Bibliothek des technischen Wissens

Fachwissen Netzwerktechnik

Modelle · Geräte · Protokolle

Bernhard J. Hauser

3. Auflage

VERLAG EUROPA-LEHRMITTEL · Nourney, Vollmer GmbH & Co. KG
Düsselberger Straße 23 · 42781 Haan-Gruiten

Europa-Nr.: 54012

Autor:
Hauser, Bernhard J. Dipl.-Ing. Bisingen

Verlagslektorat:
Alexander Barth Dipl.-Ing. Haan

Bildentwürfe: Der Autor

Bildbearbeitung:
Wissenschaftliche PublikationsTechnik Kernstock, 73230 Kirchheim unter Teck
Zeichenbüro des Verlags Europa-Lehrmittel GmbH & Co. KG, Ostfildern

Fotos:
siehe Seite 262

3. Auflage 2018, korrigierter Nachdruck 2019

Druck 5 4 3 2

Alle Drucke derselben Auflage sind parallel einsetzbar, da sie bis auf die Behebung von Druckfehlern untereinander unverändert sind.

ISBN 978-3-8085-5405-0

Alle Rechte vorbehalten. Das Werk ist urheberrechtlich geschützt. Jede Verwertung außerhalb der gesetzlich geregelten Fälle muss vom Verlag schriftlich genehmigt werden.

© 2018 by Verlag Europa-Lehrmittel, Nourney, Vollmer GmbH & Co. KG, 42781 Haan-Gruiten

http://www.Europa-Lehrmittel.de

Satz: Wissenschaftliche PublikationsTechnik Kernstock, 73230 Kirchheim unter Teck

Umschlaggestaltung: braunwerbeagentur, 42477 Radevormwald, und Grafik & Sound, Köln.

Druck: mediaprint solutions GmbH, 33100 Paderborn

Vorwort

Die moderne Netzwerk- und Kommunikationstechnik hat Einzug in alle Lebensbereiche gehalten. Ein Alltag ohne Kommunikationsnetze ist kaum mehr denkbar. Die stetig fortschreitende Vernetzung in unserem Alltag sowie die schnelle Entwicklung der Technik sorgen dafür, dass ein solides Grundwissen in diesem Bereich immer wichtiger wird.

Dieses Fachbuch **„Fachwissen Netzwerktechnik – Modelle · Geräte · Protokolle"** wendet sich an alle Leserinnen und Leser, die die Grundlagen der zeitgemäßen Netzwerktechnik lernen und verstehen möchten. Es führt die wesentlichen Begriffe ein, stellt wichtige Zusammenhänge dar und legt somit die Basis für alle, die tiefer in die Themen einsteigen möchten.

Es eignet sich daher für **Auszubildende der IT-Berufe** wie **Fachinformatiker**, **Informatikkaufleute**, **Informationselektroniker**, für **Techniker** der Elektro- und Datentechnik sowie **Studenten technischer Fächer**, für die Kenntnisse in Netzwerkgrundlagen inzwischen unabdingbar sind.

Das Buch gliedert sich in folgende Kapitel:

- 1 Einführung
- 2 Netzwerktopologien und Verkabelung
- 3 Öffentliche Netze
- 4 Referenzmodelle, Netzwerkgeräte
- 5 Adressierung
- 6 Netzwerkprotokolle
- 7 Switching und Routing
- 8 Übertragungstechnik
- 9 Netzwerkmanagement

Mit einer bewusst verständlich gehaltenen Sprache bietet das Buch einen leichten Zugang. Zahlreiche **Abbildungen** und **Tabellen** sowie praxisnahe **Beispiele** unterstützen die Vermittlung des Stoffes. Zahlreiche **Merksätze** tragen zum Lernerfolg bei. Am Ende der jeweiligen Kapitel kann mithilfe von **Übungsaufgaben** der eigene Kenntnisstand überprüft werden.

Neben kleineren Erweiterungen und Aktualisierungen, wie beispielsweise IoT oder Firewall-/DMZ-Systeme, wurde das Thema Netzwerkmanagement als neues Kapitel in diese 3. Auflage aufgenommen.

Wir wünschen den Leserinnen und Lesern viel Freude und Erfolg mit diesem Werk.

Ihre Meinung interessiert uns! Hinweise und Verbesserungsvorschläge werden unter lektorat@europa-lehrmittel.de dankbar entgegengenommen.

Frühjahr 2018 Autor & Verlag

Inhaltsverzeichnis

2.1.7 Mischtopologien

Bus-Bus und Bus-Stern

***Mischtopologien** sind möglich.*

In der Regel kommen **Mischtopologien** vor, d. h., eine oder mehrere der Grundtopologien werden miteinander kombiniert. Früher war der Bus-Bus und später der Bus-Stern weit verbreitet. Heute herrscht der *Extended Star* vor. Bustopologien sind heute in Verkabelungen sehr ungebräuchlich, aber in Altinstallationen noch anzutreffen.

***Backbone:** Rückgrat*

Reine Busverkabelungen sind sehr veraltet. Mit dem Aufkommen der Twisted-Pair-Verkabelungen kam auch die Sterntopologie auf. Häufig wurde im **Backbone**-Bereich wegen längerer Kabelstrecken eine Koaxialleitung als Busleitung benutzt, und daran waren Sternverkabelungen angeschlossen, die die Stockwerke und Räume erschlossen.

Erweiterter Stern

***Erweiterter Stern:** die Standard-Topologie in Netzen*

Der **Erweiterte Stern**, engl. *extended star*, ist die heute vorherrschende Topologie im LAN. Anstelle eines Rechners oder eines Endgerätes wird ein weiterer Sternkoppler angeschlossen (Bild 2.6).

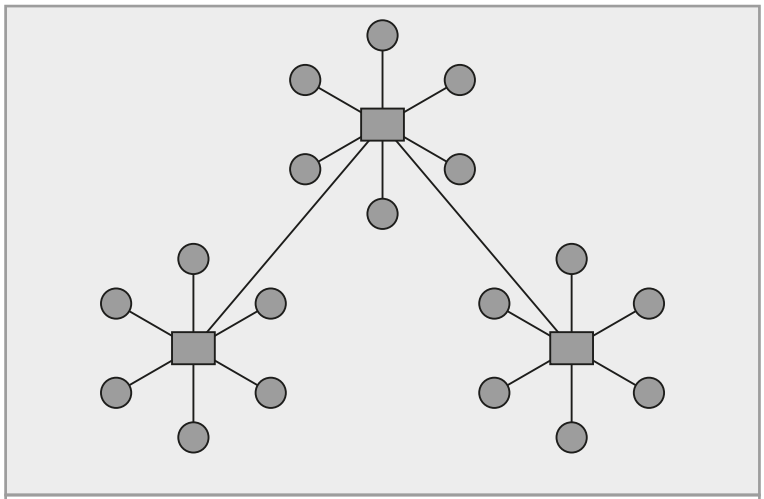


Bild 2.6: Erweiterter Stern

***Baumtopologie** ist in Wirklichkeit ein erweiterter Stern!*

Gelegentlich hört und liest man auch von der **Baumtopologie**. Diese ist nichts anderes als ein *extended star*. Eine Baum-Verkabelung gibt es nicht, auch wenn sie in Lehrbüchern gelegentlich beschrieben wird.

Stern-Zell-Topologie

Typisches Funknetz: Stern-Verkabelung mit Funkzellen.

Die Kombination aus drahtgebundener Sterntopologie und drahtloser Zelltopologie wird eingesetzt bei WLANs, DECT-Telefonie und Mobilfunknetzen (Bild 2.7).

Sonstige Mischtopologien

Beliebige andere Kombinationen von Grundtopologien wie Stern-Ring, Ring-Bus usw. sind möglich und sicher auch in einer vorhandenen

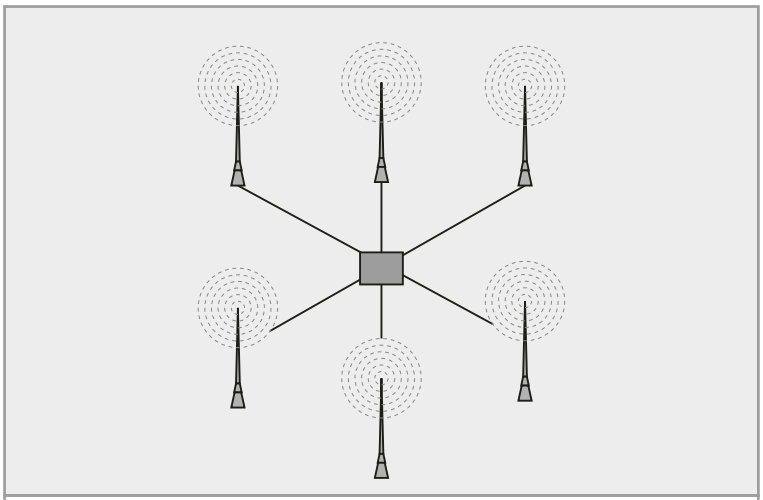


Bild 2.7: Stern-Zell-Netz

Installation zu finden. Komplexe Strukturen aus Bus-Ring-Stern-Masche-Zelle sind ebenso möglich.

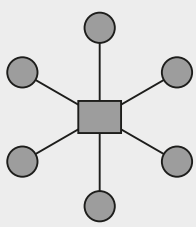
Logische und physikalische Topologien

Bei der Beschreibung der Topologie muss man zwischen der **logischen** und der **physikalischen Topologie** unterscheiden. Unter der logischen Topologie versteht man den Weg, den die Datenpakete nehmen. Die physikalische Topologie ist die Leitung, die Hardware. Eine Verkabelung kann durchaus anders aussehen, als sie funktioniert; man muss sich eine Verkabelung und Verschaltung schon genauer ansehen, um zu verstehen, um welche Art von logischer Topologie es sich handelt.

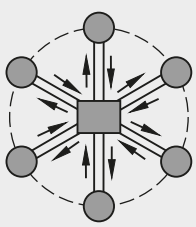
Logische Topologie: *Wie ist der Datenfluss?*

Physikalische Topologie: *Wie ist die Leitungsführung?*

Beispiel 2.1:
In Bild 2.8, links, wird ein Netzwerk sternförmig verkabelt. Im Sternmittelpunkt befindet sich ein Sternkoppler, der alle Leitungen miteinander verbindet. Wenn alle Leitungen miteinander verbunden sind, hat man einen Bus, ein *shared media* – ein geteiltes Medium. Es handelt sich hierbei also um eine physikalische Sternverkabelung (da die Leitungen sternförmig verschaltet sind) und um eine logische Busverkabelung (da alle Leitungen parallel geschaltet sind).



(a) Physikalischer Stern – Hub als Sternkoppler – Logischer Bus



(b) Physikalischer Stern – Logischer Ring

Bild 2.8: Logische und physikalische Topologie

Beispiel 2.2:
In Bild 2.8 rechts wird ein Ringnetzwerk so verkabelt, dass die Sende- und Empfangsleitungen jeder Station in einem Kabel zusammengefasst werden. Über einen Sternkoppler werden diese Leitungen sternförmig zusammengeschaltet, wobei weiterhin die Stationen hintereinander geschaltet werden. Es handelt sich hierbei also um einen logischen Ring und um eine physikalische Sternverkabelung.

2.2 Zugriffsverfahren

Am Anfang war die Busverkabelung – ein *shared media*, ein gemeinsam genutztes Medium. Wie leicht einzusehen ist, kann auf einer Busleitung immer nur eine Station senden, die anderen müssen ruhig sein und dürfen nicht zur gleichen Zeit senden. Sobald zwei oder mehrere Stationen gleichzeitig senden, überlagern sich deren Signale auf der Leitung, sodass ein fehlerfreier Empfang der Daten nicht mehr gewährleistet ist. (Wenn in einem Klassenzimmer mehrere Lehrer gleichzeitig reden, versteht kein Schüler mehr, was gesagt wird.)

Es muss also ein Verfahren zum Einsatz kommen, welches den Zugriff auf das gemeinsame Medium regelt, sodass immer nur eine Station sendet.

Es muss geregelt werden, wer wann das Medium benutzen darf.

Man kann die Rede- bzw. Sendeerlaubnis von einer Zentralstelle aus steuern, so wie beispielsweise der Bundestagspräsident den Abgeordneten das Wort erteilt. Man kann auch Regeln erlassen, wer wann senden darf (man denke hier nur an das beliebte Managerspiel: Man sitzt im Stuhlkreis und wirft sich einen Gummiball zu; wer den Ball hat, der darf reden).

Im LAN haben sich 3 Verfahren durchgesetzt:

- CSMA/CD
- CSMA/CA und
- Token Passing

2.2.1 CSMA/CD

***CSMA/CD** ist Standard in leitungsgebundenen Netzen.*

Das **CSMA/CD**-Verfahren ist das Zugriffsverfahren bei leitungsgeführten Ethernet-Netzwerken. Das Verfahren ist ganz simpel und deshalb auch sehr effektiv. Die Abkürzung steht für *Carrier Sense Multiple Access / Collision Detection*, was soviel bedeutet wie: Trägererkennung auf einem Medium mit Mehrfachzugriff und Kollisionserkennung.

CSMA/CD funktioniert wie eine Schulklasse (funktionieren sollte). Derjenige, der etwas sagen möchte, redet nicht einfach darauf los. Er hört erst eine Weile in den Raum (*carrier sense*) und bleibt ruhig, solange noch geredet wird. Prinzipiell kann jeder reden (*multiple access*). Erst wenn er sich sicher ist, dass kein anderer redet, kann er selbst anfangen zu reden. Wenn er redet, hört er weiterhin in den Raum, um sicher zu stellen, dass er der einzige ist, der redet. Stellt er fest, dass ein anderer dazwischen redet, unterbricht er sofort seine Rede, da sie durch das Zwischengerede des anderen von den restlichen Zuhörern nicht mehr korrekt empfangen werden konnte (*collision detection*).

Abbrechen der Übertragung bei Kollision, Zufalls-Wartezeit abwarten und erneut versuchen.

Soweit ist alles logisch und einfach geregelt. Der Clou an dem Verfahren setzt aber dann ein, wenn eine Kollision auftritt, wenn also mehrere

Schüler gleichzeitig reden bzw. mehrere Stationen gleichzeitig senden. Als Reaktion auf die Kollision wird nicht nur die Sendung unterbrochen, es wird sogar ein Warnsignal gesendet, das Jam-Signal. Vergleichbar wäre dies etwa mit dem Pfeifen mit einer Trillerpfeife, sobald eine Kollision auftritt. Spätestens jetzt hört auch der Störer auf zu reden. Nun beginnt eine Wartezeit und die unterbrochene Station darf nicht sofort wieder anfangen zu senden. Damit die beiden Redner oder die beiden Stationen nicht wieder gleichzeitig anfangen zu senden, läuft bei jeder Station eine andere Wartezeit. Die Wartezeit wird durch einen Zufallsgenerator festgelegt. Nach Ablauf der Wartezeit beginnt die ganze Prozedur von vorne, d. h. Hören, ob das Medium frei ist und so weiter (siehe Bild 2.9).

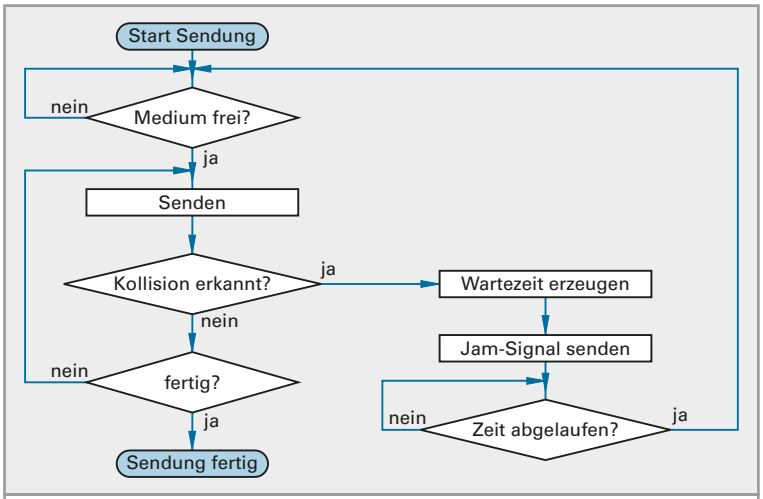


Bild 2.9: Prinzipieller Ablauf des CSMA/CD-Verfahrens

2.2.2 CSMA/CA

CSMA/CA: *Standard in Funknetzen*

Ein anderes Zugriffsverfahren ist das **CSMA/CA**-Verfahren. Diese Abkürzung steht für *Carrier Sense Multiple Access / Collision Avoidance*, also Kollisionsverhinderung anstelle der Kollisionserkennung. Dieses Verfahren ist deutlich komplizierter als das CD-Verfahren und verursacht zusätzlichen Netzwerkverkehr. Dieses Verfahren muss eingesetzt werden, wenn das Erkennen von Kollisionen nicht möglich ist. Bei Funknetzen kann die Sendestation nicht erkennen, ob eine andere Station gleichzeitig sendet. Hier kommt das CA-Verfahren zum Einsatz. Kollisionen können hier nicht vollständig verhindert werden, aber die Anzahl der Kollisionen kann reduziert werden. Vor jeder Übertragung prüft die sendewillige Station, ob das Medium frei ist (*listen before talk*). Dazu hört diese Station für eine gewisse Zeit das Medium ab. Die Dauer des Abhörens entspricht der IFS-Zeit (*interframe-spacing-Zeit*), der Zeit zwischen zwei Datenpakenten (eine Art Sicherheitsabstand zwischen den Paketen). Ist das Medium nach dieser Zeit immer noch frei, so ist die Wahrscheinlichkeit, dass es tatsächlich frei ist, ziemlich groß und die Übertragung kann beginnen.

„listen before talk“: erst hören, dann reden

Ist das Medium aber besetzt, so stellt die Station die Übertragung für eine bestimmte Wartezeit zurück.

„Hidden-Station-Problem“: zwei Stationen sehen sich nicht, wenn die Entfernung zu groß ist.

Folgendes Problem wird damit aber nicht gelöst (Bild 2.10): Zwei Stationen in derselben Zelle liegen beide nahe genug am Accesspoint, um mit ihm zu kommunizieren. Sie liegen aber zu weit auseinander, als dass die eine Station bemerken kann, wann die andere sendet. Deshalb kommt hier noch ein weiterer Mechanismus ins Spiel. Die sendewillige Station schickt, nachdem sie das Medium als nicht belegt überprüft hat, eine Sendeanfrage an den Empfänger, also den Accesspoint. Dieser beantwortet die Sendeanfrage (*Request to Send*, RTS) mit einer Sendefreigabe (*Clear to Send*, CTS), wenn diese senden darf. Klappt dieser RTS-CTS-Austausch problemlos, so kann die Sendestation nach Ablauf einer weiteren Wartezeit mit der eigentlichen Sendung beginnen. Klappt dieser RTS-CTS-Austausch nicht, so beginnt das Verfahren nach einer zufälligen Wartezeit wieder ganz von vorne.

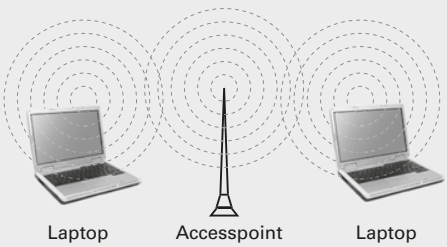


Bild 2.10: Laptops und Accesspoint

2.2.3 Token Passing

Nur wer den Token hat, darf senden.

Das englische Wort *Token* bedeutet auf Deutsch soviel wie Pfand. Token-Ring ist der bekannteste Vertreter dieser Technologie, wenngleich nicht mehr sehr gebräuchlich. Der Token-Bus gehört der Vergangenheit an. Das Verfahren besticht durch seine Einfachheit. Ein Token ist nichts anderes als ein elektronisches Telegrammformular. Es kreist im Ringnetzwerk und wird von Station zu Station weitergeschickt. Es darf zur selben Zeit nur einen Token geben. Wenn eine Station senden will, dann muss sie warten, bis der (leere) Token bei ihr vorbeikommt. Dann füllt sie ihn mit Daten. Sie trägt wie auf einem Telgrammformular die Empfänger- und die Absenderadresse sowie die zu übertragenden Nutzdaten ein. Dieser Token kreist nun genau ein Mal im Netz, bis er wieder beim Absender ankommt. Dieser löscht dann die Inhalte aus dem Formular und schickt das leere Formular weiter. Wenn keine Station senden möchte, dann kreist der Token leer im Netzwerk.

2.3 UGV – Universelle Gebäudeverkabelung

2.3.1 Strukturierte Verkabelung

Eine klare Struktur dient dem Verständnis.

Universelle Gebäudeverkabelung wird oft auch als *„strukturierte diensteneutrale Verkabelung“* bezeichnet. Um ein Netzwerk professionell und auch kostengünstig über viele Jahre betreiben zu können, ist eine klare

Struktur der Netzwerkverkabelung absolut notwendig. Diensteneutral bedeutet in Bezug auf Netzwerkverkabelung, dass die Verkabelung unabhängig von dem Dienst ist, der die Leitungswege benutzt. Über die bisher übliche Telefonverkabelung kann man nur Dienste mit geringer Bandbreite benutzen, wie eben Telefon und Fax. Eine zukunftsfähige Verkabelung muss aber alle heutigen Dienste wie Computernetzwerk, Video und eben auch Telefon bedienen können. Statt einer separaten Verkabelung für jeden gewünschten Dienst wird in einer strukturierten, diensteneutralen Verkabelung nur eine Verkabelung realisiert, auf welcher dann die unterschiedlichsten Geräte angeschlossen werden.

Unterschiedliche Dienste auf einer Verkabelung.

Selbstverständlich ist eine gute Netzwerkleitung teurer als eine Telefonleitung. Betrachtet man aber die Gesamtkosten (*Total Cost of Ownership* TCO), so ist eine einheitliche Verkabelung jedoch deutlich billiger als zwei getrennte Verkabelungen.

Die Normen EN 50173-1 bzw. ISO/IEC 11801 regeln den Aufbau einer Kommunikationsverkabelung. Die Gesamtverkabelung wird in drei Bereiche eingeteilt:

- Primärbereich
- Sekundärbereich
- Tertiärbereich

Primärbereich:
Standort-Verkabelung

Der erste Bereich, die **Primärverkabelung** eines Firmennetzwerkes, ist die Standortverkabelung. Im Primärbereich werden von einem Standortverteiler aus die einzelnen Gebäude auf einem Firmengelände miteinander angeschlossen. Diese Verkabelung wird oft auch *Backbone* (Rückgrat) bezeichnet. Ausgehend von einem Standortverteiler werden alle Gebäude sternförmig angeschlossen (Bild 2.11).

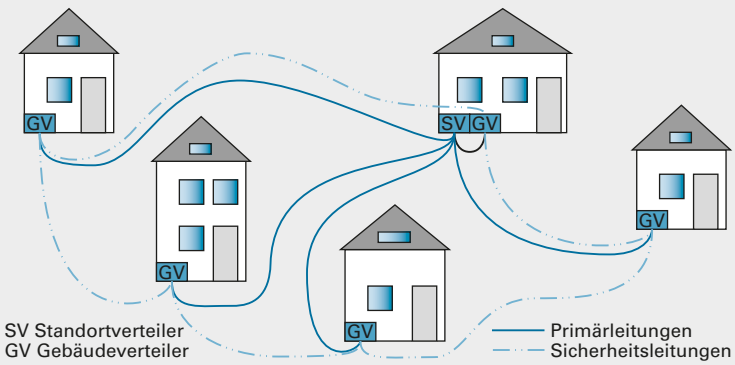


Bild 2.11: Primärverkabelung, Standortverkabelung

Sekundärbereich:
Gebäude-Verkabelung

Der zweite Bereich, die **Sekundärverkabelung** eines LANs, ist die Gebäudeverteilung. Im Sekundärbereich werden von einem Gebäudeverteiler aus die einzelnen Stockwerke angeschlossen. Diese Verkabelung nennt man oft auch Vertikal-Verkabelung und die Leitungen nennt man Steigleitungen, da die Leitungen von unten nach oben verlaufen (Bild 2.12).

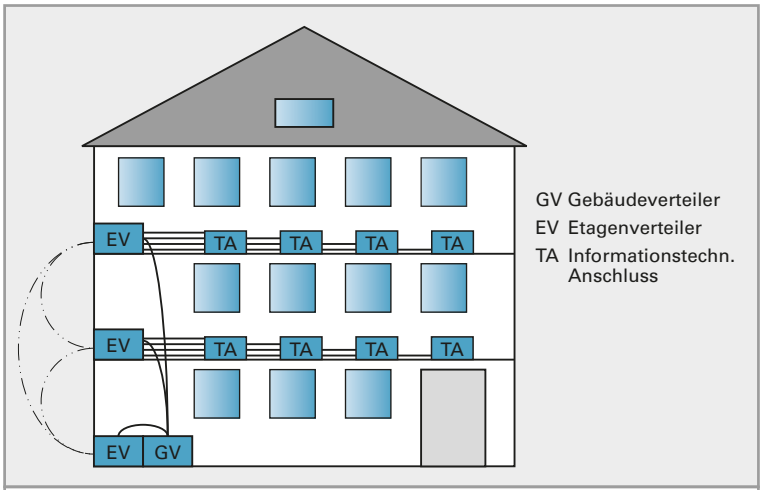


Bild 2.12: Sekundär- und Tertiärverkabelung im Gebäude und auf der Etage

***Tertiärbereich**: Etagen-Verkabelung*

Der dritte Bereich, die **Tertiärverkabelung** eines LANs, ist die Etagenverteilung. Im Tertiärbereich werden von einem Etagenverteiler aus die Steckdosen in den Büros usw. angeschlossen. Diese Dosen nennt man TAs (TA: Technischer Anschluss). Diese Verkabelung nennt man oft auch Horizontal-Verkabelung, bei der die Leitungen auf einer Ebene, dem Stockwerk, verlegt werden.

Jede Verkabelungsebene ist eine Sterntopologie. Zusammen ergibt sie einen erweiterten Stern.

Die übliche Topologie ist der Stern. Ausgehend vom Standortverteiler werden sternförmig die Gebäudeverteiler angefahren. Vom Gebäudeverteiler aus werden die Etagenverteiler eines jeden Gebäudes wieder sternförmig angefahren. Von jedem Etagenverteiler aus werden nun die TAs wiederum sternförmig angeschlossen (Bild 2.13).

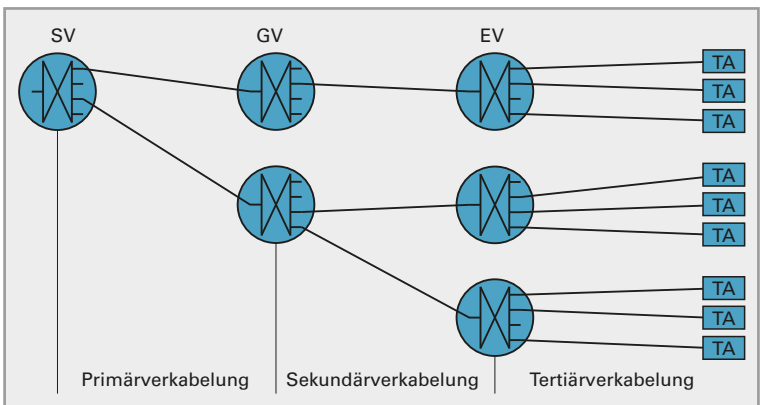


Bild 2.13: Strukturierte Verkabelung – Erweiterter Stern

Die Gesamttopologie ist also ein Erweiterter Stern. Es ergibt sich bei dieser Verkabelung folgendes Problem:

Querverbindungen dienen der Ausfallsicherheit.

Wird eine Leitung im Primärbereich, beispielsweise durch Kabelbruch unbrauchbar, dann ist ein ganzes Gebäude vom restlichen Firmennetzwerk isoliert.

Die Lösung ist sehr einfach: Man verbindet die Gebäude nach Möglichkeit auch mit ihren Nachbarn durch Reserveleitungen. Diese Leitungen sind im Regelfall unbenutzt. Im Fehlerfall können sie aber aktiviert werden, sodass das isolierte Gebäude über einen Umweg wieder mit dem restlichen LAN verbunden wird. Die daraus resultierende Topologie ist dann eine unvollständige Masche. Wie dies aber genau gemacht wird, wird im Kapitel über Switches beim Spanning-Tree-Verfahren erläutert. Hier dazu nur soviel: Es funktioniert automatisch, ohne dass Leitungen im Fehlerfall von Hand umgesteckt werden müssen.

Die Querverbindungen werden von den Switches bei Bedarf automatisch aktiviert.

Innerhalb eines Gebäudes hat man dasselbe Problem und auch hier dieselbe Lösung. Die Etagenverteiler werden ebenfalls miteinander verbunden.

Querverbindungen bilden Maschen.

Bei kleineren Netzen wird natürlich nur ein Teilbereich der Verkabelung realisiert, abhängig von den Bedürfnissen. In einer Arztpraxis mit mehreren Zimmern auf einem Stockwerk wird natürlich nur ein Etagenverteiler und die Tertiärverkabelung realisiert. Eine Firma mit einem mehrstöckigen Gebäude wird einen Gebäudeverteiler, die Sekundärverkabelung, die Etagenverteiler und die Tertiärverkabelung bekommen.

Wichtig ist, dass die Verkabelung des Netzwerkes, egal wie groß das Netzwerk auch ist, von Anfang an sauber dokumentiert wird. Die Lage der Verteiler, der Verlauf der Leitungswege und die Lage der TAs müssen in Plänen (am besten den Architektenplänen) eingetragen werden. Erweiterungen und Änderungen an der Verkabelung müssen immer sofort in den Plänen nachgetragen werden, damit immer aktuelle Unterlagen vorhanden sind.

Welche Leitungen in welchem Bereich verwendet werden, hängt von den Anforderungen des Netzwerkbereibers und von den örtlichen Gegebenheiten ab. Als Richtwert kann man sagen, dass die Primärverkabelung in Lichtwellenleitern (Glasfasern) ausgeführt wird. Oft kommen hier Singlemode-Fasern zum Einsatz. Die Sekundärverkabelung wird in der Regel auch in Lichtwellenleitern ausgeführt. Hier wird meist Multimodefaser eingesetzt. Der Endbereich, die Tertiärverkabelung, wird in Kupferleitungen ausgeführt. Hier können Leitungen der Kategorie 6, 7 oder 8 oder auch Wireless-LAN eingesetzt werden.

Der Einsatzbereich entscheidet, welche Leitungen eingesetzt werden.

Die Kategorie beschreibt die Leistungsfähigkeit der Leitung.

Bild 2.14: Verteilerschrank

Beschriftung von TAs und Verteilerschränken

Um das Ziel der strukturierten Verkabelung zu erreichen, muss die gesamte Verkabelung dokumentiert werden. Dazu dienen Lagepläne vom Architekten, in die Verteiler, Dosen und die Leitungsführung eingezeichnet werden.

Dokumentation und Beschriftung ist notwendig und hilfreich.

Pläne allein reichen aber nicht aus. Die Komponenten müssen

gut sichtbar beschriftet werden. Dazu verwendet man gut haftende Aufkleber.

Jeder Verteilerschrank wird eindeutig gekennzeichnet, beispielsweise mit SV für Standortverteiler, GV1, GV2, usw. für Gebäudeverteiler, EV1, EV2, usw. für die Etagenverteiler.

Jedes Steckfeld in den Verteilern wird ebenfalls gekennzeichnet. Hier werden am einfachsten die Steckfelder von oben nach unten durchnummeriert. Die einzelnen Steckplätze sind in der Regel auf dem Steckfeld nummeriert.

Die TAs werden ebenfalls gekennzeichnet. Sie tragen die Nummer der Buchse im Etagenverteiler, auf der ihre Leitung endet.

Beispiel: Der TA mit der Bezeichnung EV2.5.12 ist mit der Buchse 12 des 5. Patchfeldes im Etagenverteiler 2 verbunden.

Die Cisco-Einteilung

*Die Firma **Cisco** ist ein großer Pionier auf dem Gebiet der Netzwerktechnik.*

Cisco teilt eine Firmenverkabelung ebenso in drei Bereiche ein:

- Core layer
- Distribution Layer
- Access Layer

Im Core-Layer befinden sich sehr leistungsstarke Switches oder Router. Sie kommen üblicherweise im Primärbereich zum Einsatz.

Im Distribution-Layer werden Switches mit guter Leistungsfähigkeit eingesetzt – also üblicherweise im Sekundär-Bereich.

Als Access-Layer wird die Tertiärverteilung bezeichnet. Hier werden Endgeräte mit typischerweise 100 Mbps oder 1 Gbps angeschlossen.

2.3.2 Netzklassen und -kategorien

Die Klasse spezifiziert die Gesamtverkabelung.

Die Leistungsfähigkeit einer Netzwerkverkabelung mit symmetrischen Kupferleitungen wird in Netzwerk-Anwendungs-Klassen A bis F eingeteilt (Tabelle 2.1). Dabei werden ausschließlich die passiven Netzkomponenten bewertet.

Tabelle 2.1: Netzanwendungsklassen

Klasse	Frequenzbereich	Anwendungen
A	≤ 100 kHz	niederfrequente Anwendungen (z. B. Telefon, Fax)
B	≤ 1 MHz	Anwendungen mit niedriger Bitrate (z. B. ISDN)
C	≤ 16 MHz	Anwendungen mit hoher Bitrate (z. B. Ethernet)
D	≤ 100 MHz	Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet oder Gigabit-Ethernet)
E	≤ 250 MHz	Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet, Gigabit-Ethernet oder 10-Gigabit-Ethernet, Kabelfernsehen)
E_A	≤ 500 MHz	Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet, Gigabit-Ethernet oder 10-Gigabit-Ethernet, Kabelfernsehen)
F	≤ 600 MHz	reserviert für künftige Anwendungen
F_A	≤ 1000 MHz	reserviert für künftige Anwendungen

Eine höhere Klasse einer Verkabelungsstrecke beinhaltet auch die Anforderungen an die darunter liegenden Klassen – sie sind also abwärtskompatibel. Bei den Steckern und Buchsen ist dies jedoch ab Klasse F nicht mehr gegeben, wohl aber für die Verkabelung.

Tabelle 2.2 zeigt eine Übersicht mit den wichtigsten nationalen und internationalen Normen für strukturierte Verkabelungen.

Tabelle 2.2: Übersicht wichtiger Normen im Verkabelungsbereich – Normen für strukturierte Verkabelungen

Netzwerkklasse	D	E	E_A	F	F_A
Bandbreite	100 MHz	250 MHz	500 MHz	600 MHz	1000 MHz
USA-Normen	TIA/EIA 568 B.2-1:2002 CAT5e	TIA/EIA 568 B.2-1:2002 CAT6	TIA/EIA 155 CAT6 Mitigaton		
			TIA/EIA 568 B.2-1:2002 CAT6A (augmented CAT6)		
Internationale Normen	ISO/IEC 11801 Ed.2:2002 CAT5/Klasse D	ISO/IEC 11801 Ed.2:2002 CAT6/Klasse E	ISO/IEC 11801:2002 Amd.1:2008 Channel Class E_A	ISO/IEC 11801 Ed.2:2002 CAT7 / Klasse F	ISO/IEC 11801:2002 Amd.1:2008 Channel Class F_A
			ISO/IEC 11801:2002 Amd.2:draft – Link Class E_A, CAT6A		ISO/IEC 11801 Ed.2:2002 Amd.2:draft – Link Class F_A, CAT7A
			ISO/IEC TR> 24750 CAT6 / Class E Mitigaton		
EU-Normen		EN 50173-1...5:2007 CAT6 / Class E	EN 50173-1 Beiblatt 1:2008 Class E_A-Channel	EN 50173:2007 CAT7 / Class F	EN 50173-1 Beiblatt 1:2008 Class F_A-Channel
			prTR50173-99-1^CAT6 Mitigaton für 10G Base-T		

Leitungskategorien

***Kategorien** spezifizieren einzelne Leitungen, Stecker, Dosen.*

Aufgrund der in einer Verkabelung verwendeten Leitung und Komponenten kann die Netzwerkanwendungsklasse festgelegt werden (Tabelle 2.3). Die endgültige Einteilung in eine Klasse kann aber nur über einen messtechnischen Nachweis erfolgen. D.h., jede Verkabelungsanlage muss, auch bei sorgfältigster Planung und Installation, vor der Übergabe an den Kunden vermessen werden! Die Messprotokolle sind dem Betreiber der Kabelanlage zu übergeben. Anhand dieser Protokolle kann später entschieden werden, ob eine neue Anwendung auf der bestehenden Anlage betrieben werden kann oder nicht.

Tabelle 2.3: Leitungs-Kategorien

Kategorie	Frequenzbereich	Anwendung	geeignet für Klasse
3	≦ 16 MHz	Telefon, Token-Ring, Ethernet	C
5	≦ 100 MHz	Fast Ethernet, Gigabit-Ethernet	D
6	≦ 250 MHz	Gigabit-Ethernet, 10-Gigabit-Ethernet	D, E
6_A	≦ 625 MHz	Gigabit-Ethernet, 10-Gigabit-Ethernet	D, E, E_A
6_E	≦ 500 MHz	Gigabit-Ethernet, 10-Gigabit-Ethernet	D, E, E_A
7	≦ 600 MHz	10-Gigabit-Ethernet, Kabelfernsehanlagen	D, E, E_A, F
7_A	≦ 1000 MHz	10-Gigabit-Ethernet, Kabelfernsehanlagen	D, E, E_A, F, F_A

2.3.3 Abnahmemessung

Jede Installation muss durchgemessen und abgenommen werden.

Nach Fertigstellen einer Verkabelung muss diese durchgemessen werden. Das sorgfältige Aussuchen der verwendeten Komponenten ist Grundvoraussetzung, um eine bestimmte Netzwerkklasse zu erreichen.

Es werden grundsätzlich 2 Arten von Firewall unterschieden:

- Paket-Filter
- Content-Filter

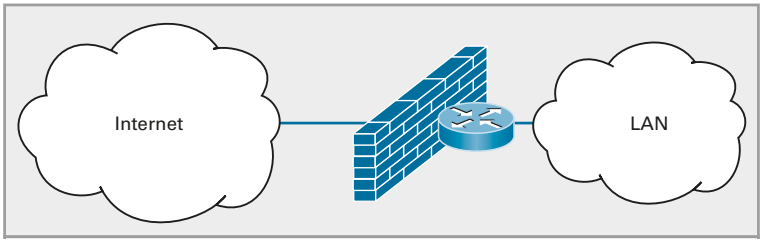


Bild 4.18: Firewall schützt das LAN

*Ein **Paketfilter** prüft die eingehenden Pakete und entscheidet, ob sie ins Netzwerk weitergeleitet werden.*

Eine Paketfilter-Firewall prüft die ankommenden Pakete, ob sie an einen TCP- oder UDP-Port adressiert sind, der geöffnet ist. Sind sie an einen geschlossenen Port adressiert, dann werden sie an der Firewall geblockt. (Siehe Kapitel 5 „Adressierung")

Eine weitere Prüfung erfolgt bei der zustandsabhängigen Paketüberprüfung, der Stateful Packet Inspection. Dabei werden geöffnete Kommunikationssitzungen überprüft. Bei der Datenübertragung über TCP (Kapitel 6.2) wird vor der Datenübertragung eine Sitzung (engl. Session) aufgebaut. Nach dem Ende der Übertragung wird diese Session wieder geschlossen. Mit der Stateful Packet Inspection werden diese offenen Sitzungen überwacht und ggf. auch geschlossen, wenn sie zu lange ohne Datenverkehr geöffnet bleiben.

***Content Filter** schauen in die Pakete hinein und entscheiden inhaltsabhängig über das Weiterleiten.*

Content-Filter inspizieren den Inhalt der eingehenden Daten. Sie können beispielsweise Viren und andere Schadsoftware im Inhalt einer Email oder einer Webseite erkennen und blockieren. Mit Content-Filtern lassen sich auch einzelne IP-Adressen oder Webseiten sperren. Der Admin kann eine Liste von gesperrten URLs anlegen, so dass auf diese Seiten vom LAN aus nicht mehr zugegriffen werden kann.

Die Vorgehensweise beim Öffnen und Schließen von Ports und beim Einrichten von Sperrlisten veranschaulicht die folgende kleine Urlaubsgeschichte:

Es treffen sich drei IT-Verantwortliche an einer Hotelbar. Der Engländer sagt: Bei uns ist alles erlaubt, was nicht explizit verboten ist! Der Deutsche sagt: Bei uns ist alles verboten, was nicht explizit erlaubt ist! Da meldet sich lachend der Italiener und meint: Bei uns ist alles erlaubt – besonders das, was verboten ist!

So unterschiedlich wie diese Urlauber ihre Einschätzung von ihrem Heimatland erklären, so verschieden sind auch die Herangehensweisen bei Firewalls.

Eine Firewall hat die Aufgabe, ein Netzwerk vom öffentlichen Netz zu isolieren und nur bestimmte Zugriffe von außen auf das Netz zu erlauben. Zwei grundsätzliche Varianten werden dabei unterschieden:

Bei einer Blacklist werden alle Zugriffe, die nicht erlaubt sind, eingetragen. Alle anderen Zugriffe sind erlaubt. Bei einer Whitelist werden alle erlaubten Zugriffe eingetragen. Alle anderen Zugriffe werden geblockt.

***Blacklist** = Sperrliste*
***Whitelist** = alles, was erlaubt ist*

Man erkennt an dieser Stelle die Ähnlichkeiten mit den Urlaubern.

4.4 DMZ – Demilitarisierte Zone

Unter einer Demilitarized Zone versteht man ein Netz, welches sich zwischen einem Firmennetz und dem Internet befindet.

Zweistufige DMZ

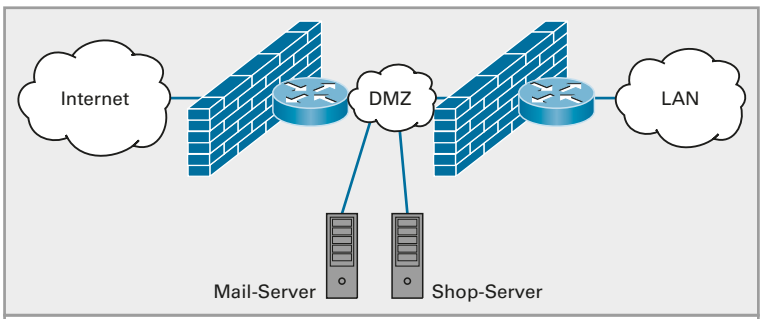


Bild 4.19: Zweistufige DMZ

Eine Firewall schützt die DMZ gegen Angriffe von außen. Eine weitere Firewall verbindet die DMZ mit dem internen LAN. So ist das LAN doppelt geschützt und das Eindringen von außen wird erschwert. Um es den Angreifern noch schwerer zu machen, sollten für die äußere und die innere Firewall verschiedene Systeme verwendet werden.

***DMZ** ist ein Zwischennetz zwischen Internet und Firmen-LAN*

In der DMZ stehen Rechner, die von außen zugreifbar sein sollen – etwa eMail-Server oder Shop-Systeme. Rechner in der DMZ nennt man auch Bastion Hosts, da sie hinter einer Bastion geschützt sind.

Manche Administratoren platzieren in der DMZ auch Honeypods. Diese „Honigtöpfe“ sind Server, die ein vermeintlich leichtes Opfer für Hackerangriffe darstellen, aber keine Daten von Nutzen beherbergen. Dadurch werden mögliche Angreifer auf eine falsche Fährte gelockt.

Einstufige DMZ

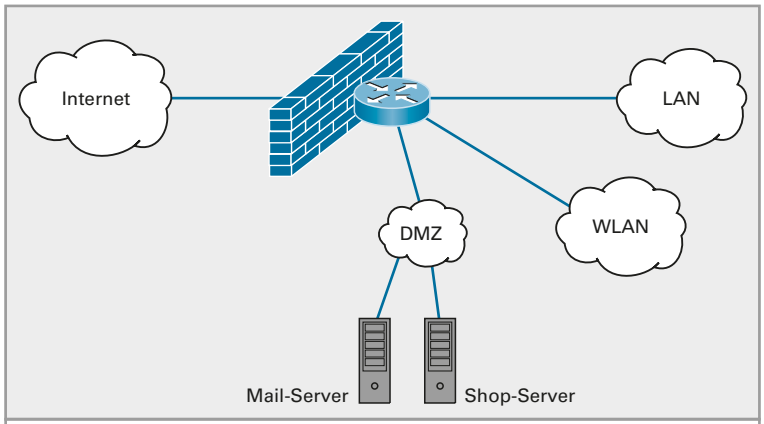


Bild 4.20: Einstufige DMZ

Einstufige DMZ hat mehrere voneinander isolierte Netzwerke

Ein einstufiges Firewall-Konzept ist einfacher als ein zweistufiges. Die Firewall hat mehrere LAN-Anschlüsse. An einen LAN-Anschluss schließt man das interne LAN an. An einem weiteren, für den andere Filterregeln einstellbar sind, schließt man die Rechner der DMZ an. Oftmals kann man über einen weiteren LAN-Anschluss die WLAN-Accesspoints anschließen, um das WLAN separat zu managen. Dies ist mittlerweile fast eine Notwendigkeit, da viele Mitarbeiter ihre WLAN-fähigen Geräte mit in die Firma bringen und mit dem Firmennetz verbinden.

Solch einstufige Firewalls sind beispielsweise IPCOP oder IPFire – Linux-basierte Komplettlösungen. Sie sind kostenlos (open source, GPL) und brauchen den Vergleich mit kommerziellen Systemen nicht fürchten.

4.5 SDN – Software Defined Networking

Eine neue Technik drängt seit einigen Jahren auf den Markt – Software Defined Networks. Netzwerke, wie wir sie bisher kennen, bestehen aus Leitungen, Switches, Routern, Firewalls und anderen Geräten. Sie sind starr und sehr hardwarenah. Mit SDN bekommen die Systeme ein „Betriebssystem“. Sie werden flexibel und können ihr Verhalten den Anforderungen anpassen.

Das Netz wird virtualisiert und programmiert.

Es wird in absehbarer Zeit nur noch eine Art von Netzwerkgeräten geben. Sie werden in sehr großen Stückzahlen gefertigt werden und dadurch sehr preiswert sein. Ob sich ein solches Gerät wie ein herkömmlicher Switch verhält oder wie ein Router, all das regeln die Regeln, die dem Netz vom Netzwerker gegeben werden. Wie diese Geräte heißen werden, ist noch unklar. Bisher nennt man sie „SDN-Switches“.

Die Regeln für das Verhalten des gesamten Netzes werden in SDN-Controllern auf dem Control-Layer erstellt und verwaltet. Diese Regeln werden in sogenannten Flow-Tables gespeichert. Die SDN-Switches holen sich ihre Regeln nach Bedarf. Trifft ein Datenpaket erstmalig auf einen solchen Switch, so fragt dieser bei einem Controller nach, was er damit tun soll. Gibt es keine spezielle Regel für dieses Paket, so bekommt der

Switch eine Standard-Regel. Der Switch speichert die Regel und weiß dann später immer, was er mit einem Paket dieser Art anfangen soll.

Der Netzwerkadmin erstellt die Regeln für die Datenflüsse auf dem Control-Layer.

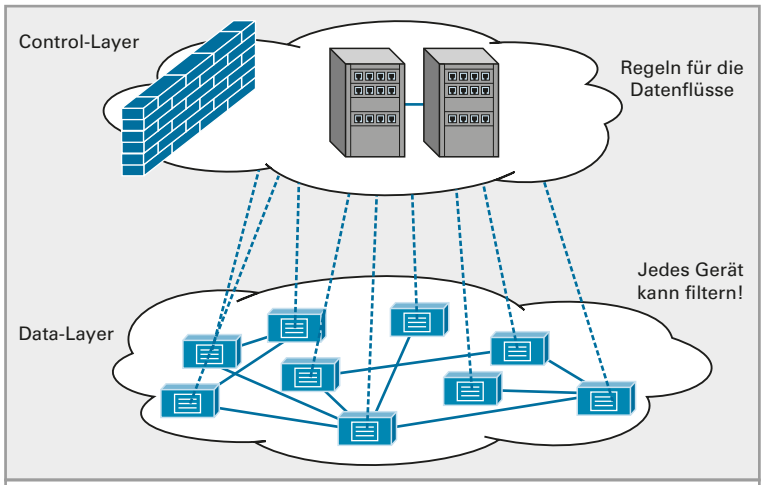


Bild 4.21: Netz mit SDN-Switches

Nun ist es egal, ob das Gerät wie ein herkömmlicher Switch funktioniert oder wie ein Router. Die Regel kann auch lauten, das Paket zu verwerfen. Eine spezielle Firewall gibt es dann nicht mehr. Vielmehr werden die Firewall-Regeln auch auf die SDN-Switches verteilt. Somit kann jeder Switch auch Firewall sein.

Hier ein Beispiel einer einfachen Flowtable:

Tabelle 4.1: Flowtable

Regel-Nr.	Quell-MAC	Ziel-MAC	Quell-IP	Ziel-IP	Ziel-Port	...	Action
1	*	00:10:*	*	*	*		Port 1
2	*	*	*	*	20		Drop
3	*	*	*	10.10.2.3	*		Port 2
4	*	*	10.10.3.5	10.20.30.*	*		Port 1, Port 2
5	*	*	1.2.3.4	*	*		Drop
6							

Interpretation der obigen Flowtable:

- Regel Nr. 1: Alle Pakete an die Ziel-MAC, die mit 00:10 beginnen werden an Port 1 geschickt.
- Regel Nr. 2: Alle Pakete an TCP-Port 20 werden gelöscht
- Regel Nr. 3: Alle Pakete an die IP-Adresse 10.10.2.3 werden an Switch-Port 2 weitergeschickt
- Regel Nr. 4: Alle Pakete von IP-Adresse 10.10.3.5 an einen Rechner im Netz 10.20.30.* werden an Port 1 und an Port 2 geschickt (beispielsweise zum Monitoring, zur Kontrolle was ein bestimmter Rechner in ein bestimmtes Netz schickt)
- Regel Nr. 5: Alle Pakete von der IP-Adresse 1.2.3.4 werden gelöscht

4.6 Übungen Schichtenmodelle

Übungsaufgabe Nr. 1

Ordnen Sie die Netzwerkgeräte den Schichten des OSI- und TCP/IPModells zu:

- Switch:
- Hub:
- Router:
- Repeater:
- Gateway:
- Bridge:

Übungsaufgabe Nr. 2

Welches Netzwerkgerät verbindet einzelne Netzsegmente und welches ganze Netzwerke (Bild 4.18)?

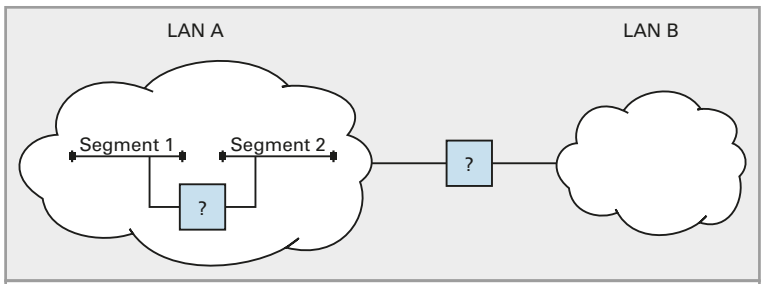


Bild 4.22: Netzwerkgeräte

5 Adressierung

Auf drei Ebenen des OSI-Schichtenmodells und des TCP/IP-Schichtenmodells werden jeweils verschiedene Adressierungen verwendet:

Oben beginnend, wird eine Anwendung über **Portnummern** adressiert. Eine Ebene darunter erhält ein Host eine **IP-Adresse**. Unten schließlich werden Netzwerkkarten per **MAC-Adresse** angesprochen (Bild 5.1).

Ports und IP-Adressen sind logische Adressen. Die MAC-Adressen sind physikalische Adressen. Die Kombination von Port und IP-Adresse nennt man **Socket**. Ein Socket hat die Form:

IP-Adresse: Port-Nummer,
z. B. 10.1.2.3:80.

Dies adressiert die Applikation von Port 80 auf IP-Adresse 10.1.2.3.

OSI	Layer	Adressen
L7	Application	
L6	Presentation	
L5	Session	
L4	Transport	Port-Adressen
L3	Network	IP-Adressen
L2	DataLink	MAC-Adressen
L1	Physical	

Bild 5.1: Zuordnung von Adressen und Schichten

Es gibt 3 unterschiedliche Adressen:
Port**, **IP** und **MAC

***Socket:** Sockel*

5.1 Ports – Transport-Layer

Auf der Schicht 4 des OSI-Modells (Transport-Layer) bzw. auf der Schicht 3 des TCP/IP-Layers werden die Anwendungen adressiert. Jede Anwendung bekommt eine eigene Nummer zugewiesen. Eine Port-Nummer ist eine 16 Bit umfassende Nummer.

Im TCP- und im UDP-Protokollkopf ist jeweils ein 16 Bit großer Bereich für die Portnummer vorhanden. Es lassen sich somit 216 Ports unterscheiden. Die wichtigsten und geläufigsten Ports sind vordefiniert. Es handelt sich um die Portnummern 0 bis 1023. Man nennt sie die *well known ports*, die „gut bekannten Ports“. Von Port 1024 bis 49151 befinden sich die Registered Ports: Diese wurden von Firmen für ihre Anwendungen registriert. Registrierte Ports haben den Vorteil, dass sich die Anwendung anhand der Portnummern sofort erkennen lässt. Die restlichen Portnummern bis 65535 sind frei und können nach Belieben verwendet werden.

L7	Application
L6	Presentation
L5	Session
L4	Transport
L3	Network
L2	Data Link
L1	Physical

Port-Adressen
⇒ Transport-Layer

Beispiel 5.1:
An einem PC ist ein Browserfenster geöffnet und es wird eine Domain-Adresse ins Adressfeld eingegeben. Dann startet der PC zuerst die Namensauflösung, um die IP-Adresse der Domäne zu erfragen. Diese Anfrage schickt er mit seinem Absender-Port 53 (für DNS) an den DNS-Server aus seiner Netzwerkkonfiguration. Als Ziel-Port wird auch der Port 53 angegeben, weil auf diesem Server vielleicht noch andere Anwendungen laufen. Dadurch wird der DNS-Dienst auf diesem Server adressiert.

Der DNS-Server schickt nun die angefragte IP-Adresse an den PC zurück und adressiert wiederum den dortigen DNS-Port.

Dann startet der PC seine eigentliche Anfrage. Er adressiert die Anfrage an den Ziel-Server und schickt dabei die Portnummer des angefragten Dienstes mit, hier also Port 80 für HTTP. Der Absenderport ist ebenfalls HTTP.

Auf einem Unix-Rechner ist diese Liste in der Datei `/etc/services` definiert.

Unter Betriebssystemen der Windows-NT-Linie findet sich diese unter: `\%\system32\drivers\etc\services`

Es folgt eine Liste der wichtigsten Portnummern:

Tabelle 5.1: Einige wichtige Port-Nummern-Belegungen

Portnummer	Bezeichnung	Bemerkung
20	ftp-data	Datenkanal bei FTP
21	ftp-ctrl	Steuerkanal für FTP
22	ssh	Secure Shell (wie Telnet – aber verschlüsselt)
23	Telnet	Terminalemulation
25	SMTP	E-Mail-Versand
53	DNS	Namensauflösung in IP-Adressen
67	DHCP	automatische IP-Adressvergabe an Clients
80	HTTP	Webserver
110	POP3	PostOfficeProtocol, E-Mail-Verkehr
123	NTP	Network Time Protocol, Zeitsynchronistation
143	IMAP	E-Mail-Verkehr
443	HTTPS	Webserver, verschlüsselt
1521	Oracle	Zugriff auf Oracle-Datenbanken
1723	VPN	Virtuelle private Netzwerke
3306	MySQL	Zugriff auf MySQL-Datenbanken
3389	RDP	Windows Remotedesktopzugriff, Windows Terminal Services
5190	ICQ	Instant-Messaging-Programm ICQ
5432	PostgreSQL	Zugriff auf PostgreSQL-Datenbanken
6667	IRC	Chatserver

sind Bestandteil der IP-Adressen und dienen damit als Routinginformation für den Transport der Pakete (Bild 7.8).

Geroutet wird, wenn mit einem Host außerhalb des eigenen Netzes kommuniziert wird!

Die IP-Adressen von Sender und Empfänger bleiben über die gesamte Übertragungsstrecke unverändert! Die physikalischen Adressdaten werden von Teilstrecke zu Teilstrecke verändert!

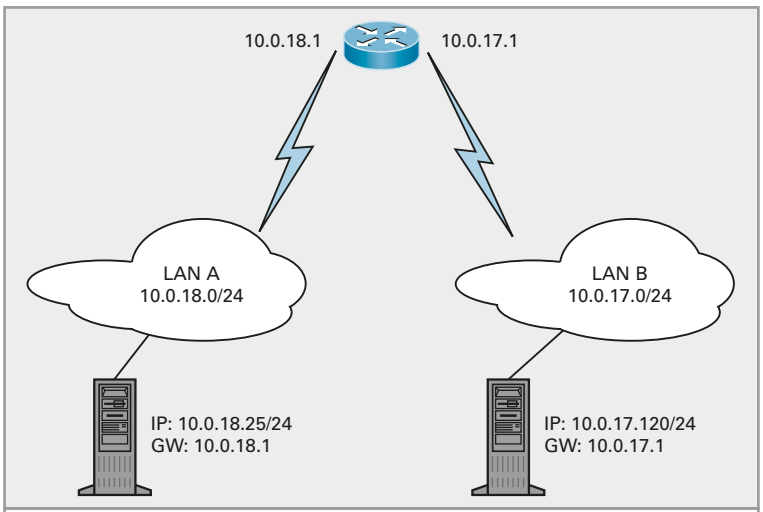


Bild 7.7: Ein Router verbindet zwei Netze

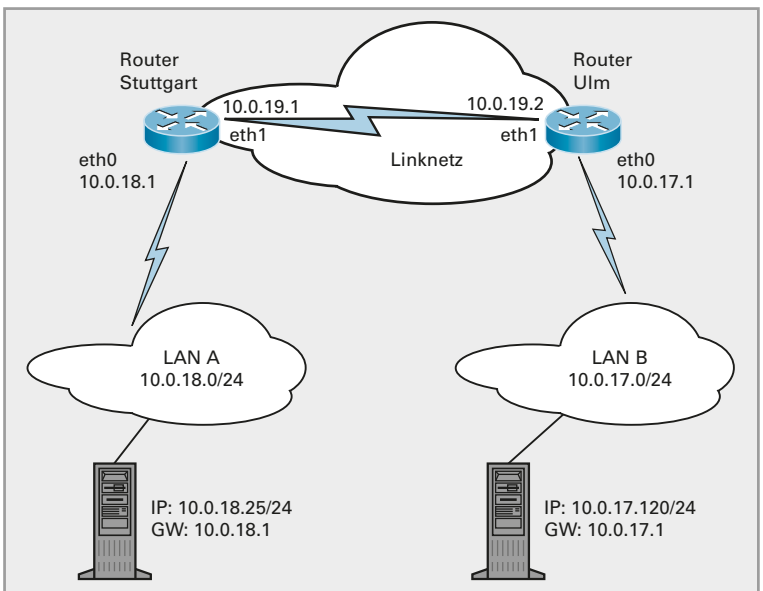


Bild 7.8: Zwei Router verbinden zwei Netze über eine Linkstrecke

7.2.1 Routing – Wie arbeitet ein Router?

Was geschieht im Router mit einem empfangenen Datenframe? An welchen Port leitet der Router einen empfangenen Datenframe weiter?

Bild 7.9 zeigt den Ablauf des Routing-Vorganges.

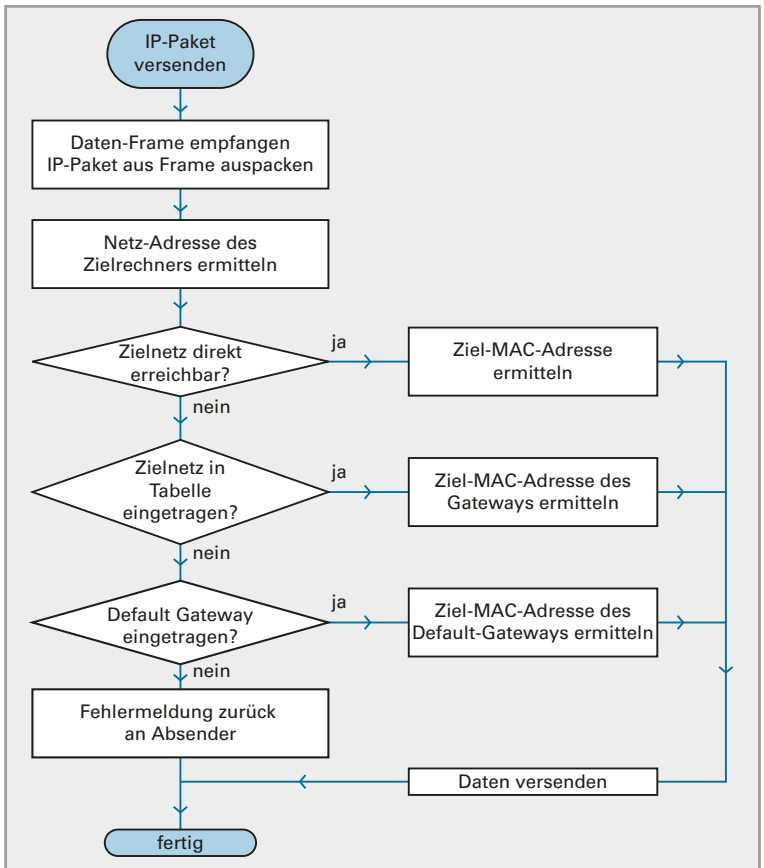


Bild 7.9: Routing-Diagramm

Der Router entpackt den empfangenen Datenframe bis auf OSI-Layer 3, der Netzwerkschicht.

Er liest die IP-Adresse des Zielrechners und trifft seine Entscheidung, wohin er das Paket weiterleiten soll. Ziel- und Quell-IP-Adresse bleiben dabei unverändert. Die Adressierung auf der darunter liegenden Schicht 2 wird verändert. Es wird von jedem Router der nächste Router adressiert. Der letzte Router adressiert den Zielknoten.

Eine Verbindung zwischen zwei Routern nennt man Route oder Link. Es werden statische und dynamische Routen unterschieden.

***Statische Routen** sind fest.*

***Dynamische Routen** ändern sich, wenn sich die Netzstruktur ändert.*

Statische Routen werden vom Administrator von Hand fest in die Routingtabelle eingetragen.

Dynamische Routen werden vom Router selbst während des Betriebes in die Tabelle eingetragen und verwaltet.

Die Default-Route ist eine statische Route, die verwendet wird, wenn kein passendes Netz gefunden wird. Dies ist vergleichbar mit Default-Gateway bei jedem Rechner. Diese Route wird auch als *„Gateway of last resort"* bezeichnet, also in etwa „der letzte Ausweg".

Datensicherheit

Die Daten gelangen unverändert von einem Netz ins andere. Jeder, der Zugang zu den physikalischen Übertragungswegen hat, Leitungen oder Router, kann die Daten mitlesen. Dies stellt ein erhebliches Sicherheitsrisiko dar!

Abhilfe schafft hier das Verschlüsseln der Daten von Endgerät zu Endgerät, sodass auf dem Weg zwischen den beiden Rechnern die Daten zwar mitgelesen, aber nicht ausgewertet werden können.

7.2.2 Routing Protocols / Dynamisches Routing

Informationen, die den Router veranlassen, die Routingtabelle zu verändern, nennt man Routing-Protokolle. Router senden in regelmäßigen Abständen Angaben über ihren Zustand und über die angeschlossenen Netzwerke usw. an die benachbarten Router.

Beispiel 7.1: Routingprotokolle

- RIP – Router Information Protocol
- RIPv2 – RIP Version 2
- IGRP – Interior Gateway Routing Protocol
- EIGRP – Extended IGRP
- OSPF – Open Shortest Path First

7.2.3 Count-to-Infinity

Damit der Router Entscheidungen treffen kann, welche Route ein Datenpaket nehmen soll, werden die Routen mit „Metrics" bewertet. Metrics sind Gewichtungsfaktoren wie z. B. die Distanz (RIP), Bandbreite oder die Auslastung einer Leitung.

Ältere Routingprotokolle benutzen einfache Metrics. Die einfachste Metric ist die Anzahl der Router, die bis zum Ziel übersprungen werden müssen. Man nennt dies Hops (Sprünge).

Wird nur die Anzahl der zu passierenden Router verarbeitet (Hops), so werden langsame Routen über wenige Router gegenüber längeren aber schnelleren Routen vorgezogen. Da hierbei nur die Anzahl der Router eine Rolle spielt, bezeichnet man diese Protokolle als Distance-Vector-Protokolle.

Beispiel 7.2: Distance-Vector-Protokolle

- RIP – Router Information Protocol
- RIPv2 – RIP Version 2
- IGRP – Interior Gateway Routing Protocol
- EIGRP – Extended IGRP

Im Beispiel aus Bild 7.10 werden zwei Netzwerke LAN A und LAN B über die Router R1, R2 und R3 mit schnellen Fast Ethernet-Leitungen verbunden. Als Ausfallsicherung wird eine langsame Wählverbindung über ISDN von Router R1 zu Router R3 eingerichtet. Die langsame Route über die ISDN-Wählleitung hat dabei eine Metrik von 2 Hops, die wesentlich schnellere Leitung hat hingegen eine Metrik von 3. Bei reinem Distance-Vector-Routing würde also immer die kürzeste, hier die langsame Leitung verwendet, was nicht erwünscht ist.

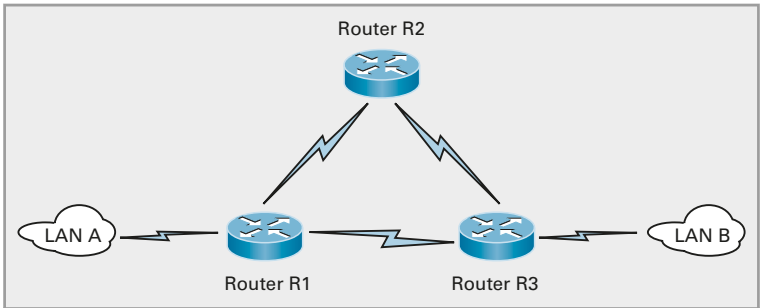


Bild 7.10: Routingschleife

Aus diesem Grund sind reine Distance-Vector-Protokolle in größeren Netzen nicht mehr üblich. Sie kommen nur noch im LAN zum Einsatz. Komplexere Routingprotokolle berücksichtigen andere Metrics der Leitungen, wie beispielsweise die Kosten von Leitungen, deren Bandbreite und die momentane Auslastung. Man nennt diese Protokolle Link-State-Protokolle, weil die Routenauswahl von dem Zustand des Links abhängig ist.

Beispiel 7.3: Link-State-Protokolle

- OSPF – Open Shortest Path First
- IS-IS – Intermediate System to Intermediate System

7.2.4 Routing-Tabellen

In Bild 7.11 werden 2 Netzwerke, links 10.0.18.0 und rechts 10.0.17.0 über ein drittes Netz in der Mitte 10.0.19.0 miteinander verbunden.

Jeder PC hat als Standard-Gateway die IP-Adresse seines Routers, also des Routers in seinem Netz, eingestellt.

Der linke Router erreicht das rechte Netz über seinen Port mit der Adresse 10.0.19.1. Die Entfernung zwischen den beiden Netzen beträgt 2 Hops.

Der Weltrekord liegt derzeit bei 420 km Streckenlänge ohne Repeater. Betrieben wird diese Strecke von der Deutschen Telekom und der France Télécom (siehe hierzu die Empfehlung ITU-T G.698.1).

8.9 DSL

***DSL** benutzt die Leitungen des Telefonnetzes.*

DSL steht für *Digital Subscriber Line*, zu deutsch: Digitale Teilnehmerleitung. Im eigentlichen Sinne ist damit jeder digitale Telefonanschluss gemeint, also auch ein ISDN-Telefonanschluss. Im engeren Sinne versteht man unter DSL heute nur noch den breitbandigen Internetanschluss über die Telefonleitung.

Als das Internet in Privathaushalte Einzug hielt, musste man sich Gedanken machen, wie man die immer größer werdende Datenflut bis zum Endteilnehmer transportieren kann. Neue breitbandige Leitungen zu verlegen, schied aus Kostengründen aus. Man suchte nach einer Lösung, die die bestehenden Leitungen nutzen konnte. Da jeder Haushalt einen Stromanschluss und einen Telefonanschluss hat, machte man sich Gedanken, die Daten auf einem dieser Netze zu übertragen. Das Telefonnetz ist für ein Übertragungsspektrum der menschlichen Sprache von 300 Hz bis 3400 Hz ausgelegt. Das Energieversorgungsnetz ist überhaupt nicht für höherfrequente Signale ausgelegt.

Die ersten DSL-Modems wurden Ende der 1980er Jahre in den USA entwickelt. Sie benutzten die herkömmlichen Telefonleitungen, mussten aber die Grenze von 3400 Hz ganz deutlich überspringen, um höhere Datenübertragungsraten zu erreichen, als es bis dahin mit der Analogtechnik möglich war.

8.9.1 ADSL

***ADSL**: Asymmetic DSL, Downloadbandbreite ist größer als Upload-Bandbreite.*

ADSL steht für *asymmetric* DSL. Der Name sagt aus, dass die Kanäle für Upload (vom Teilnehmer zum Netz hin) und Download (vom Netz zum Teilnehmer hin) ungleich, also unsymmetrisch verteilt sind. Da in den meisten Fällen wenig Daten von einem PC ins Netz geschickt werden, aber große Datenmengen vom Netz auf einen PC oder ein Heimnetz, sind entsprechend viele DSL-Kanäle für den Download und nur wenige für den Upload vorgesehen.

In dem Fall, dass man selbst Daten im Internet anbieten möchte, benötigt man oftmals eine größere Upload-Bandbreite. Hierfür wird SDSL, das symmetrische DSL benutzt. Bei SDSL sind Upload- und Download-Bandbreiten gleich groß.

Eine Eigenheit in Deutschland ist in Bild 8.56 zu erkennen: Die ersten DSL-Kanäle sind ungenutzt, da hier die Signale des Telefons übertragen werden. Es werden nur die Kanäle oberhalb des ISDN-Frequenzbereiches genutzt – auch wenn nur ein Analogtelefon angeschlossen ist.

Höhere Übertragungsfrequenzen werden stärker gedämpft als niedere Frequenzen. Bei höheren Frequenzen steigt das Übersprechen von einer Leitung zur anderen. Dies wird im oberen Teil des Bildes deutlich. Es wird der gemessene Signal-Rauschabstand einer DSL-Leitung dargestellt. Diese Grafik ändert sich im Laufe des Tages. Gibt es tagsüber wenig Störungen von benachbarten Leitungen, so kann sich dies am Abend ändern, wenn viele andere Menschen das Internet nutzen.

Man kann auch leicht erkennen, dass die spektrale Effizienz mit steigender Frequenz abnimmt (untere Hälfte des Bildes).

Auf Kanal 96 ist ein Pilotton zu sehen: Dies ist ein Signal mit definiertem Sendepegel. Der Empfänger misst den Empfangspegel dieses Tones und kann daraus die Leitungsdämpfung berechnen. Der Kanal des Pilottones kann nicht zur Datenübertragung verwendet werden.

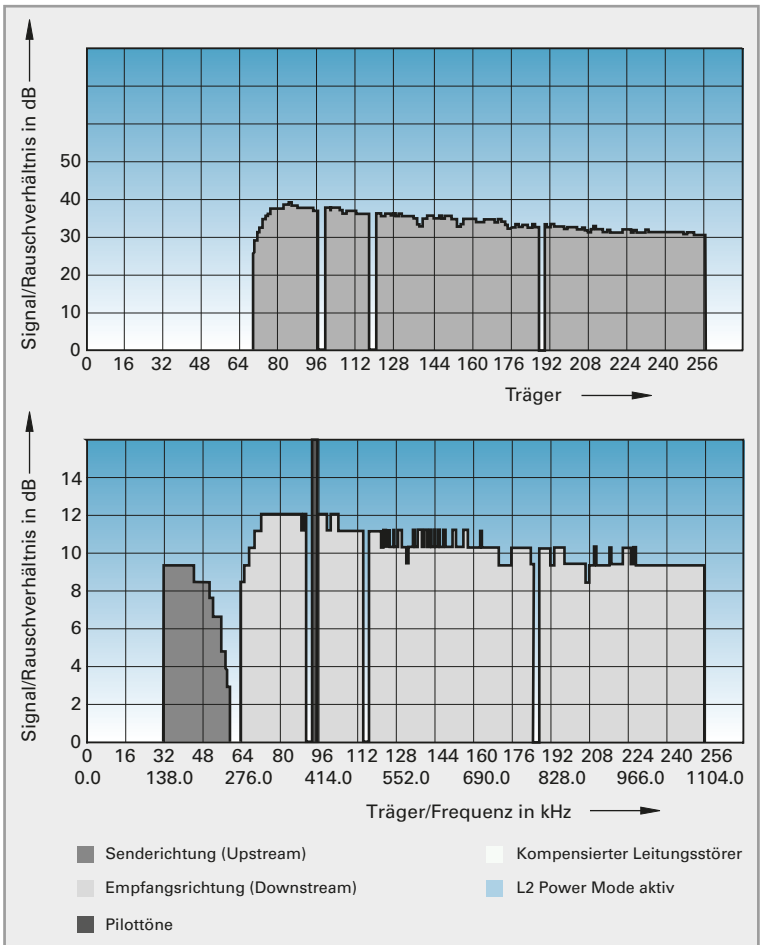


Bild 8.56: DSL-Spektrum

Bild 8.57 zeigt den Anschluss eines DSL-Routers. Die vom Telefonnetzbetreiber ankommende Leitung endet im Haus an der sogenannten Netzübergabedose. An diese Dose wird der Splitter angeschlossen. Der Splitter ist eine Frequenzweiche mit 2 Anschlüssen. Der niederfrequente Anschluss ist für den Anschluss der Telefone oder einer Telekommunikationsanlage (TK-Anlage) vorgesehen. Der hochfrequente Anschluss überträgt die Frequenzen oberhalb des Telefoniebereiches. Hier wird das DSL-Modem angeschlossen.

Am DSL-Modem wird ein Router angeschlossen. Dieser verbindet nun das DSL-seitige Internet mit dem lokalen Netzwerk. Der interne An-

schluss ist ein Ethernet-LAN-Anschluss. Hier wird ein Ethernet-Switch angeschlossen.

Meist sind Modem, Router und Switch in einem Gerät zusammengefasst. Oft ist in diesem Gerät auch eine WLAN-Einheit mit untergebracht.

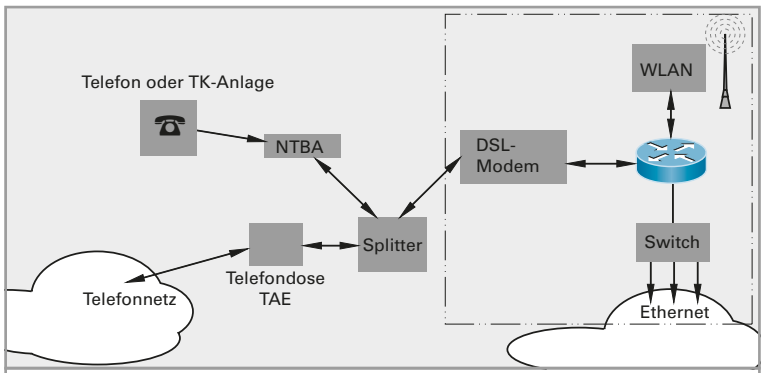


Bild 8.57: Anschluss eines DSL-Routers

8.9.2 DSL in der Gegenwart

Man benutzt das Frequenzmultiplexverfahren (siehe Kapitel 1.8.3) und überträgt auf vielen einzelnen Frequenzkanälen separate Datenströme. Jeder Frequenzkanal stellt eine eigene Schnittstelle dar. Man nutzt beim herkömmlichen DSL Übertragungsfrequenzen bis 1,1 MHz und teilt den gesamten Frequenzbereich von 0 Hz bis 1,1 MHz in 256 separate Frequenzkanäle ein.

Jeder Datenkanal hat eine Bandbreite von 4 kHz. Der Abstand zwischen den Kanälen beträgt 4,3125 kHz. Durch entsprechend aufwendige Signalcodierung lassen sich im Idealfall 15 bit/Hz übertragen. Es kommt dabei eine 2^{15}-QAM, also ein Quadraturamplitudenmodulation mit 2^{15} = 32 k Werten zum Einsatz. Die maximale Datenübertragungsrate ist somit pro Einzelkanal 4 kHz · 15 bit pro Sekunde pro Hertz = 60 kbit pro Sekunde (Bild 8.58). Wenn alle Kanäle zur Verfügung stehen, beträgt die maximale Datenübertragungsrate beim normalen DSL etwa 15 Mbit pro Sekunde.

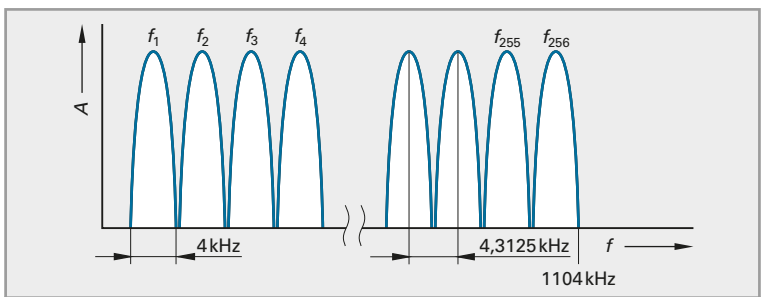


Bild 8.58: DSL-Spektrum

ADSL2+ nutzt Frequenzen bis 2,2 MHz und 512 Frequenzkanäle. Damit sind dann theoretisch 30 Mbit/s erreichbar.

VDSL2 basiert auf derselben Technik wie ADSL2+. Dabei werden Frequenzen bis zu 30 MHz benutzt. Upstream und Downstream werden über den Frequenzbereich verteilt, um Störungen zu verhindern (Bild 8.59).

Mehrere VDSL-Profile wurden definiert: Ein Profil beschreibt die maximale Übertragungsfrequenz, die Anzahl der Frequenzkanäle, die Bandbreite jedes Kanals und die Sendeleistung, mit der ein DSL-Modem sendet. In der Tabelle 8.8 sind die aktuellen Profile und die damit erreichbaren Übertragungsraten aufgelistet.

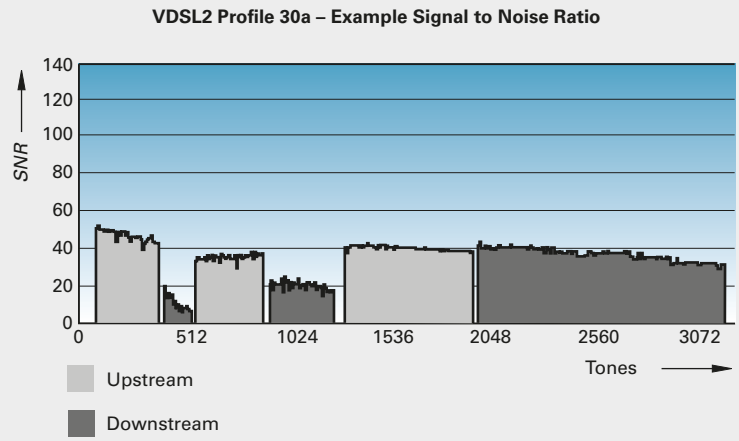


Bild 8.59: DSL-Spektrum, man erkennt die verschiedenen Up- und Downlink-Bereiche

Tabelle 8.8: VDSL-Profile

Profil	Bandbreite	Frequenz-kanäle	Kanal-abstand	Pegel	Übertra-gungsrate *C*
8a	8,832 MHz	2047	4,3125 kHz	+17,5 dBm	50 Mbit/s
8b	8,832 MHz	2047	4,3125 kHz	+20,5 dBm	50 Mbit/s
8c	8,5 MHz	1971	4,3125 kHz	+11,5 dBm	50 Mbit/s
8d	8,832 MHz	2047	4,3125 kHz	+14,5 dBm	50 Mbit/s
12a	12 MHz	2782	4,3125 kHz	+14,5 dBm	68 Mbit/s
12b	12 MHz	2782	4,3125 kHz	+14,5 dBm	68 Mbit/s
17a	17,664 MHz	4095	4,3125 kHz	+14,5 dBm	100 Mbit/s
30a	30 MHz	3478	8,6250 kHz	+14,5 dBm	200 Mbit/s

Da bei hohen Frequenzen die Signaldämpfung sehr groß wird, sind damit die Leitungslängen (Entfernungen) relativ gering. Da die Kunden nicht näher an die Vermittlungsstellen gebracht werden können, werden Anlagenteile der Vermittlungsstelle näher zum Kunden gebracht. Die DSL-Access-Multiplexer (**DSLAM**), das Gegenstück des DSL-Modems beim Kunden, werden in die Wohn- und Industriegebiete verlegt. Diese abgesetzten DSLAMs werden meist als Aufsatz auf die bestehenden Kabelverzweiger montiert. Sie werden von der Vermittlungsstelle über schnelle Glasfaserleitungen angeschlossen (Bild 8.60). Dadurch ver-

***DSLAM**: DSL Access Multiplexer*

ringert sich die Kupferleitung bis zum Kunden ganz wesentlich, sodass hier entsprechend hohe Frequenzen benutzt werden können.

Bild 8.60: Abgesetzter DSLAM in einem Wohngebiet

8.10 Drahtlose Netze, Wireless LANs

Drahtlose Netzwerke, Wireless LANs, verwenden anstelle von Leitungen hochfrequente Funkwellen. Da sich alle Stationen die Funkzelle teilen müssen, handelt es sich hierbei um eine logische Bustopologie, bei der jeder hören kann, was der andere sagt.

8.10.1 WLAN-Standards

Diese Technologie wurde von der IEEE-Arbeitsgruppe 802.11 festgelegt. In Europa ist der Standard 802.11b und 802.11g verbreitet. In Nordamerika wird außerdem der Standard 802.11a häufig eingesetzt. Seit Ende 2009 ist der Standard 802.1n genormt und ersetzt die vorherigen Standards (Tabelle 8.9).

Tabelle 8.9: WLAN-Standards

Norm	Jahr	Frequenz	Netto-Daten-durchsatz	Brutto-Daten-durchsatz	Reich-weite im Haus	Reich-weite Freifeld
802.11	1997	2,4 GHz	0,9 Mbit/s	2 Mbit/s	≈ 20 m	≈ 100 m
802.11a	1999	5 GHz	23 Mbit/s	54 Mbit/s	≈ 35 m	≈ 100 m
802.11b	1999	2,4 GHz	4,3 Mbit/s	11 Mbit/s	≈ 38 m	≈ 140 m
802.11g	2003	2,4 GHz	19 Mbit/s	54 Mbit/s	≈ 38 m	≈ 140 m
802.11n	2009	2,4/5 GHz	74 Mbit/s	600 Mbit/s	≈ 70 m	≈ 250 m
802.11ac	2013	5 GHz		1700 Mbit/s	≈ 35 m	≈ 100 m
802.11ad	2014	60 GHz	1000 Mbit/s	7000 Mbit/s	≈ 10 m	≈ 20 m

In diesen Standards werden Übertragungsraten bis 11 MBits pro Sekunde (802.11a und b) und 54 MBits pro Sekunde (802.11g) festgelegt. Der seit Anfang September 2009 verabschiedete Standard 802.11n erlaubt Bruttodatenraten bis 300 Mbps.

In Deutschland sind Sendeleistungen bis 100 mW erlaubt (entsprechend 20 dBm), in anderen Ländern zum Teil deutlich mehr. Der Standard 802.11a erlaubt sogar bis zu 1 Watt Sendeleistung.

Der zur Verfügung stehende Frequenzbereich wird in Europa in 13 Kanäle aufgeteilt, die sich teilweise überlappen (Bild 8.61). Nur drei Kanäle sind überlappungsfrei (Kanäle 1, 7 und 13). In USA werden 11 Kanäle verwendet, von denen drei überlappungsfrei sind (Kanäle 1, 6 und 11). Siehe auch Kapitel 1.8.3 „Frequenzmultiplex".

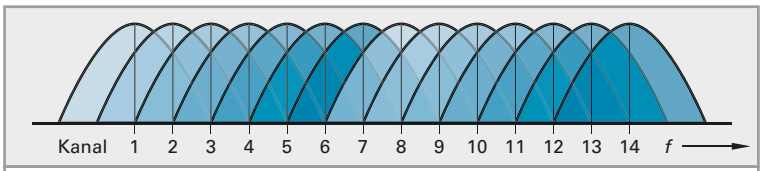


Bild 8.61: WLAN-Kanalüberlappung

In Europa werden die Kanäle 1 bis 13 benutzt. In USA werden nur die Kanäle 1 bis 11 benutzt. Japan benutzt noch einen weiteren Kanal, den Kanal 14.

Tabelle 8.10: Frequenzkanäle und Frequenzen bei WLAN 802.11b und 802.11g

Kanal	Mittenfrequenz
1	2,412 GHz
2	2,417 GHz
3	2,422 GHz
4	2,427 GHz
5	2,432 GHz
6	2,437 GHz
7	2,442 GHz
8	2,447 GHz
9	2,452 GHz
10	2,457 GHz
11	2,462 GHz
12	2,467 GHz
13	2,472 GHz
14	2,484 GHz

Vorsicht ist bei den Kanälen 9 und 10 geboten. Diese Kanäle werden gelegentlich durch eine Störquelle gestört, die man nicht unbedingt als solche vermutet: **Mikrowellenherde** benutzen die Frequenz 2,455 GHz! Ein defekter Herd kann die Kommunikation im WLAN empfindlich stören. Da diese Herde Sendeleistungen von mehreren hundert Watt haben, können sie auch über große Entfernungen noch stören.

Mikrowellenherde *senden auf derselben Frequenz wie WLAN.*

Die Standards 802.11b und 802.11g arbeiten im 2,4 GHz-Bereich, 802.11a arbeitet im 5 GHz-Bereich. Das 2,4 GHz-Band ist als ISM-Band (*Industrial Scientific Medical*) weltweit lizenz- und genehmigungsfrei (Tabelle 8.10). Es reicht von 2,4 GHz bis 2,4835 GHz. Der neue Standard 11n kann sowohl im 2,4-GHz- als auch im 5-GHz-Band arbeiten.

Der 5-GHz-Bereich wurde von den zuständigen Behörden in Europa aber teilweise schon für ähnliche Dienste freigegeben, sodass Geräte nach 802.11a in Europa nicht ohne Weiteres betrieben werden können.

802.11n ist derzeit Stand der Technik.

Der Nachfolger von 802.11n wird der Standard 802.11ad werden, an dem bereits seit der Verabschiedung des n-Standards entwickelt wird.

802.11ad ist der kommende WLAN-Standard.

Die WiGig (*Wireless Gigabit Alliance*) arbeitet mit der Wi-Fi-Alliance zusammen. Daher ist zu erwarten, dass der neue Standard kompatibel mit den bisherigen WLAN-Standards sein wird. Dieser Standard bringt Gigabit-Geschwindigkeit auch ins WLAN. Datenübertragungsraten von über einem Gigabit pro Sekunde sind damit machbar. Die maximale Bruttodatenrate wird bei 7 Gbps liegen. Die Trägerfrequenz beträgt 60 GHz.

Auch bei Funk gilt: Je höher die Frequenz, desto größer die Dämpfung! Bei gleicher Sendeleistung ist die Reichweite im 5 GHz-Bereich geringer als im 2,5 GHz-Bereich. Die geringste Reichweite erreicht deshalb man mit dem neusten 60 GHz-WLAN.

8.10.2 WLAN-Betriebsarten

Es gibt 3 Betriebsarten für WLANs:

- Ad-Hoc-Mode
- Infrastructure-Mode
- Wireless-Distribution-System WDS

Ad-hoc-Mode

Ad hoc: *sofort, jeder Rechner bildet eine Funkzelle.*

Der **Ad-hoc**-Mode ist für das schnelle und unkomplizierte Aufbauen von Sofortverbindungen zwischen mehreren Rechnern. Keine Station ist dabei privilegiert, alle Stationen sind gleichberechtigt.

Dazu muss jeder Rechner, der Mitglied eines solchen Ad-hoc-Netzes werden möchte, die Kennung des Netzes haben. Diese Kennung ist die SSID, die „Service Set Identifier". Jeder Rechner mit derselben SSID gehört zu diesem Netzwerk.

Infrastructure-Mode

Infrastructure-Mode: *ein oder mehrere Accesspoints zur Kommunikation.*

Im **Infrastructure-Mode** steht ein WLAN-Accesspoint in der Mitte des Funknetzes. Jeder Rechner muss sich mit diesem Accesspoint verbinden, wenn er in dieses Netzwerk möchte. Der Accesspoint sendet regelmäßig eine Kennung aus, im Normalfall zweimal pro Sekunde. Diese Kennung, man nennt sie Beacon, enthält die SSID des Funknetzes, die Datenübertragungsrate und die Art der Verschlüsselung.

WLANs immer mit Passwort oder -satz versehen!

Wenn sich ein Rechner mit einem Accesspoint (AP) verbindet, dann muss er sich am AP authentifizieren. Es empfiehlt sich, am AP ein möglichst kompliziertes Passwort zu hinterlegen, welches dann am PC oder Laptop eingegeben werden muss. Am besten sind hier Passsätze, da sie leichter als Passwörter zu merken und somit schwerer zu knacken sind.

Aus Gründen des Abhörens muss die Datenübertragung verschlüsselt erfolgen. Ursprünglich wollte man mit einem Verschlüsselungsverfahren dieselbe Abhör-Sicherheit herstellen wie bei verkabelten Netzen. Das hierzu entwickelte Protokoll WEP (*Wired Equivalent Privacy*) hält aber nicht, was es verspricht. Heute gilt das WPA2-Verschlüsselungsverfahren als sicher. Da Funkwellen von jedem, der sich im Bereich der Funkzelle aufhält, empfangen werden können, ist hier allergrößte Vorsicht geboten.