht zur gleichen Zeit über den Bus schicken.	
Mesh-Topologie	
Tree-Topologie	

2.7 Netzwerkgrössen

- Ein LAN hat man bereits ab 2 PCs
- LON bis GAN gehört jemanden. Eine Firma kann z.B. Ein GAN rund um den Globus haben.

LON	Local Operating Network	Wird in Bussystemen eingesetzt
LAN	Local Area Network	Lokales Netzwerk in einem Gebäute
CAN	Campus Area Network	Mehrere Gebäude auf dem selben Grundstück (keine Strasse dazwischen)
MAN	Metropolian Area Network	Netzwerk über mehrere Grundstücke (z.B. In einem Dorf)
WAN	Wide Area Network	Netzwerk über mehrere Städte
GAN	Global Area Network	Weltumspannendes Netzwerk (jeder Kontinent)
Internet	öffentliches Netzwerk, das allen gehört.	

3 Layer 2: Data Link Layer

3.1 Aufgaben

- Versand und Empfang von Ethernet-Frames im gleichen IP-Teilnetz.
- Einpacken der IP-Datagramme vom Layer 3 in den Layer 2
- Adressieren der Frames mit MAC-Adressen für den Zielhost und Absender-Host.
- Zugriffsregelung auf das gemeinsam genutzte Übertragungsmedium.
- Flusskontrolle, die das Überlaufen des internen Puffers verhindert.
- Bit-Übertragungsfehler werden erkannt

3.2 2a: MAC Sublayer

3.2.1 MAC-Adressen Aufbau

I/G	U/L	Hersteller	Karten-ID
1 Bit	1 Bit	22 Bit	24 Bit
48 Bit = 6 Byte			

- I = 0 = Individuell = Unicast
- G = 1= Gruppe = Multicast oder Broadcast
- U = 0= Universell = von IEEE-OUI Konvention erzeugte Adresse
- L = 1 = Lokale Adresse = nur lokal verwendbar (durch Software erzeugte MAC-Adresse, die sich nicht an die OUI Einteilung der IEEE hält

Unicast	Zustellung an ein Ziel (00:45:A9:A8:F1:69)
Multicast	Zustellung an mehrere Ziele (Streaming, Spanning Tree Protocol (STP), IRC)
Broadcast	Zustellung an alle Hosts innerhalb der gleichen Broadcast-Domäne (FF:FF:FF:FF:FF:FF)
Promiscous Mode	Wennn die Netwerkkarte im promiscous mode ist, dann werden auch Pakete empfangen, welche nicht an die eigene adressiert ist.

3.2.2 Aufbau Ethernet II Frame (Ethernet DIX)

Das DIX-Konsortium standardisierte die Darstellung von Ethernet-Frames. Diese nennt man auch Ethernet II Frames.

Destination Address	Source Address	Type	Data / Nutzlast	Trailer
6 Byte	6 Byte	2 Byte	46 bis 1500 Byte	4 Byte
Ethernet II Header			Data	Checksum

Ethernet-Type-Field (für Nutzdaten)

IANA definiert diesen Standard: http://www.iana.org/assignments/ethernet-numbers

Zu welchem Layer 3-Protokoll gehört die zu transportierende Nutzlast?

Ether-Type	Layer 3 Protokoll
0x0800	IP
0x0806	ARP
0x8100	VLAN tagged Frames

> In einem Ethernet II-Frame werden praktisch nur IP-Datagramme und ARP-Pakete transportiert!

Trailer / FCS / CRC

Das FCS-Feld (Frame Check Sequence) dient der Integritätsprüfung auf Bitebene:

1. Sende-Netzwerkkarte berechnen eine 32 Bit (=4 Byte) lange CRC-Prüfsumme (cyclic redundancy check), welche in das FCS Feld eingesetzt wird.

2. Die empfangende Karte berechnet die selbe CRC-Prüfsumme und vergleicht mit der ankommenden Prüfsumme. Sind diese identisch, ist alles OK!

3. Falls die Summen nichCRCt identisch sind, wird das Frame weggeworfen. Dies tönt schlimm, ist aber nicht so, weil das TCP-Protokoll die Verbindung prüft. Das stillschweigende wegwerfen wird als silend discard bezichnet.

FCS ist kein Sicherheitsprotokoll, da ein Man in the Middle trotzdem manipulieren kann.

Es können nur physikalische Fehler gefunden werden.

3.2.3 Medien Zugriffsverfahren

CSMA/CD

Carrier Sense Multiple Access / Collision Detection ist ein Zugriffsverfahren bei Ethernet-Netzwerken.

Wenn innerhalb der Kollisionsdomäne eine Kollision entsteht, wird ein JAM-Signal (Engpass, Stau) ausgesendet.

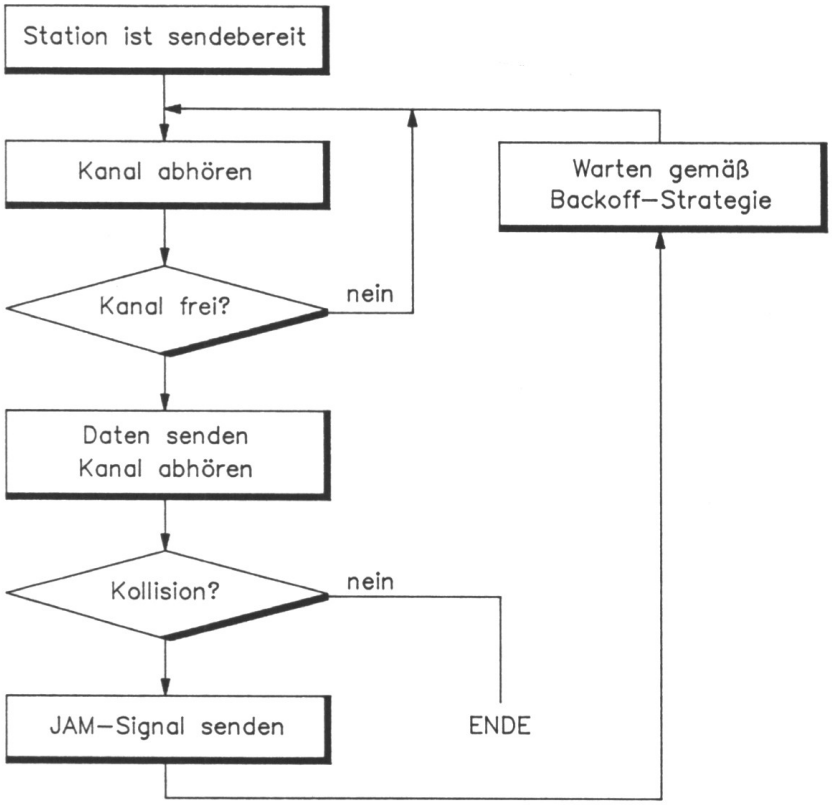


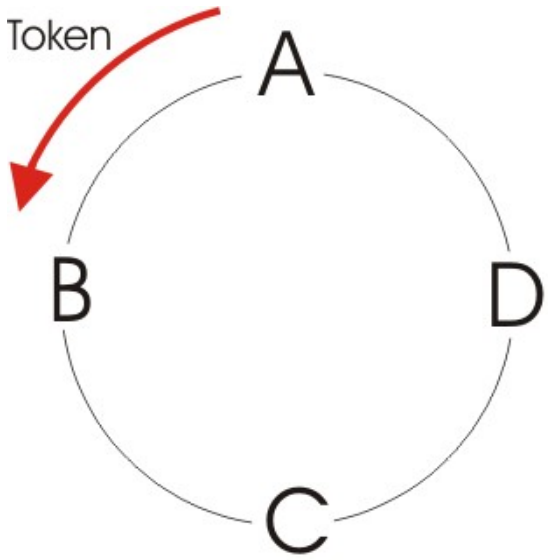
Abbildung 5: CSMA/CD Zugriffsverfahren

Token Passing

Der Begriff **Tokenweitergabe** oder englisch **Token Passing** bezeichnet ein Medienzugriffsverfahren in Rechnernetzen.

Grundlage von Token Passing ist das Token, das im Netzwerk von einer Station zur benachbarten Station in einer logischen Ringtopologie weitergeleitet wird. Es existieren zwei unterschiedliche Realisierungsformen des Token Passing: Token Ring und Token Bus.

Bei Token Ring ist der Nachbar die physisch nächste erreichbare Station, bei Token Bus ist es die logisch nächste erreichbare Station (realisiert durch die Adressen der Netzwerkkarte).



Ein Freitoken (bestehend aus 3 Bytes bzw. 24 Bit) wird von Punkt zu Punkt ständig weitergeschickt. Möchte ein Computer **A** Daten an Computer **C** übermitteln, wartet er darauf, dass das Token ihn passiert und hängt dann dem Token, sofern es frei ist, das Datenpaket an, adressiert es an Computer **C** und markiert das Token als besetzt.

Das gesamte Paket schickt Computer **A** an seinen Nachbar Computer **B**. Computer **B** erkennt, dass nicht er der Empfänger des Datenframes ist und sendet es an seinen Nachbar Computer **C**. Da **C** als Empfänger eingetragen ist, kopiert er das Datenframe und modifiziert das Token auf *empfangen*. Dann sendet er den Frame wieder auf den Ring. Da das Token immer noch besetzt ist, kann kein Computer Daten anhängen. Beim Eintreffen des Frames bei Computer **A** überprüft **A**, ob der Inhalt mit dem versendeten übereinstimmt und die Empfangsmarkierung gesetzt ist.

Ist dies der Fall, so war die Übertragung erfolgreich. Der Datenframe wird entfernt und das Token wird wieder auf frei gesetzt. Selbst wenn eine Übertragung fehlgeschlagen ist, muss der Sender nach dem Empfang der Empfangsmarkierung (Quittung) auf jedenfall ein freies Token senden. So wird gewährleistet, dass nach jeder Datenübertragung ein freies Token im Ring ist.

Verwendet wird Token Passing für Netzwerke mit hoher Last, aber auch für Echtzeitanwendungen.

3.3 2b: LLC Sublayer

LLC steht für Logical Link Control

3.3.1 Flusskontrolle (Flow Control)

Wenn ein schneller Sender mit einem langsamen Empfänger zusammenarbeitet, muss die Datenübertragung zeitweise unterbrochen werden. Der Empfänger würde sonst mit Daten überlastet werden, die er nicht verarbeiten könnte. Die Steuerung dieser Unterbrechungen ist die Aufgabe der Datenflusssteuerung.

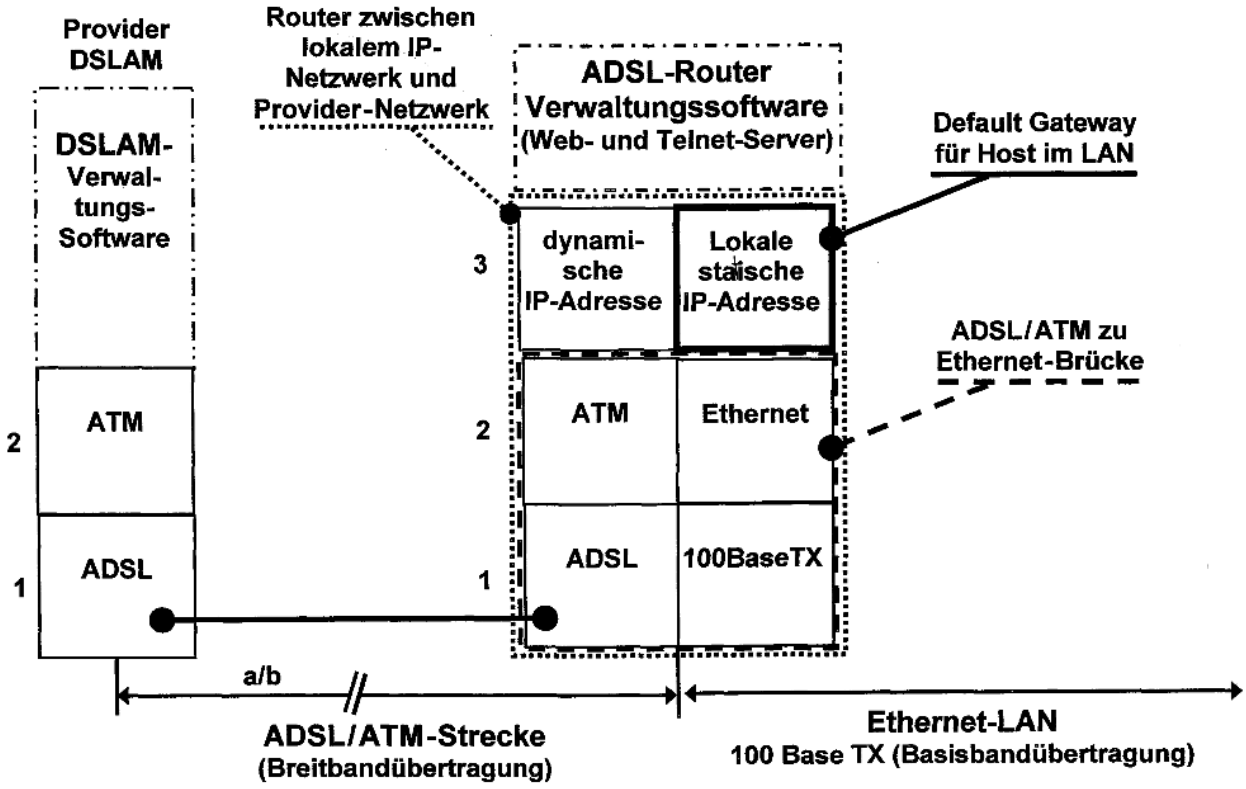
In sehr schnellen Netzwerken wird mit PAUSE-Signalen verhindert, dass Frames ausgesendet werden, die gar nicht verarbeitet werden könen.

3.4 Bridge

- Eine Bridge verbindet zwei LAN-Segmente innerhalb des gleichen IP-Teilnetzes.

- Die Bridge trennt Kollisionsdomänen → bessere Performance.
- Die Abhörsicherheit steigt.
- Wegen der Lasttrennung erhöht sich der Datendurchsatz.
- Die Ethernet-Ports der Bridge besitzen eigene MAC-Adressen (steht so in den Unterlagen!!!! ?????)
- Es werden nur jene Pakete weitergeleitet, für die es wirklich nötig ist. Dabei wird mit Hilfe einer Tabelle nachgeschaut: Welche Port-Nr. gehört zu welchen MAC-Adressen.
- Nach dem Start befindet sich die Bridge im Learning-Mode (Layer 1 Modus). In diese Phase werden die Infos für die Tabelle gesammelt.
  Danach kommt die Bridge in den Forwarding-Mode. Dort werden die Daten gezielt weitergeleitet.

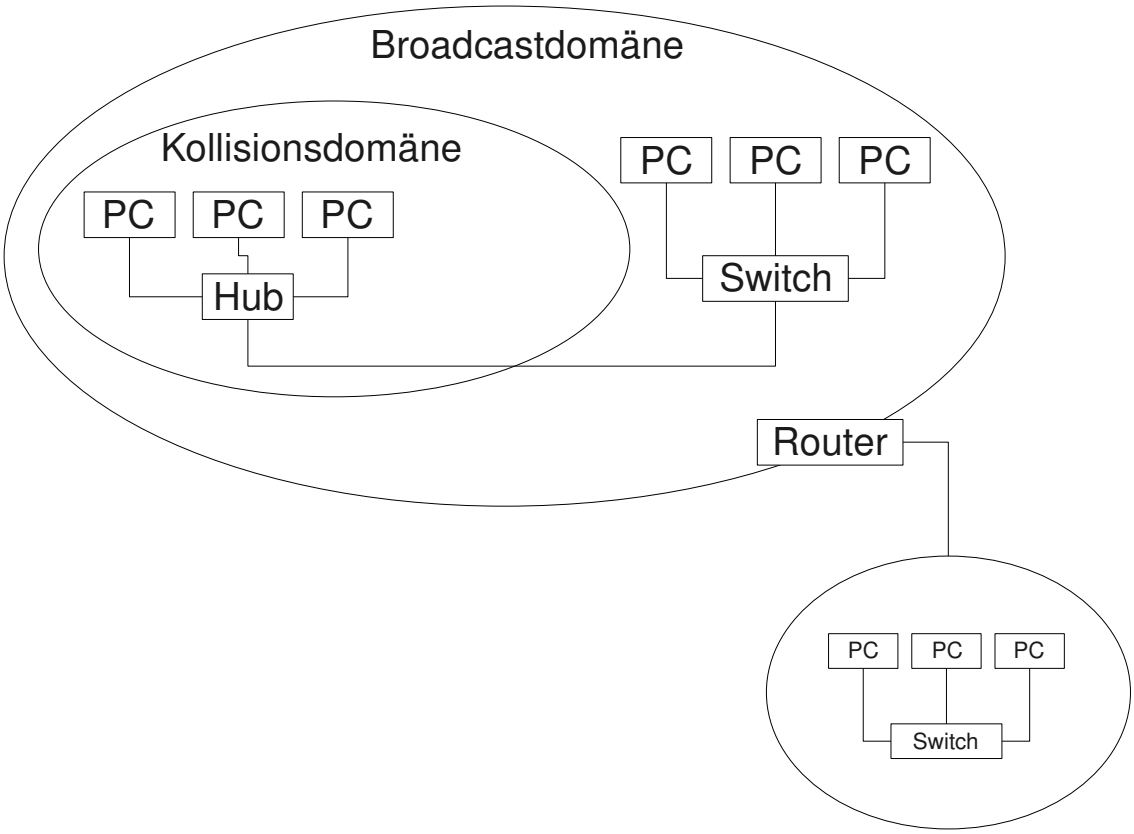
ADSL-Router enthält eine ADSL/ATM zu Ethernet Bridge



3.5 Switch

- Switch ist eine Multiport-Bridge.
- Ersetzt den Layer 1 Hub.
- Die Kollisionsdomäne beschränkt sich das kleine Mikrosegment zwischen den beteiligten Hosts.
- Unterstützt Voll-Duplex-Mode. Deshalb gibt es keine Kollisionen.
- Broadcast-Frames werden an alle Ports weitergeleitet.
-

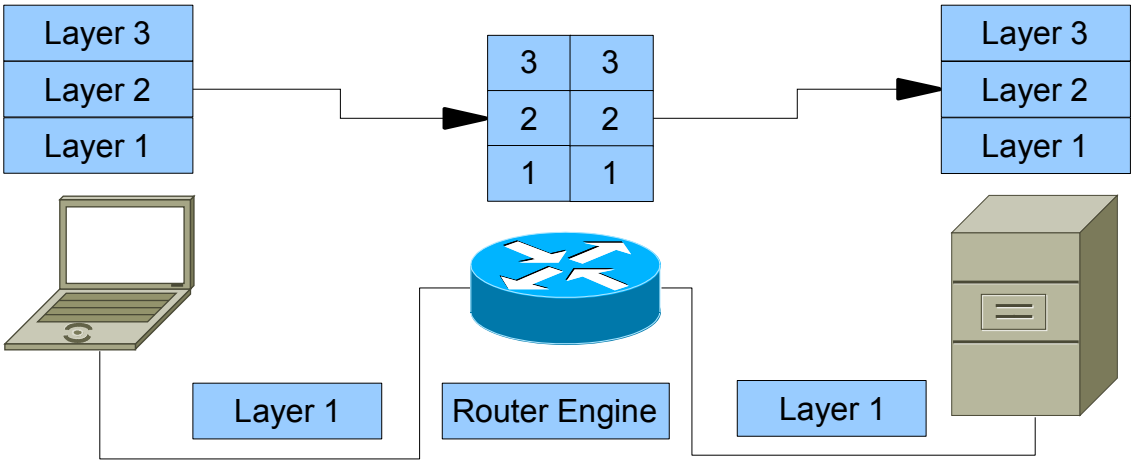
- Alle an einem Switch angeschlossenen Hosts gehören zur gleichen MAC-Broadcastdomäne.



Vorteile gegenüber dem Hub

- Der Switch leitet Datenpakete gezielt weiter.
- Die Kollisionsdomäne beschränkt sich auf ein dynamisch entstehendes Mikrosegment (ist also sehr klein).
- Autonegotation: Der Switch handelt automatisch die schnellste Übertragungsrate pro Verbindung aus.
- Full-Duplex-Mode: Der Switch kann gleichzeitig senden und empfangen.
- Der Switch unterstützt die Flusskontrolle
- Schleifenbildung können durch das Spanning Tree Protocol (STP) verhindert werden.
- Bei Layer-3-Switches kann man VLANS einrichten.

4 Layer 3: Network Layer



4.1 Der IP-Datagramm-Header

Er enthält die Steuerdaten, die das IP-Protokoll zu einem Datenpaket hinzufügt, das ihm vom übergeordneten Transportprotokoll übergeben wird.

Der IPv4-Protokoll-Header wird wie das gesamte Protokoll in RFC 791 definiert. Seine Länge beträgt mindestens 20 Byte, dazu können bis zu 40 Byte Optionen kommen.

Byte	0	1	2	3
0	Version / IHL	Type of Service	Paket-Gesamtlänge	
4	Identifikation		Flags	Fragment-Offset
8	Time to Live	Protokoll	Header-Prüfsumme	
12	**Quell-Adresse**			
16	**Ziel-Adresse**			
20	Optionen			Padding
...	evtl. weitere Optionen			

In diesem Modul beschränken wir uns auf die Quell-Adresse und auf die Ziel-Adresse.

4.2 IP-Adressen

4.2.1 Schreibweise

- Eine IP hat 4 Byte (deshalb Ipv4). Das sind 24 Bit.
- Der Binärwert wird in 4 Oktette aufgeteilt und jeweils durch einen Punkt getrennt dezimal geschrieben.

4.2.2 Typen von IP-Adressen

Unicast IP-Adressen	1:1 Kommunikation 192.168.1.1 → Oft genutzte IP im Home-Umfeld
Multicast IP-Adressen	1:n Kommunikation 239.255.255.250 → UpnP Geräte kündigen Dienste an
Broadcast IP-Adressen	1:alle Kommunikation 255.255.255.255 → Dieses IP-Datagramm geht überall hin 192.168.1.255 / 24 → Das ist die Broadcastadresse von diesem Netz.

4.2.3 Aufbau der IPv4-Unicastadressen

Jede Ipv4-Unicastadresse besteht aus einem Netzwerk- und aus einem Host-Teil.

Netzwerk-ID	Host-ID
192.168.1.	1
255.255.255.	0

Die Subnetzmaske trennt den Host-Anteil und den Netz-Anteil.

Netzwerk-ID-Anteil

Der Netzwerbereich, in dem eine bestimmte Netzwerk - ID Gültigkeit hat, wird als IP - Teilnetz, bzw. als IP-Subnetz oder häufig einfach nur als „Subnetz“ bezeichnet.

Host-ID-Anteil

Der Host - ID - Anteil einer IPv4 - Unicastadresse kennzeichnet die IP - Schnittstelle eines Netzwerkknotens („IP-Host“ oder meistens nur als „Host“ bezeichnet) in einem IP-Teilnetz. Die Host - ID muss innerhalb des IP - Teilnetzes eindeutig sein.

Subnetzmaske

Mit der Subnetmaske gibt man an, wo zwischen Net-ID und Host-ID getrennt wird. Um die Subnetmaske zu bilden, setzt man einfach alle Bits der Net-ID auf 1.

- Hostadresse AND Subnetzmaske

Hostadresse	**11**000000	000**1**000**1**	0000**1**000	00**1**00111	192.17.8.39
Subnetzmaske	**11**111111	111**1**111**1**	1111**1**111	11**1**00000	255.255.255.224
Hostaddr. AND Subnetmaske	**11**000000	000**1**000**1**	0000**1**000	00**1**00000	**192.17.8.32**

Darstellung

- Angabe von IP-Adresse und Subnetzmaske: 192.168.1.10, 255.255.255.0

- Angabe von IP-Adresse und Länge der 1-Bit-Kette der Subnetzmaske als Präfix: 192.168.1.10 / 24

Minimale IP-Konfiguration

Die minimale IP-Konfiguration eines Hosts benötigt sicherlich folgende Sachen:

- IP-Adresse
- Subnetzmaske
- Standardgateway
- (DNS-Server)
- (WINS-Server)

Meistens wird diese Konfiguration über einen DHCP-Server verteilt!

4.2.4 DHCP – Vorgang

Folgendermassen läuft der Vorgang ab, wenn ein Client bei einem DHCP-Server eine IP-Adresse holt:

1. **DHCPDISCOVER:** Ein Client ohne IP-Adresse sendet eine Broadcast-Anfrage nach Adress-Angeboten an den/die DHCP-Server im lokalen Netz.
2. **DHCPOFFER:** Der/die DHCP-Server antworten mit entsprechenden Werten auf eine DHCPDISCOVER-Anfrage.
3. **DHCPREQUEST:** Der Client fordert (eine der angebotenen) IP-Adresse(n), weitere Daten sowie Verlängerung der Lease-Zeit von einem der antwortenden DHCP-Server.
4. **DHCPACK:** Bestätigung des DHCP-Servers zu einer DHCPREQUEST-Anforderung

Es gibt noch andere DHCP-Meldungen:

- **DHCPNAK:** Ablehnung einer DHCPREQUEST-Anforderung durch den DHCP-Server
- **DHCPDECLINE:** Ablehnung durch den Client, da die IP-Adresse schon verwendet wird.
- **DHCPRELEASE:** Der Client gibt die eigene Konfiguration frei, damit die Parameter wieder für andere Clients zur Verfügung stehen.
- **DHCPINFORM:** Anfrage eines Clients nach Daten ohne IP-Adresse, z. B. weil der Client eine statische IP-Adresse besitzt.

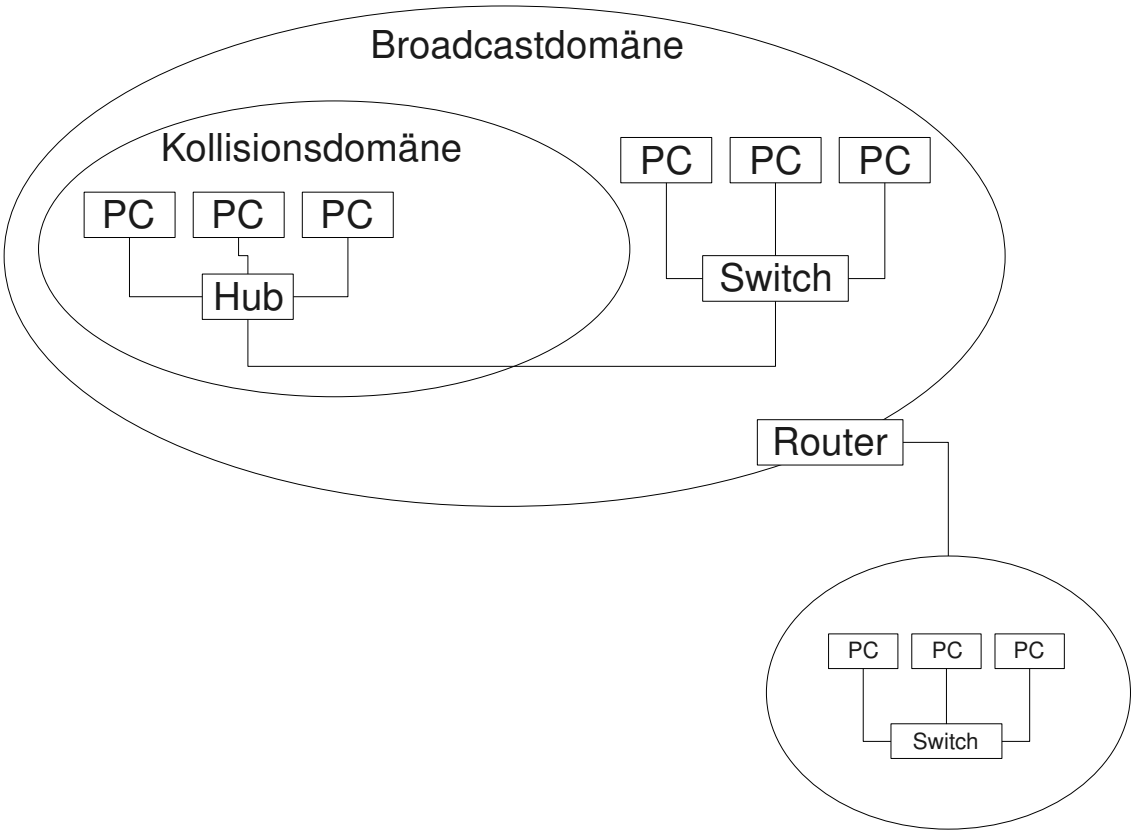
Eine 169.254.12.42 IP-Adresse gibt an, dass es einen Fehler gab! Der Client konfiguriert sich so selber.

4.2.5 Namensauflösung

Eingesetzte Namensauflösungssysteme

- **Linux:** DNS, NetBIOS über Samba
- **Windows:** NetBios, Wins

MAC-Broadcastdomänen und IP-Teilnetze



Durch einen Router können wir mehrere Subnetze zusammenhängen. Um vom einen ins andere Subnetz zu kommen, müssen wir den Default-Gateway kennen.

Es gibt weniger Broadcast.

4.3 Netzklassen

IANA regelt den Verbrauch von IP-Adressen.

Der grundsätzliche Adressraum geht von 0.0.0.0 bis 255.255.255.255. Das gäbe 255^4 = etwa 4,23 Mio IP-Adressen.

Anhand der IP-Adresse erkennt man jedoch nicht, wo die Netz-ID und wo die Host-ID getrennt werden. Deshalb hat IANA mit dem Konzept „Klassenorientierte IP-Adressen“ geholfen:

Klasse	Präfix	Adressbereich	Netzmaske	Netzlänge (mit Präfix)	Netzlänge (ohne Präfix)	Hostlänge	Netze	Hosts pro Netz
A	0...	0.0.0.0 – 127.255.255.255	255.0.0.0	8 Bit	7 Bit	24 Bit	128	16'777'214
B	10...	128.0.0.0 – 191.255.255.255	255.255.0.0	16 Bit	14 Bit	16 Bit	16.384	65'534

C	110...	192.0.0.0 – 223.255.255.255	255.255.255.0	24 Bit	21 Bit	8 Bit	2'097'152	254
D	1110...	224.0.0.0 – 239.255.255.255	Verwendung für Multicast-Anwendungen					
E	1111...	240.0.0.0 – 255.255.255.255	reserviert					

Wenn eine IP-Adresse mit der Subnetzmaske genau diesem Konzept entspricht, ist es Klassenorientiert.

Entspricht eine IP-Adresse und die dazugehörige Subnetzmaske diesem Konzept nicht, dann ist dies ein klassenloses Teinletz.

> Bis zum heutigen Tag wird das Konzept der Netzklassen vielerorts als immer noch gültig gelehrt, so beispielsweise in Vorlesungen und Praktika über Netzwerktechnik an Hochschulen. Diese Lehre der Netzklassen führt oft jedoch nur zu Verwirrung, da sie mit der Einführung von CIDR überholt ist. Da das Wissen über Netzklassen nicht mehr praktisch einsetzbar ist, stellt es lediglich einen historischen Sachverhalt und keine Referenz für praktischen Einsatz dar.

4.4 Spezielle IP-Netzwerke und Private Ranges

Klasse	Netzwerk-Adresse	Verwendungszweck
A	0.0.0.0 / 8	Default-Route in der Routing-Table
A	**10.0.0.0 / 8**	Zur privaten Nutzung freigegeben (wird nicht geroutet)
A	127.0.0.0 / 8	Internes IP-Netzwerk eines jeden IP-Fähigen Host. Konkret: 127.0.0.1 für localhost
B	**172.16.0.0 / 16 – 173.31.0.0 / 16**	Zur privaten Nutzung freigegeben (wird nicht geroutet)
B	169.254.0.0 / 16	Zur automatischen Vergabe von APIPA-Adressen
C	**192.168.0.0 / 24 – 192.168.255.255 / 24**	Zur privaten Nutzung freigegeben (wird nicht geroutet)
	IP: 255.255.255.255	Broadcast

Klasse A Netzwerk 0.0.0.0 / 8

Der Default-Gateway wird verwendet, wenn man ein IP-Datagramm in ein anderes Subnetz verschicken will. Folgendermassen werden IP-Datagramme in andere Subnetze weitergeleitet:

- Man nimmt die Destination IP-Adresse.
- Diese wird mit der ersten Subnetzmaske der Routing-Tabelle übereinandergelegt.
- Anhand der Subnetzmaske der Routing-Tabelle errechnen oder „erlugen aus der Tabelle“ die Subnetzadresse.
- Stimmt diese Subnetzadresse mit der Subnetzadresse der Routing-Table überein, kann diese passen.
    - Es kann jedoch sein, dass noch eine weitere Route übereinstimmt. Deshalb gehen wir ALLE EINTRÄGE der Tabelle durch!
    - Wenn mehrere übereinanderstimmen, nimmt man die „more specific“ bzw. eifach die „grössere“ Subnetzadresse (mit der kleineren Blockgrösse).

(Das gibt weniger Broadcast :D – oh ja – schön.)

- Wenn quasi keine übereinanderstimmt, ausser 0.0.0.0, dann wird diese genommen. Diese stimmt immer und wird auch Default-Route genannt.

- Nun schauen wir beim passenden Eintrag, an welchen Next-Hop das IP-Paket weitergeleitet werden soll. Dies machen wir auch so.

Kurz gesagt: Netzwerkadresse erstellen und vergleichen. Wenns passt, nimmt man den Next-Hop beim Eintrag mit der „grössten“ Subnetzmaske.

Das Klasse A Netzwerk 127.0.0.0 / 8

Jeder IP-Konfigurierter Host gehört zu zwei Netzwerken: Zu dem physikalisch angeschlossenen und zu dem logischen Klasse A Neztwerk 127.0.0.0 / 8 Netzwerk.

Das Netz 127.0.0.0 und die IP-Adresse 127.0.0.1 sind für die Kommunikation des lokalen Rechners reserviert.

Private IP-Netzwerke

IP-Datagramme mit privaten IP-Ziel-Adressen werden von den Routern im Internet nicht weitergeleitet. Dies wird durch entsprechende Paketfilter-Regeln auf den Routern verhindert.

Bei NAT werden die privaten IP-Absender-Adressen der versendeten IP-Datagramme gegen die WAN-Seitige, öffentliche IP-Adresse (des ADSL-Routers) ausgetauscht. Dies geschieht auch umgekehrt!

Klasse B Netzwerk APIPA 169.254.0.0/16

- APIPA steht für Automatic Private IP Adressing
- Soll ein IP-Host vom DHCP-Server eine IP beziehen, der DHCP-Server jedoch nicht erreichbar ist, konfiguriert sich der IP-Host selber mit einer IP-Adresse aus dem 169.254.0.0 / 16 Netz.
- Den anderen Hosts im Netzwerk wird es genau gleich gehen. Deswegen wird die Eindeutigkeit der zufällig festgelegten IP-Adresse durch eine spezielle Funktion von ARP durchgesetzt.
- Windows und auch aktuelle Linux-Distrubutionen unterstützen das APIPA-Verfahren.

4.4.1 Übersicht über die IP-Klassen

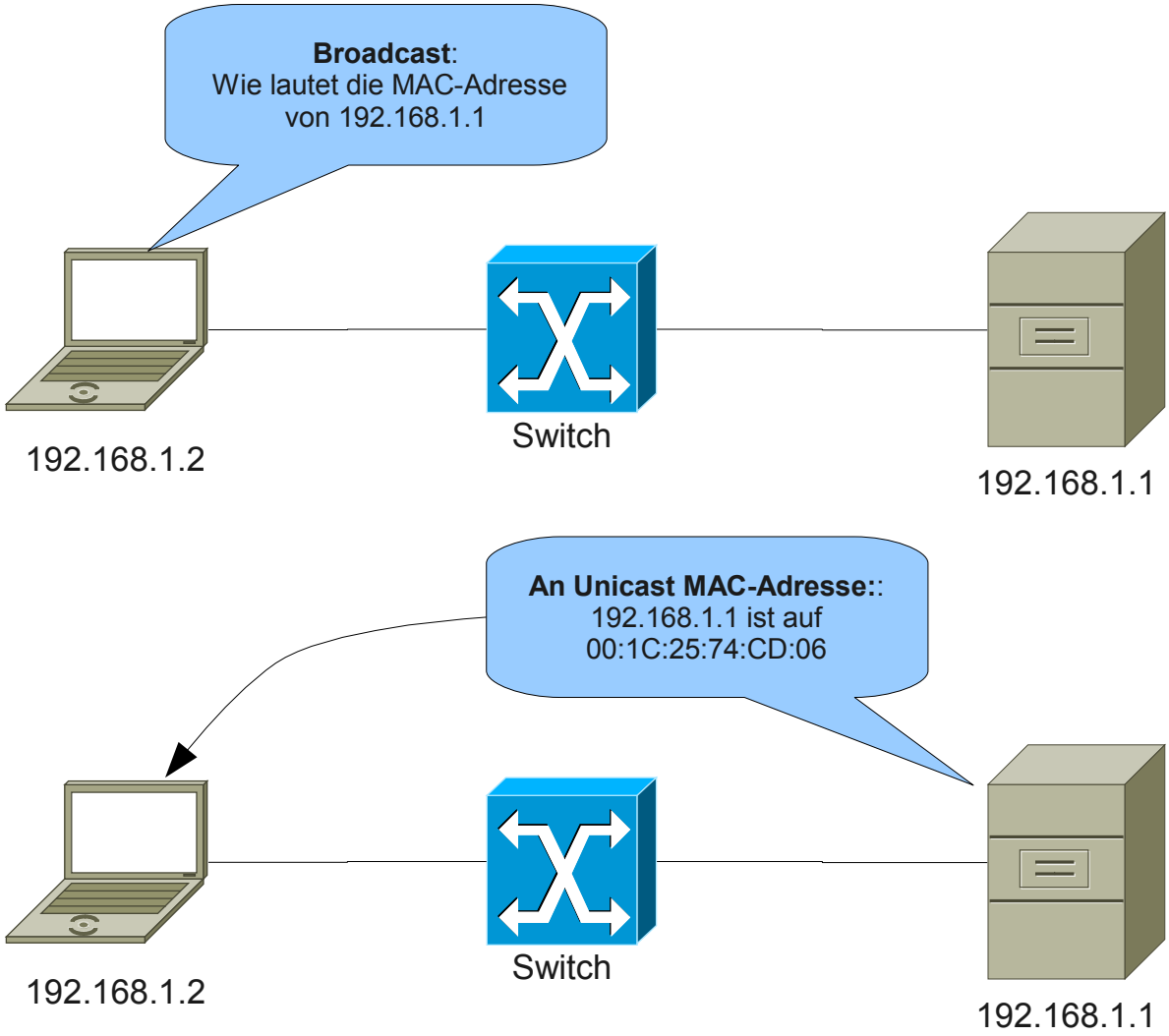
8-Bit-Netz Klasse A Netz	16-Bit-Netz Klasse B	24-Bit-Netz Klasse C
64 = Netz-ID 168.100.25 = Host-ID	128.168 = Netz-ID 100.25 = Host-ID	192.168.100 = Netz-ID 25 = Host-ID
Kleinste Addr.: 1.0.0.0 Grösste Adrdr.: 126.0.0.0	Kleinste Addr.: 128.0.0.0 Grösste Addr.: 191.255.0.0	Kleinste Addr.: 192.0.0.0 Grösste Adr.: 223.255.255.0
Kleinste Rechneraddr: 1.0.0.1 Grösste: 162.255.255.254	Kleinste Rechneraddr: 128.0.0.1 Grösste: 191.255.255.254	Kleinste Rechneraddr: 192.0.0.1 Grösste:223.255.255.254
Subnetmaske: 255.0.0.0	Subnetmaske: 255.255.0.0	Subnetmaske: 255.255.255.0
Nummernkreis: 10.0.0.0 – 10.255.255.255	Nummernkreis: 172.16.0.0 – 172.31.255.255	Nummernkreis: 192.168.0.0–192.168.255.255
Linkes Bit: 0	Linkes Bit: 10	Linkes Bit: 110

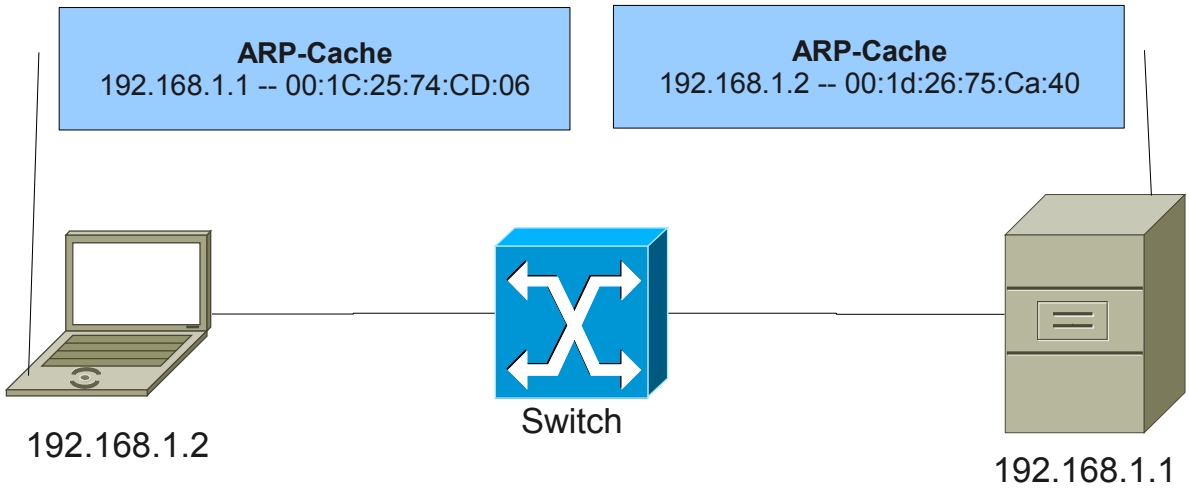
4.5 ARP – Adress Resolution Protocol

Will ein Rechner in einem Ethernet an einen Rechner in demselben Subnetz ein IP-Paket senden, muss er die Information in einen Ethernetframe verpacken. Dazu muss er die MAC-Adresse des Zielrechners kennen und im entsprechenden Feld des Ethernetframes einfügen. Ist ihm diese nicht bekannt, kann er das IP-Paket nicht zustellen. Stattdessen ermittelt er dann mit Hilfe des ARP zunächst die MAC-Adresse des Zielrechners.

Vorgehen

Host 192.168.1.**2** will Host 192.168.1.**1** ein Ethernet-Frame schicken.

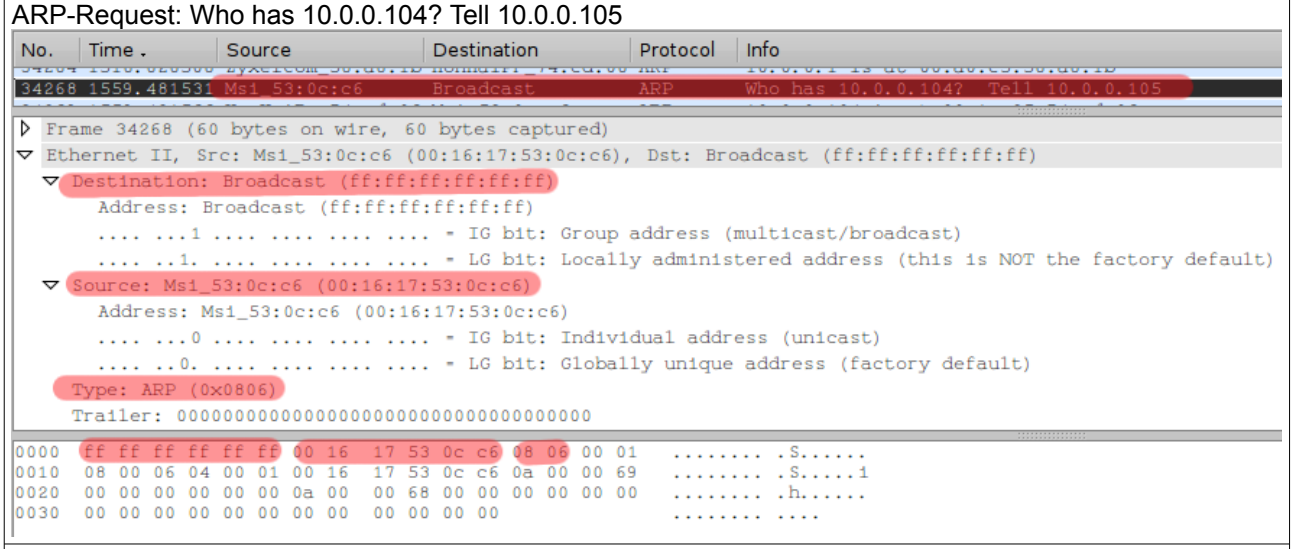




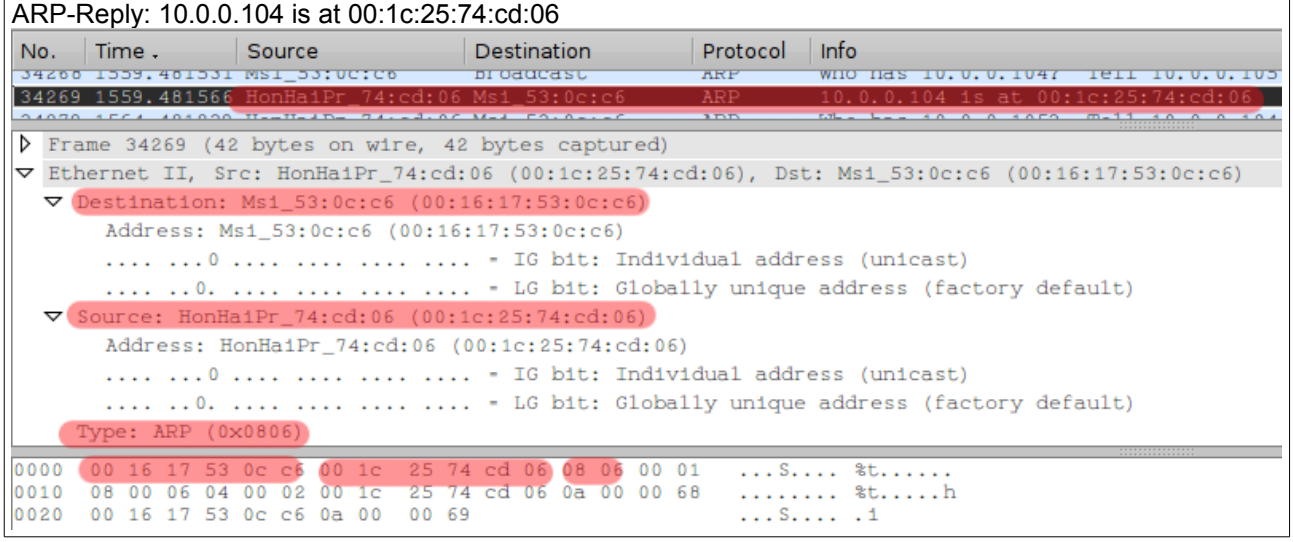
- Die MAC-Adressen werden in beiden ARP-Caches eingetragen.
- Ein Host nimmt auch MAC-Adressen auf, nach denen er nicht explizit fragte. Wenn also ein ARP-Päckchen herumgesitert, wird es in den ARP-Cache aufgenommen.

Paketanalyse mir Wireshark:

ARP-Request: Who has 10.0.0.104? Tell 10.0.0.105



ARP-Reply: 10.0.0.104 is at 00:1c:25:74:cd:06



4.5.1 Gratious ARP[1]

Gratuitous ARP (engl. „unaufgefordertes ARP“) bezeichnet eine spezielle Verwendung von ARP. Dabei sendet ein Host ein ARP-Anforderungs-Broadcast, bei dem er seine eigene IP-Adresse als Quell- und Ziel-IP-Adresse einträgt. Damit teilt er seine ggf. neue MAC-Adresse unaufgefordert mit. Das kann mehreren Zwecken dienen:

1. Normalerweise darf keine Antwort kommen, denn eine IP-Adresse muss in einem Netz eindeutig sein. Bekommt er trotzdem eine Antwort, ist das für den Administrator ein Hinweis darauf, dass ein Host nicht richtig konfiguriert ist.
   Dann wird der Bentutzer benachrichtigt, dass ein IP-Adressenkonflikt herrscht.

2. Jeder Host aktualisiert seinen ARP-Cache. Das ist beispielsweise dann nützlich, wenn die Netzwerkkarte eines Rechners ausgetauscht wurde und die anderen Hosts über die neue MAC-Adresse informiert werden sollen. Gratuitous ARP geschieht deshalb normalerweise beim Booten eines Computers.

3. Wenn zwei Server aus Gründen der Ausfallsicherheit als Server und Ersatzserver aufgebaut sind

1 Quelle: Wikipedia

und sich eine IP-Adresse teilen und der aktive Verkehr vom einen auf den anderen geschwenkt werden soll, ist die IP-Adresse jetzt über eine andere MAC-Adresse zu erreichen. Diese neue MAC-/IP-Adress-Zuordnung muss bekannt gemacht werden. Sonst bekommt niemand den Wechsel mit.

4. In einem Mobile IP-Szenario sendet der Home Agent einen Gratuitous ARP, wenn sich der Mobile Host aus dem Heimatnetz entfernt, um die Pakete stellvertretend für diesen zu empfangen. Analog sendet der Mobile Host einen Gratuitous ARP, sobald er sich wieder im Netz befindet.

Gratious ARP wird auch nach der Neukonfiguration des Hosts ausgesendet.

4.6 Merkmale von Netzwerk-Geräten

Behauptung	**NIC in einem Windows-/Linux-Host**	**Hub-Port**	**Switch-Port**
Besitzt eine MAC-Adresse	Ja, es sind die Layer 1 und 2 vorhanden	Nein, Hub arbeitet nur auf Layer 1	Ja. Es sind die Layer 1, und 2 vorhanden
Kann mehrere MAC-Adressen besitzen	Nein	--	nein
Leitet Frames mit MAC-Broadcasts an andere Netzwerkgeräte weiter	Nein. Ein Host ist standardmässig kein Weiterleitungsgerät	Ja (leitet aber ohnehin alle Frames weiter)	Ja (Switches trennen keine MAC-Braodcastdomänen) Dürfen sie auch nicht, wegen ARP-Broadcasts!!!
Verarbeitet Frames mit MAC Dest-Adr = MAC-Broadcast (Weiterverarbeitung auf Layer 2, 3, …) Falls Ja: Noch ein Beispiel für Layer 3 Nutzlast angeben	Ja z.B: wegen ARP-MAC-Broadcasts	Nein, keine Verarbeitung der Frames auf Layer 2 ff,	Ja, wenn es sich um einen managebaren Switch handelt. Dann hat er TCP/IP implementiert, damit er z.B. mit dem Webbrowser ansprechbar wird.
Verarbeitet Frames mit der MAC-Multicast-Adresse 01-80-C2-00-00-00 (STP-Multicast-MAC-Adresse)	Nein, ausser der Host ist per SW (Windows XP, Server + Linux) zu einer Brücke konfiguriert werden	Nein, keine Verarbeitung der Frames auf Layer 2ff	Ja, Zur Verarbeitung des Spanning Tree Protokolls (STP)
Arbeitet im standardmässig promiscuous Modus (in diesem Modus wird jedes Frame vollständig in den Layer 2a-Puffer eingelesen)	Nein, Das Einschalten des Promiscuous-Mode ist im betrieblichem Umfeld verboten	---	Ja, Switches leiten Frames von Hosts gemäss der <Port – MAC-Adress-Tabelle> weiter
Teilt ein LAN in Layer 2a CSMA/CD -Kollisionsdomänen auf	Nein, eine NIC ist ohnehin kein Vermittlungsgerät	Nein	Ja
Teilt ein LAN in mehrer MAC-Broadcastdomänen auf	Nein eine NIC ist ohnehin kein Vermittlungsgerät	Nein	nein

Unterstützt den Voll-Duplex Übertragunsmodus	Ja Bei allen modernen 10/100 Mbps – Karten für 10BaseT und 100BaseTX implementiert	Nein	Ja
Optimale Übertragungsrate und optimaler Übertragungsmodus wird pro Link und nicht für das ganze LAN ausgehandelt (Kommunikation zwischen NICs)	-- Vermittelt keine Links Kann aber beim Autonegotiationsprozess mitmachen	Nein	Ja
NIC mit den schwächsten Übertragungsparametern bestimmt die Übertragunsrate und den Übertragungsmodus im ganzen LAN	Ja, im ge-Hub-ten LAN Nein, im ge-Switch-ten LAN	Ja	Nein, Switch vermittelt Übertragungsrate und Übertragungsmodus pro Link im Mikrosegment
Das Netzwerkverbindungsgerät kann gleichzeitig mehrere Links bedienen	--	Nein	Ja
Das Gerät verfügt über eine Tabelle für die Zuordnung von MAC-Adr zu Port-Nummer	Nein	Nein	Ja
An einem Port ist immer die Summe aller Signale zu „hören“	---	Ja	Nein, Ausser der Switch befindet sich noch im Lernmodus
Das Gerät baut die MAC-Adress-Tabelle aufgrund der Destination-MAC Adr und(!) der Source-MAC-Adr der einlaufenden Frames auf	--	--	Der Switch baut die Adress-Tabelle auf-grund der Source-MAC-Adressen der einlaufenden Frames auf.
Das Gerät kann Frames von der 100Base-TX Technologie in die 100Base-FX umsetzten (d.h. das Gerät unterstützt Fiber-Optic-Ports)	--	Nein	Ja
Das Gerät kann den MDI/ MDIX-Standard unterstützen	--	Ja	Ja

Quelle: Aufgabe vom Lehrer

5 Layer 4: Transport Layer

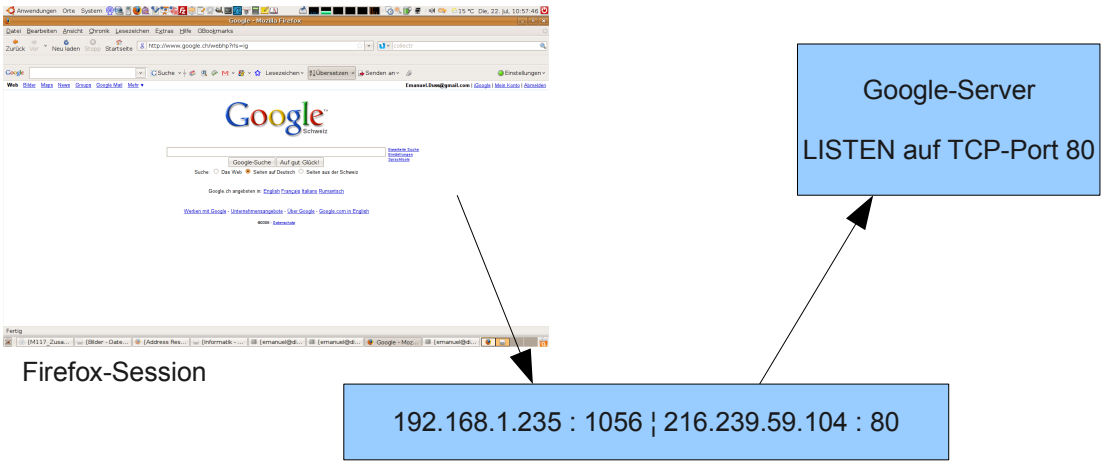
5.1 Verbindungsbeziehung

Auf dem Transport-Layer gibt es zwei Protokolle: TCP und UDP.

Durch die Adressierung auf Layer 3 (IP-Adressen) und Layer 4 (Port-Nummern), werden die Kommunikationsendpunkte eindeutig festgelegt.

IANA hat Portnummern zwischen 1 und 1023 festgelegt. Diese werden als bevorzugte Portnummern bezeichnet.

Beim Start eines Webbrowsers wird eine Clientprozess-Portnummer ber 1023 gewählt. Somit ist eine eindeutige Beziehung zwischen Client- und Serverprozess möglich.



Socket

Die vollständige Beschreibung einer Verbindungsbeziehung mit zwei IP-Adressen und zwei Port-Nummern wird als Socket bezeichnet:

IP-Adresse-Client : Port-Nr-Client-Prozess ¦ IP-Adresse-Server : Port-Nr-Server-Prozess

5.2 Portliste

Siehe Anhang!

6 Layer 5: Presentation Layer

7 Layer 7: Application Layer

7.1 DHCP - Dynamic Host Configuration Protocol

Der DHCP konfiguriert folgende Sachen:

- Pflicht
  - IP-Adresse
  - Subnetzmaske
  - Standardgateway
- Optional
  - (DNS-Server)
  - (WINS-Server)
  - (Art des WINS)
  - (Domainname)
  - (Timeserver)
  - (Hostname)

Meistens wird diese Konfiguration über einen DHCP-Server verteilt!

7.1.1 Warum einen DHCP-Server

1. Zentralisierte Administration der IP-Konfiguration
   1. Manuelle Konfiguration wird vermieden
   2. Viele Hosts gleichzeitig anpassen
   3. Bei neuem Router kann der nur im DHCP konfiguriert werden. Die Clients spüren nichts davon.
2. Transparente IP-Hostkonfiguration
   1. Ohne Benutzereingriff
   2. Zeitgerecht exakte IP-Adresse
   3. Automatische Konfiguration
   4. Weniger „menschliche“ Fehler
3. Flexibilität
   1. Die IP-Konfiguration ist viel einfacher und schneller zu ändern.
4. Skalierbarkeit

1. Von kleinen bis ganz grossen Netzwerken

   Alternativ könnte man auch die automatischen IP-Adressen von APIPA verwenden. Dies macht aber niemand so.

7.1.2 DHCP – Der Vorgang

Folgendermassen läuft der Vorgang ab, wenn ein Client bei einem DHCP-Server eine IP-Adresse holt:

1. **DHCPDISCOVER:** Ein Client ohne IP-Adresse sendet eine Broadcast-Anfrage nach Adress-Angeboten an den/die DHCP-Server im lokalen Netz.
2. **DHCPOFFER:** Der/die DHCP-Server antworten mit entsprechenden Werten auf eine DHCPDISCOVER-Anfrage.
3. **DHCPREQUEST:** Der Client fordert (eine der angebotenen) IP-Adresse(n), weitere Daten sowie Verlängerung der Lease-Zeit von einem der antwortenden DHCP-Server.
4. **DHCPACK:** Bestätigung des DHCP-Servers zu einer DHCPREQUEST-Anforderung

Es gibt noch andere DHCP-Meldungen:

- **DHCPNAK:** Ablehnung einer DHCPREQUEST-Anforderung durch den DHCP-Server
- **DHCPDECLINE:** Ablehnung durch den Client, da die IP-Adresse schon verwendet wird.
- **DHCPRELEASE:** Der Client gibt die eigene Konfiguration frei, damit die Parameter wieder für andere Clients zur Verfügung stehen.
- **DHCPINFORM:** Anfrage eines Clients nach Daten ohne IP-Adresse, z. B. weil der Client eine statische IP-Adresse besitzt.

Eine 169.254.12.42 IP-Adresse gibt an, dass es einen Fehler gab! Der Client konfiguriert sich so selber.

Die Pakete genauer analysiert

- Wir setzten einen Filter: up.port == 67 || udp.port == 68. Somit hören wir nur noch DHCP-Nachrichten.
- Damit ein PC eine neue IP-Adresse bekommt, sind mindestens 4 Frames nötig:

Type		Richtung	Port (UDP)	
			SRC	DST
DHCP-Discover	**0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x8ea11101** Frame 45 (344 bytes on wire, 344 bytes captured) Linux cooked capture **Internet Protocol**, **Src: 0.0.0.0 (0.0.0.0)**, **Dst: 255.255.255.255** (255.255.255.255) **User Datagram Protocol**, Src Port: bootpc (68), Dst Port: bootps (67) Source port: bootpc (68) Destination port: bootps (67) Length: 308 Checksum: 0xd8eb [correct]	PC – Srv	68	67

	Bootstrap Protocol Message type: Boot Request (1) Hardware type: Ethernet Hardware address length: 6 Hops: 0 Transaction ID: 0x8ea11101 Seconds elapsed: 3 Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0 (0.0.0.0) Your (client) IP address: 0.0.0.0 (0.0.0.0) Next server IP address: 0.0.0.0 (0.0.0.0) Relay agent IP address: 0.0.0.0 (0.0.0.0) Client MAC address: 00:1d:e0:b6:94:a5 (00:1d:e0:b6:94:a5) Server host name not given Boot file name not given Magic cookie: (OK) Option: (t=53,l=1) DHCP Message Type = DHCP Discover Option: (t=50,l=4) Requested IP Address = 10.0.0.102 Option: (t=12,l=6) Host Name = "fuckup" Option: (t=55,l=9) Parameter Request List End Option Padding			
DHCP-Offer	**10.0.0.1 10.0.0.102 DHCP DHCP Offer - Transaction ID 0x8ea11101** Frame 47 (592 bytes on wire, 592 bytes captured) Linux cooked capture Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.102 (10.0.0.102) User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Source port: bootps (67) Destination port: bootpc (68) Length: 556 Checksum: 0x9be1 [correct] Bootstrap Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware address length: 6 Hops: 0 Transaction ID: 0x8ea11101 Seconds elapsed: 0 Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0 (0.0.0.0) Your (client) IP address: 10.0.0.102 (10.0.0.102) Next server IP address: 10.0.0.1 (10.0.0.1) Relay agent IP address: 0.0.0.0 (0.0.0.0) Client MAC address: 00:1d:e0:b6:94:a5 (00:1d:e0:b6:94:a5) Server host name: router Boot file name not given Magic cookie: (OK) Option: (t=53,l=1) DHCP Message Type = DHCP Offer Option: (t=1,l=4) Subnet Mask = 255.0.0.0 Option: (t=3,l=4) Router = 10.0.0.1 Option: (t=15,l=1) Domain Name = ""	Srv – PC	67	68

	Option: (t=6,l=8) Domain Name Server Option: (t=12,l=7) Host Name = "dhcppc2" Option: (t=58,l=4) Renewal Time Value = 1 day, 12 hours Option: (t=59,l=4) Rebinding Time Value = 2 days, 15 hours Option: (t=51,l=4) IP Address Lease Time = 3 days Option: (t=54,l=4) Server Identifier = 10.0.0.1 End Option Padding			
DHCP-Request	**0.0.0.0 255.255.255.255 DHCP DHCP Request - Transaction ID 0x8ea11101** Frame 50 (344 bytes on wire, 344 bytes captured) Linux cooked capture Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255) User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67) Source port: bootpc (68) Destination port: bootps (67) Length: 308 Checksum: 0xd1ab [correct] Bootstrap Protocol Message type: Boot Request (1) Hardware type: Ethernet Hardware address length: 6 Hops: 0 Transaction ID: 0x8ea11101 Seconds elapsed: 3 Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0 (0.0.0.0) Your (client) IP address: 0.0.0.0 (0.0.0.0) Next server IP address: 0.0.0.0 (0.0.0.0) Relay agent IP address: 0.0.0.0 (0.0.0.0) Client MAC address: 00:1d:e0:b6:94:a5 (00:1d:e0:b6:94:a5) Server host name not given Boot file name not given Magic cookie: (OK) Option: (t=53,l=1) DHCP Message Type = DHCP Request Option: (t=54,l=4) Server Identifier = 10.0.0.1 Option: (t=50,l=4) Requested IP Address = 10.0.0.102 Option: (t=12,l=6) Host Name = "fuckup" Option: (t=55,l=9) Parameter Request List End Option Padding	PC – Srv	68	67
DHCP-Ack	**10.0.0.1 10.0.0.102 DHCP DHCP ACK - Transaction ID 0x8ea11101** Frame 51 (592 bytes on wire, 592 bytes captured) Linux cooked capture Internet Protocol, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.102 (10.0.0.102) User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68) Source port: bootps (67)	Srv - PC	67	68

	Destination port: bootpc (68) Length: 556 Checksum: 0x98e1 [correct] Bootstrap Protocol Message type: Boot Reply (2) Hardware type: Ethernet Hardware address length: 6 Hops: 0 Transaction ID: 0x8ea11101 Seconds elapsed: 0 Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0 (0.0.0.0) Your (client) IP address: 10.0.0.102 (10.0.0.102) Next server IP address: 10.0.0.1 (10.0.0.1) Relay agent IP address: 0.0.0.0 (0.0.0.0) Client MAC address: 00:1d:e0:b6:94:a5 (00:1d:e0:b6:94:a5) Server host name: router Boot file name not given Magic cookie: (OK) Option: (t=53,l=1) DHCP Message Type = DHCP ACK Option: (t=1,l=4) Subnet Mask = 255.0.0.0 Option: (t=3,l=4) Router = 10.0.0.1 Option: (t=15,l=1) Domain Name = "" Option: (t=6,l=8) Domain Name Server Option: (t=12,l=7) Host Name = "dhcppc2" Option: (t=58,l=4) Renewal Time Value = 1 day, 12 hours Option: (t=59,l=4) Rebinding Time Value = 2 days, 15 hours Option: (t=51,l=4) IP Address Lease Time = 3 days Option: (t=54,l=4) Server Identifier = 10.0.0.1 End Option Padding			

Wir sehen, dass der DHCP-Client den Port 68 und der Server den Port 67 nutzt.

Aufteilung des IP-Adressraumes

Man vergibt nicht alles verfügbaren IP-Adressen. Einige IP-Adressen reserviert man für folgende Zwecke:

- Default Gateway
- Domänencontroller
- Netzwerkdrucker
- Spezielle Server
- Fileserver
- Datenbankserver
- Infrastruktur-Dienste
  - DHCP
  - DNS
  - Proxy

Den Rest der verfügbaren IP-Adressen kann man durch den DHCP-Server den Clients vergeben. Wie man das macht ist Sache des IP-Konzepts vom Administrator.

7.1.3 Was macht der DHCP-Server bei einer Anfrage?

1. Client übermittelt dem Server seine MAC-Adresse.

2. Der Server sucht einen Eintrag in der statischen Liste.
    1. Findet er einen Eintrag zu der MAC-Adresse, weist der Server dem Client die dazugehörige IP-Adresse zu.
3. Falls er in der statischen Liste nichts findet, sucht er in der dynamischen Liste.
    1. Findet er einen Eintrag zu der MAC-Adresse, weist der Server dem Client die dazugehörige IP-Adresse zu.
4. Findet er keinen Eintrag in der dynamischen Liste, weist der Server dem Client eine dynamische IP-Adresse vom freien Pool zu.

7.1.4 Hinweise zum DHCP

- Der DHCP-Server muss im selben Subnetz sein, wie die Clients, da die Broadcast-Anfrage der Clients nicht geroutet wird.
- Der DHCP-Eintrag läuft in der Regel nach 3 Tagen ab. Diese IP-Adresse kann dann erneut vergeben werden. Diese drei Tage gelten nur, wenn diese IP-Adresse drei Tage lang nicht gebraucht wird!
    - Eine statische Adresse läuft nie ab.
- Die Leasedauer wird auch übermittelt!

> Man kann auch fixe IP-Adressen über DHCP vergeben!

7.1.5 DHCP-Relay-Agent[2]

Bei DHCP-Relay und BOOTP-Relay handelt es sich prinzipiell um den gleichen Mechanismus.

Die beiden Bezeichnungen werden oft synonym verwendet, besonders wenn es um Router-Eigenschaften geht.

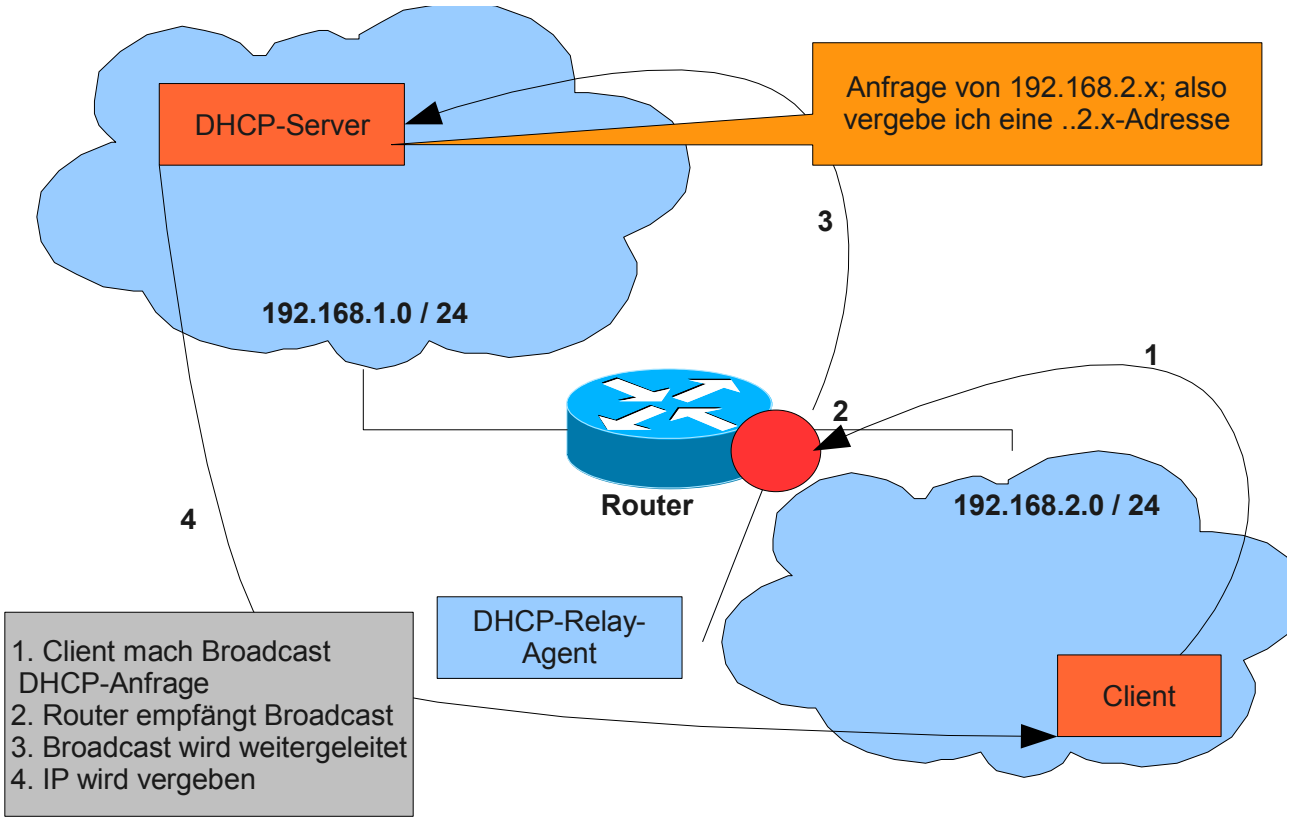
Ein Router, der DHCP-Relay bzw. BOOTP-Relay beherrscht (ein sogenannter **RFC 1542-kompatibler Router**), kann **DHCP-Rundsendungen** (Broadcasts) aus einem seiner angeschlossenen Segmente an einen **DHCP Server weiterleiten, der in einem anderen Segment arbeitet.**

So können Rechner ihre IP-Adressen und -Parameter dynamisch übers Netzwerk erhalten, auch wenn kein **DHCP Server im gleichen Segment** steht (normalerweise würden die Broadcasts einen Router nicht überqueren).

Wenn der **Router diese Technik nicht beherrscht**, kann als Alternative auch auf einer NT- oder Windows 2000 -Maschine der **DHCP-Relay-Agent-Dienst aktiviert** werden.

Der Rechner mit diesem Dienst fängt dann DHCP-Broadcasts in seinem Segment auf und kann sie an einen DHCP-Server in einem anderen Segment weiterleiten.

2 Quelle: http://www.computerlexikon.com/begriff-dhcp-relay



7.2 Namensauflösung

> Vergleiche die Zusammenfassung vom Modul 127! dort steht mehr darin!

Damit Menschen keine IP-Adressen eingeben müssen, wurden Namen erfunden. Wir können uns diese Namen besser merken.

Diese Namen müssen jeoch in eine IP-Adresse umgewandelt werden. Dieser Vorgang heisst Namensauflösung.

Namenssysteme

- Host-Datei
- NetBIOS
- DNS

Die Doppelspurigkeit begründet sich durch die Technologien von UNIX- und Windows-Betriebssystemen.

7.2.1 Host-Datei

- Früher wurde zur Namensauflösung die Hosts-Datei benutzt.
- Unter Windows findet man diese Datei hier: C:\Windows\System32\drivers\etc\hosts
- In Unix-Systemen findet man diese Datei unter /etc/hosts

Hier ist ein Auszug daraus:

```
emanuel@discordia:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       discordia
emanuel@discordia:~$
```

Der Localhost-Eintrag befindet sich immer noch in dieser Datei.

Diese Datei wird heute für andere Zwecke nicht mehr verwendet.

7.2.2 WINS

WINS bedeutet Windows Internet Name Service

- Einträge können auch manuell gemacht werden.
- Wie DNS dient WINS der zentralen Namensauflösung.
- Wenn ein Gerät ans Netz geht, registriert es seinen Namen und seine IP-Adresse automatisch beim WINS-Server.
- Microsoft empfiehlt, so wenige WINS-Server wie möglich einzusetzen.
    - Im Unterschied zu DNS kann WINS keine Hierarchie abbilden. Zudem hat WINS ein Problem damit, veraltete Zuordnungen wieder los zu werden.
- Folgendes wird in der WINS-Datenbank gespeichert:
    - Computername
    - Username
    - Domain / Workgroup

7.2.3 DNS (Domain Name System)

DNS ist einer der wichtigsten (wenn nicht sogar der wichtigste) Dienst im Internet.

- DNS stellt ein verteiltes System dar. Es gibt einige Root-DNS-Server. Diese sagen den untergeordneten DNS-Servern die verlangten IP-Adressen und Namen.

> ??? (vom Lehrer)
>
> Man kann WINS und DNS zusammenarbeitet lassen. Dabei erledigt DNS die oberen Schichten des Domänennamens und überträgt die restlichen Auswertungen an WINS.
>
> ???

Aufgaben

- IP-Adressen in Namen auflösen.
- Namen in IP-Adressen auflösen.
- Zeigt auf gewisse Dienste

- MX-Mailsystem
  - Prioritäten
    - 1. MX Priorität 20 (1. Versuch)
    - 2. MX Priorität 70 (2. Versuch)
  - Wenn der erste MX-Server versagt (mit Priorität 20) dann geht's automatisch zum 2. MX-Server.

7.2.4 NetBIOS[3]

Namensauflösung

NetBIOS erlaubt einer Applikation, einen 16 Zeichen langen Namen netzwerkweit zu registrieren. Ursprünglich wurden die Zuordnungen von Namen zu Netzwerkadressen per Broadcast an alle Teilnehmer bekanntgegeben. Jeder NetBIOS-Name ist entweder als eindeutiger Name (exklusiv) oder als Gruppenname (nicht exklusiv) konfiguriert.

In Microsoft-Netzen werden von den 16 möglichen Zeichen 15 für Namen verwendet; das 16. Zeichen wird als Suffix benutzt, um verschiedene Dienste wie Server, RAS, Messenger usw. anzusprechen:

Rechnername + 00h	exklusiv	Arbeitsstationsdienst
Rechnername + 03h	exklusiv	Nachrichtendienst
Rechnername + 20h	exklusiv	Serverdienst
Benutzername + 03h	exklusiv	Name des angemeldeten Benutzers
Domänenname + 1Bh	nicht exklusiv	Name der Domäne, deren Mitglied der Rechner ist

(Wenn der Name aus weniger als 15 Zeichen besteht, wird er mit Leerzeichen aufgefüllt).

Verbindungsloser Datenaustausch (datagram service)

Die entsprechenden Funktionen realisieren die ungesicherte, paketweise Kommunikation zwischen zwei Endpunkten, ähnlich zu UDP im Internet. Der verbindungslos arbeitende Datagramm-Modus unterstützt einige Broadcast-Funktionen und bietet die Möglichkeit des Aufbaus virtueller Transportverbindungen sowie die Verwaltung symbolischer Namen für Endadressen. Dabei ist die Anwendung verantwortlich für die Aufrechterhaltung der Session.

Verbindungsorientierter Datenaustausch (session service)

Analog zu TCP bietet NetBIOS gesicherte, serialisierte Punkt-zu-Punkt Verbindungen an, d.h. es können Nachrichten übermittelt werden, die größer sind als die maximale Länge eines einzelnen Datenpaketes, und eventuell fehlerhaft angekommene oder verlorene Pakete werden erneut angefordert. Somit wird in diesem Modus eine Fehlererkennung und Fehlerkorrektur durchgeführt.

3 Quelle: Wikipedia

8 Tools

Folgendes sind alles CLI-Tools (Comand Line Interface):

Zweck	Windows	Linux
Zeigt die IP-Adresse	ipconfig	ifconfig
Mehr Infos zur IP# (z.B. MAC-Adresse)	ipconfig /all	ifconfig
ARP-Cache ausgeben	arp -a	arp
ARP-Cache löschen	arp -d *	arp -d <hostname>
IP-Adresse per DHCP erneuern	Ipconfig /release ipconifg /renew	Dhclient
Routing-Tabelle anzeigen	route print netstat -r	route netstat -r
Route zu einem Rechner	tracert <host>	tracert <host>
Verbindung zum Rechner?	ping <host>	ping <host>
Protokollstatistik anzeigen	netstat	netstat

9 Portliste

Original-Dokument von IANA: http://www.iana.org/assignments/port-numbers
Auszug aus Wikipedia:

Nr.	Dienst	Beschreibung
7	Echo	Zurücksenden empfangener Daten
20	FTP-Data	Dateitransfer (Datentransfer vom Server zum Client)
21	FTP	Dateitransfer (Initiierung der Session und Senden der FTP-Steuerbefehle durch den Client)
22	SSH	Secure Shell
23	Telnet	Terminalemulation
25	SMTP, ESMTP	E-Mail-Versand (siehe auch Port 465)
42	Nameserver	Host Name Server (TCP und UDP)
43	Whois	Whois-Anfragen
53	DNS	Auflösung von Domainnamen in IP-Adressen
67	BOOTPS	BootStrap Protokoll server, auch genutzt von DHCP-Anfrage
68	BOOTPC	BootStrap Protokoll client, auch genutzt von DHCP-Antwort
80	HTTP	Webserver
110	POP3	Client-Zugriff für E-Mail-Server
119	NNTP	Usenet (Newsgroups)
123	NTP	Zeitsynchronisation zwischen Computern
143	IMAP	Zugriff und Verwaltung von Mailboxen
161	SNMP (UDP)	Überwachung und Steuerung von Netzwerkelementen
443	HTTPS	Verschlüsselte Webserver Übertragung, meist mit SSL- oder TLS-Verschlüsselung
445	Microsoft-DS	Microsoft Directory Server, Windows Dateifreigabe
465	SMTPS	gesicherter E-Mail-Versand
993	IMAPS	gesicherter Zugriff und Verwaltung von Mailboxen
995	POP3S	gesicherter Client-Zugriff für E-Mail-Server
1723	PPTP	Point-to-Point Tunneling Protocol VPN
3306	MySQL	Zugriff auf MySQL-Datenbanken
3389	RDP	Windows Remotedesktopzugriff, Windows Terminal Services
5060	SIP	IP-Telefonie
5800	VNC	Virtual Network Computing (Port für Java-Zugriff)
5900	VNC	Virtual Network Computing (Port für VNC Viewer-Zugriff)
6667	IRC	Chatserver
10000	Webmin	Webmin - Web-basierende Oberfläche für Systemadministratoren unter Linux
20000	Usermin	Oberfläche für Systemadministratoren unter Linux (ähnlich Webmin)

- Auf einem Unix-Rechner ist diese Liste in der Datei /etc/services definiert.
- Unter Windows ist diese Liste in der Datei %WINDIR%\system32\drivers\etc\services

10 Glossar

Begriff	**Erklärung**
DHCP	Dynamic Host Configuration Protocol; Das Protokoll dient der Konfiguration der Workstations per Server.
DNS	Domain Name System
EIA	Verband der elektronischen Industrie der USA. Der Verband erlässt einige Normierungen, z.B. für die Belegung von Twisted-Pair-Kabeln nach EIA/TIA 568.
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocoll
IANA	Internet Assigned Numbers Authority; Organisation, die die Vergabe von IP-Adressen, Top Level Domains und IP-Protokollnummern, sowie die Zuordnung der Haupt-Ports 0 bis 1023 regelt
IEEE	Institute of Electrical and Electronical Engineers; Amerikanischer Verband, der sich ua um die Standardisierung von lokalen Netzwerken (Arbeitsgruppe IEEE 802) kümmert.
IP	Internet Protocol
ISO	Internationale Organisation für Ordnung
LAN	Local Area Network
LLC	
MAC	Medium Access Control
OSI	Open Systems Interconnectrion
POP3	Post Office Protocol Version 3
SMB	Service Message Block; Windows-Datei- und Druckerfreigaben verwenden ua SMB. Unter UNIX werden solche Freigaben mittels Samba nutzbar.
SMTP	Simple Mail transfer Protocoll
TCP	Transmission Controll Protocoll
VLAN	Virtual LAN
WAN	Wide Area Network
WLAN	Wireless LAN
FCS	Frame Check Sequence
Integrität	Vollständigkeit und Richtigkeit der Daten
CSMA/CD	Carrier Sense Multiple Access / Collision Detection; Zugriffsverfahren
CRC	cyclic redundancy check
ADSL	
WINS	Windows Internet Name System
RAID	Redundant Array of Inexpensive Disks
USV	Unterbrechungsfreier Stromversorgungen
DFS	Distributed File System
FRS	Fire Replication Service
Telematik	Zusammensetzung aus Telekommunikation und Informatik. Verknüpft diese

	Technologien. Telematik ist also das Mittel der Informationsverknüpfung von mindestens zwei EDV-Systemen mit Hilfe eines Telekommunikationssystems, sowie einer speziellen Datenverarbeitung.
Telekommunikation	Kommunikation (mit elektronischen Hilfsmittel) über die Ferne.
Informatik	Informatik ist die Wissenschaft von der systematischen Verarbeitung von Informationen, insbesondere der automatischen Verarbeitung mit Hilfe von Rechenanlagen. Historisch hat sich die Informatik als Wissenschaft aus der Mathematik entwickelt, während die Entwicklung der ersten Rechenanlagen ihre Ursprünge in der Elektrotechnik und Nachrichtentechnik hat
Dedizierterer Server	Ein Dedizierter Server (engl. dedicated server, DS) ist ein Server, der nur für eine Aufgabe abgestellt wird (dedicated to service) oder nur einem Kunden zugeordnet ist (dedicated to customer).
Zugriffsverfahren	CSMA / CD oder TokenPassing

11 Gute Links

- http://www.heineshof.de/lan/lan.html
-

Stichwortverzeichnis