Bibliothek des technischen Wissens

Fachwissen Netzwerktechnik

Modelle · Geräte · Protokolle

Bernhard J. Hauser

4. 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

Bildentwürfe: Der Autor

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

Fotos:
siehe hintere Umschlaginnenseite

4. Auflage 2022

Druck 5 4 3 2 1

Alle Drucke derselben Auflage sind parallel einsetzbar, da sie bis auf die Korrektur von Druckfehlern identisch sind.

ISBN 978-3-8085-5406-7

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

© 2022 by Verlag Europa-Lehrmittel, Nourney, Vollmer GmbH & Co. KG, 42781 Haan-Gruiten

www.europa-Lehrmittel.de

Satz: Wissenschaftliche PublikationsTechnik Kernstock, 73230 Kirchheim unter Teck
Umschlaggestaltung: braunwerbeagentur, 42477 Radevormwald, und Grafik & Sound, Köln
Druck: LD Medienhaus GmbH & Co. KG, 44149 Dortmund

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 **Studierende 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 Virtualisierung
- 9 Cloud-Computing
- 10 Security und Verschlüsselungstechnik
- 11 Netzwerktechnik
- 12 Übertragungstechnik

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 die 3. Auflage aufgenommen. In diese 4. Auflage wurden Themen aufgenommen, die seit einiger Zeit dabei sind, die IT komplett umzukrempeln. Dies sind die Themen Virtualisierung, Cloud-Computing und Security, an denen kein Netzwerker mehr vorbeikommt. Diese Änderungen in der IT schlagen sich auch in den Lehrplänen nieder, die bspw. bei den IT-Berufen 2020 überarbeitet wurden. Diesen Neuerungen wird in dieser Auflage Rechnung getragen.

In der EUROPATHEK (siehe vordere Umschlaginnenseite) stehen eine Reihe von digitalen Zusatzmaterialien zur Verfügung: Informationen zu Normen und Normungsgremien, die Lösungen zu den Übungsaufgaben aus diesem Buch sowie Formeln und Tabellen.

Passend zu diesem Lehrbuch ist auch ein Aufgabenheft mit Übungsaufgaben zum Vertiefen des Lehrstoffes erhältlich (Europa-Nr. 54111). Der Verweis auf die Übungsaufgaben im Aufgabenheft ist anhand des Icons erkennbar.

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.

Sommer 2022 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).

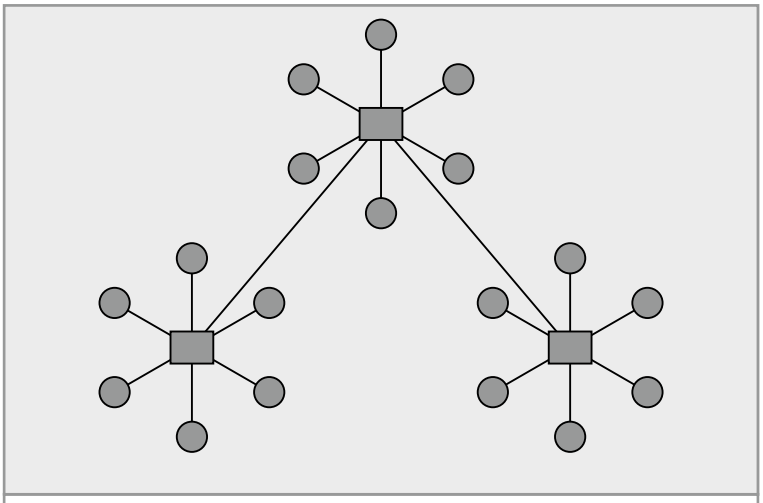


Bild 2.6: Erweiterter Stern

***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

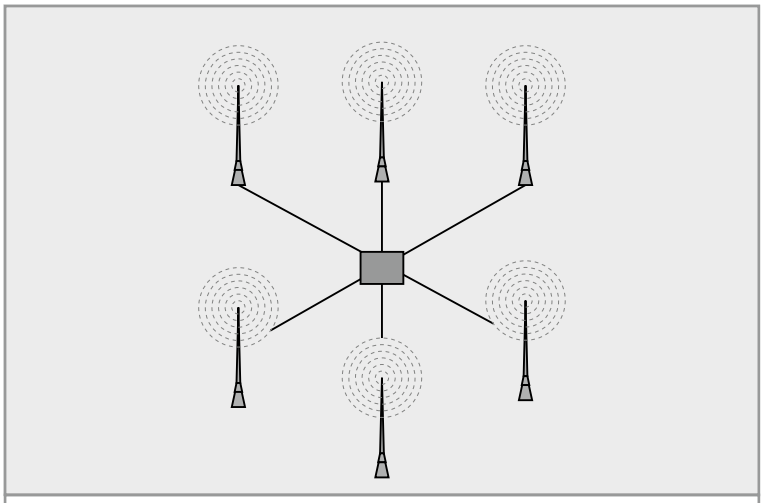


Bild 2.7: Stern-Zell-Netz

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

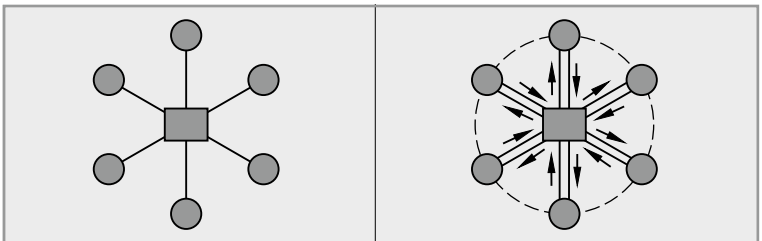
Logische und physikalische Topologien

Logische Topologie: *Wie ist der Datenfluss?*

Physikalische Topologie: *Wie ist die Leitungsführung?*

Bei der Beschreibung der Topologie muss man zwischen der **logischen** und der **physikalischen Topologie** unterscheiden (Bild 2.8). 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.

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).

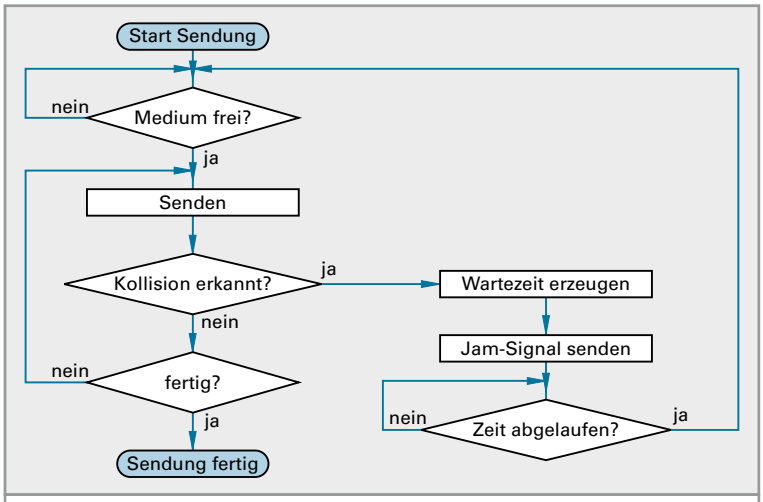


Bild 2.9: Prinzipieller Ablauf des CSMA/CD-Verfahrens

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.

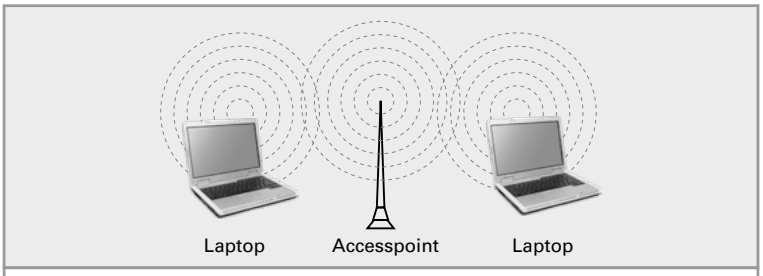


Bild 2.10: Laptops und Accesspoint

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 Telegrammformular 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 dienstneutrale 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).

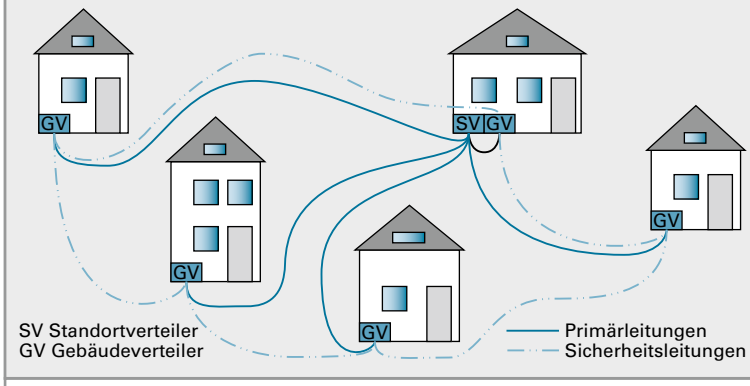


Bild 2.11: Primärverkabelung, Standortverkabelung

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).

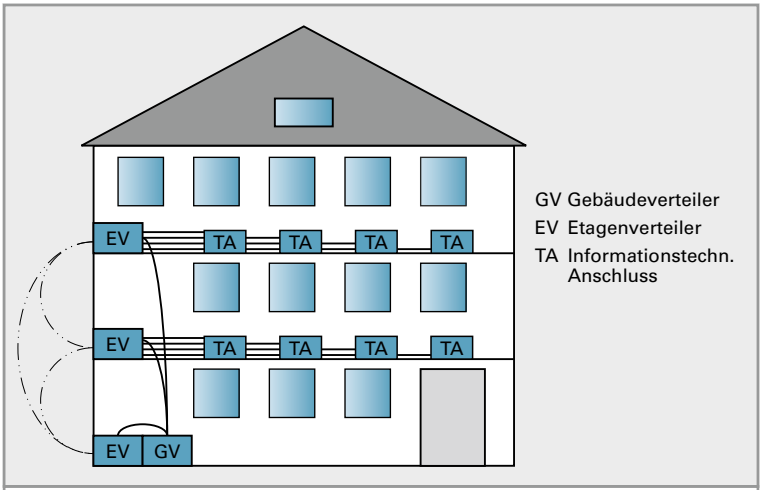


Bild 2.12: Sekundär- und Tertiärverkabelung im Gebäude und auf der Etage

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).

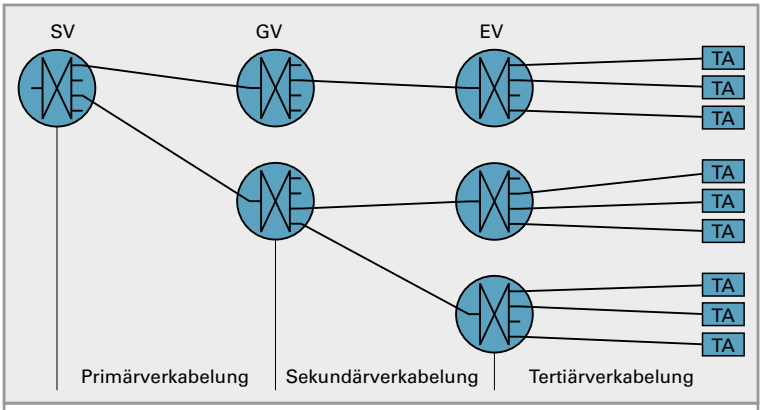


Bild 2.13: Strukturierte Verkabelung – Erweiterter Stern

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 Querverbindungen werden von den Switches bei Bedarf automatisch aktiviert.

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.

Querverbindungen bilden Maschen.

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

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. Ein Unternehmen 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.

Der Einsatzbereich entscheidet, welche Leitungen eingesetzt werden.

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.

Die Kategorie beschreibt die Leistungsfähigkeit der Leitung.

Bild 2.14: Verteilerschrank

Beschriftung von TAs und Verteilerschränken

Dokumentation und Beschriftung ist notwendig und hilfreich.

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.

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.

Jeder Switchport bildet eine Kollisionsdomäne.

Heutzutage werden weder Repeater noch Hubs oder Bridges eingesetzt. Es kommen in LANs ausschließlich Switches zum Einsatz. Ein Switch verfügt genauso wie die Bridge über eine Bridging-Table, in der die Zuweisung von MAC-Adresse zum Switchport vermerkt wird.

***Twisted Pair:** verdrilltes Adernpaar*

Switches benötigen **Twisted-Pair**-Leitungen. Switches mit Koaxialleitungen gibt es nicht. Mit dieser Technik ist eine Vollduplex-Übertragung möglich. Bei einer 100 Mbps-Verkabelung hat man somit 100 Megabits pro Sekunde in Sende- und ebensoviel in Empfangsrichtung, zusammen also 200 MBit/s. Schließt man an jeden Switchport nur eine Station an, dann spricht man von einem „**vollgeswitchten Netz**“ (Bild 4.15). Da die Station mit keiner anderen die Leitung teilen muss, ist ein solches Netz völlig kollisionsfrei! Man spricht in diesem Fall auch von Mikrosegmentierung! Dies ist heute der Normalzustand, alle neueren Netze sind mikrosegmentiert.

*Ein **vollgeswitchtes Netz** ist kollisionsfrei.*

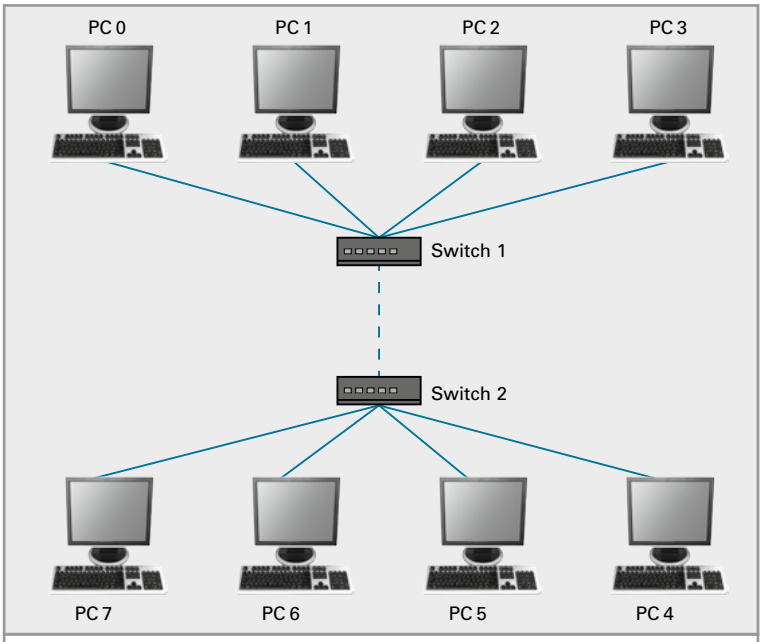


Bild 4.15: Geswitchtes Netz

Fazit:

Ein Switch teilt ein Netzwerk in kleinere Kollisionsdomänen auf. Broadcastdomänen werden nicht aufgeteilt. Ein Switch wertet MAC-Adressen aus und arbeitet daher auf Layer 2. Ein Switch verbindet Netzwerksegmente.

4.2.3 Router

Router arbeiten auf Layer 3.

Um große Netzwerke zu unterteilen, muss man sie in einzelne Netzwerke, nicht nur in Segmente, zerlegen.

Diese Aufgabe übernimmt der Router (Bild 4.16). Er wertet die Netzwerkadresse aus (Layer 3) und leitet nur diese Pakete weiter, die in ein bestimmtes Netzwerk gehören. Broadcasts werden nicht weitergeleitet.

Router, die verschiedene Netzwerkprotokolle beherrschen, wie z. B. IPX/SPX und TCP/IP, nennt man Multiprotokollrouter.

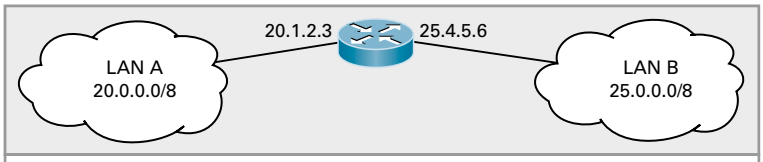


Bild 4.16: Ein Router verbindet unabhängige Netze

Fazit:

Jeder Routerport bildet eine Broadcastdomäne.

Ein Router teilt ein großes Netzwerk in kleinere Netzwerke auf. Oder er verbindet verschiedene Netze miteinander. Jeder Routeranschluss bildet eine Kollisionsdomäne und eine Broadcastdomäne. Ein Router wertet Netzwerk-Adressen (z. B. IP-Adressen) aus und arbeitet daher auf Layer 3 (Bild 4.17).

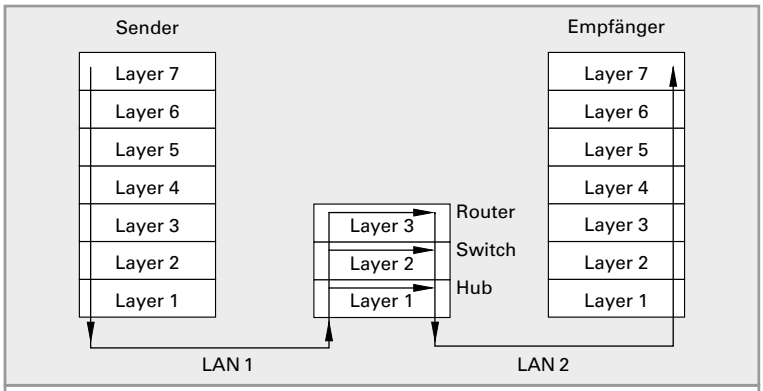


Bild 4.17: Router arbeiten auf Layer 3

Router arbeiten auf Layer 3 und werten Netzwerkadressen aus. Switches arbeiten auf Layer 2 und werten MAC-Adressen aus. Hubs arbeiten ohne Adressauswertung auf Layer 1.

4.2.4 Gateway

Netzwerkgeräte, die auf allen Schichten des OSI-Modells arbeiten, nennt man Gateways. Gateways bilden oft die Übergänge von einer Technologie zu einer anderen, beispielsweise von der IP-Telefonie über ein LAN zu einer älteren Telefonanlage oder ins Telefonnetz.

4.3 Firewall

Eine Firewall, zu deutsch etwa „Brandschutzmauer“, ist ein Netzwerkgerät, welches das LAN gegen Angriffe und Schadsoftware schützt. Oft ist die Firewall in den Router zum Internet eingebaut (siehe hierzu auch Kapitel 10.3 „Schutz durch Firewall und DMZ“).

Es werden grundsätzlich 2 Arten von Firewall unterschieden:

- Paket-Filter
- Content-Filter

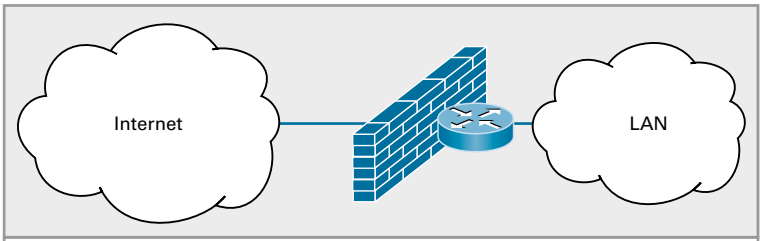


Bild 4.18: Firewall schützt das LAN

*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.

Weitere Firewallsysteme sind verfügbar: Zum Schutz von Webanwendungen (auf OSI-Schicht 7, mit HTTP, XML, ...) wird eine spezielle **Web Application Firewall**, **WAF**, eingesetzt. Sie schützt Webanwendungen gegen Angriffe wie SQL-Injection oder Session Hijacking.

***WAF** schützt Webserver und Webanwendungen*

Spezielle Firewalls sind in der Lage Angriffe und Eindringlinge zu erkennen und das Eindringen zu verhindern. Ein **Intruder Detection System**, **IDS**, erkennt Eindringlinge bzw. Eindring-Versuche. Ein **Intruder Prevention System**, **IPS**, ist in der Lage Eindringlinge abzuwehren.

***Intruder** (Eindringlinge) werden mit **IDS** erkannt, mit **IPS** verhindert*

Neuere Firewalls sind in der Lage den Datenverkehr zu untersuchen und darauf zu reagieren. Sie beinhalten heute meist ein IDS oder ein IPS. Darüber hinaus sind sie in der Lage Malware (wie Viren, Spam, ...) im Datenfluss zu erkennen und zu blockieren. Oft haben solche Firewalls auch VPN-Gateways zum Anbinden von Heimarbeitsplätzen u.ä. und Proxy-Speicher für das Zwischenspeichern von Webseiten integriert. Eine solche Firewall nennt man **Next Generation Firewall**, **NGFW**.

***Next Generation FW** kombiniert viele Firewall-Funktionen*

4.4 DMZ – Demilitarisierte Zone

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

Zweistufige DMZ

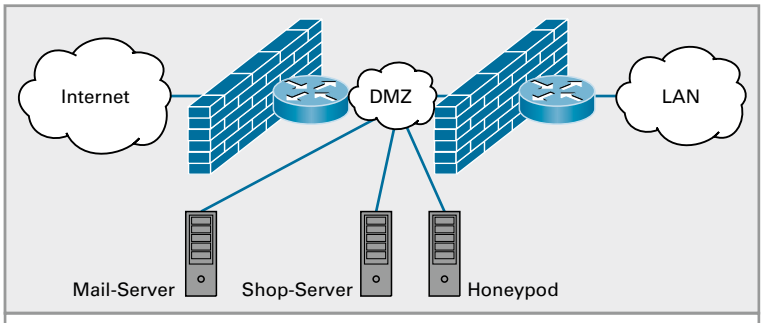


Bild 4.19: Zweistufige DMZ

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 dem lokalen Netzwerk (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 Hacker-

angriffe darstellen, aber keine Daten von Nutzen beherbergen. Dadurch werden mögliche Angreifer auf eine falsche Fährte gelockt.

Einstufige DMZ

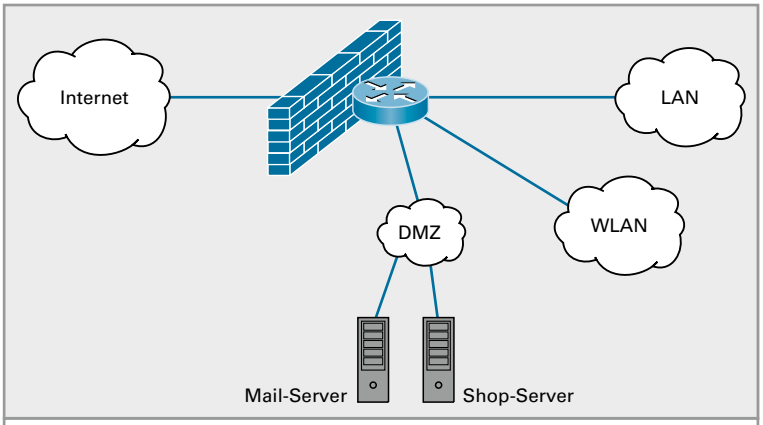


Bild 4.20: Einstufige DMZ

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 den Betrieb 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.

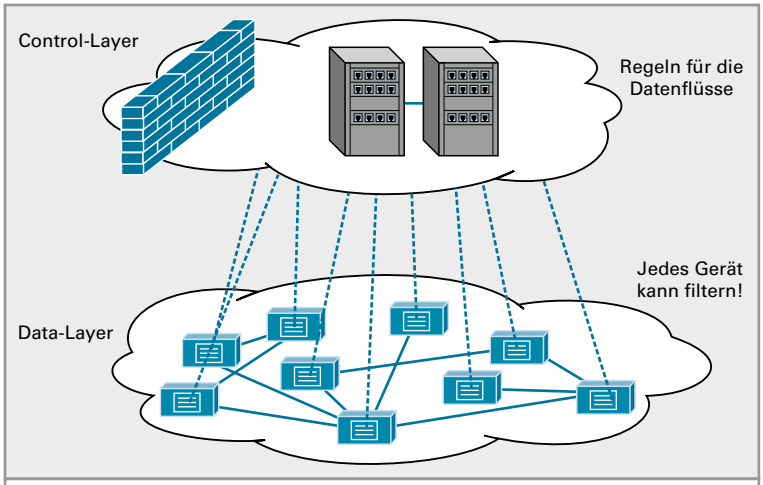


Bild 4.21: Netz mit SDN-Switches

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 4.22)?

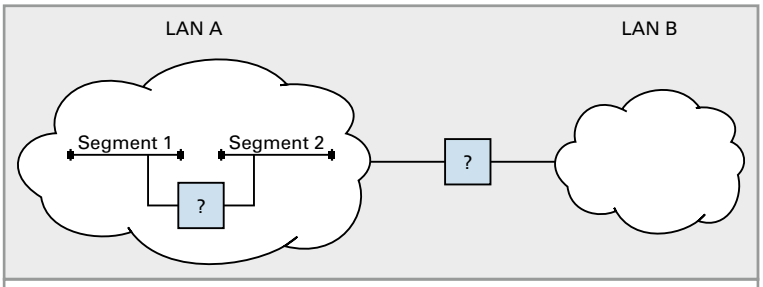


Bild 4.22: Netzwerkgeräte

Aufgabe 1

Übungsaufgabe Nr. 3

Bearbeiten Sie Aufgabe 1 im Arbeitsheft. Ordnen Sie die Schichten des ISO/OSI-Schichtenmodells und des TCP/IP-Modells Geräten und Aufgaben zu.

Aufgabe 2

Übungsaufgabe Nr. 4

In Aufgabe 2 im Arbeitsheft vertiefen und überprüfen Sie Ihr Wissen über Protokolle und Netzwerkgeräte.

Die Lösung sieht ganz einfach aus:

Querverbindungen werden zwar gesteckt, die Switchports werden allerdings nicht aktiviert. Fällt nun eine aktive Leitung aus, so muss nur die Querverbindung aktiviert werden, und der Betrieb kann weiter gehen.

Dieses Auftrennen von Schleifen durch Deaktivieren von gesteckten Leitungen, sowie das Aktivieren von Leitungen im Fehlerfall, muss der Switch selbständig übernehmen.

Spanning tree, Spanning tree protocol, STP (auch Spannbaum oder gespannter Baum) ist nun eine Methode in der Netzwerktechnik, um redundante geswitchte Netzwerke aufzubauen. Dabei wird jegliche Topologie auf eine einzige Baumstruktur reduziert, die in der Rootbridge (Wurzelbrücke) ihren Ursprung hat.

Jeder Switch ist durch seine **BID (Bridge-Identification)** eindeutig gekennzeichnet. Diese BID besteht aus 8 Byte, wobei die ersten, höchstwertigen Bytes eine vom Admin einstellbare Priorität sind. Die restlichen 6 Bytes ergeben sich aus der MAC-Adresse des Switches. Somit ist gewährleistet, dass jeder Switch eine eindeutige Kennung und somit auch eine eindeutige Priorität hat.

Tabelle 7.1: BID

Priority	MAC-Adresse
2 Byte	6 Byte

Die niedrigste **BID** hat die höchste Priorität. Root-Bridge wird der Switch mit der höchsten Priorität. Alle anderen Switches suchen sich nun den bestmöglichen Pfad zur Rootbridge. Diese Verbindungen werden aktiviert, die restlichen deaktiviert.

*Je kleiner die **BID**-Nummer, desto höher die Priorität.*

Bei mehreren Verbindungen eines Switches zur Root-Bridge hin, die dieselben Pfadkosten aufweisen, wird der Port mit der höchsten Priorität aktiviert. Dies ist der Port mit der kleinsten Portnummer.

Um den bestmöglichen Pfad zur Rootbridge zu finden, muss die Beschaffenheit der Verbindung mit berücksichtigt werden. Als Entscheidungskriterium werden hier „Pfadkosten" definiert (dies sind keine wirklichen Kosten). Eine schnelle Verbindung ist einer langsamen Verbindung vorzuziehen. Also definiert man für die langsame Verbindung hohe Pfadkosten, für die schnelle Verbindung geringe Pfadkosten. Als Pfadkosten können vom Administrator Werte von 1 bis 65536 eingestellt werden.

Der Pfad mit den geringsten Kosten ist der beste.

Anforderungen an den Spanning Tree Algorithmus:

- Automatisches Rekonfigurieren der Baumstruktur bei Änderungen an der Topologie (bei manuellen Änderungen oder bei auftretenden Fehlern)
- Möglichst geringe Netzlast durch das eigentliche Einrichten der Baumstruktur
- Stabilisierung der Netzstruktur unabhängig von der Netzgröße
- Stabilisierung innerhalb einer bekannten (kurzen) Zeit
- Vorbestimmte, reproduzierbare Netzstruktur, die durch den Netzwerkadmin vorgegeben wird

*Die **Pfadkosten** können selbst frei definiert werden und von der IEEE-Empfehlung abweichen.*

Tabelle 7.2: Empfohlene Pfadkosten (nach IEEE), abhängig von der Übertragungskapazität

Übertragungskapazität	empfohlene Pfadkosten	empfohlener Bereich
10 MB/s	100	50 ... 600
100 MB/s	19	10 ... 100
1000 MB/s	4	2 ... 10
10 GB/s	2	1 ... 4

Der Rootpath (Wurzelpfad) ist der Pfad von einem Switch zur Rootbridge, der die geringsten Gesamtkosten aufweist (Summe aller Einzelpfade). Jeder Switch darf nur einen Pfad zur Rootbridge haben.

Die kleinste Bridge-ID hat die höchste Priorität!

Die kleinste Port-ID hat die höchste Priorität!

Bei mehreren Pfaden mit denselben Root-Pfadkosten wird die Priorität der Switchports interessant. Je kleiner die Switch-Port-Nummer (Anschlussnummer am Switch), desto höher die Priorität. Steckt also eine Leitung auf Port 2 und eine andere auf Port 5 und beide haben gleich hohe Wurzelpfadkosten, dann wird Port 2 der Rootport und Port 5 wird deaktiviert.

Bridge Protocol Data Unit

Die Switches müssen Daten über ihren eigenen Zustand und ihre ID austauschen. Dies geschieht mit PDPUs, Bridge Protocol Data Units.

Die Rootbridge teilt den untergeordneten Switches alle 2 Sekunden mit, dass sie noch vorhanden ist. Die untergeordneten Switches geben diese Meldungen weiter. Beim Ausbleiben dieser „Hallo-Pakete“ hat sich offensichtlich das Netzwerk verändert und muss neu organisiert werden. Die Reorganisation läuft genau so ab wie die Neuorganisation beim Einschalten eines Netzwerkes. Die Reorganisation kann bis zu 30 Sekunden dauern.

Ablauf der Netz-Organisation

1. Einschalten der Switches, alle Switchports sind im „Blocked-Mode“, d. h., es werden keine Datenpakete weitergeleitet außer den Switch-Informationen (BPDUs).
2. Jeder Switch sendet Informationen über seine ID an alle Anschlüsse. Der Switch mit der kleinsten ID wird Root-Bridge.
3. Nachdem die Root-Bridge ermittelt wurde, bestimmt jeder Switch seinen Root-Port. Das ist der Port, der mit den geringsten Kosten zur Rootbridge führt. Bei gleichen Kosten für mehrere Ports, wird der Port mit der kleinsten Port-Nummer der Root-Port. Die anderen Ports, die Wege zur Rootbridge haben, werden deaktiviert (Designated Ports).
4. Danach werden die Switchports in den „Learning-Modus“ gesetzt und die Bridging-Tabellen angelegt.
5. Nach Aufbau der Bridging-Tabellen schalten die Switches ihre Ports in den „Forwarding-Modus“ und transportieren fortan ankommende Datenpakete an die richtigen Ports weiter.

Vorsicht! Eine Verbindung an einem einzigen Switch von einem Switchport zu einem anderen verursacht auch einen Broadcaststurm! Einfache Switches können keine STP und können somit diese Schleife auch nicht auftrennen.

7.1.5 Virtuelle LANs, VLANs

In einem Großraumbüro befinden sich Mitarbeiter unterschiedlicher Abteilungen. Alle Arbeitsplätze sind miteinander vernetzt und „hängen" auf einem Etagenswitch. Aus Sicherheitsgründen sollten aber die Rechner der verschiedenen Abteilungen jeweils in getrennten Netzen stehen, nämlich jeweils auf eigener Netzwerk-Hardware.

Ein weiteres Problem ist, dass Broadcast-Messages das Netz sehr belasten. Je größer die Anzahl der Rechner, desto größer die Anzahl der Broadcasts.

Lösung: Der Etagenswitch wird in mehrere „logische Switches" aufgeteilt, die voneinander isoliert arbeiten.

Bild 7.6 zeigt das Aufteilen in 2 getrennte virtuelle Netze, ein Netz *Vertrieb* und ein Netz *Einkauf*. Beide Netze nutzen zwar dieselben Switches, sind aber logisch völlig voneinander isoliert.

Damit zwei Rechner, die in unterschiedlichen VLANs stehen, miteinander kommunizieren können, müssen die VLANs über einen Router verbunden werden!

Jedes VLAN bildet ein eigenes Netz. Jedes LAN bildet eine Broadcastdomäne. Broadcasts bleiben somit im eigenen VLAN und gelangen nicht in andere VLANs.

*Verbindungen zwischen Switches mit VLAN-TAGs werden „tagged" oder **„VLAN-Trunks" (VLTs)** genannt.*

Die Uplinks der einzelnen logischen Switches werden physikalisch zu einem Link zusammengefasst. Damit die Datenframes der einzelnen logischen virtuellen Netzwerke dem jeweiligen VLAN zugeordnet werden können, müssen die Frames modifiziert werden. Die Zugehörigkeit zum virtuellen Netzwerk muss zusätzlich im Frame transportiert werden.

Dazu wird ein VLAN-Tag eingebaut. Das VLAN-Tag ist 4 Byte groß und wird vor dem Typ-Feld im Ethernet-Frame eingefügt. Der Ethernetrahmen hat normalerweise eine maximale Größe von 1518 Bytes.

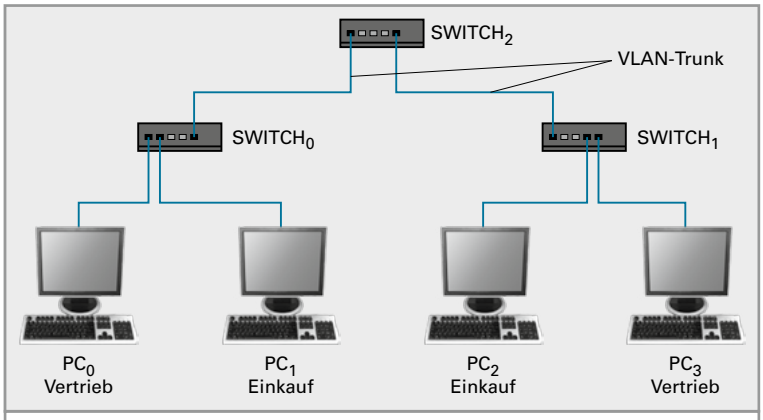


Bild 7.6: Netzwerkaufteilung mit 2 getrennten VLANs

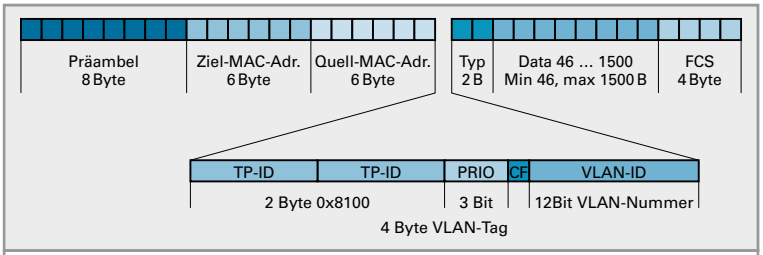


Bild 7.7: Ethernetframe mit VLAN-Tag

Durch den VLAN-Tag wird die Maximalgröße um 4 Byte auf 1522 Byte vergrößert (siehe Bild 7.7).

Der PC schickt einen normalen Datenrahmen heraus. Der Switch macht die Zuordnung zum virtuellen LAN und erweitert den Frame mit dem Tag. Der so gekennzeichnete Ethernetrahmen wird wie gewohnt durch das Netzwerk transportiert. Der letzte Switch entfernt diesen VLAN-Tag wieder, bevor er die Daten an den Zielrechner schickt.

Das VLAN-Tag besteht aus der Kennung **0x8100**, was anzeigt, dass hier eine VLAN-Kennung eingebaut wurde.

Dann folgen 3 Prioritätsbits. Hiermit lassen sich Datenströme innerhalb eines LANs priorisieren. So haben beispielsweise Telefonie-Daten eine höhere Priorität als Datei-Downloads oder E-Mail-Verkehr. Man nennt diese Einstellung QoS, Quality of Service, oder auch CoS, Class of Service (Tabelle 7.3).

Tabelle 7.3: Die 8 Prioritätsstufen im Einzelnen

Priorität	Anwendung
7	reserved
6	reserved
5	voice services
4	video conferencing
3	excellent load
2	high priority data
1	medium priority data
0	best effort (so gut es geht)

*Neue Bezeichnung für **CF-Bit**: DEI – Drop Eligible Indicator.*

Das CF-Bit steht für Canonical-Flag und gibt die Bit-Reihenfolge an, also ob das höchstwertige Bit (MSB) oder das niederwertigste Bit (LSB) zuerst übertragen wird. Bei Ethernet ist das CF-Bit immer null. Token-Ring und Ethernet handhaben dies genau umgekehrt.

Im VLAN-Tag bleiben dann noch 12 Bit für die Kennung der virtuellen Netze. Somit sind 2^{12} VLANs realisierbar.

FIT Failure In Time

Der FIT-Wert gibt an, wie viele Fehler pro Zeitbereich auftreten. Dabei werden üblicherweise als Bezugszeit 109 Stunden verwendet. Diese Bezugszeit wird nicht explizit angegeben.

Ein FIT-Wert von 1000 bedeutet, dass in 1 Milliarde Stunden (10^9 h) 1000 Fehler auftreten.

Aus dieser Fehlerrate lässt sich auch die MTBF berechnen:

$$\text{MTBF} = \frac{10^9\,\text{h}}{\text{FIT}} = \frac{114\,000\ \text{Jahre}}{\text{FIT}}$$

Ein FIT von 11400 ergibt somit eine MTBF von 10 Jahren, also eine zu erwartende Lebensdauer von 10 Jahren.

Verfügbarkeit

MTBF, die mittlere Betriebszeit bis zum Fehlerfall, kann auch als Uptime T_{up} angesehen werden. Die mittlere Reparaturzeit *MTTR* kann als Downtime T_{down} betrachtet werden. Beide Werte zusammen ergeben die Gesamtbetriebszeit T_{tot}. Somit lässt sich die Verfügbarkeit A auch folgendermaßen berechnen:

$$A = \frac{MTBF}{MTBF + MTTR} \cdot 100\,\% = \frac{MTBF}{t_{tot}} \cdot 100\,\%$$

11.3 Fehlervorhersage

Um ein System, egal in welcher Größe, sinnvoll managen zu können, muss man die Risiken und Wahrscheinlichkeiten einschätzen und kalkulieren können. Dazu dient:

- die Fehlerbaum-Analyse,
- die Risikomatrix
- die ABC-Analyse.

Zunächst müssen einige Grundlagen aus der Wahrscheinlichkeitslehre erläutert werden.

- Eine Wahrscheinlichkeit von 0 (Null) bedeutet, dass ein Ereignis nie eintritt.
- Eine Wahrscheinlichkeit von 1 (Eins) bedeutet, dass ein Ereignis ganz sicher eintritt (100-prozentig).
- Eine Wahrscheinlichkeit nahe 0 bedeutet, dass ein Ereignis sehr wahrscheinlich nicht eintritt.
- Eine Wahrscheinlichkeit nahe 1 bedeutet, dass ein Ereignis sehr wahrscheinlich eintritt.

Zahlen und Fakten sind wichtiger als ein „Bauchgefühl"!

Der Mensch neigt dazu, Wahrscheinlichkeiten, die ihn persönlich betreffen, falsch einzuschätzen. So liegt die Wahrscheinlichkeit, innerhalb eines Jahres bei einem Verkehrsunfall ums Leben zu kommen, bei ungefähr $80 \cdot 10^{-6}$. Die Wahrscheinlichkeit, dass man 6 Richtige im Lotto tippt, liegt bei etwa 1 zu 14000000, also ungefähr $71 \cdot 10^{-9}$. Trotzdem glaubt jeder Lottospieler, dass er bald die Millionen holt. Er glaubt aber nicht, dass er bei einem Autounfall sterben wird, obwohl dieses Risiko 1000 mal größer ist!

Wer glaubt, dass das Risiko, vom Blitz erschlagen zu werden, sehr unwahrscheinlich ist, der irrt. Diese Chance liegt bei rund 1:16000000, also ungefähr bei $62{,}5 \cdot 10^{-9}$ und ist somit in der gleichen Größenordnung wie ein Lottogewinn.

Genauso verhält es sich mit den Systemkomponenten eines IT-Systems. Zu gerne glaubt der Admin, dass seine Hardware nicht ausfallen wird, dass sein System nicht von Hackern übernommen wird und so weiter. Um dieses trügerische Bauchgefühl zu umgehen, helfen uns kühle Daten, Zahlen und Fakten, um eine wirkliche Sicherheit anstatt einer trügerischen Sicherheit herzustellen.

11.3.1 Fehlerbaumanalyse

Die Fehlerbaumanalyse wird eingesetzt, um die Wahrscheinlichkeit eines bestimmten Ereignisses vorherzusagen (Bild 11.4).

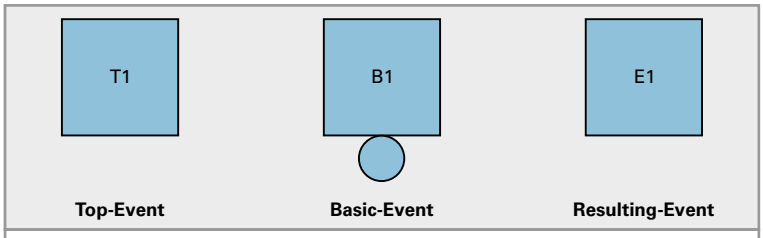


Bild 11.4: Events oder Ereignisse

Das zu berechnende Ereignis nennt man Top-Event.

Die Eintrittswahrscheinlichkeit dieses Top-Events hängt von anderen Ereignissen ab. Es wird zerlegt in mehrere Einzel-Ereignisse. Jedes dieser Einzel-Ereignisse kann wiederum von mehreren untergeordneten Ereignissen abhängen. Ereignisse, die von anderen Ereignissen abhängen, nennt man Resulting-Events.

Das Top-Event ist somit das letzte Resulting-Event aus untergeordneten Ereignissen.

Grund-Ereignisse, die nicht weiter in Einzel-Ereignisse zerlegt werden, nennt man Basic-Events. Die Wahrscheinlichkeit für das Auftreten der Basic-Events wird aus Datenblättern entnommen, sie wird aus Erfahrungswerten gewonnen oder sie wird geschätzt.

Basic-Events werden in atomare und nicht atomare Events eingeteilt. Atomare Events lassen sich nicht weiter unterteilen. Nicht atomare Events lassen sich zwar in weitere Events unterteilen, was aber nicht gemacht wird, um das Verfahren zu vereinfachen.

Die Events (Ereignisse) werden durchnummeriert in der Form:

$$T_1, T_2, \ldots T_n, E_1, E_2, \ldots E_n, B_1, B_2, \ldots B_n$$

Events werden mit logischen Verknüpfungen miteinander verknüpft und ergeben ein Resulting-Event. Dabei werden die aus der Booleschen Logik bekannten Verknüpfungen verwendet.

Die UND-Verknüpfung

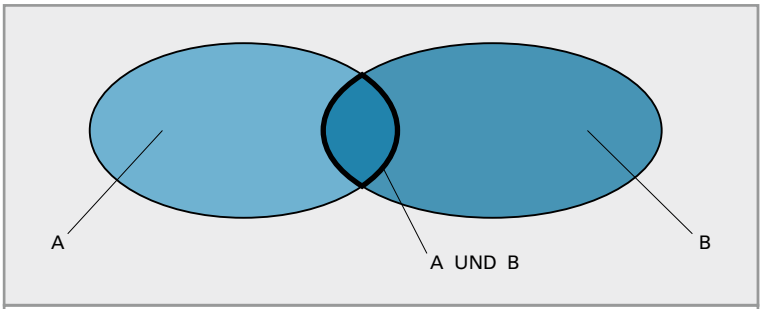


Bild 11.5: UND ist die Schnittmenge

Wenn alle Eingangs-Events eintreten müssen, also wenn Ereignis1 UND Ereignis2 UND Ereignis3 usw. eintreten müssen, dann handelt es sich um ein logisches UND (Bild 11.5).

Beispiel 11.1:
Wenn die Netzstromversorgung (Ereignis E_1) ausfällt UND die USV ausfällt (Ereignis E_2), dann ist der Server ohne Stromversorgung (Ereignis T_1). Das heißt, solange eines von beiden noch funktioniert, wird auch der Server mit Strom versorgt.

Die Gleichung für das Auftreten des Top-Events T1 lautet:

$$T_1 = E_1 \text{ UND } E_2 = E_1 \text{ AND } E_2 = E_1 \wedge E_2 = E_1 \cdot E_2$$

Dabei sind alle gezeigten Schreibweisen üblich.

Die Wahrscheinlichkeit berechnet sich zu:

$$T_1 = E_1 \cdot E_2$$

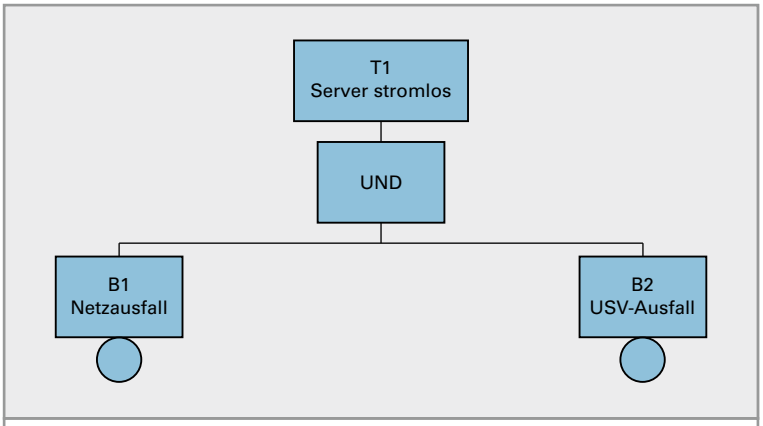


Bild 11.6: Der Server ist stromlos, wenn das Stromnetz ausfällt UND die USV versagt

Beispiel 11.2:
Nimmt man an, die Wahrscheinlichkeit für einen Netzstromausfall liege bei 0,001. Dann bedeutet dies anders ausgedrückt, dass man eine Netzverfügbarkeit von 0,999 oder 99,9 % hat.
Die Wahrscheinlichkeit, dass die USV ausfällt, liege bei 0,1 oder 10 %. Damit ergibt sich für T_1 eine Ausfallwahrscheinlichkeit von:

$$T_1 = E_1 \cdot E_2 = 0{,}001 \cdot 0{,}1 = 0{,}0001 = 0{,}01\,\%$$

Die Gesamt-Verfügbarkeit beträgt demnach 99,99% und ist somit höher als die Verfügbarkeit der einzelnen Teile. Durch den Einsatz einer USV wurde die Zuverlässigkeit der Stromversorgung des Servers um eine Größenordnung verbessert!

Die ODER-Verknüpfung

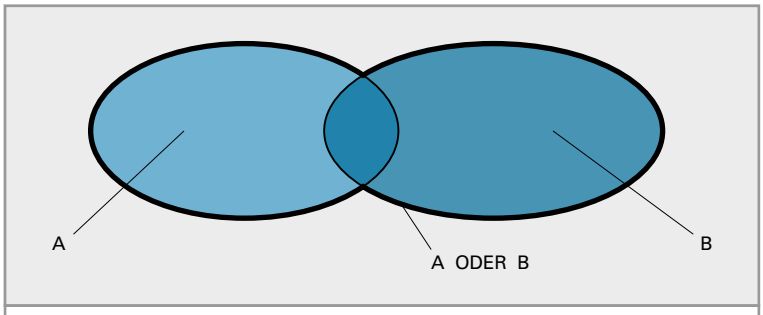


Bild 11.7: ODER ist die Summe aus A und B

Der einer ODER-Verknüpfung ist ein Top-Event 1, wenn mindestens eins der Einzel-Ereignisse eintritt (Bild 11.7).

Die Gleichung für das Auftreten des Top-Events T_1 lautet:

$$T_1 = E_1 \text{ ODER } E_2 = E_1 \text{ OR } E_2 = E_1 \vee E_2 = E_1 + E_2$$

Die Wahrscheinlichkeit für eine ODER-Verknüpfung errechnet sich:

$$T_1 = E_1 + E_2 - E_1 \cdot E_2$$

*Die Schnittmenge A*B ist beim ODER 2 Mal vorhanden und muss daher 1 Mal abgezogen werden*

Beispiel 11.3:
Nehmen wir an, die Wahrscheinlichkeit für einen Programmfehler liege bei 0,01 oder 1 %. Nehmen wir weiterhin an, die Wahrscheinlichkeit für einen Hardwarefehler liege bei 0,0001 oder 0,01 %. Dann ist die Wahrscheinlichkeit, dass der Rechner eine Fehlfunktion hat bei:

$$\begin{aligned} T &= E_1 + E_2 - E_1 \cdot E_2 \\ &= 0{,}0001 + 0{,}001 - 0{,}001 \cdot 0{,}0001 = 0{,}0011 - 0{,}00001 \\ &= 0{,}00109 = 0{,}109\,\% \end{aligned}$$

Die Wahrscheinlichkeit für dieses Ereignis wird also wesentlich größer als die Wahrscheinlichkeit der Einzelevents.

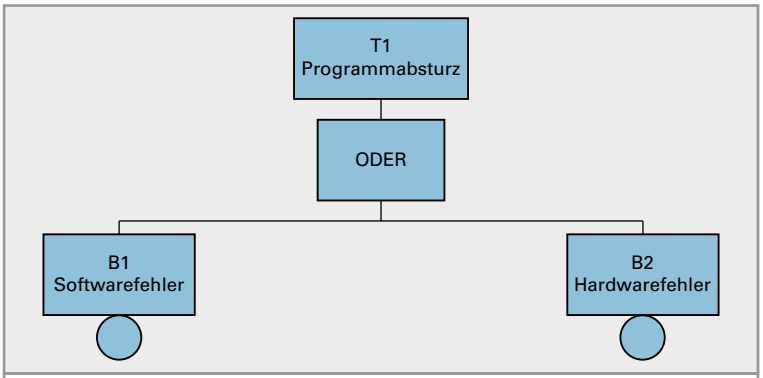


Bild 11.8: Programmabsturz bei Hardware- oder Softwarefehler

Kombination von Verknüpfungen

In Wirklichkeit sind die Abhängigkeiten natürlich wesentlich komplexer.

Aufgabe: Überlegen Sie sich ein praxisnahes Beispiel. Schätzen Sie die Ausfallwahrscheinlichkeiten der einzelnen Basic-Events. Überlegen Sie, wie die Abhängigkeiten sind und halten Sie diese in einem Fehlerbaum fest. Berechnen Sie dann die Eintrittswahrscheinlichkeit Ihres Top-Ereignisses.

11.3.2 Risikomatrix

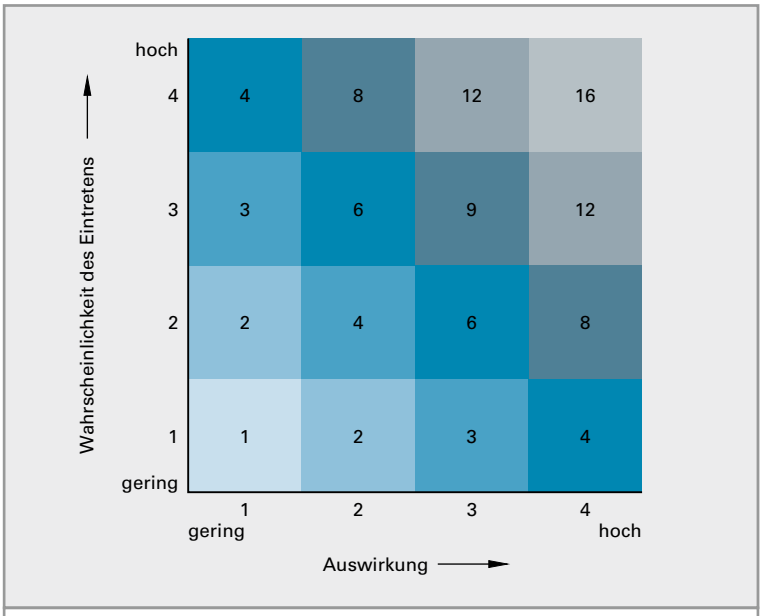


Bild 11.9: Das Risiko ist kalkulierbar

Die Risikomatrix ist ein einfaches Hilfsmittel, um ein Risiko einzustufen. Dabei werden die Auswirkungen auf einer Achse und die Wahrschein-

lichkeit des Auftretens eines Ereignisses auf der anderen Achse aufgetragen.

Die Auswirkungen können sehr gering sein, sodass das Eintreten dieses Falles keine oder nur unwesentliche Auswirkungen auf den Betrieb hat. Die Auswirkungen eines Ereignisses können auch unternehmenskritisch sein, sodass das Auftreten wesentlichen Einfluss auf die Arbeit eines Unternehmens oder eines Systems hat. Die Auswirkungen werden oft auf der x-Achse aufgetragen. Auswirkungen können teilweise auch als Kosten oder als Schadenspotenzial angegeben werden.

Die Wahrscheinlichkeit des Eintretens dieses Ereignisses wird auf der zweiten Achse aufgetragen. Sie reichen von sehr unwahrscheinlich bzw. nicht vorstellbar bis sehr wahrscheinlich bzw. wird sicher eintreten.

Die Risikomatrix kann durch Vergrößern oder Verkleinern an die jeweiligen Bedürfnisse angepasst werden. Durch eine größere Matrix, beispielsweise eine 6×6-Matrix, lassen sich feinere Abstufungen realisieren.

Ein unternehmenskritischer Datenbankserver (Auswirkung hoch) wird über eine alte wackelige Dreifachsteckdose mit Strom versorgt (Eintrittswahrscheinlichkeit des Stromausfalls sehr hoch). Das Risiko ist dann 16, also maximal. Hier ist sofortiges Handeln notwendig!

Um das Risiko eines Ereignisses zu berechnen, legt man die Auswirkungen und die Eintrittswahrscheinlichkeit fest. Das Produkt dieser beiden Werte ergibt das Risiko.

Risiko = Auswirkungen $\times$ Eintrittswahrscheinlichkeit

Beispiel 11.4:
Sind die Auswirkungen eines Ereignisses hoch – Stufe 3 einer 4-stufigen Skala, und die Eintrittswahrscheinlichkeit vorstellbar – Stufe 2 einer 4-stufigen Skala, dann beträgt das Risiko $3 \cdot 2 = 6$. Die Skala des Risikos reicht in diesem Fall von 1 bis 16.

11.3.3 ABC-Analyse

Wir leihen uns auch Methoden der Kaufleute.

Die ABC-Analyse ist ein in der Betriebswirtschaft häufig eingesetztes Instrument, um beispielsweise Kunden oder Lieferanten zu klassifizieren. A-Kunden sind die kleinste Kundengruppe, generieren aber den meisten Umsatz. B-Kunden erzeugen einen mittelmäßigen Umsatz. C-Kunden sind die größte Kundengruppe, die aber nur einen kleinen Umsatz erzeugt. Kümmert man sich um alle Kunden gleichermaßen, so bleibt das Verhältnis gleich. Kümmert man sich verstärkt um A-Kunden, kann mit wenig Einsatz (da wenig Kunden) ein großer Erfolg erzielt werden. Folgende Tabelle veranschaulicht diese Einteilung:

Klasse	Umsatz	Kunden
A	80 %	10 %
B	15 %	20 %
C	5 %	70 %

Diese Tabelle zeigt, dass nur 10 % aller Kunden 80 % des Umsatzes erzeugen. Wogegen aber 70 % der Kunden zusammen nur 5 % des Umsatzes bringen.

Hieraus wird ersichtlich, um welche Kunden man sich kümmern sollte, um den Umsatz zu steigern.

Ebenso lässt sich die ABC-Analyse für viele andere Zwecke einsetzen. Im IT-Management kann man beispielsweise eine Liste von Support-Anfragen erstellen und mit dem Instrument der ABC-Analyse auswerten.

Mit der ABC-Analyse der Supportanfragen ist es möglich,

- das „Wesentliche" vom „Unwesentlichen" zu trennen,
- festzustellen, welche Fehler den größten Support-Aufwand benötigen,
- wirtschaftliche Anstrengungen und unwirtschaftliche zu erkennen,
- Schulungsbedarf der User zu erkennen,
- die Wirtschaftlichkeit der IT zu steigern.

11.4 Übungsaufgaben

Übungsaufgabe Nr. 1

Berechnen Sie die Ausfallzeit und die Betriebszeit, wenn Ihnen Ihr Dienstleister eine Verfügbarkeit von 99,5 % garantiert.

Übungsaufgabe Nr. 2

Berechnen Sie die Wahrscheinlichkeit, dass Sie einen Datenverlust erleiden. Die Ausfallwahrscheinlichkeit, dass Ihre Festplatte ausfällt, liegt bei 0,01 %. Wenn Sie eine Sicherung Ihrer Daten haben, so ist das kein Problem. Nehmen wir an, Sie haben vergessen, ein Backup zu erstellen, dann haben Sie einen Daten-Totalverlust. Wie groß ist die Wahrscheinlichkeit eines Totalverlustes, wenn die Wahrscheinlichkeit, dass Sie kein Backup haben, bei 30 % liegt. Verwenden Sie zum Berechnen die Fehlerbaumanalyse.

Aufgabe 1

Übungsaufgabe Nr. 3

Definieren Sie in Aufgabe 1 im Arbeitsheft die Prioritäten von verschiedenen Ereignissen im Netzwerkbereich.

Aufgabe 2

Übungsaufgabe Nr. 4

Erstellen Sie mit „Bordmitteln", die Ihnen Ihr Betriebssystem zur Verfügung stellt, eine Baseline für Ihren Rechner.