Netzwerktechnik 1 - Grundlagen, Aufbau und Funktionsweise

2022-03-09

Zusammenfassung Diese Unterlagen sind ausschließlich für den Unterricht erstellt. Die dargestellten Inhalte stützen sich auf gängige Fachliteratur und im Internet frei zugänglichen Informationen zu den Themen. Dieses Skriptum soll in der zur Verfügung stehenden Zeit, die elementaren Grundbegriffe sowie die technische Zusammenhänge der Themen, auf einfache Weise vermitteln. Die dazu erforderlichen Fakten und Methoden, werden hauptsächlich aus der Sicht eines versierten Anwenders betrachtet. Tieferes Verständnis der dargestellten Materie, muss einschlägiger Fachliteratur entnommen werden.

Inhaltsverzeichnis

1 Einführung

Aus dem Alltag sind viele Netzwerke (technische Einrichtungen) bereits bekannt, zB.

- Telefonnetze → Festnetz, Mobil
- Infrastrukturnetze → Wasser, Kanal, Strom, Gas
- Verkehrsnetze → Strasse, Bahn, Flugverkehr
- Datennetze → Kommunikationsnetze in Technik und Industrie (Bussysteme zur internen Komm.)

Darüber hinaus gibt es auch soziale Strukturen die als Netzwerk bezeichnet werden können. In diesem Skriptum wird im weiteren nur mehr das IT-Netzwerk (kurz Netzwerk) betrachtet. Als Beispiel ist hier ein klassisches Heimnetzwerk zu sehen, wie es bei Festnetzanschluss oft vorkommt.

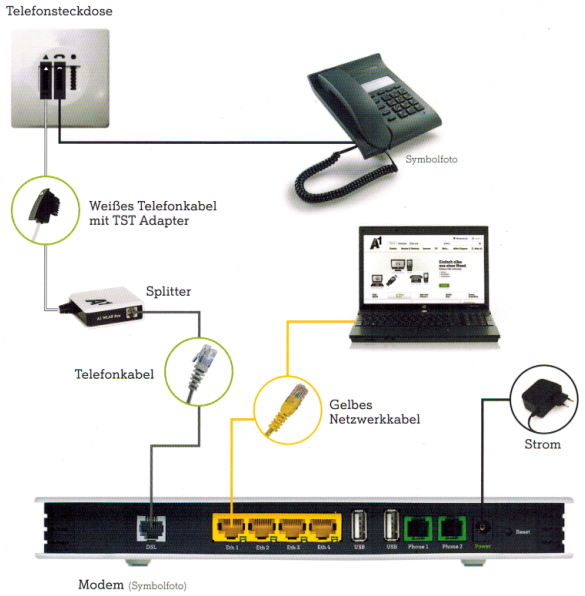


Fig. 1: Heimnetzwerk

In den technischen Daten des „Routers“ (DSL Modem TG788) finden Sie unter anderem folgende Begriffe:

- ADSL2+, Annex A, PPPoE
- *Ethernet-LAN 10/100Mbit/s*
- *2.4GHz WLAN 802.11b/g*
- *DHCP, DynDNS, NAT, ...*

Diese „Router“ bauen meist Punkt-zu-Punkt Verbindungen zum ISP auf. Die Technologien dazu sind u.a. ADSL, ATM, LTE. Bei

intensivem Studium dieses Skriptums werden sich dem Leser diese Begriffe und einige wichtige Grundlagen der Netzwerktechnik erschließen. Es soll in erster Linie die Zusammenhänge erkennbar machen, nicht die genauen technischen Details beschreiben.

2 Historische Entwicklung

Rückblickend seien folgende Ereignisse in der Geschichte erwähnt:

1955: Erster Computer (Mailüfterl, TU-Wien)

1969: ARPANET, erste Vernetzung zentraler Großcomputer

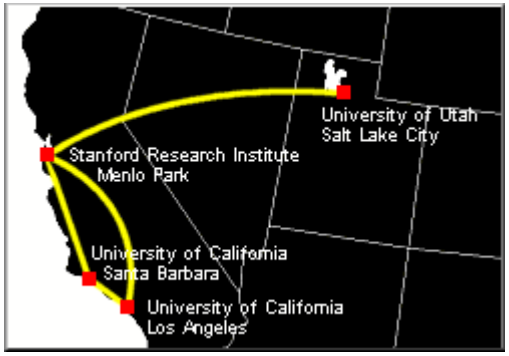


Fig. 2: ARPANET

1972: ARPANET bekommt Ethernet, FTP und e-Mail als Services

1973: ALOHA, erstes Funk-Netzwerk über große Distanzen

1975: Einführung des TCP-Protokolls

1984: OSI-Schichtenmodell wird verpflichtend eingeführt

1991: Das WWW entsteht am CERN

1995: Fast Ethernet

1999: Gigabit Ethernet

Im März 2019 waren alleine mehr als 138 Millionen .com-Domains weltweit registriert.

Teil I. Klassifizierung

3 Grundlagen

Das einfachste Netzwerk bilden zwei Computer, die direkt durch ein Kabel verbunden sind. Jeder Computer in einem Netzwerk benötigt einen Netzwerkadapter (oft im Motherboard integriert), an dem das Verbindungskabel angeschlossen wird. Grundsätzlich besitzt jedes aktuelle IT-Netzwerk viele unterschiedliche Elemente. Dies sind vor allem

- Workstations → lokale Teilnehmer
- Übertragungsmedium → Verbindung

- Vermittlungsstellen → Verteilzentren
- Netztopologie → Struktur
- Netzwerktechnologie → Transportmethode
- Übertragungsprotokolle → Nutzungsregeln
- Server → zentrale Dienste
- Verbindungen zur Außenwelt → Router

Ein IT-Netzwerk ist ein Zusammenschluss verschiedener selbstständig arbeitender Komponenten (Switches, Hubs, Router, ...) der die Kommunikation der einzelnen Knoten untereinander ermöglicht. Zweck ist der Transport von Information mit Hilfe elektrischer, optischer oder elektromagnetischer Signale. Ziel ist heute oft auch die gemeinsame Nutzung von Ressourcen aller Art (Cloud-Dienste).

1. Knoten → Endgeräte (WS, Server, Mobilgeräte, IoT-Geräte, Maschinen, Anlagenkomp.)
2. Übertragungsmedien → Kupferkabel, Glasfaserkabel, Funkwellen
3. Technologien → Token Ring, Ethernet, ADSL, UMTS, LTE
4. Topologien → Bus, Stern, Ring

Die Gründe zur Errichtung von IT-Netzwerken sind vielfältig. Je nach Anforderung sind daher Topologie, Technologie und Management der Netze recht unterschiedlich. Meist jedoch braucht man

- Kommunikation der Arbeitsgeräte (Workstations)
- Nutzung zentrale Dienste (Server, interne Daten)
- Anbindung an das Internet (entfernte Netze, öffentliche Daten)

Nicht alle Netzwerke oder Einzelgeräte haben Zugang zum Internet. Es gibt viele Anwedungen die dies Untersagen (Inselsysteme). Maschinen und Anlagen einer Produktion sind zwar vernetzt, aus Gründen der Unabhängigkeit und vor allem der Sicherheit aber vom Internet getrennt.

4 Einteilung nach Größe

4.1 Lokale Netzwerke

Ein Local Area Network (LAN) ist ein Computernetz, das üblicherweise Geräte in einem direkten Umfeld miteinander verbindet. Ein LAN wird daher in privaten Heimnetzwerken oder Gebäude-Netzwerken eingesetzt. Es ist auf einzelne Gebäude, Stockwerke oder Abteilungen beschränkt. Alle Knoten liegen in diesen beschränkten Arealen. Die Übertragungstechnologie die hier verwendet wird, ist Ethernet.

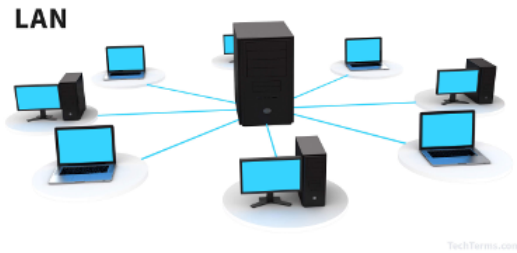


Fig. 3: Lokales Netzwerk

4.2 Regionalnetzwerke

Metropolitan Area Networks (MAN) sind Netzwerke die in Städten Gebäude mit einander verbinden. Ein ISP der seine Kunden mit Internet-Verbindungen versorgt, bildet ein MAN. Die Übertragungsgeschwindigkeit solcher Stadtbereichsnetze kann sehr hoch werden. MAN-Netzwerke sind durch die Standards IEEE 802.6 genormt.

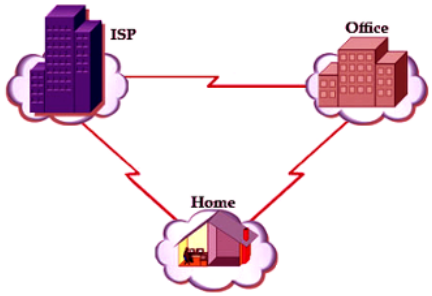


Fig. 4: Regionalnetz

4.3 Weitverkehrsnetze

Ein Wide Area Network (WAN) ist ein Computernetz, das sich bereits über einen sehr großen geografischen Abstand erstreckt. Städte, einzelne Ländern und alle Staaten werden damit verbunden. Typischerweise werden damit die dort vorhandenen MAN verbunden. Die verwendete Übertragungstechnik ist schnelles Ethernet aber teilweise auch noch ATM (Breitband-Technologie, Multiplexing-Verfahren).

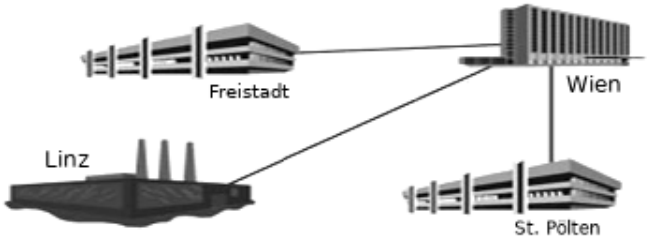


Fig. 5: Weitverkehrsnetz

WAN mit besonders hoher Übertragungsgeschwindigkeit wird auch als Information Highway oder Datenautobahn bezeichnet. Hier wird als Übertragungsmedium Glasfaser verwendet.

5 Einteilung nach Organisation

5.1 Peer-to-peer Netze

P2P-Netz ist eine synonyme Bezeichnung für eine gleichrangige Kommunikation unter allen Teilnehmern. In einem reinen P2P-Netz sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen, als auch zur Verfügung stellen. P2P stellt eine logische Netzwerkstruktur dar und kann daher parallel in einem LAN neben einer anderen Struktur existieren.

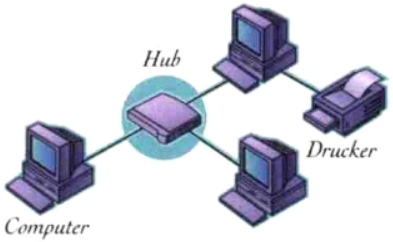


Fig. 6: Peer-to-Peer

Workgroup ist die bekannte Bezeichnung von Microsoft für ein P2P-Netz. Mit aktuellen Smart-Phones kann man ganz einfach ein WLan P2P-Netz aufbauen um Daten (sehr schnell) auszutauschen. Die Bezeichnungen für diese P2P-Netze sind aber herstellerabhängig unterschiedlich. Man findet die Begriffe „Wi-Fi Direct“ oder „Quick Connect“ sowie „Airplay“ als Synonyme für P2P. Im Gegensatz zum P2P-Netz ist ein ad-hoc Netzwerk eine physische Struktur.

5.2 Client-Server Netze

Das Client-Server-Modell beschreibt eine Möglichkeit, Aufgaben und Dienstleistungen innerhalb eines Netzwerkes zu verteilen. Der Client kann dabei auf Wunsch einen Dienst vom Server anfordern. Der Server stellt darauf hin die Anforderung für den Client zur Verfügung. Alle zentral organisierten Netze sind CS-Netze. Die Kommunikation der Rechner untereinander ist aber immer noch P2P.

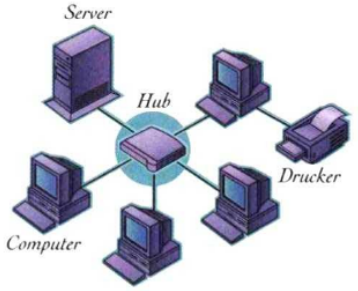


Fig. 7: Client-Server

Üblicherweise kann ein Server gleichzeitig für mehrere Clients arbeiten und auch mehrere Services gleichzeitig anbieten. Mit Linux lassen sich sehr einfach DHCP-, DNS-, LDAP-, VPN-, FTP-, SMB/Cifs-, Cups-, Web-Server, usw. sogar auf einem Raspberry einrichten. Zu Übungszwecken und um das Verständnis über diese Dienste zu vertiefen, ist dies sehr zu empfehlen.

Teil II. Topologien

6 Grundlagen

Unter der Topologie versteht man die Art, wie die verschiedenen beteiligten Komponenten (also zumeist Computer) im Netz durch physische oder logische Leitungswege verbunden sind. Die Anordnung der Knoten und deren Verbindungen, lässt sich dazu graphisch sehr anschaulich darstellen. Es gibt logische und physikalische Topologien. Ein Netzwerk kann bei der Verkabelung mit TP-Kabeln physisch wie ein Sternnetz aussehen, logische aber Busstruktur oder Ringstruktur besitzen.

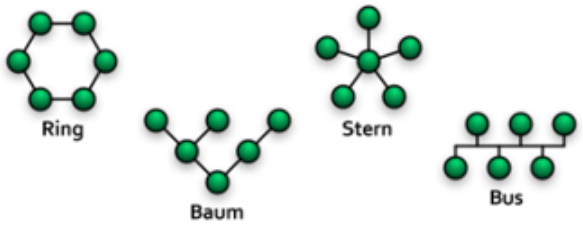


Fig. 8: Einfache Topologien

6.1 Ringtopologie

Es gibt keine Zentrale, alle Stationen sind gleichberechtigt. Jeder Teilnehmer ist mit seinem linken und rechten Partner verbunden. Übertragung erfolgt in einer Richtung von Knoten zu Knoten. Bei Ausfall eines Knotens sind sämtliche Kommunikationswege unterbrochen.

Nachteil Eine Störstelle betrifft alle, jeder Knoten braucht 2 Anschlüsse

Vorteil Viel Weniger Kabel nötig, keine zentralen Knoten nötig

6.2 Sterntopologie

Alle Teilnehmer sind an einen zentralen Knoten angeschlossen. Direkte Kommunikation der Teilnehmer untereinander nicht möglich. Bei Ausfall der Zentrale sind sämtliche Kommunikationswege unterbrochen.

Vorteil Kabelbruch trifft nur einen Knoten, hinzufügen von Netzknoten ohne Stillstand möglich

Nachteil Viel Kabel nötig, zentrale Knoten sind nötig

6.3 Bustopologie

Es gibt keine Zentrale und keine Knoten. Die Verbindung aller Teilnehmer erfolgt über einen gemeinsamen Übertragungsweg. Zu einem Zeitpunkt kann immer nur eine Nachricht über den Bus transportiert werden. Bei Ausfall einer Station bleibt die Kommunikation der anderen Stationen erhalten. Busnetze müssen auf beiden Seiten

mit der Leitungsimpedanz abgeschlossen werden, damit keine Echos auftreten, die zu Empfangsfehlern führen.

Nachteil Kabelbruch trifft alle, hinzufügen eines Zusatzknotens erfordert Stillstand

Vorteil Wenig Kabel nötig, kein zentraler Knoten nötig

6.4 Komplexe Topologien

Je nach Bedarf können die obige einfache Topologien auch miteinander kombiniert werden, zB. Bus mit angeschlossenen Sternen oder Bus mit angeschlossenen Bussen, was zu einer Baumstruktur führt. Teilweise ergeben sich dabei redundante Leitungswege, die auch bei Unterbrechung eines Wegs den Datentransport sicherstellen.

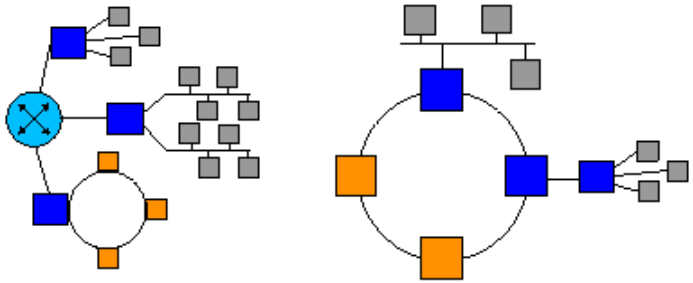


Fig. 9: Komplexe Topologie

6.5 Das Ur-Ethernet Netzwerk

Das Ethernet Netzwerk ist ursprünglich eine Bus-Topologie. Zur Verbindung der Computer untereinander wurde die Thin-Wire Verkabelung (RG58 Koaxialkabel) eingeführt. Die Computer wurden mit BNC-Steckern angeschlossen. Dies ergab die folgende Anordnung.

Fig. 10: Ur-Ethernet

Die Stranglänge für alle Rechner betrug max. 185m und jeder Strang musste an beiden Ende mit 50Ohm Terminatoren abgeschlossen sein (Signalreflexion). Als Zugriffsverfahren wurde CSMA/CD entwickelt, das heute noch immer verwendet wird. Die Übertragungsgeschwindigkeit betrug 10Mbit/s. Das Netzwerk stellte ein P2P-Netzwerk dar.

7 Universelle Gebäudeverkabelung

7.1 Wandel zur Sternverkabelung

Die Geschwindigkeit des Ur-Ethernet stieß bald an seine Grenzen (Kollisionen beim Zugriff). Daher wurden Bridges zwischen die ein-

zelnen Computer geschaltet, um die Stränge zu segmentieren. Eine Bridge merkt sich welche Computer direkt links und rechts angeschlossen sind. In den einzelnen Strangabschnitten waren daher weniger Computer. Datenpakete wurden so nicht mehr überall hin weitergeleitet. Man erhielt eine Trennung in kleinere Kollisionsdomänen.

Fig. 11: Ur-Ethernet mit Bridges

Ein Problem blieb immer noch bestehen, die Bus-Topologie. Wenn der Strang unterbrochen wird, fällt immer noch das gesamte Netz aus. Es wurden also Konzentratoren entwickelt, die die Anschlüsse des Koaxialkabels (BNC T-Anschlüsse) in 1 Gerät konzentrierte und so für jeden Computer einen Anschluss bot - mit Bridge je Anschluss. Diese Bridge erkennt nun auch ob ein Gerät angeschlossen ist. Wenn nicht wird der Anschluss automatisch terminiert. Damit hat man Kollisionsdomänen erzeugt mit nur 2 Geräten je Segment (Bridge und Computer) und es sind keine Abschlusswiderstände mehr notwendig.

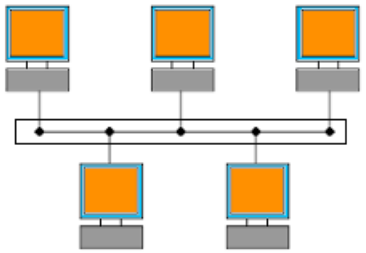


Fig. 12: Netz-Konzentrator

Mit diesen Konzentratoren konnte man nun anders verkabeln. Die Segmentlänge kann auf ihre max. Länge ausgedehnt werden.

7.2 Strukturierte Verkabelung

Strukturierte Verkabelung ist dienst- und anwendungsneutral. Das Kabel ist für verschiedenste Technologien geeignet, zB.: Twisted-Pair, Token-Ring, Glasfaser. Die Struktur einer UGV wird, ausgehend von einem zentralen Standortverteiler, nun in vier Bereiche unterteilt:

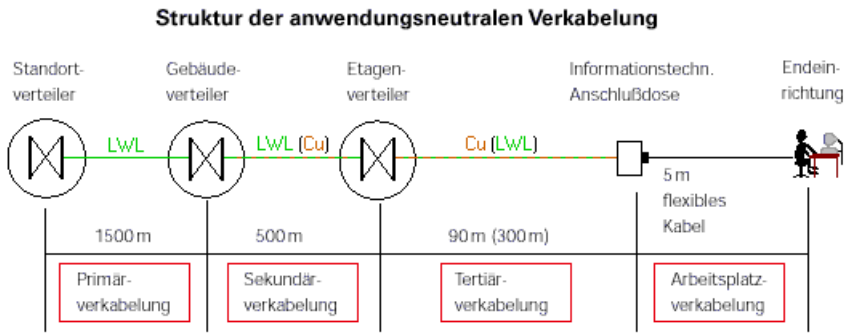


Fig. 13: Strukturierte Verkabelung

1. Primärbereich: für die Verbindung (vom Standortverteiler) zu den Gebäuden

2. Sekundär- oder Vertikalbereich: für die Verbindung zu den einzelnen Etagen im Gebäude

3. Tertiär- oder Horizontalbereich: für die Verbindung zu den Anschlussdosen

4. Arbeitsplatzbereich: für den Anschluss der Endgeräte an die Anschlusseinheiten

Primärbereich Der Knoten des Primärbereiches ist ein Standortverteiler. Aufgrund der Entfernungen zu seinem nächsten Knoten, ist er heute oft in Glasfaser-Technik angeschlossen.

Sekundärbereich Bildet auf Gebäudeebene ein Backbone-Netz. Die Ausführung kann sowohl mit Kupferkabeln erfolgen, als auch in Glasfaser-Technik.

Tertiärbereich Im Etagenbereich werden die Anschlussdosen sternförmig mit dem Etagenverteiler verbunden. Die Entfernungen von Etagenverteiler bis zu den Anschlussdosen sollen 90m nicht überschreiten.

Arbeitsplatzverkabelung Die Computer werden über flexible TP-Kabel an den Netzwerkdosen angeschlossen. Diese Kabel sollen immer so kurz wie möglich gehalten werden. Sie sind empfindlich und sollen daher geschützt liegen. Eine große Störquelle stellen die Steckverbindungen dar. Sie sind besonders vorsichtig zu handhaben.

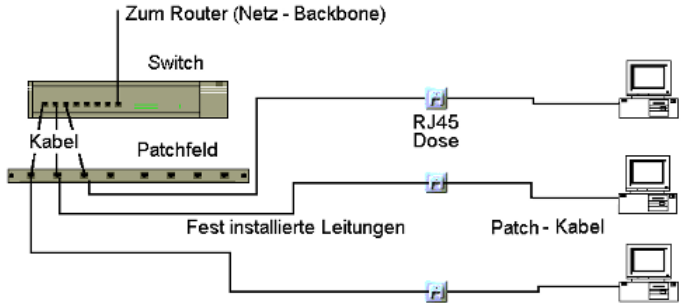


Fig. 14: Kabellegung

Damit ist nun die Verkabelung eines Gebäudes im Prinzip beschrieben. Aktuell werden alle Netzwerke nach diesem Schema verkabelt.

7.3 Das Backbone

Backbone (Rückgrat, Hauptverbindung) bezeichnet einen verbindenden Strang eines Netzwerkes mit sehr hohen Datenübertragungsraten. Größere Netzwerke sind oft durch einen einzigen Stern nicht mehr realisierbar. Man verbindet dann mehrere Sterne mittels sogenannter Backbones.
Da die Anforderungen an die Backbone-Technologie (Geschwindigkeit, Störsicherheit, ...) die Möglichkeiten von Kupferkabeln übersteigen, wird dafür üblicherweise Glasfaserkabel verwendet. Es gibt verschiedene Topologien von Backbone-Netzen:

Stern-Topologie Collapsed Backbone

Ring-Topologie Distributed Backbone

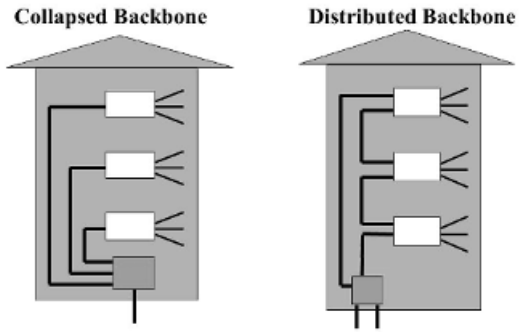


Fig. 15: Backbone

Beim Collapsed Backbone handelt es sich um ein virtuelles Backbone, das von nur einem Knoten, meist dem zentralen Main-Switch gebildet wird.
Das Fiber Distributed Data Interface FDDI ist eine spzielle Hardware für Distributed Backbones. Als Medium werden Glasfaserkabel in einem doppelten, gegenläufigen Ring mit Token-Zugriffsmechanismus verwendet (100Mbit/s).

Fig. 16: FDDI-Adapter

Das Backbone muss heute jedenfalls folgende Dienste bieten:

- Zentrales Management
- Hohe Datenrate
- Hohe Ausfallssicherheit

Durch wenige aktive Netzwerkkomponenten ist ein zentrales Management eines Backbones möglich, was zu einer einfachen Wartung und damit einem zuverlässigeren, sichereren Netz führt.

Teil III. Komponenten

Im folgenden werden Komponenten eines IT-Netzwerkes vorgestellt. Ihre Funktion und Verwendung wird aber vorerst nur oberflächlich betrachtet. Folgende Kopplungselemente sind heutzutage üblich und fast überall zu finden

Hub	Konzentrator (ohne Kollisionstrennung)
Bridge	Koppler zwischen Systemen (Kollisionstrennung, Ethernet / Token-Ring)
Switch	Konzentrator (mit Kollisionstrennung)
Router	Kopplung unterschiedlicher Protokoll-Systeme (IP / PPPoE)
Gateway	kein Gerät sondern eine Funktion (in Routern)
Transducer	Medienkonverter (Ethernet / Glasfaser)

8 Kopplungselemente

Im folgenden werden die Kopplungselemente beschrieben. Ihre Aufgaben sind sehr unterschiedlich, daher auch ihre Funktionen sowie ihre Anschaffungskosten. Je besser konfigurierbar die Geräte sind, desto teurer werden sie. In modernen Netzwerken müssen aber viele Konfigurationsmöglichkeiten genutzt werden (Segmentierung, Sicherheit).
Zu Beginn werden wir jedoch das wichtigste Element besprechen, den Transceiver. Transceiver ist ein Kofferwort aus Transmitter (Sender, Tx) und Receiver (Empfänger, Rx). Alle Netzwerkadapter verfügen über eine solche Hardware. Je nachdem, welches Übertragungsmedium eingesetzt wird, handelt es sich dabei um elektrische Impulse, Licht (IR) oder Funkwellen (Bluetooth).

8.1 Hub

Als Hub werden Geräte bezeichnet, die einen scheinbaren Sternknoten bilden. Hubs lösen die Bus-Topologie jedoch nicht auf, sie ist nur auf den inneren Aufbau der Hubs reduziert.

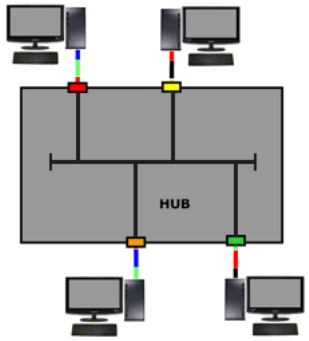


Fig. 17: Hub

Hubs leiten jedes Datenpaket weiterhin an alle anderen weiter. Hubs sollen daher auch nicht mehr verwendet werden (Vorsicht bei billigen Mini-Switches)! Bussysteme sind aber sehr wohl in Verwendung (Maschinen, Fahrzeuge, Motherboards).

8.2 Bridge

Allgemein wurden Bridges zum Segmentieren von Netzwerksträngen und zum Verbinden unterschiedlicher Architekturen entwickelt (zB. Ethernet mit Token-Ring). Bridges führen Adresstabellen, anhand der entschieden wird, wie Datenpakete weitergeleitet werden müssen. Broadcasts werden dabei immer weitergeleitet. Die Bridge in nachfolgender Abbildung trennt einen Netzwerkstrang in 2 Kollisionsdomänen.

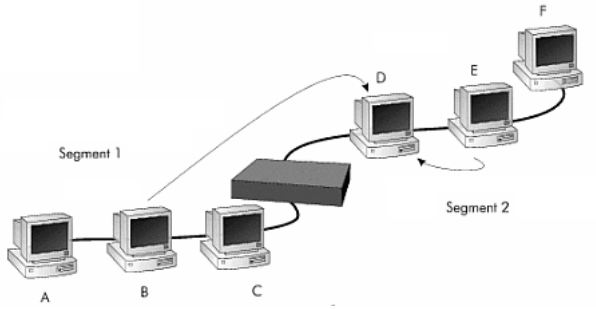


Fig. 18: Bridge

Bridges zum Verbinden eines LANs mit einem WLAN lassen sich recht einfach auf einem Raspberry einrichten. Mit dem Aufkommen von Switches sank die Bedeutung von Bridges. Mit dem Aufkommen von WLAN wurden diese aber wieder aktuell. Bridges sind auch in der Architektur von Motherboards vorhanden (North-, South-Bridge).

8.3 Switch

Ein Switch verbindet Computer ähnlich einem Hub, jedoch ist hier an jedem Anschluss auch eine Bridge installiert. Damit trennt ein Switch alle Anschlüsse in eigene Kollisionsdomänen. Dies ist optimal, weil damit jedes Segment die volle Segmentlänge nutzen kann (100m) und es keine Kollisionen mehr gibt (nur mehr 2 Teilnehmer je Strang).

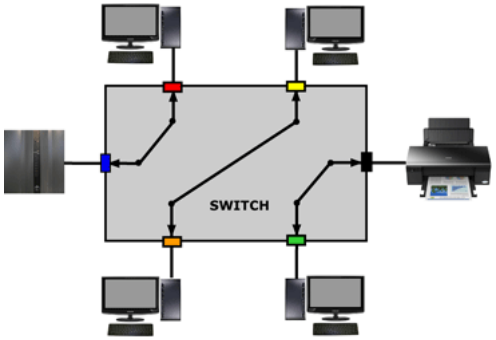


Fig. 19: Switch

- Bildet Netze mit Sterntopologie
- Leitet Pakete nur an Empfänger weiter
- Jeder Host kann volle Bandbreite nutzen
- Bietet bestmögliche Kollisionstrennung
- Bietet volle Ausnutzung der Segmentlänge

Auto-Sensing Fähigkeit eines Switch-Ports, sich auf die Geschwindigkeit des Clients einstellen zu können.

Auto-Negotiation Zusätzlich kann hier auch noch der beste Betriebsmodus der Übertragungsleitung (Half / Full Duplex) bestimmt werden. Der Client und der Switch müssen dabei gleich konfiguriert werden.

Uplink-Port Der Uplink-Port ist ein spezieller Port zum Aufbau einer kaskadierenden Baumstruktur. An diesem Uplink-Port darf dann kein Endgerät hängen, sondern der übergeordnete Switch. Switches können auch mit mehreren Uplink-Ports ausgestattet sein.

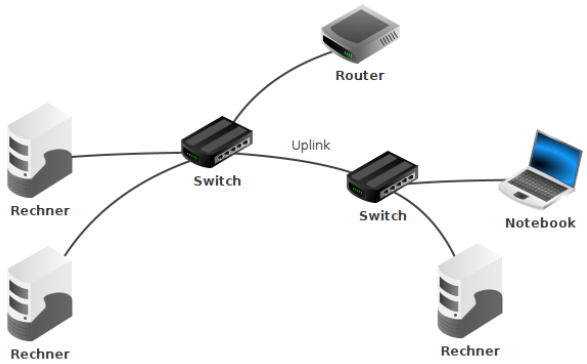


Fig. 20: Uplink-ports

8.4 Router

Router verbinden einzelne Rechner oder Teilnetze zu anderen Netzwerken hin. Ein Router braucht daher mindestens zwei Netzwerkschnittstellen. Home-Router vermitteln zwischen privaten und öffentlichen Netzwerken und bieten viele weitere Funktionen an (DHCP, SMB, Firewall, etc). Es gibt

1. Unmittelbare Verbindung von Netzen

2. Vermittelte Verbindung von Netzen

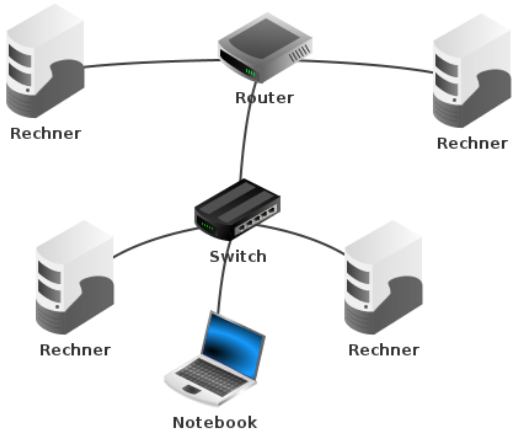


Fig. 21: Router

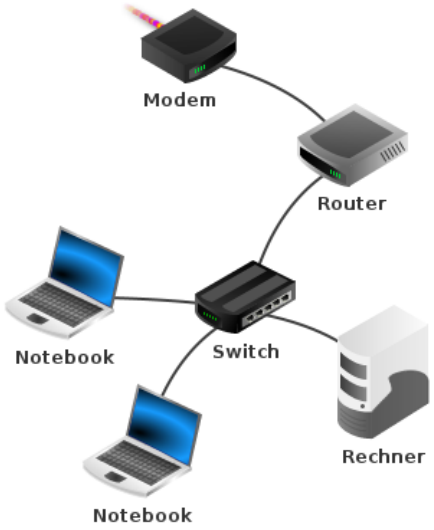


Fig. 22: Heimnetz-Anbindung

Durch Router abgetrennte Netze bilden eigene Broadcast-Domains. In einer solchen Domain sieht ein Computer die Computer jenseits des Routers nicht mehr. Die Broadcasts, mit denen Computer im Netz suchen (zB. mittels ARP, Avahi, etc.), enden am Router. Die Vermittlung ins andere Netzwerk erfolgt jetzt durch Adressierung des Empfängers in Layer III (Gateway). Viele einfache Router lassen nur bestimmte Protokolle durch, Multiprotokollrouter sind entsprechend aufwendiger. Die Internetanbindung eines Heimnetzes erfolgt, wie bereits gezeigt, ebenfalls durch Home-Router.

8.5 Gateway

Das Gateway bezeichnet eine Funktion, welche alle nicht ins eigene Subnetz gehörenden Verbindungen über Routing in ein anderes Subnetz weiterleitet. Diese Funktion zur Wegfindung, ist in Routern implementiert. Daher ist dem Gateway keine eigene Hardware zuzuordnen.

8.6 Transducer

Ein Transducer ist eine Komponente zur Umwandlung einer Signalform in eine andere. Typischerweise bei der Umsetzung von TP-Verkabelung auf LWL kommen solche Medienkonverter zum Einsatz. Damit kann man deutlich größere Abstände zwischen den Netzwerkknoten überbrücken.

Fig. 23: Transducer

Teil IV. Leitergebundene Datenübertragung

9 Übertragungsmedien

Die Verbindung der einzelnen Netzwerkknoten setzt eine Vielzahl von Entscheidungen hinsichtlich der Struktur des Netzwerks voraus. Die Wahl des Verbindungsmediums spielt eine wichtige Rolle. Die Übertragungsmedien in einem Netzwerk sind heutzutage Kupferkabel, Lichtwellenleiter oder Funk.

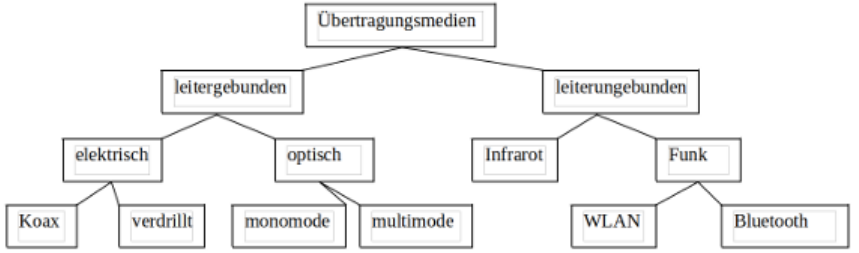


Fig. 24: Überblick

9.1 Koaxialkabel

Koaxialkabel sind zweipolige Kabel mit konzentrischem Aufbau. Sie bestehen aus einem Innenleiter, der in konstantem Abstand von einem hohlzylindrischen Außenleiter umgeben ist. Der Außenleiter schirmt den Innenleiter gleichzeitig vor Störstrahlung ab (Erdung). Es gibt unterschiedliche Koaxialkabel, die Typen RG-11 und RG-58 sind für Ethernet.

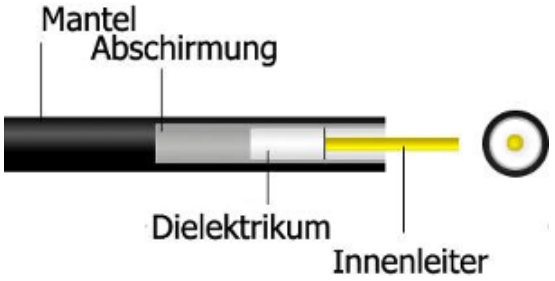


Fig. 25: Koaxialkabel

- Innenleiter ist Kupferdraht
- Äußerer Leiter ist Drahtgeflecht, dient gleichzietig als Abschirmung
- Korrekte Erdung ist wichtig
- Datendurchsatz 10Mbit (Ethernet)
- Max. Länge 185m (Ethernet)
- Steckverbindung BNC-Kupplung

9.2 Twisted-pair Kabel

Die einzelnen Adern sind dünne Einzeldrähte. Die Kabel sind leicht zu biegen (Mindestbiegeradius) und daher ideal zum Verlegen im Gebäude, im Verteilerschrank und am Arbeitsplatz. Es gibt sie als Endlos- oder Fertigware. Fertige Kabel werden auch als Patchkabel bezeichnet.

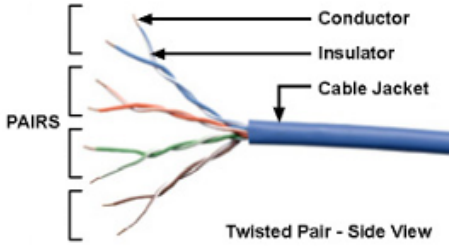


Fig. 26: TP-Kabel

- Vier verdrillte Drahtpaare
- Verdrillung bewirkt Auslöschung von Signalstörungen
- Verdrillung schützt auch gegen elektromagnetische Störungen
- Datendurchsatz 10Gbit (Ethernet)
- Max. Länge 100m (bei Ethernet)
- Steckverbindung RJ-45

Sie bieten verbesserten Schutz vor äußeren elektrischen Feldern, besonders durch eine zusätzliche elektrisch leitenden Abschirmung (muss geerdet werden). Adernfarben, Pins und Verwendung sind in der folgenden Abbildung zu sehen.

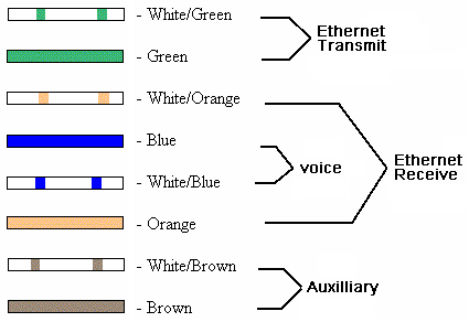


Fig. 27: Adernpaare

9.2.1 Belegungsarten

Es gibt zwei Belegungsarten (nach EIA/TIA) der Stecker für den Einsatz in der Ethernet-Technologie, T568A und T568B. Im europäischen Raum wird im Allgemeinen nach TIA-568A verkabelt. Die meisten Kabel die Produkten beigepackt sind, sind aber nach T568B belegt.

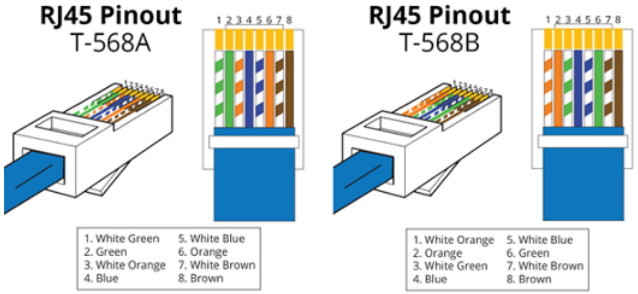


Fig. 28: Belegungsarten

9.2.2 Adernführung

Mit TP-Kabel kann man auch eine Direktverbindung zweier Computer herstellen. Dazu ist aber eine spezielle Verdrahtung zu verwenden, das Cross-Over Kabel. Eine einfache Regel zur Benutzung von Cross-Over- oder Straight-through-Kabel ist: Gleiches und Gleiches wird immer Cross-Over verbunden.

Fig. 29: Adernführung

9.2.3 Kabelaufbau

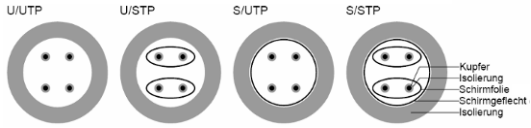


Fig. 30: Kabelquerschnitt

U/UTP-Kabel Nicht abgeschirmte verdrillte Leitungen, keine Gesamtabschirmung - unshielded/unshielded twisted pair

U/STP-Kabel Abschirmung für jedes verdrillte Kabelpaar aber ohne Gesamtabschirmung - unshielded/shielded twisted pair

S/UTP-Kabel Gesamtabschirmung, darunter nicht abgeschirmte verdrillte Leitungen - shielded/unshielded twisted pair

S/STP-Kabel Abschirmung für jedes Kabelpaar sowie Gesamtabschirmung, optimale Störungsunterdrückung - shielded/shielded twisted pair

9.2.4 Kabelverlegung

Verlegekabel werden im dauerhaft verlegten Teil der Netzwerkverkabelung verwendet. Die Drähte werden mittels LSA-Tool (Auflegewerkzeug) auf Schneidklemmen in der Dose und am Patchfeld aufgelegt. Mit speziellen Crimp-Zangen werden die RJ45-Stecker geklemmt.

Fig. 31: Werkzeug

9.2.5 Kabelqualität

Überprüfbare Qualität erfordert definierte Standards. Verschiedene Institutionen definieren daher Standards für Verkabelungssysteme, zB.:

- Deutsches Institut für Normungen DIN
- Internationale Standardisierungsorganisation / Internationale Elektrotechnische Kommission ISO/IEC
- Electronic Industries Alliance / Telecommunications Industries Association EIA/TIA

Folgende Dokumente legen Verkabelungsstandards fest:

ISO/IEC 11801 „Eigenständige Verkabelung für Kundenbedarf“, International

DIN EN 50173 „Anwendungsneutrale Verkabelung“, EU

EIA/TIA 568A/B „Belegung von 8-poligen TP-Kabeln“, US

Es gibt weitgehende Parallelen in den verschiedenen Standardisierungen, aber auch Differenzen. Die Kupferkabel wurden in diesen Standards in Kategorien eingeteilt, welche die maximale Übertragungsfrequenz festlegen. Die Qualität der Einzelkomponenten einer LAN-Übertragungsstrecke (Kabel, Stecker, Dose, Patchpanel) wird ebenfalls beschrieben durch Kategorien. Es gibt:

Cat.1 Analoge Sprachübertragung, Gegensprechanlagen, Alarmsysteme, etc.

Cat.2 Digitale Sprach- und Datenübertragung (ISDN)

Cat.4 Tauglich für 10Mb/s Ethernet (10Base-TX)

Cat.5/5e Tauglich für 100Mb/s Ethernet (100Base-TX)

Cat.6 Tauglich für 1Gb/s Ethernet (1000Base-TX)

9.3 Glasfaserkabel

Glasfaserkabel sind sogenannte Lichtwellenleiter. Die Datenübertragung erfolgt mit Licht verschiedener Wellenlänge. Der eigentliche Lichtwellenleiter im Glasfaserkabel ist in der Regel sehr dünn. Seine äußere Dicke entsteht durch die mehrfache Ummantelung zu seinem Schutz.

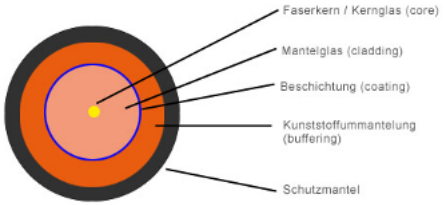


Fig. 32: LWL-Querschnitt

Es gibt Techniken wo nur 1 Wellenlänge übertragen wird und solche wo mehrere Wellenlängen gleichzeitig übertragen werden. Die physikalischen Effekte bei der Übertragung eines Signales im LWL sind recht kompliziert und werden hier nur vereinfacht dargestellt.

9.3.1 Eigenschaften

- Von Mantel umgebene Glasfaser
- Innere Totalreflexion durch Änderung des Brechungsindexes
- Übertragen mit moduliertem Licht
- Empfindlich in der Handhabung
- Unempfindlich gegen elektromagnetische Störungen
- Höhere Datenübertragungsraten als alle anderen Netzwerkmedien
- Max. Länge derzeit 120km ohne Verstärkung oder Regeneration (1Gbit/s)

Glasfaserkabel sind in Verlegung und Nutzung viel empfindlicher als TP-Kabel (mech. Beanspruchung). Mindestbiegeradien sind unbedingt einzuhalten, Kopplungsverluste treten an den Steckverbindern auf und die Signalübertragung ist erschütterungsempfindlich.

9.3.2 Vergleich Single- / Multimode

LWL deren Kerndurchmesser lediglich wenige Vielfache der Wellenlänge des verwendeten Lichts beträgt, werden Singlemode Fasern genannt. Multimode Fasern weisen einen Kerndurchmesser von 50 bis 150 µm auf (~ Haar).

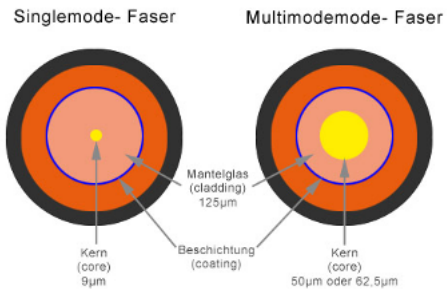


Fig. 33: LWL

Bei den Multimode Fasern wird noch zwischen Stufenindex- und Gradientenindexfaser unterschieden, wobei sich bei ersterer, der Brechungsindex vom Kern zum Mantelschicht, radial nach außen hin in sprungartig, und bei letzterer kontinuierlich in Form einer Parabel ändert. Singlemode Fasern gibt es typischerweise nur als Stufenindexfasern.

Brechung Je höher der Brechungsindex der Glasfaser ist, desto optisch dichter ist das Medium. An der Grenzen zweier optisch unterschiedliche Medien kommt es zur Brechung oder Reflexion des Lichts (Beispiel Luft / Wasser).

Apertur Die Apertur beschreibt die Einkopplung eines Signals in den Kern. Sie muss unterhalb eines bestimmten Winkels erfolgen (Aperturkegel), sonst wird das Signal nicht innerhalb des Kerns weitergeleitet. Wird ein LWL zu stark gebogen, kann es sein, dass dieser Winkel lokal überschritten wird. Das Signal tritt dann aus dem Kern aus. Die Übertragung bricht ab.

Dispersion Die Dispersion sorgt dafür, das ein in eine Glasfaser eingespeister Impuls über seinen Weg der Ausbreitung zeitlich immer breiter wird. Dies kann zu Überlappungen mit nachfolgenden Impulsen führen und Übertragungsfehler verursachen. Laserdioden erzeugen Impulse von wenigen Nanometern Breite.

Grafisch dargestellt, sehen die Ausbreitungprofile Single- bzw. Multimode daher so aus.

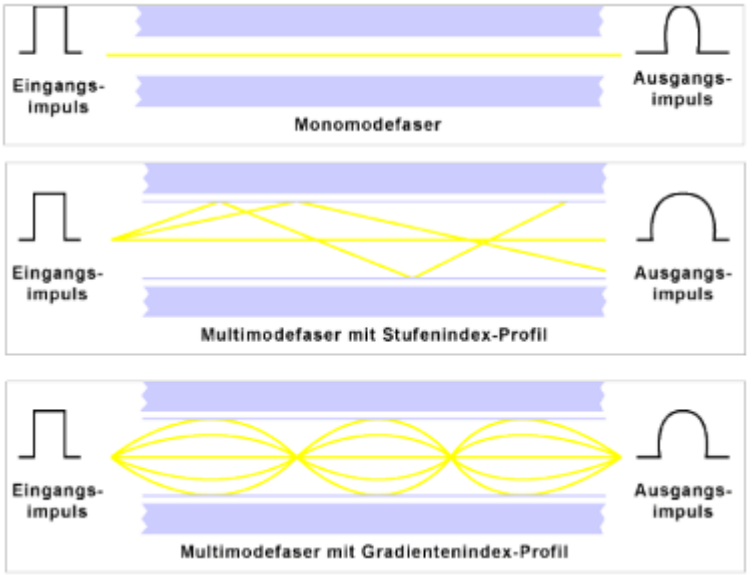


Fig. 34: Wellenausbreitung

Für LWL gibt es viele unterschiedliche Steckverbinder, die aber hier nicht näher betrachtet werden. Nur die folgenden zwei seien erwähnt, weil sie im Netzwerktechnik-Labor verwendet werden.

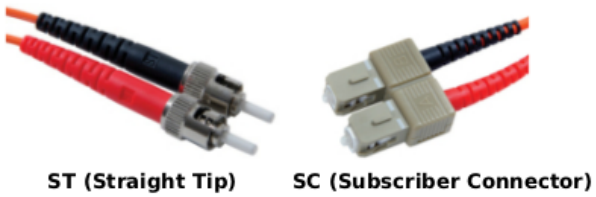


Fig. 35: Terminator

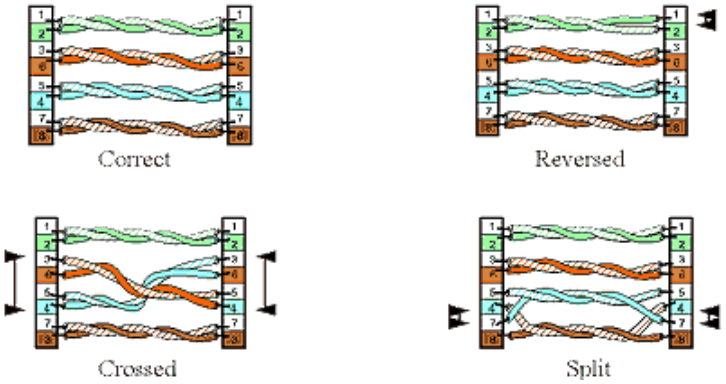


Fig. 36: Belegungsfehler

10 Kabelprüfung

10.1 Grundlagen

Bei der Verkabelung von Netzwerken sind viele Aspekte zu berücksichtigen, will man störsichere, robuste und schnelle Verbindungen (Ausnutzung der Übertragungstechnik) garantieren. Viele Fehler sind denkbar, treten auch auf und müssen daher gezielt gesucht werden. Die einfachsten davon sind die Belegungsfehler.

In Prüfverfahren sind diese aber leicht zu finden. Fehler, die die Übertragungsgeschwindigkeit reduzieren, sind nicht mehr so einfach zu finden, da das Netzwerk dabei ja grundsätzlich funktioniert. Als Beispiel sei hier die Störung des WLANs durch andere Funk-Technologien erwähnt (zB. alte Brandmelde- oder Alarmanlagen).

10.2 Kabelmesstechnik

Die Messung der Netzwerkverkabelung erfolgt immer mit speziellen sehr guten Messgeräten und zugehörigen Prüfkabeln. Die Kabelprüfung erfordert somit Standards für die Kabelqualität, das anzuwendene Messverfahren und die Messgeräte selbst. Das TIA-Dokument TSB-67 beinhaltet dazu eine Definition der Verbindungsformen Permanent-, und Channel-Link, die Definition der dabei zu messenden Parameter und die Grenzwerte für diese Parameter. Ein

großes Problem ist die Reproduzierbarkeit der Messung. Die Eigenschaften der Patchkabel verändern sich durch mechanische Beanspruchung.

10.2.1 Verbindungsdefinitionen

Zur Messung der Netzwerkleitungen sind verschiedene Verbindungsmodi definiert. Zwei davon werden hier vorgestellt. Die zulässigen Grenzwerte für die einzelnen Strecken, sind aufgrund der unterschiedlichen Komponenten ebenfalls unterschiedlich vorgegeben.

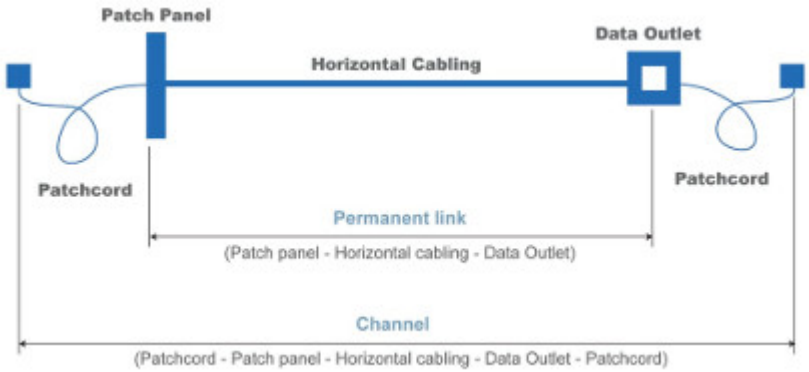


Fig. 37: Verbindungsdefinitionen

Permanent Link Er ist die Strecke vom Patchfeld bis zur Anschlussdose - die fix verlegte Installationsstrecke also (hier kan man kein Kabel umstecken).

Channel Der Channel ist die Strecke vom Switch, über den Permanent-Link bis hin zur WS.

Ein Channel schließt zum oben genannten Permanent Link also auch die Anschlussleitungen (die Patchkabel) mit ein. Die Testergebnisse enthalten im übrigen keinen Beitrag der Messleitungen (Beitrag der Messgeräte ist bekannt und wird vom Messgerät herausgerechnet). Bei Cat.5 (Link-Klasse D) ist die Messung folgender Parameter vorgeschrieben:

1. Wire Map (Verdrahtung)
2. Length (Länge)
3. Resistance (Widerstand)
4. Attenuation (Leitungsdämpfung)
5. NEXT (Nahnebensprechdämpfung)
6. ACR (Attenuation/Crosstalk-Ratio)

Zusätzlich können die meisten Testgeräte die folgenden, für Cat.6 (Link-Klasse E) vorgeschriebenen Parameter, messen:

1. Return Loss (Rückflussdämpfung)
2. Power Sum NEXT (summierte Nahnebensprechdämpfung)
3. Power Sum ACR

Die Parameter mit der größten Auswirkung auf die Übertragungsrate sind:

- bei Cat.5: Dämpfung und NEXT
- bei Cat.6: Return Loss

10.2.2 Signaldämpfung

Alle schwingfähigen Systeme unterliegen einer Dämpfung (sie würden sonst ewig schwingen). Ursache der Dämpfung auf Leitungen ist der ohmscher Widerstand der Leitung. Die Dämpfung ist somit längenabhängig. Sie ist aber auch frequenzabhängig, da der kapazitive Widerstand der Leitungen mit steigender Frequenz sinkt. Jede Steck- oder Klemmverbindung erzeugt zusätzliche Dämpfung (Übergangswiderstand).

Fig. 38: Dämpfung

Die Signaldämpfung G gibt grundsätzlich ein normiertes Verhältnis zwischen der Eingangsgröße x und Ausgangsgröße y an (Spannung). Ihre Darstellung erfolgt logarithmisch mit Basis 10. Ihre Einheit ist daher das Dezibel (dB). Es ist

$$G = 20 * log(\frac{x}{y})$$

Allgemein wird die Dämpfung, wenn sie graphisch dargestellt wird, negativ angegeben.

Beispiel Wie groß ist die Dämpfung wenn an einer Leitung $U_{in} = 1V$ und $U_{out} = 0.5V$ gemessen wurden?

$$G = 20 * log(\frac{1}{0.5}) = 6dB$$

Beispiel Wie viel Prozent der Eingangsspannung ist am Ausgang bei einer Dämpfung von 60dB noch vorhanden?

$$60 = 20 * log(\frac{U_{in}}{U_{out}})$$

Daraus folgt unmittelbar $U_{out} = \frac{U_{in}}{1000}$

Beispiel Ein Kabel mit 20dB Dämpfung wird mit zwei Steckern von je 3dB Dämpfung versehen. Wieviel Gesamtdämpfung entsteht?

$$G_{ges} = 3 + 20 + 3 = 26dB$$

Dies bedeutet bei einer Signalübertragung einen Spannungsabfall am Ausgang auf 1/20!

Beispiel Wie viel Dämpfung liegt vor, wenn die Ausgangsleistung halb so groß ist wie die Eingangsleistung?

$$G = 10 * log(\frac{1}{0.5}) = 3dB$$

10.2.3 NEXT

Near-end-crosstalk stellt ein Verfahren dar, bei dem gemessen wird, wieviel eines Signals von einem Leiterpaar in ein anderes Leiterpaar induziert wird.
Diese Messung findet für alle Leiterpaare statt. Sie wird immer an einem Ende des Kabels gemessen.

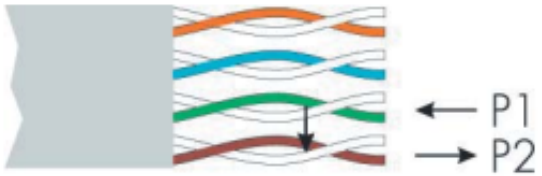


Fig. 39: NEXT - Prüfverfahren

Die Eigenschaften sind:

- Stark frequenzabhängig aber kaum längenabhängig
- Wird vermindert durch Verdrillung und Abschirmung
- Entsteht vorwiegend in den Steckern

Fehler entstehen recht schnell bei Kabelschäden, die Schadstelle kann dann durch Reflexionsmessungen gefunden werden. Bei vielen NEXT-Fehlern ist oft eine 1GBit/s Verbindung nicht mehr möglich, die Switches schalten dann automatisch auf 100MBit/s zurück. Ein gutes Kabel hat einen großen Wert für NEXT und eine kleine Dämpfung.

10.2.4 ACR

Die Messwerte aus NEXT und Dämpfung werden daher oft durch einen einzigen Wert ausgedrückt - ACR (attenuation crosstalk ratio). Dabei ist dieser Wert berechnet, nicht gemessen. Es ist

$$ACR\,[dB] = NEXT\,[dB] - a\,[dB]$$

Eine Signalübertragung ist nur möglich, wenn der Wert für NEXT immer größer bleibt als die Dämpfung.
Wer einen Festnetz-Anschluss für seinen Internet-Zugang hat, kann von seinem Netzbetreiber eine Leitungsprüfung durchführen lassen. Diese dauert in der Regel nur wenige Minuten.

11 Ethernet

Mit dem Begriff Ethernet werden Netze bezeichnet, die topologisch zu den Busnetzen zählen. Im Ethernet kommen spezifische Übertragungsprotokolle zum Einsatz. Alle Ethernet-Verfahren gehören zu den klassischen LAN-Übertragungsprotokollen. Ethernet bildet

die am häufigsten verwendete LAN-Technologie. Sie wurde von Robert M. Metcalfe 1977 zum Patent angemeldet. Die Geschwindigkeit war in der Anfangszeit 3Mbit/s. Aktuell sind 40Gbit/s in Spitzenanwendungen realisiert, 100Gbit/s erscheinen möglich.

11.1 Grundlagen

Es gibt mehrere Varianten des Ethernet-Protokolls. Weitest verbreitet sind heute zwei Formen der Ethernet-Technologie:

1. *Ethernet II (aus Ur-Ethernet I von DEC, Intel und Xerox)*
2. *Ethernet 802.3 (Erweiterung nach IEEE)*

Diese Ethernet-Formen unterscheiden sich nur minimal. IEEE (Institute of Electrical and Electronics Engineers) ist ein Projekt, welches im Februar 1980 begann und sich mit Standards im Bereich der lokalen Netzwerke beschäftigt. Ethernet 802.3 hatte zu Beginn eine Übertragungsgeschwindigkeit von bis 10Mbit/s. Heute gibt es bereits:

- *Fast Ethernet mit 100Mbit/s*
- *Gigabit Ethernet mit 1000Mbit/s*
- *10-Gigabit Ethernet mit 10000Mbit/s*

Übertragungsraten von 400Gbit/s sind bereits im RFC definiert. Für alle Formen gilt, die eigentlichen Daten werden in die Ethernet-Pakete eingebettet um diese zu übertragen. Dazu wird das Ethernet-Paket genau unterteilt in bestimmte Bereiche mit exakt definierten Längen.

11.1.1 Aufbau von Ethernet-Paketen

Jeder Ethernet-Knoten ist durch seine einzigartige MAC-Adresse (Medium Access Control) eindeutig identifizierbar. Sie ist fest in der Netzwerk-Hardware verankert und ist vergleichbar mit der KFZ-Fahrgestellnummer. Später wird mit Einführung der IP-Adressen, jedem Gerät auch eine Kennzeichennummer zugeordnet.
Das ursprüngliche Konzept des Ethernet II basiert auf der gemeinsamen Nutzung eines Koaxialkabels für alle Teilnehmer und der Anwendung des Verfahrens CSMA/CD. Ein Ethernet-Frame muss mindestens 64Byte lang sein, um beim Senden mindestens die Laufzeit (max. Kabellänge) eines 10Mbit-LAN zu verbrauchen (ein Paket belegt das gesamte Kabel). Damit Kollisionen sicher erkannt werden, werden zu kleine Frames daher mit Füllbits ergänzt. Die maximale Länge eines Frames beträgt 1518Byte. Der Ethernet-Frame wird weiters mit einer Präambel ausgestattet, um die Kollisionserkennung sicher durchführen zu können. Eine Startsequenz zeigt dann den Anfang des eigentlichen Frames an. In diesem Ethernet-Paket (enthält den Ethernet-Frame) sind nun folgende Datenfelder definiert:

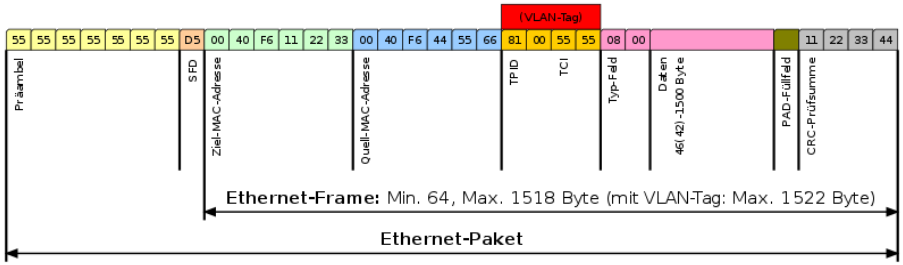


Fig. 40: Ethernet 802.3

Präambel (Kollisionserkennung) und SFD (Startsequenz) gehören nicht zum eigentlichen Ethernet-Frame, werden aber beim Verschicken vorne angestellt. Der Frame beinhaltet somit:

1. *Destination Address (MAC)*
2. *Source Address (MAC)*
3. Length, Type (4Byte)
4. *Payload (Nutzdaten)*
5. *FCS (Fehlererkennung)*

Bei Ethernet 802.3 gibt ein weiteres Feld Auskunft über das verwendete Protokoll der nächsthöheren Schicht (ARP, WoL, IPv4, Novell, etc.). Durch eine Rahmenprüfsumme hinten, kann im Empfänger auch eine fehlerhafte Übertragung erkannt werden. Daraufhin wird der Frame einfach verworfen (keine Korrektur).

11.2 Standards

Bei der sogenannte Thin-Wire Verkabelung waren alle Computer eines Stranges in Reihe verschaltet (max. 185m). Der Anschluss der Computer erfolgte über ein T-Stück (BNC-Stecker). Am Anfang und am Ende des Kabelstrangs befanden sich je ein 50Ohm Terminator. Maximal 30 Stationen pro Segment bildeten eine Kollisionsdomäne.

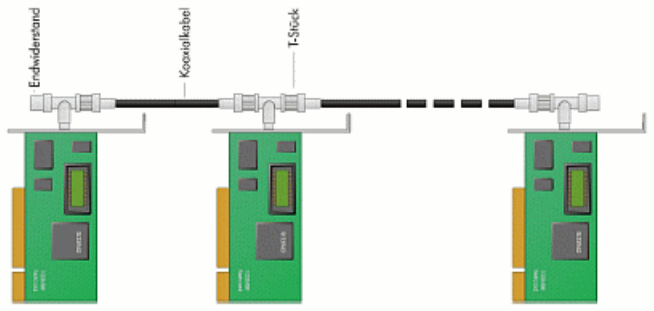


Fig. 41: 10Base-2

10Base-2: RG58 Kabel, 10Mbit/s

Ein Ethernet Netzwerk ist zumeist sternförmig aufgebaut. Von einem zentralen Verteiler - dem Switch - führen Twisted-Pair Kabel zu den einzelnen Computern. Der Anschluss erfolgt über RJ45-Stecker. Diese Verkabelungsart beseitigt einen gravierenden Nachteil obiger Bus-Strukturen, den Totalausfall bei Unterbrechung einer Leitung.

Fig. 42: 10Base-T

Die Standards für solche Twisted-Pair Verkabelungen lauten

10Base-T: Cat.3, 10Mbit/s

100Base-TX: Cat.5, 100Mbit/s

1000Base-T: Cat.5 (4 Adernpaare), 1000Mbit/s

1000Base-TX: Cat.6, 1000Mbit/s

Alle TP-Verkabelungen verwenden die Anschlussstecker RJ45. Durch die Verwendung von Bridges (in den Switches) wird die Kollisionsproblematik beseitigt und die max. Segmentlänge von 100m kann voll genutzt werden.

Teil V. Leiterungebundene Datenübertragung

Leiterungebundene Datenübertragung umfasst neben WLAN auch Bluetooth, NFC und Infrarot. Während WLAN allen ein Begriff ist, ist vielen noch unbekannt welche Möglichkeiten Bluetooth bietet. Infrarot bietet als einziges Verfahren eine sehr hohe Störsicherheit und Sicherheit gegen abhören bei gleichzeitig sehr viel höherer Reichweite als WLAN und BT. NFC dient einem anderen Zweck und wird nicht weiter betrachtet.

12 WLAN

12.1 Grundlagen

Wireless LAN (Wi-Fi) bezeichnet eine nach IEEE 802.11 standardisierte Technik zur Kommunikation in Funknetzwerken. Die erste Version dieses Standards wurde 1997 verabschiedet. Sie spezifiziert den Zugriff und die physikalische Schicht für lokale Funknetzwerke. Für die physikalische Schicht wurden zwei Funkverfahren und eines zur Datenübertragung per Infrarotlicht spezifiziert. Zur Datenübertragung über Funkwellen wird das lizenzfreie 2,4GHz ISM-Band verwendet. Die Kommunikation zwischen Teilnehmern kann direkt im so genannten Ad-hoc-Modus, oder im Infrastruktur-Modus mit Hilfe einer Basisstation, dem Access Point (AP), erfolgen. Um einen gemeinsamen Zugriff von mehreren Geräten auf das Medium zu ermöglichen, wird innerhalb des 802.11-Standards verpflichtend CSMA/CA verwendet.

12.2 Standards

802.11 stellt heute eine ganze Normenfamilie für WLAN dar. Sehr weit verbreitet sind

802.11a: 5GHz (20MHz), 54Mbit/s

802.11b: 2,4GHz (22MHz), 11Mbit/s

802.11g: 2,4GHz (20MHz), 54Mbit/s

802.11n: 2,4+5GHz (20,40MHz), 150Mbit/s

12.2.1 Kompatibilitäten

Der Standard 802.11b ist aufgrund seiner 22MHz Bandbreite eher ein Störsender und sollte nicht mehr verwendet werden. Der Standard 802.11g ist kompatibel zu 802.11b, 802.11n kann kompatibel zu 802.11b/g arbeiten.

12.3 Kanalbelegung

Die Kanalbelegungen sind selbst in Europa nicht einheitlich. In Österreich regelt dies die Rundfunk und Telekom Regulierungs-GmbH (RTR). Es sind erlaubt:

2,4GHz: 13 Kanäle (1-13) mit 5MHz Abstand, 100mW

5GHz: 19 Kanäle (36-64, 100-140) mit 20MHz Abstand, 200mW

WLAN soll ohne Kanalüberdeckung betrieben werden. Daher sind viel weniger Kanäle tatsächlich nutzbar. Dies sind für 20MHz Kanalbreite im 2,4GHz-Band nur die Kanäle 1, 5, 9 und 13. Im 5GHz-Band sind es 19 Kanäle. Vermeiden sie unbedingt jegliche Abweichung davon. Die Signalstärke der einzelnen Radios kann recht einfach mit Apps gemessen werden.

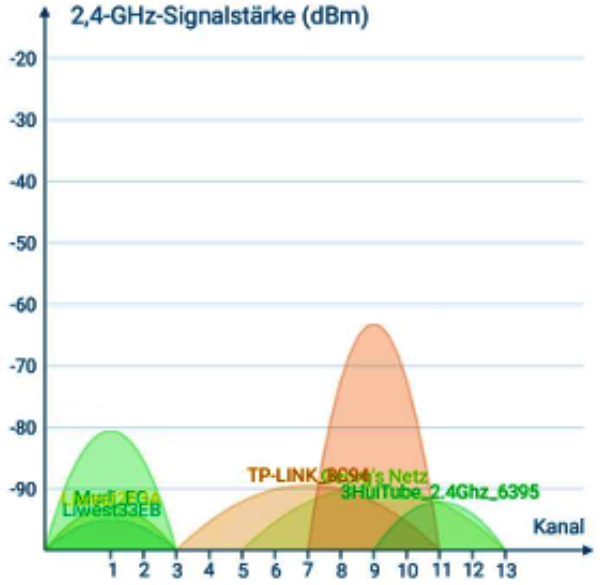


Fig. 43: Kanalbelegung

Das Maß dBm (Dezibel-mW) ist die Einheit für die Signalstärke L im WLAN, wenn die Strahlungsleitung P auch in mW angegeben wird. Sie wird berechnet mit

$$L = 10 * log(P)$$

und ist bezogen auf 1mW. Ein AP der eine Abstrahlungsleistung an seiner Antenne von 100mW hat, sendet also mit 20dBm. Misst man an einer Position -30dBm, hat das Signal somit eine Leistung von $\frac{1}{1000}mW$. Damit kann man also die Qualität eines Signals einschätzen. Als Faustregel für solche Messungen gilt:

Sehr gute Signalstärke: bis -40dBm

Ausreichendes Signal: bis -67dBm

Unzureichendes Signal: unter -72dBm

Das 2,4GHz-Band ist lizenzkostenfrei nutzbar und daher zu bevorzugen. Das 5GHz-Band eignet sich besser, um das Signal auf einzelne Räume zu konzentrieren. Seine Reichweite ist deutlich geringer, seine Dämpfung höher. 2,4GHz wird bereits durch die feuchte Luftmoleküle gedämpft und damit die endlose Ausbreitung verhindert.

13 Bluetooth

Bluetooth (IEEE 802.15) ist ein weiterer Standard zur Funkübertragung zwischen Geräten. BT arbeitet wie WLAN im lizenzfreien 2,4GHz-Band und darf daher weltweit zulassungsfrei betrieben werden. Um die Störsicherheit von BT zu verbessern, wird ein Frequenzsprungverfahren verwendet, bei dem das Frequenzband in 79 Kanäle mit 1MHz Abstand eingeteilt wird. Bis zu 1600 mal in der Sekunde, wird der Kanal gewechselt.
Grundsätzlich sind verbindungslose sowie verbindungsbehaftete P2P und Ad-hoc-Netze möglich. Eine Verbindung kann von jedem beliebigen Gerät ausgehen, das sich dadurch zum Master macht.

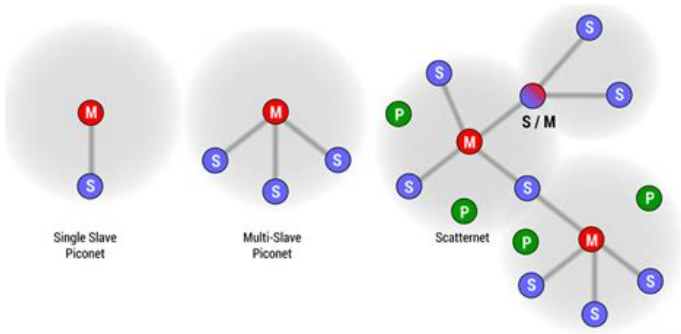


Fig. 44: BT-Piconet

Ein Bluetooth-Netzwerk kann aus bis zu 8 aktiven Teilnehmern bestehen. Die Geräte identifizieren sich über ihre MAC-Adressen. Im Bereitschafts-Modus lauschen die Geräte in Abständen von bis zu ∼2,5s nach Nachrichten. Bis zu 255 nicht aktive Geräte können in einem Parkmodus gehalten werden.

13.1 Betriebsmodi von BT-Geräten

Grundsätzlich kann jedes aktiv steuerbare BT-Gerät (vom Master) in folgende Betriebszustände versetzt werden.

Aktive Mode Voll aktiver Betriebszustand.

Sniff Mode BT-Gerät lauscht nur alle 100ms nach Anfragen.

Hold Mode Längeren Schlafphasen. Das BT-Gerät wacht periodisch selbst auf.

Park Mode Dauerhafter Energiesparmodus. BT-Gerät muss geweckt werden.

Im aktiven Modus gibt es Funktionen die ein BT-Gerät anbieten oder ausführen kann. Diese sind zB. inquiring, paging oder pairing. Dabei bedeutet:

Inquiring Scannen der BT-Umgebung um andere BT-Geräte zu finden. Diese müssen aber sichtbar sein.

Paging Austausch der Kenndaten zweier Geräte, die sich zuvor im Scan-Modus bekannt gemacht haben.

Pairing Binden zweier Geräte durch anlegen eines Profiles vom anderen Gerät. Geräte die durch pairing verbunden wurden. Verbinden sich von nun an automatisch.

Darüber hinaus kann man gekoppelte Geräte immer auch gezielt verbinden (connecting) und wieder trennen (disconnecting). So kann man Verbindungen zu mehreren Geräten herstellen. Ein Gerät muss dabei immer Master sein, die restlichen sind Slaves.

13.2 Standards

Bluetooth gibt es in bereits 5 Generationen. Mit BT-4 wurde auch eine low energy Variante eingeführt, genannt BLE. 3 Klassen werden nach ihrer Sendeleistung unterschieden. Sie bieten folgende Eigenschaften.

Leistungsdaten der Klassen

Class 1: Reichweite 100m, 100mW

Class 2: Reichweite 10m, 2.5mW

Class 3: Reichweite 1m, 1mW

Der Kommunikationsablauf in Bluetooth erfolgt grundsätzlich über einen sogenannten Protokollstapel. Um bestimmte Funktionalitäten über BT zu ermöglichen sind daher je Funktion eigene Profile notwendig. Da es unglaublich viele Profile gibt, werden wir diese hier nicht aufzählen. Die max. Datenrate liegt derzeit bei ca. 24Mbit/s (BT-4), sie ist aber stark abhängig von der BT-Klasse (BLE).

Teil VI. Zugriffstechnologien

14 Betriebsarten von Signalleitern

In der Übertragungstechnik finden immer wieder folgende Begriffe Verwendung. Sie beschreiben die Art wie eine Kommunikation zwischen zwei Teilnehmern abläuft. Folgende Übertragungsarten sind technisch realisiert und auch gebräuchlich.

Simplex Die Daten können in nur eine Richtung übertragen werden, diese Technik ermöglicht keine Antwort des Empfängers. Beispiel: Rundfunk, Druckerverbindung

Half Duplex Die Daten können abwechselnd in beide Richtungen übertragen werden, aber nicht gleichzeitig. Beispiel: Sprechfunk, Ethernet mit Hubs, SATA

Full Duplex Hier können die Daten gleichzeitig in beide Richtungen übertragen werden. Beispiel: Ethernet in geswitchten Segmenten, PCI, SAS

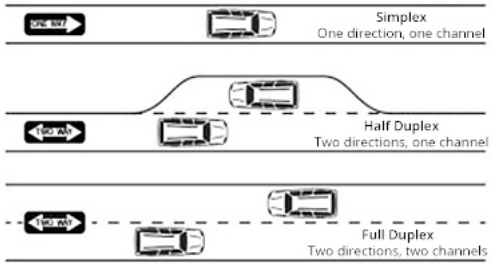


Fig. 45: Betriebsarten

Anmerkung Oft findet man noch den Begriff Dual simplex. Er ist ähnlich dem Full Duplex, es gibt aber hier physisch getrennte Übertragungswege (TP-Verkabelung).

15 Grundproblem in Netzwerken

Beim Ur-Ethernet-Netzwerk hingen alle Computer in einem Strang. Alle Computer bekamen so die gesamte Kommunikation aller anderen Computer mit. Es brauchte daher ein strukturiertes intelligentes und schnelles Verfahren für den Zugriff mehrerer Teilnehmer auf nur ein Übertragungsmedium. Es können ja nicht alle gleichzeitig reden - zumindest versteht dann niemand den anderen.

Lösungsansätze

1. Zuteilung eines Senderechts: Wie die Friedenspfeife bei Indianern wird ein Signal - das Token - von Station zu Station wei-

tergereicht. Nur wer das Token hat, darf etwas senden. Möchte eine Station nichts senden, gibt sie das Token weiter.

2. Senden auf gut Glück: Wer etwas zu senden hat, sendet. Er prüft allerdings vorher, ob gerade eine andere Station sendet. Es ist allerdings möglich, dass im gleichen Moment eine andere Übertragung gestartet wird, was zu einer Kollision der Daten führt.

Man unterscheidet daher

1. Deterministische Verfahren: Zuteilungsverfahren, Token-passing-Verfahren - realisiert in Token-Ring Netzen.

2. Chaotische Verfahren: Zufallsverfahren, konkurrierende Verfahren - realisiert in Ethernet-Netzen.

15.1 Token Ring

Gänzlich kollisionsfreie Kommunikation bietet Token Ring. Diese Verfahren war sehr verbreitet im Einsatz. Seine Geschwindigkeit (16MBit/s) ist allerdings heute zu langsam geworden (Entwicklung wurde eingestellt). Der Ablauf der Kommunikation ist wie folgt. Es herrscht Ruhezustand, keine Station will senden. Ein kleines Datenpaket - das Free Token - wird kontinuierlich ringförmig weitergereicht.

Ablauf einer Datenübertragung

1. Der Knoten, der das Free Token hat, darf senden

2. Er fügt seine Daten samt Empfängeradresse an das Token an (Busy Token)

3. Das Paket wird bis zum Empfänger weitergereicht, dieser liest die Daten, fügt eine Acknowledge-Markierung hinzu, die mit dem Token wieder beim Absender eintrifft

4. Der Absender entfernt die Daten und schickt das Token wieder auf den Ring

15.2 CSMA/CD

„Carrier Sense Multiple Access / Collision Detection“ ist ein Zufallsverfahren. Wichtigster Vertreter ist das Ethernet. Ein Rechner der senden will horcht das Medium ab. Falls Ruhe am Medium herrscht, kann er zu senden beginnen. Alle Teilnehmer hören immer mit, ob eine Kollision entstanden ist. Die erste Station die eine solche bemerkt, sendet ein Jam-Signal ins Netz. Alle Rechner beenden sofort das Senden und warten eine Zeit lang. Das Verfahren beginnt erneut nach Zufallsprinzip.

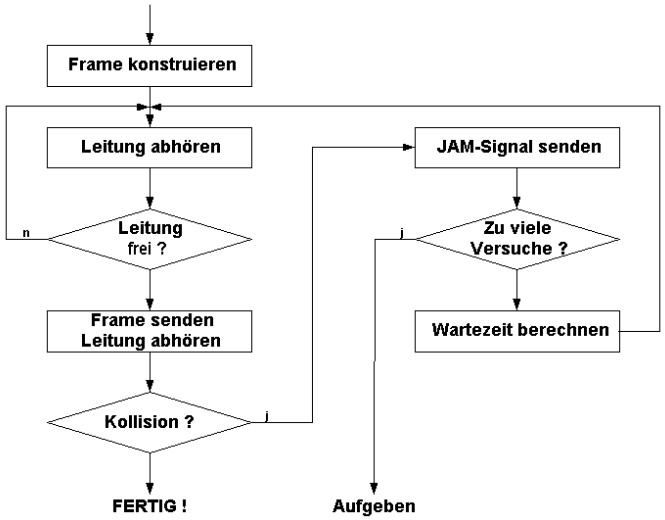


Fig. 46: CSMA/CD

Das Jam-Signal bedeutet allen lauschenden Stationen, dass das eben gesendete Paket unbrauchbar ist. Da jede Station immer Mithört, kann jede Station eine Kollision erkennen. Die erste die dies tut (Präambel im Ethernet-Frame), unterbricht jedes Senden.

Kollisionsauflösung Eine wichtige Rolle spielt dabei die Signallaufzeit. Diese Slot-Time ist jene Zeitspanne, die ein Signal braucht um das Medium hin und retour zu durchlaufen. Kann ein Sender diese Zeit lang ungestört senden, war keine Kollision vorhanden. Ein Datenpaket muss daher mindestens so lange sein, dass das Senden länger dauert als die Slot-Time. Daher ist die Mindestlänge eines Frames bei Ethernet 64Byte. Bei Kollision warten beide Sender eine zufällige Zeit und senden dann wieder. Falls wieder Kollision auftritt, Vergrößerung der Wartezeit und weiterer Sendeversuch. Nach 15 Fehlversuchen, Abbruch und Fehlermeldung.

Anmerkung CD wird von der Hardware selber durchgeführt, wenn diese Half Duplex betrieben wird. Das Netzwerk arbeitet dann signaltechnisch wieder wie die originale Bus-Topologie. Full Duplex ist nur zwischen Switches (Bridges) und Endgeräten möglich. In jedem Strang der Stern-Topologie kann also die CD abgeschaltet werden. Die Konfiguration der Schnittstellen muss zwingend gleich erfolgen. Auto/Auto oder beide Seiten gleich konfiguriert. Leider heben manche Betriebssysteme diese Einstellungen oftmals auf.

15.2.1 Vergleich CSMA/CD mit Token-Ring

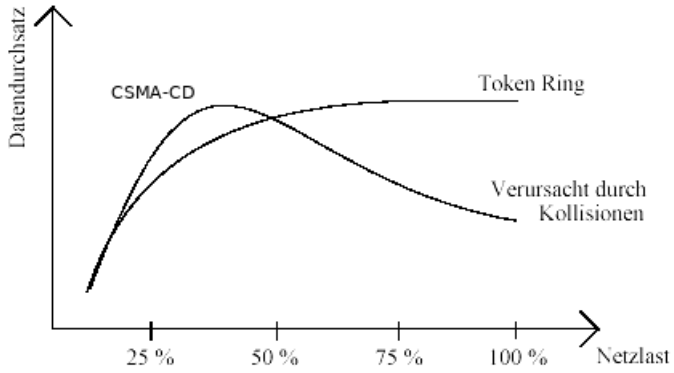


Fig. 47: Vergleich

CSMA/CD Bei steigender Netzlast sinkt der Datendurchsatz wegen der ansteigenden Kollisionen, es gibt eine kritische Last die bereits bei ca. 30% liegt. Darüber hinaus nimmt der Durchsatz deutlich ab!

Token Ring Token Ring verträgt eine höhere Netzlast, die Limitierung erfolgt praktisch nur durch die Geschwindigkeit der Hardware-Komponenten. Token Ring kommt nur mehr bei bestehenden Token Ring Netzwerken zum Einsatz. Ein bemerkenswerter Vorteil von Token Ring war, dass mehrere Stationen gleichzeitig Daten senden konnten. Alle Daten wurden dazu zu einem langen Datenpaket zusammengehängt. Jeder Station musste sich herausschneiden was für sie bestimmt war.

15.3 CSMA/CA

„Carrier Sense Multiple Access / Collision Avoidance“ ist ebenfalls ein Zufallsverfahren. Wichtigster Vertreter ist das WLan. Ein Netzwerkadapter der senden will, horcht das Medium ab und - wenn frei - sendet er ein Request-to-Send-Signal (RTS) ins Medium. Gibt es keine Kollision mit einem anderen RTS-Signal, scheint das Medium frei und es gehört diesem Rechner alleine. Alle anderen wissen, dass sie nicht senden dürfen, denn jeder hat dieses RTS gesehen. Nach der Sendung generiert der Rechner ein Clear-to-Send-Signal (CTS) und gibt damit das Medium wieder frei. Dieses Zugriffsverfahren ist bei Wireless LAN realisiert.
Stehen zwei Clients nun so weit auseinander, dass sie zwar den Access-Point erreichen, sich aber gegenseitig nicht empfangen können, senden sie, und Kollisionen treten ein.

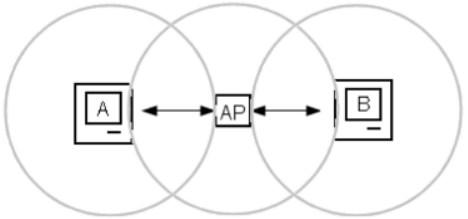


Fig. 48: Hidden Node

Der Access-Point selbst muss also das Verfahren RTS/CTS koordinieren. Er muss auf Anfrage publizieren, ob das Medium jetzt zur Verfügung steht oder nicht.

Teil VII. Das Internet

16 Grundlagen

Es sollte ein dezentrales Netzwerk geschaffen werden, das unterschiedliche US-amerikanische Universitäten, die für das Verteidigungsministerium forschten, miteinander verband. Das damals revolutionäre dezentrale Konzept enthielt schon die grundlegenden

Aspekte des heutigen Internets. Die Verbindungen wurden damals über Telefonleitungen hergestellt (waren schon vorhanden).

1969: *ARPANET (4 vernetzte UNI-Computer)*

1975: *TCP/IP entsteht*

1983: *ARPANET wird Internet, TCP/IP wird das Internet-Protokoll*

Die Computer sollten auch bei Ausfall einzelner Computer oder Verbindungen noch kommunizieren können (militärische Sicherheit). Unmittelbare Verbindung aller Computer erfordert aber viele Leitungen und ist daher unrealisierbar.

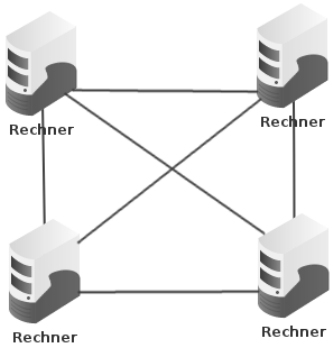


Fig. 49: Unmittelbares Netzwerk

In der Praxis realisierbar sind daher nur vermittelte Verbindung aller Computer über spezielle Vermittler - die Router der ISP. Dies führt zur gemeinsamen Nutzung von Leitungen für mehrere Verbindungen. Vereinfacht dargestellt sieht die Struktur wie folgt aus.

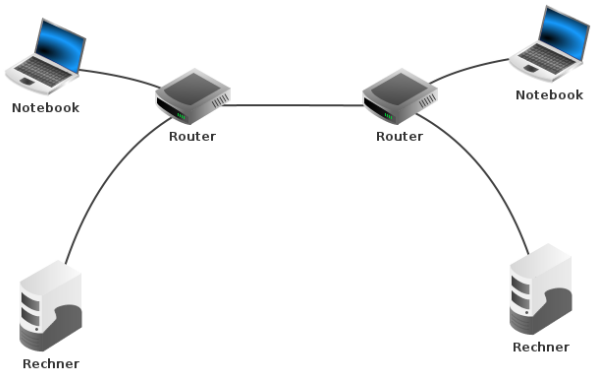


Fig. 50: Vermitteltes Netzwerk

Tatsächlich ist die gesamte Welt heutzutage stark vernetzt. Viele Verbindungen zwischen großen Internetknoten sind redundant. Ein Blick auf `https://www.itu.int/itu-d/tnd-map-public/` zeigt das volle Ausmaß der bestehenden Datenleitungen.

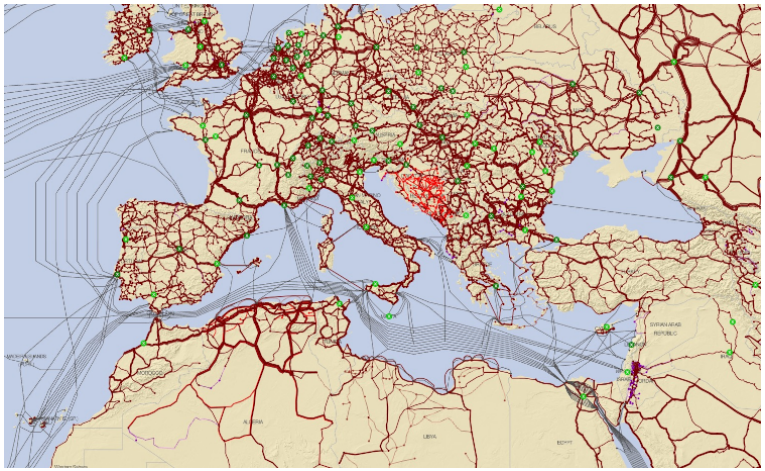


Fig. 51: Internet

Das österreichische Weitverkehrsnetz zwischen den zentralen Knoten in den Bundesländern, wird hauptsächlich gebildet aus

ACOnet Österreichisches Wissenschaftsnetz

GOVnet Österreichisches Behördennetz

EDUnet Österreichisches Bildungsnetz

ACOnet ist das österreichische Hochleistungs-Datennetz für gemeinnützige Einrichtungen der Wissenschaft, Forschung, Bildung und Kultur. Es wird vom ZID der Universität Wien betrieben, in Kooperation mit seinen Teilnehmern in ganz Österreich.

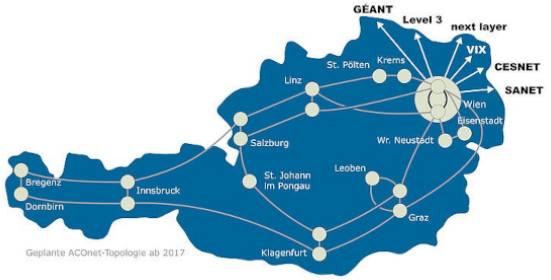


Fig. 52: ACONet

ACOnet und GOVnet laufen auf der selben technischen Infrastruktur. Die Edugroup hat eine redundante 10Gbps Anbindung an das österreichische Wissenschaftsnetz.
Grundsätzlich werden alle Daten im Netzwerk des Internets, wie sonst auch, paketweise transportiert. Das bedeutet

1. *Nachrichten werden in kleine Pakete zerlegt, nummeriert und verschickt*
2. *Nicht alle Pakete müssen den gleichen Weg zum Empfänger gehen*
3. *Empfänger fügt die Pakete in der richtigen Reihenfolge wieder zusammen*

Die Datenpakete werden gleichmäßig auf vorhandene Leitungen verteilt. Es ist keine für längere Zeit stabile Verbindung nötig. Bei Übertragungsfehlern muss nur ein Teil der gesamten Nachricht (das

defekte Paket) erneut versandt werden. Diese paketorientierte Verbindungsart ist auch der Grund, warum Kommunizieren im Internet billiger ist als zB. traditionelle Telefonie. Traditionelle Telefonie ist leitungsorientiert. Es wird eine Verbindung reserviert, auch bei Sprechpausen ist diese für andere blockiert (gilt nur für analoge Telefonie). Das Internet ist paketorientiert. Die Leitung ist nur dann belegt, wenn ein Paket übertragen wird. In Übertragungspausen kann sie von anderen benutzt werden. Die Leitungen werden daher viel besser ausgelastet.

17 Struktur des Internets

Ein globales Computernetzwerk (WAN) ist wie bei Postadressen auch ein Verbund von Gruppen (Städte, Häuser mit Hausnummern). IP-Pakete werden daher zunächst ins Zielnetz geroutet (wie beim Paketdienst), dort werden sie vom Eingangsrouter nun dem Zielcomputer zugestellt. Daher müssen alle Netzwerkknoten im Internet permanent über eine eindeutige IP-Adresse verfügen. Diese Netzknoten bilden stehende Verbindungen zwischen den Subnetzen.

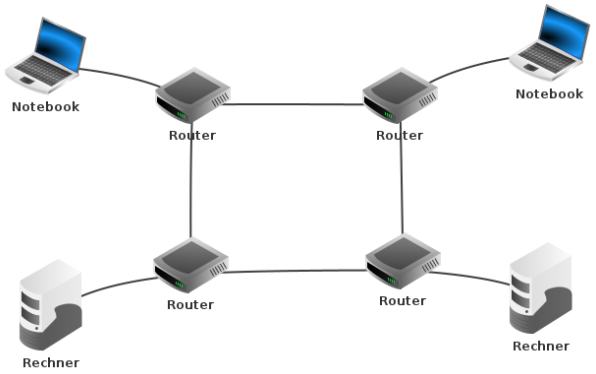


Fig. 53: Internet

18 Kommunikationsmodelle

18.1 Grundlagen

Es gibt mehrere Modelle, die das Zusammenspiel der beteiligten Ebenen beschreiben und festlegen. Wir lernen zuerst das DoD-Schichtenmodell kennen (1970 von der DARPA entwickelt). Dieses Modell ist ein Schichtenmodell, das die Kommunikation nachwievor prägt. Da das Internet eine Entwicklung des amerikanischen Verteidigungsministeriums ist, wurde die Bezeichnung dieses Schichtenmodells von der englischen Bezeichnung Department-of-Defense abgeleitet. Insgesamt sind 4 Schichten im DoD-Schichtenmodell definiert. Dies sind:

- Anwendungsschicht

- Transportschicht
- Internetschicht
- Netzzugangsschicht

Das DoD-Schichtenmodell ist eines der Vorläufer des OSI-Schichtenmodells. In der Praxis sind die meisten Abläufe nach diesem Modell strukturiert. Diese 4 Schichten stellen eine ausreichende Abstrahierung dar. Betrachten wir diese Schichten etwas genauer.

Anwendungsschicht In der Anwendungsschicht sind die Anwendungen und Protokolle definiert, die über das Internet miteinander kommunizieren. Hierzu zählen HTTP, FTP, SMTP und viele mehr.

Transportschicht Die Transportschicht dient als Kontrollprotokoll des Datenflusses zwischen der Anwendung und der Internetschicht. Hier arbeiten die Protokolle TCP und UDP.

Internetschicht Auf der Internetschicht werden die einzelnen Datenpakete mit einer Adresse versehen und ihre Größe an das Übertragungssystem angepasst. Die Datenpakete werden in der Regel mit IP übertragen. Auf dieser Schicht sind mehrere Steuerungsprotokolle aktiv, die mit IP stark verknüpft sind.

Netzzugangsschicht Diese Schicht ist die unterste Schicht des DoD-Schichtenmodells und stellt das Zugriffsprotokoll dar. In lokalen Netzwerken ist das Ethernet, in WAN zB. ISDN, ADSL, ATM, LTE und weitere.

18.2 IP-Protokollstapel

Wir betrachten hier vorerst nur die Protokolle des Internet-Transportsystems, da vieles dazu bereits besprochen wurde. Grundsätzlich ist in IP-Netzwerken die Kommunikation durch einen Protokollstapel organisiert. Das bedeutet, dass jede Anwendung, die Informationen verschicken will, dies nach dem gleichen Schema tun muss.
Ein Protokoll ist eine Vereinbarung über den Aufbau von Datenpaketen und die Bedeutung deren Inhalte. Wichtige Informationen in den Datenpaketen sind:

1. Empfänger und Absender
2. Der Pakettyp (Verbindungsaufbau, Verbindungsabbau oder nur Nutzdaten)
3. Die Paketlänge
4. Eine Prüfsumme

Diese Informationen werden den Nutzdaten als sogenannter Header oder Trailer beigefügt.
Die Datenübertragung in einem Netzwerk (so auch im Internet)

muss streng nach einheitlichen Protokollen abgewickelt werden. Daher gibt es eine Sammlung von Protokollen, die wie ein Stapel organisiert sind. Der Informationsfluss verläuft dabei vertikal. Beim Senden nach unten, beim Empfangen nach oben.

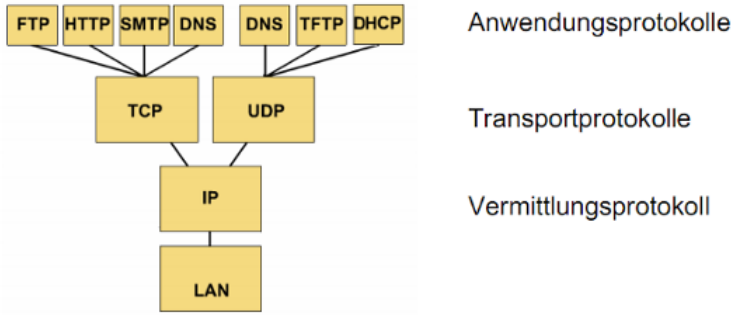


Fig. 54: IP-Stack

Anwendungsprotokolle sind Vereinbarungen, mit denen die Anwendung direkt zu tun hat (http, ftp, dns, dhcp). Die Anwendungsprotokolle werden erst später betrachtet.

18.2.1 Transportprotokolle

TCP und UDP dagegen sind Transportprotokolle, die auf dem Vermittlungsprotokoll IP aufsetzen. IP selbst braucht als Basis eine Netzwerktechnologie wie zB. Ethernet, WLan, Bluetooth, etc.

Verbindungsorientiertes TCP

- Kommunikation erst möglich, wenn Verbindung zwischen zwei Endpunkten hergestellt ist
- Erfordert Mechanismen für Verbindungsaufbau und -abbau (ähnlich zur Telefonie)
- Übertragung ist begleitet von Überprüfungen, Bestätigungen und ev. Wiederholungen (wie bei Telefonie)
- Folge davon ist ein großer Datenoverhead

Verbindungsloses UDP

- Kein Verbindungsaufbau (wie Rundfunk)
- Keine Empfangsbestätigung und Wiederholung (wie Rundfunk)
- Unzuverlässig, dafür aber einfacher und schneller
- Geringer Datenoverhead, bessere Ausnutzung der Leitungskapazität

18.2.2 Vermittlungsprotokolle

Über das IP werden Daten im Internet paketweise transportiert. IP sucht dazu immer den optimalen Weg von der Quelle zum Ziel. IP ist verbindungslos d.h. jedes Paket wandert unabhängig von seinem Vorgänger und Nachfolger durch das Netz. Nur sehr leistungsstarke

Netzwerke können Pakete der max. Größe transportieren (64kB). Es kommt daher vor, dass ein Paket in mehrere Teilpakete zerlegt und wieder zusammengesetzt werden muss (Fragmentierung).

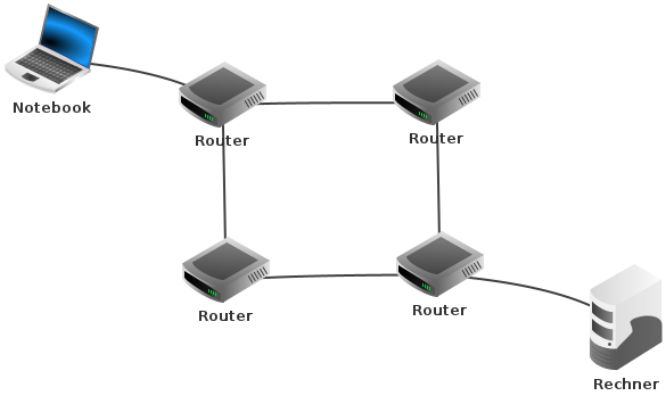


Fig. 55: Transportwege

18.2.3 Aufbau von IP-Paketen

Ein IP-Paket besteht immer aus einem Header und den Nutzdaten. Der Datenteil enthält ein weiteres Protokoll, meist TCP oder UDP. Die maximale Länge eines IP-Pakets beträgt 65535Bytes (Mindestlänge 576Bytes). Heim-Netzwerke beschränken die Größe der IP-Pakete normalerweise auf 1518Byte. Der Parameter dazu heißt MTU (Max. Transport Unit).

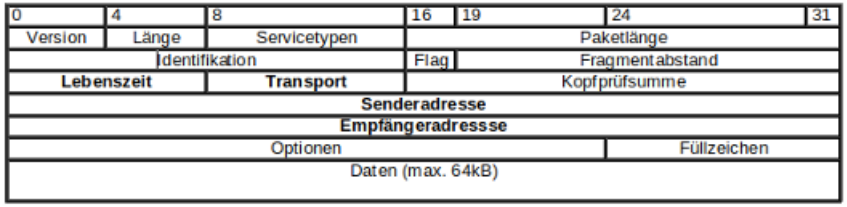


Fig. 56: IP-Pakete

Felder (in einer Breite von 32bit folgen nach unten einzelne Worte):

Servicetypen: spezifizierte Übertragungsgüte (Vorrang)

Flag: dieses Paket wurde fragmentiert

Fragmentabstand: Lage des Fragments im Gesamtpaket

Lebenszeit: max. Lebensdauer (pro Netzknotendurchlauf um 1 verringert, 0 -> verworfen)

Transport: Nummer des Transportprotokolls (6 TCP / 17 UDP)

Adressen: Internet Adresse des Senders bzw. Empfängers

Optionen: Optionen des Senders (Spezifikation der Route)

Danach kommen die Nutzdaten bis das gesamte max. Paket 64kB hat. Die minimale Headerlänge ist dabei 20Byte.

Teil VIII. Netzwerkadressierung

19 Grundlagen

Jeder Knoten im IP-Netzwerk braucht eine eindeutige Kennung (Fahrgestellnummer beim Auto). Die physikalische Adressen sind aber ungeeignet, da sie für uns Menschen schlecht verarbeitbar sind. Daher gibt es die Zuweisung einer standortbezogenen IP-Adresse (Kennzeichen beim Auto).
Die IPv4-Adresse ist eine 32bit Zahl. Sie besteht aus 4 Byte. Jedes Byte besteht aus 8 bit. Daher sind Ipv4-Adressen 4 Oktetts aus {0,1} im Bereich

00000000.00000000.00000000.00000000 -
11111111.11111111.11111111.11111111

Diese Zahlen im maschinenlesbaren Binärsystem haben auch eine für uns lesbare Darstellung im Dezimalsystem. Für den Adressbereich von oben sind diese 4 Oktetts

0.0.0.0 - 255.255.255.255

Nachfolgende Abbildung zeigt eine beispielhafte Umrechnung aus dem Binärsystem ins Dezimalsystem.

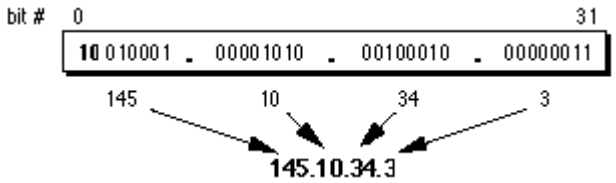


Fig. 57: IP-Adresse

Jeder Teilnehmer im Netzwerk muss sich nun diese IP-Adresse selber merken (Auswahl und Zuweisung passiert meist über den Dienst DHCP).
Um logisch unterschiedliche Netzwerke realisieren zu können, gibt es eine Unterteilung der Adressen in Netz- und Hostadresse. Jede IP-Adresse besteht daher aus zwei Teilen, dem sog. Netzanteil - er adressiert das Netz (Telefon-Vorwahl) und dem Hostanteil - er adressiert den Computer im Netz (Telefon-Nr.). Dadurch entstehen so genannte Adressklassen.

Klasse A: *Netzwerke mit sehr vielen Hosts*
Klasse B: *mittelgroße Netzwerke*
Klasse C: *Netzwerke mit wenigen Hosts*

Es sind noch zwei weitere Klassen definiert, D und E. Diese sind jedoch reserviert und werden nicht weiter betrachtet. Im folgenden wird die Struktur einer IP-Adresse genauer betrachtet.

20 IPv4-Adressbereiche

Eine IP-Adresse besteht also aus zwei Anteilen. Einer Information zum Netz und einer zum Host. Netzadressierung erfolgt in den vorderen Oktetts, Hostadressierung in den hinteren Oktetts. Theoretisch ergibt dies die folgenden Netze (erkennbar am 1. Oktett):

Klasse A: *00000000 – 01111111 (0-127)*
Klasse B: *10000000 – 10111111 (128-191)*
Klasse C: *11000000 – 11011111 (192-223)*

Über diese Netzklassen wurde früher der gesamte Adressraum in zunächst drei (später fünf) Netzklassen fix unterteilt. Die Netzgrößen dieser Klassen unterscheiden sich sehr stark. So sind dadurch grundsätzlich folgende Anzahlen an Netzen und Hosts möglich.

	Adressbereich	*Netze*	*Adressen*
Klasse A:	*0.0.0.0 - 127.255.255.255*	*128*	*16777216*
Klasse B:	*128.0.0.0 - 191.255.255.255*	*16384*	*65536*
Klasse C:	*192.0.0.0 - 223.255.255.255*	*2097152*	*256*

Die logische Zuordnung eines Hosts anhand seiner IP-Adresse wird durch diese Strukturierung nun sehr erleichtert. Gehört ein anderer Host in mein Subnetz oder in ein anderes, ist in Standardnetzen sofort zu erkennen. In allen drei Netzklassen sind spezielle Bereiche für private Verwendung reserviert.

20.1 Private IP-Adressen

Die Internet Assigned Numbers Authority - IANA vergibt weltweit die öffentlichen IP-Adressen. Es ist festgelegt welche Adressen für öffentliche Zwecke (Internet) und welche für private Netze (Intranet) verwendet werden dürfen. So sind für private Netze nur die folgenden Adressbereiche festgelegt.

	Adressbereich	*Netze*	*Adressen*
Klasse A:	*10.0.0.0 - 10.255.255.255*	*1*	*?*
Klasse B:	*172.16.0.0 - 172.31.255.255*	*?*	*?*
Klasse C:	*192.168.0.0 - 192.168.255.255*	*?*	*256*

Diese Adressen dürfen im Internet nicht öffentlich vergeben werden. Sie können in privaten Netzen daher mehrfach verwendet werden. Das erweitert die Möglichkeiten ungemein.

Beispiel Ein Unternehmen bekommt von der IANA die öffentliche Adresse 188.56.3.161 (+ Domain Name) zugewiesen. Dieses entscheidet sich intern für die privaten Adressen 192.168.100.0 - 192.168.102.255. Es kann in diesem Adressbereich also insgesamt

$$3 * (256 - 3) = 759$$

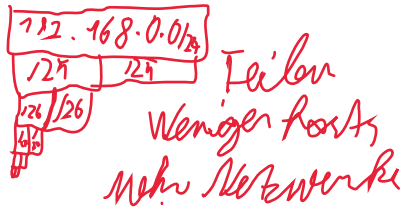
Geräten eine IP-Adresse zuweisen. Wie bereits erwähnt, werden immer die Adressen 0 und 255 reserviert für organisatorische Zwecke

(Netzwerk und Broadcasts), sowie eine Adresse für den Gateway (zB. 138).

20.2 Die Netzmaske

Die Subnetzmaske ist aufgebaut wie eine IP-Adresse. Sie legt fest, welche Bits der IP-Adresse als Netzwerkanteil bzw. Hostanteil dienen sollen. Die Bits des Netzwerkanteils der IP-Adresse werden dabei in der Subnetzmaske auf 1 gesetzt (von links). Die Bits des Hostanteils der IP-Adresse werden in der Subnetzmaske auf 0 gesetzt. Daher sind die Netzmasken für die Standardklassen wie folgt:

Klasse A:	*255.0.0.0*
Klasse B:	*255.255.0.0*
Klasse C:	*255.255.255.0*



IP-Adresse und Subnetzmaske werden nun logisch addiert (1+1=1) um zu erkennen was Netzwerkadresse und was Hostadressen sind. Sie werden durch die Subnetzmaske getrennt.

Netzklasse C	*192.168.32.0 / 255.255.255.0*			
IP-Adresse	*11000000*	*10101000*	*00100000*	*00000000*
Netzmaske	*11111111*	*11111111*	*11111111*	*00000000*
1+1=1	*11000000*	*10101000*	*00100000*	*00000000*
Netzwerk	*192*	*168*	32	*0*
Hosts		$2^8 = 256 \Rightarrow$	(0..255)	*1..254*

Die Grenze zwischen Netzwerkanteil und Hostanteil kann aber auch verschoben sein. Diese Überlegung wird zur Teilnetzbildung verwendet. Das folgende Beispiel zeigt eine IP-Adresse mit vergrößerter Netzmaske. Angenommen wir haben auf unserem PC die folgende Adresse bekommen.

Netzklasse C	*inet4 192.168.32.188/27*			
IP-Adresse	*11000000*	*10101000*	*00100000*	*101/11100*
Netzmaske	*11111111*	*11111111*	*11111111*	*111/00000*
1+1=1	*11000000*	*10101000*	*00100000*	*10100000*
Netzwerk	*192*	*168*	32	*160*
Hosts		$2^5 = 32 \Rightarrow$	*(160..191)*	*161..190*

21 Kommunikationsprotokolle

21.1 Address Resolution Protocol

Das ARP ist ein Protokoll mit dem jeder Netzwerkteilnehmer seinen Empfänger für die zu sendenden Daten finden kann. Das Protokoll speichert dazu IP-Adresse und die dazugehörige MAC-Adresse lokal in einer Tabelle. Man bekommt damit die gespeicherten Verbindungsdaten, IP-Adresse und zugehörige MAC-Adresse.

Beispiel In einem ersten Beispiel wollen wir Hosts statisch konfigurieren und erkunden wie sie miteinander kommunizieren können. Wir tun dies mit der Lern- und Simulationssoftware Filius [7]. Wir

verändern IP-Adresse und Netzmaske und testen, ob sich die Computer gegenseitig finden.

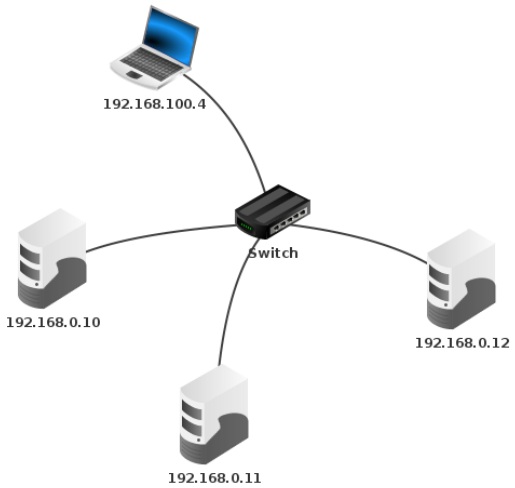


Fig. 58: IPv4-Adresse, -Netzmaske und ARP

Mit dieser Übung kann man auch die arbeitsweise des ARP kennenlernen. Ein zweites Protokoll der Netzwerktechnik ist das DHCP, das wir aber erst später kennenlernen werden.

Teil IX. Addressübersetzung

22 Grundlagen

Die Anbindung privater Netzwerke ans Internet erfolgt über spezielle Geräte, die dazu eine Adressübersetzung durchführen müssen. Man nennt dies allgemein Network Address Translation - NAT. Die speziellen Geräte werden häufig als Router bezeichnet, wobei anzumerken ist, dass Routing etwas anderes darstellt.
Um mehrere Computer von außen erreichbar zu machen, ist eine Zuordnung der IP-Adressen notwendig. Die private Adresse eines internen Netzes wird dabei durch die öffentliche Adresse des Geräts ersetzt. Für die interne Kommunikation werden so keine öffentlichen IP-Adressen verbraucht. Interne Computer sind von außen nicht sichtbar. Das ist aber auch so erwünscht (Schutzfunktion).
Es werden zwei unterschiedliche Verfahren angewendet. Beiden ist jedoch gemeinsam, dass sie eine 1:1-Zuordnung zweier IP-Adressen herstellen.

23 Statisches und dynamisches NAT

Für Computer, die von außen immer mit gleicher Adresse erreichbar sein sollen (Server) wird immer dieselbe Zuordnung verwendet. Sie erfolgt daher manuell als statische Route. Für Computer die von außen nur bei Bedarf erreichbar sein müssen, wird die Zuordnung

private Adresse zu öffentlicher Adresse automatisch und zufällig aus einem Adresspool erzeugt.

Beispiel Folgendes Bild zeigt ein einfaches Beispiel für statisches NAT. Zwei Computer haben einen Zugang zum Internet über NAT. Man erkennt die direkte Zuordnung von 2 öffentlichen zu 2 privaten IP-Adressen. Der Router muss dazu offensichtlich über 2 Netzwerkschnittstellen sowie 2 öffentlichen IP-Adressen verfügen. Zwei davon liegen im WAN und zwei im LAN. Dadurch können aber auch nur diese 2 Hosts gleichzeitig ins Internet kommunizieren.

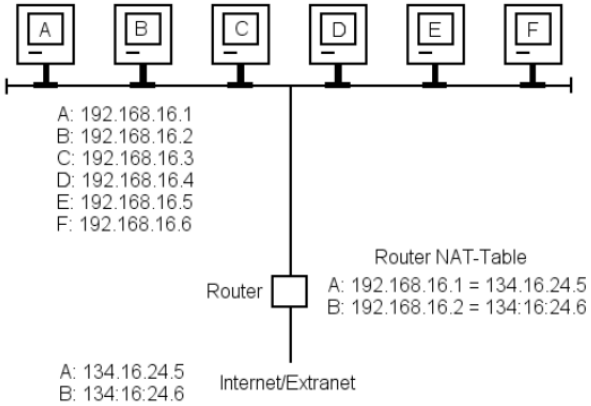


Fig. 59: NAT

Da heute sehr viele Hosts eines Netzwerkes Zugang zum Internet brauchen, wurde NAT durch ein erweitertes Verfahren ersetzt, dass IP-Adressen spart. Das Verfahren NAT lässt sich leider nicht in Filius simulieren.

24 Port and Address Translation

24.1 Grundlagen

PAT ist eine spezielle Form der NAT und wird oft auch IP-Masquerading genannt. Hier werden auch die Port-Nummern umgeschrieben. PAT wird daher eingesetzt, wenn viele private IP-Adressen zu einer öffentlichen IP-Adresse übersetzt werden sollen. Damit benötigt ein privates Netz nur mehr eine einzige öffentliche Adresse - wie bei Heimnetzwerken üblich. Wenn ein Datenpaket mit einer Ziel-Adresse außerhalb des lokalen Netzwerks adressiert ist, ersetzt der Router die Quell-Adresse durch seine öffentliche IP-Adresse. Die Port-Nummer wird durch eine andere Port-Nummer ersetzt. Um später die Antwortpakete der richtigen Station wieder zuordnen zu können

24.1.1 Ports

Jede IP-Kommunikation benutzt neben ihrer IP-Adresse auch sogenannte Ports. Die IP-Adressen stellen dabei etwa die Hausnummern dar, die Ports wären dazu die Türnummern im Gebäude. Hinter jeder Tür wartet nun ein spezielle Dienst auf Daten. Daher ist die Zustellung von Daten auch genau genommen nicht bloß an eine IP-Adresse, sondern zB. an 172.20.132.74:201 (Apple Talk). Die Ports

sind streng strukturiert nach folgenden Regeln:

Ports 0..255: Für TCP/IP-Anwendungen reserviert

Ports 256..1023: Für Unix-Anwendungen reserviert

Ports 1024..49151: Von der IANA verwaltete Port-Nummern

Ports 49152..65535: Port-Nummern für jeden anderen Zweck

Unter Linux findet man in /etc/services die Ports zugeordnet zu den Diensten, so wie es von der IANA vorgegeben ist. Alle Anwendungsprogramme müssen sich daran halten. Es gibt aber auch freie Ports die beliebig genutzt werden dürfen (Datenübermittlung). Die Kenntnis der zugeteilten Ports spezieller Anwendungen ist für die Netzwerktechnik unerlässlich.

Beispiel In jedem IP-Paket sind Source-Adresse und -Port genauso wie Destination-Adresse und -Port enthalten. Der Router ersetzt Absender-Adressen und -Portnummern der Pakete beim Weiterreichen gegen seine eigene öffentliche Adresse. Er führt tabellarisch darüber Buch, wie in der Abbildung unterhalb dargestellt. Kommen die Antworten zurück, weiß der Router daher, welche Quelladresse gemeint ist, und er kann Adresse und Portnummer der IP-Pakete wieder zurücksetzen.

Fig. 60: PAT

Da sich sowohl die Adressen als auch die Ports ändern, bleibt die eindeutige Zuordnung erhalten, auch wenn der Source-Port derselbe sein sollte. Das Verfahren PAT lässt sich leider nicht in Filius simulieren.

Vorteil dieser Lösung Man braucht nur 1 öffentliche IP-Adresse für ein ganzes Teilnetz. Die Computer im privaten Netzwerk können nicht aus dem Internet erreicht werden. Meist will man das aber so (Schutzfunktion).

25 Port Forwarding

Durch Portweiterleitung wird es Computern innerhalb eines LANs ermöglicht, Dienste nach außerhalb dieses Netzes anzubieten, da diese somit über einen festgelegten Port (und mittels NAT) eindeutig ansprechbar gemacht werden. Für alle Rechner im öffentlichen Netz sieht es so aus, als ob der Router den Serverdienst anbietet.

Beispiel Der externer Computer 225.213.7.32 möchte über Port 80 einen Web-Server auf einem Computer nutzen. Er kann aber

nur Anfragen an den Router unter dessen öffentlichen IP-Adresse 127.34.73.214 stellen. Dieser weiß nun nicht, für welchen internen Computer diese Abfrage bestimmt ist.

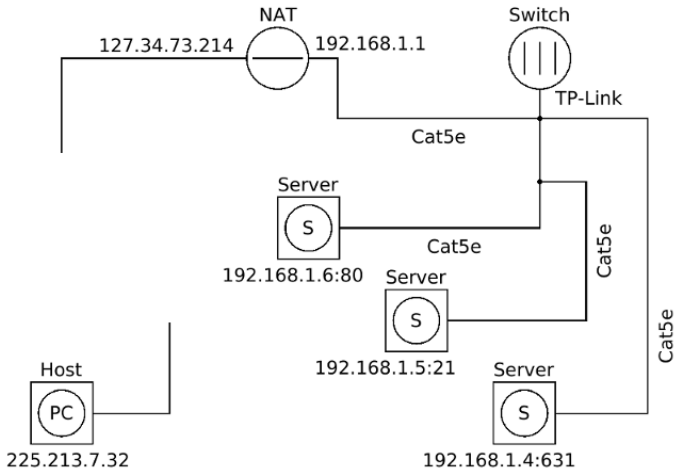


Fig. 61: Port-Forwarding

Der Router wird nun so konfiguriert, dass er Anfrage für bestimmte Dienste (Port 80) an den zuständigen Server im lokalen Netzwerk weiterleitet. Für Computer im externen Netz sieht es damit so aus, als ob der Router den Serverdienst anbietet. Dieses Verfahren lässt sich auf viele Dienste anwenden (SSH, FTP, Web, ...)

Teil X. Routing

Die Art und Weise, wie Datenpakete in einem dezentralen Netzwerk (Internet) verarbeitet werden, bezeichnet man als Routing. Man bezeichnet Routing auch als Wegfindung durch ein Netzwerk. Dabei wird der Weg zum Ziel anhand unterschiedlicher Kriterien ermittelt. Routing bezeichnet also in der Netzwerktechnik das Festlegen von Wegen für Datenpakete.

26 Grundlagen

In paketorientierten Netzwerken wird genauer zwischen den beiden Techniken Routing und Forwarding unterscheiden. Routing bestimmt den gesamten Weg der Datenpakete durch das Netzwerk. Forwarding hingegen beschreibt die Weitergabe eines Datenpaketes an einem Computer zwischen dessen Schnittstellen (Port-Forwarding). Jeder der einen Internetzugang über einen Festnetzanschluss (DSL über Telefonleitung) betreibt, hat daher meist die folgende einfache Netzwerkstruktur.

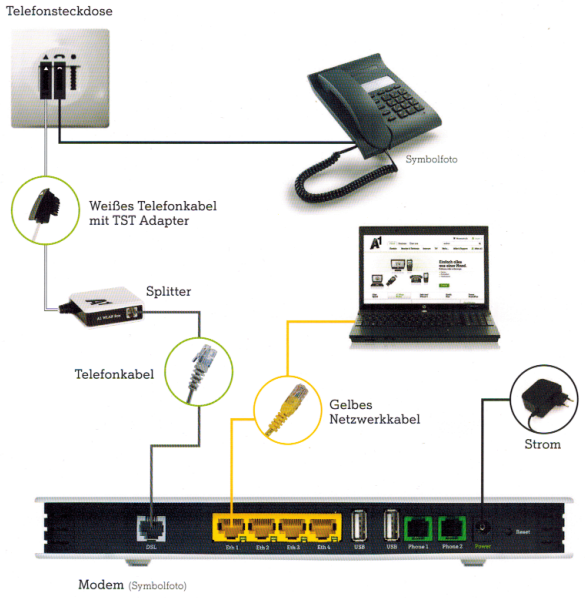


Fig. 62: Heimnetzwerk

Der dabei verwendete Router bietet auch erweiterte Funktionalität wie zB. einen Switch und notwendige Dienste um das dahinter liegende Netzwerk zu organisieren (DHCP, Gateway, NAT, Firewall, WLAN-Accesspoint, ...).

Grundsätzlich gilt Router verbinden Netze - keine Computer. Router sind aufgebaut wie Computer, jedoch ohne E/A-Komponenten. Router besitzen ein eigenes Betriebssystem - fast immer Linux. Daher sind diese Router oft sehr ähnlich in ihrer Funktionalität.

Sieht ein Computer, dass Daten nach außerhalb des eigenen Netzwerksegments verschickt werden müssen, muss dieser den Gateway als Ziel verwenden. Daher muss auch jeder Computer einen Gateway eingetragen haben. Dieser hat üblicherweise immer als IP-Adresse die Netzwerkadresse +1 oder die Broadcastadresse -1. Es gibt keinen allgemeinen ARP-Ruf nach dem Empfänger, da der Router diesen sowieso nicht weiterleitet. Router teilen sich fortwährend gegenseitig mit, welche Nachbar-Router sie haben.

27 Segmentierung

Mit Router kann man große Netzwerke aufteilen, um kleinere überschaubare Segmente zu erzeugen. Dies dient dem Management, der Geschwindigkeit und vor allem der Sicherheit des Netzwerkes. Jeder Computer erzeugt störende Broadcasts. Ein Router überträgt aber nur die adressierten Datenpakete ins andere Segment und schützt dieses somit vor den Broadcasts.
Im folgenden werden wir mit Hilfe der Netzmaske bewusst asymmetrische Subnetze erzeugen. Diese Technik wird angewendet um eine klare Trennung einzelner Netzwerkbereich zu erzeugen. In Netzwerken muss nicht jeder Teilnehmer jeden anderen sehen, sondern nur diejenigen, mit denen er auch zu tun hat (Sicherheit, Datenschutz).

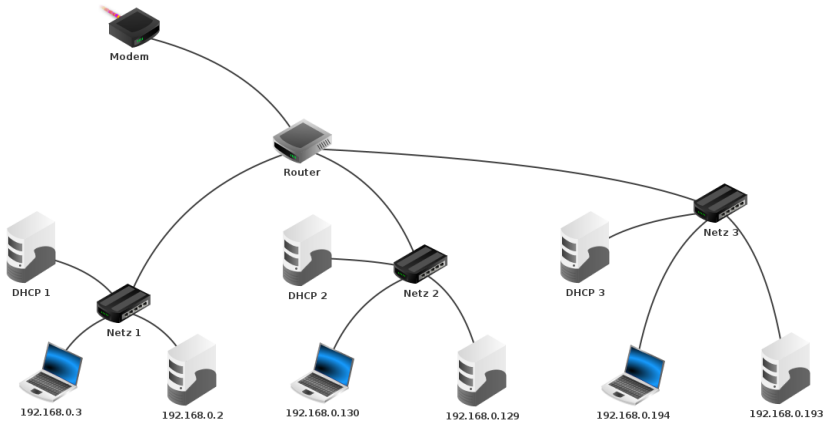


Fig. 63: Segmentierung

Die in obigem Beispiel dargestellten DHCP-Server sind normalerweise im Router implementiert. In Filius müssen sie separat installiert werden. Wir betrachten dazu folgendes Beispiel.

Beispiel Eine Firma hat 3 Abteilungen: Forschung, Vertrieb und Betriebsleitung. Aus Gründen der Sicherheit sollen alle Abteilungen eigene Subnetze bekommen. DHCP-Server und Router werden diese Aufgabe übernehmen. Zugeteilt ist ein Netz mit der Adresse 178.16.35.0/24. Man kann also grundsätzlich 256 Adressen vergeben. Die Forschung benötigen rund 100 Computer, der Vertrieb ca. 45 sowie die Betriebsleitung ca. 25. Wir werden daher die Subnetze entsprechend dimensionieren.

1. Forschung: 178.16.35.0/25 (SNM: 255.255.255.128)
   Netzwerkadresse 178.16.35.0
   Gateway 178.16.35.1
   Broadcastadresse 178.16.35.127

2. Vertrieb: 178.16.35.128/26 (SNM: 255.255.255.192)
   Netzwerkadresse ist 178.16.35.128
   Gateway 178.16.35.129
   Broadcastadresse 178.16.35.191

3. Betriebsleitung: 178.16.35.192/26 (SNM: 255.255.255.192)
   Netzwerkadresse 178.16.35.192
   Gateway 178.16.35.193
   Broadcastadresse 178.16.35.255

Damit haben wir allen Abteilungen ausreichend IP-Adressen in eigenen Subnetzen zur Verfügung gestellt. Alle Computer innerhalb eines Subnetzes bekommen die zugewiesene Konfiguration.

Will ein Host nun Daten an einen anderen außerhalb seines Subnetzes verschicken, erkennt er anhand der Subnetzmaske, dass die Empfängeradresse nicht in seinem Subnetz liegt. Es bringt also nichts, die MAC-Adresse auf Layer II zu ermitteln (ARP). Die Kommunikation erfolgt auf nun Layer III. Er schickt damit die Daten an den Gateway. Dieser vermittelt dann weiter.

28 Statisches und dynamisches Routing

Beim Routing werden Datenpakete aus einem Ursprungs-Netz in ihr Ziel-Netz weitergeleitet. Sie können dabei viele Zwischennetze durchlaufen. Router müssen dazu die Struktur des Netzwerks kennen. Router speichern dazu in Routing-Tabellen, welche Netze sie über welche Schnittstelle erreichen können. In kleinen Netzen sind Routing-Tabellen einfach und werden oft per Hand erstellt. In großen Netzen ändert sich die Struktur oft, Router müssen in regelmäßigen Abständen ihre Tabellen erneuern und untereinander austauschen. Ziel ist, dass nach einer gewissen Zeit alle Router dieselbe Information über das gesamte Netzwerk besitzen (Konvergenz). Man unterscheidet dazu zwei Arten des Routings.
Die Aufgabe eines Routers besteht darin, Pakete zwischen mehreren Netzen zu vermitteln. Dazu muss dem Router bekannt sein, wie ein Zielnetzwerk zu erreichen ist. Der Aufwand, diese Information manuell zu pflegen, steigt mit jedem angeschlossenen Router. Kommt es noch zu häufigen Änderungen in der Netztopologie, werden Technologien benötigt die auf diese Änderungen dynamisch reagieren.

28.1 Statisches Routing

Wenn alle Netze bekannt sind (und bleiben) wird meist über fixe Einträge in Routing-Tabellen vermittelt. Auch Routen zu speziellen Servern kann man so definieren. Die Wegfindung ist hier recht einfach und schnell.

- Routing-Tabellen werden händisch gepflegt
- Für unbekannte Netze gibt es den Gateway
- Für bekannte Netze einen Router dorthin

Ein Vorteil vom statischen Routing ist die Tatsache, dass der Administrator die Kontrolle über das Routingverhalten eines Netzwerkes behält. Für eine statische Route werden folgende Informationen benötigt.

1. Zielnetz (Netzadresse / Netzmaske)
2. Hop (das nächste Gerät am Weg zum Zielnetz)

28.2 Dynamisches Routing

Wenn die Router nicht mehr alle beteiligten Netze direkt angeschlossen haben, wird über ein Routing-Protokoll vermittelt. Beim dynamischen Routing geht es um die Fähigkeit eines Routers, die angeschlossene Netzwerktopologie selbständig zu erkunden, auf Veränderungen zu reagieren und daraus Rückschlüsse auf die optimale Route zum Zielnetzwerk zu ziehen.

- Routen werden über Routing-Algorithmen ermittelt
- Tabellen werden über spezielle Routing-Protokolle weitergegeben
- Bei Änderungen werden Routen automatisch angepasst

28.3 Routing Protokolle

Beim dynamischen Routing gibt es verschiedene Arten von Routing-Protokollen. Jedes Verfahren hat jedoch zum Ziel einen möglichst kurzen und schnellen Weg für ein IP-Paket zu finden. Dies wird durch spezielle Algorithmen erreicht, die recht unterschiedlich arbeiten. Jeder dieser Algorithmen durchforstet sein Netzwerksegment und kommuniziert mit seinen Nachbarn.

28.3.1 Distance Vector Protocols

Die Protokolle dieser Familie funktionieren nach dem Prinzip „Teile dein Wissen mit deinen Nachbarn“. Alle Router tauschen demnach fortwährend ihre Routing-Tabellen mit den direkten Nachbarn aus. Damit ergibt sich ein großes Bild des Netzwerkes für jeden Router. Es findet in IP-Netzwerken Anwendung. RIP ist ein bekannter Vertreter dieser Familie.

28.3.2 Link State Protocols

Ein Link-State-Protokoll wird von Routern benutzt wird, um eine komplexe Datenbank mit Topologie-Informationen aufzubauen. Mit Hilfe dieser Datenbank werden die Pakete dann im Netzwerk weitergeleitet. Alle Router senden periodisch Information über den Zustand der angeschlossenen Netzsegmente an eingetragen Router. Jeder Router ermittelt daraus den Netzzustand und daraus den jeweils besten Weg zu jedem anderen Netz. OSPF ist ein bekannter Vertreter dieser Familie.

28.4 Interne Routing-Tabellen

Auch Hosts besitzen Routing-Tabellen für den internen Datenverkehr via IP. Diese Informationen kann man sich sehr einfach anzeigen lassen. Unter Linux sieht dies so aus

```
$ ip route show
default via 192.168.178.1 dev eno1 proto dhcp
        metric 20100
169.254.0.0/16 dev eno1 scope link metric 1000
192.168.178.0/24 dev eno1 proto kernel scope link
        src 192.168.178.21 metric 100
```

Daran erkennt man welche Verbindungswege der eigene Computer in seinem Netzwerk kennt. Alle IP-Pakete die keine Adresse des eigenen Netzes Tragen, werden automatisch zum Gateway geschickt. Dieser hat offenbar die Adresse 192.168.178.1 (default) und ist über die Schnittstelle eno1 erreichbar.

Literatur

[1] Schreiner R.: Computernetzwerke, 6. Auflage: Hanser, 2016

[2] Schnabel P.: Netzwerktechnik-Fibel, 4. Auflage, Schnabel 2016

[3] Bratvogel K., Dehn S.: Netzwerke, Netzwerktechnik, 1. Ausgabe, Herdt 1019

[4] Wikipedia: `de.wikipedia.org`, 2018

[5] Glasfaser: `www.glasfaserkabel.de`, 2018

[6] Filius: `www.lernsoftware-filius.de`, 2019

[7] RTR: `www.rtr.at`, 2020