

Berufsbildende Schule I Mainz

In Kooperation mit dem HERDT-Verlag stellen wir Ihnen eine PDF inkl. Zusatzmedien für Ihre persönliche Weiterbildung zur Verfügung. In Verbindung mit dem Programm HERDT|Campus ALL YOU CAN READ stehen diese PDFs nur Lehrkräften und Schüler*innen der oben genannten Lehranstalt zur Verfügung. Eine Nutzung oder Weitergabe für andere Zwecke ist ausdrücklich verboten und unterliegt dem Urheberrecht. Jeglicher Verstoß kann zivil- und strafrechtliche Konsequenzen nach sich ziehen.

Netzwerke Grundlagen

Karsten Bratvogel

1. Ausgabe, Dezember 2021

NW_2022



ISBN 978-3-98569-047-3

1 Informationen zu diesem Buch	4	7 Arbeitsweise lokaler Netze	61
1.1 Voraussetzungen und Ziele	4	7.1 Umsetzung im LAN	61
1.2 Aufbau und Konventionen	5	7.2 Ethernet	61
1.3 Bevor Sie beginnen ...	6		
2 Grundbegriffe und Konzepte zu Netzwerken	7	8 Betriebssysteme und Server	66
2.1 Vorbemerkungen zum Thema Netzwerk	7	8.1 Einteilung von Betriebssystemen	66
2.2 Der Weg zu Netzwerken	8	8.2 Aufgabengebiete von Betriebssystemen	67
2.3 Grundkonzepte von Netzwerken	9	8.3 Microsoft Windows	69
2.4 Wichtige Netzwerk-Kürzel und deren Bedeutung	13	8.4 UNIX	71
2.5 Gründe und Ziele einer Vernetzung	15	8.5 Interaktion in heterogenen Netzen	73
2.6 Vorstellung des Fallbeispiels	17	8.6 Kennzeichen der Hardware eines Servers	74
		8.7 Exkurs: Speichern von Daten	78
		8.8 Übung	82
3 Topologien	19	9 Praxis 1	83
3.1 Der Begriff Topologien	19	9.1 Planung	83
3.2 Bus	20	9.2 Allgemeine Abschätzung	84
3.3 Stern	21	9.3 Realisierung	86
3.4 Ring	22	9.4 Auswirkungen	91
3.5 Mischformen	22		
3.6 Wolke (Cloud)	24		
4 Übertragungsmedien	25	10 Normen und Modelle	95
4.1 Einteilung der Medien	25	10.1 Gremien	95
4.2 Koaxialkabel	27	10.2 Schichten-Modelle	98
4.3 Twisted-Pair-Kabel (TP)	28	10.3 Das OSI-Referenz-Modell allgemein	99
4.4 Glasfaserkabel	30	10.4 Die sieben Schichten des OSI-Modells	103
4.5 Drahtlose Übertragung per WLAN	35	10.5 Das OSI-Modell und IEEE 802	105
4.6 Bluetooth	43	10.6 Exkurs: Frames	105
4.7 Weitere Funktechniken und das Internet der Dinge	43	10.7 Übung	107
4.8 Übertragung per Licht bzw. Laser	45		
4.9 Übung	46		
5 Schnittstellen	47	11 Protokolle	108
5.1 Netzwerkarten	47	11.1 Der Begriff Protokolle	108
5.2 Weitere Anschlussmöglichkeiten	50	11.2 TCP/IP	109
5.3 Fernwartung bei Büro-Rechnern und Servern	53	11.3 IP-Adressierung	111
		11.4 Umsetzung der IPv4-Adressierung in der Praxis	117
		11.5 Zuordnung zum OSI-Modell	121
		11.6 Übung	124
6 Zugriffsverfahren	54	12 Erweiterung der Netzwerkstruktur	125
6.1 Zugang zum Übertragungsmedium regeln	54	12.1 Überlegungen zur Vergrößerung eines Netzwerks	125
6.2 CSMA/CD	55	12.2 Strukturierte Verkabelung	127
6.3 Von Shared Media zu Switched Networks	57	12.3 Collapsed Backbone	129
6.4 CSMA/CA	58	12.4 VLAN (Virtual Local Area Network)	130
6.5 Zusammenfassung und Ausblick	59	12.5 Industrie-LAN	134
		12.6 Übung	134

13 Kopplung von Netzwerken	135	17.3 Verbindungsarten	181
13.1 Aktive Komponenten	135	17.4 Vermittlungsprinzip	184
13.2 Repeater und Hub (Schicht 1)	136	17.5 Netzneutralität	185
13.3 Bridge (Schicht 2)	137	17.6 Privatsphäre im Internet	186
13.4 Switch (Schicht 2)	139		
13.5 Router (Schicht 3)	143		
13.6 Firewall	149	18 Übertragung in Weitverkehrsnetzen	189
13.7 Gateway (Schicht 7)	150	18.1 Übertragungsverfahren	189
13.8 Multifunktionsgeräte	151	18.2 Analoge Übertragung	190
13.9 Übung	151	18.3 DSL	191
		18.4 SDH/SONET	194
		18.5 Protokolle der Sicherungsschicht	195
14 Erweiterung der Geschwindigkeit	152	18.6 Übung	202
14.1 Gigabit-Ethernet	152		
14.2 Weitere Überlegungen	156		
15 Netzwerküberwachung und Fehlersuche	159	19 Zugangsmöglichkeiten	203
15.1 Protokolle	159	19.1 Telefonnetz	203
15.2 Hinweise zur Umsetzung	163	19.2 Mobilfunknetz	206
15.3 Begleitende Maßnahmen	165	19.3 Weitere Netze	209
15.4 Troubleshooting	166	20 WAN-Anbieter	211
15.5 Übung	170	20.1 Übersicht WAN-Zugänge	211
		20.2 WAN-Standardangebote	215
16 Praxis 2	171	21 Praxis 3	219
16.1 Planung des Ausbaus	171	21.1 Vorüberlegungen	219
16.2 Umsetzung	172	21.2 Umsetzung	220
17 Weitverkehrsnetze	175	Stichwortverzeichnis	222
17.1 Einführung in Weitverkehrsnetze	175		
17.2 Begriffe	179		

1

Informationen zu diesem Buch

1.1 Voraussetzungen und Ziele

Empfohlene Vorkenntnisse

Die wichtigste Voraussetzung für die Lektüre dieses Buchs sind fundierte Kenntnisse der PC-Technik. Vorkenntnisse in Bezug auf Netzwerke, z. B. als Anwender oder als Internetbenutzer, sind an vielen Stellen hilfreich, aber nicht zwingend erforderlich.

Lernziele

Dieses Buch soll Ihnen einen fundierten Einstieg in das Thema Netzwerke geben. Sie werden in die Lage versetzt, den grundlegenden Aufbau verschiedenster Netzwerke nachzuvollziehen und die darin ablaufenden Vorgänge zu verstehen. Die theoretischen Grundlagen werden dabei immer wieder anhand praktischer Beispiele bezogen auf eine Musterfirma dargestellt.

Das Buch stellt ein aktuelles, erklärendes Abbild der momentanen technischen Möglichkeiten im Netzwerkbereich dar. Soweit für das allgemeine Verständnis notwendig, werden auch geschichtliche Entwicklungen geschildert und dabei Techniken beschrieben, die heute kaum noch zum Einsatz kommen.

Ziel des Buchs ist, den Leser strukturiert an die Vielzahl von Begriffen und Abkürzungen des Themenbereichs heranzuführen und ihn so in die Lage zu versetzen, weiterführende und damit auch zwangsläufig detailliertere und tiefer gehende Literatur lesen und einordnen zu können.

Nach dem Durcharbeiten dieses Buchs kennen Sie Zielsetzungen, Vorteile, Einsatzmöglichkeiten, Technologien und aktuelle Risiken von lokalen Netzen und Weitverkehrsnetzen. Sie kennen Übertragungsmedien und die Kommunikationsprotokolle, einschließlich der Grundlagen zu TCP/IP und IPv6. Sie kennen und verstehen das OSI-Referenzmodell, Aspekte des Netzwerkmanagements und der Sicherheit.

1.2 Aufbau und Konventionen

Inhaltliche Gliederung

Der **erste Teil** (Kapitel 2–9) legt den Schwerpunkt auf **kleine lokale Netzwerke**. Hier werden für alle Bereiche, die bei einer Vernetzung relevant sind, die notwendigen Grundlagen so kompakt und übersichtlich wie möglich vermittelt.

Der **zweite Teil** (Kapitel 10–16) erweitert den Schwerpunkt des ersten Teils auf **große lokale Netzwerke**. Er beinhaltet alles, was nötig ist, um lokale Netze sukzessive zu vergrößern. Dies betrifft z. B. die weitere räumliche Ausdehnung eines Netzwerks über mehrere Etagen oder Gebäude, die Erhöhung der Geschwindigkeit der Datenübertragung oder die effektive Strukturierung eines Unternehmensnetzwerks.

Der **dritte Teil** (Kapitel 17–21) geht zuerst weg von lokalen Netzen und bietet die Grundlagen zum Thema **Weitverkehrsnetze**. Danach werden die Anbindung lokaler Netze an Weitverkehrsnetze und mögliche Nutzungen für globale Firmennetze erläutert.

Da Techniken aus dem Weitverkehrsbereich inzwischen verstärkt auch im Bereich lokaler Netze eingesetzt werden, ist vor allem die Trennung zwischen dem zweiten und dritten Teil eine künstliche, aber bewusst gewählte. Sie ist besser geeignet, eine Zuordnung der Begriffe zu unterstützen, reduziert die Komplexität des Themas und ist für die systematische Darstellung von Grundlagen sehr hilfreich. Generell werden in diesem Buch Techniken und Verfahren vorrangig jeweils in dem Teil dargestellt, in dem sie im Laufe der Entwicklung primär aufgetaucht sind und eingesetzt wurden.

Typografische Konventionen

Im Text erkennen Sie bestimmte Programmelemente an der Formatierung:

Kursivschrift kennzeichnet alle von Programmen vorgegebenen Bezeichnungen für Schaltflächen, Dialogfenster, Symbolleisten, Menüs bzw. Menüpunkte, Datei- und Verzeichnisnamen sowie Internetadressen.

Courier wird für Systembefehle verwendet. In Syntaxangaben werden Parameter kursiv ausgezeichnet (z. B. *cd Verzeichnisname*). Eckige Klammern [] kennzeichnen optionale Elemente. Alternative Eingaben sind durch einen senkrechten Strich | getrennt. Benutzereingaben auf der Konsole werden **fett** hervorgehoben.

1.3 Bevor Sie beginnen ...

HERDT BuchPlus – unser Konzept:

Problemlos einsteigen – Effizient lernen – Zielgerichtet nachschlagen

(weitere Infos unter www.herdt.com/BuchPlus)

Nutzen Sie dabei unsere maßgeschneiderten, im Internet frei verfügbaren Medien:



Wie Sie schnell auf diese BuchPlus-Medien zugreifen können, erfahren Sie unter www.herdt.com/BuchPlus.

2

Grundbegriffe und Konzepte zu Netzwerken

2.1 Vorbemerkungen zum Thema Netzwerk

Komplexität des Themas

Netzwerke werden in kleinen Firmen mit wenigen Mitarbeitern auf einer Etage genauso eingesetzt wie in Firmen mit Tausenden von Mitarbeitern, weltweit verteilt auf mehrere Filialen. Der Anspruch an die Technik kann extrem unterschiedlich sein. Aus der Vielzahl der möglichen Umsetzungen heraus erklärt sich die Komplexität des Themas.

Hinweise zur Planung von Netzwerken

Das Ziel dieses Buchs ist es, Ihnen eine breite Basis an Grundwissen zu vermitteln, die es Ihnen ermöglicht, bei der Planung und Verwirklichung eines Netzwerks teure Irrwege oder gar Sackgassen zu vermeiden.

Dies ist nicht so einfach, da einerseits die technischen Möglichkeiten immer weiter verbessert werden, andererseits die Ansprüche der Benutzer steigen, sodass Sie mit einer permanenten Migration und einer stetigen Weiterentwicklung mit zum Teil sehr kurzen Innovationszyklen konfrontiert werden. Dem Aspekt der Planung kommt deshalb eine enorme Bedeutung zu. Die erfolgreiche Planung komplexer, verteilter Netzwerke kann dabei nur mit entsprechender Erfahrung durchgeführt werden und wird darum häufig an externe Dienstleister vergeben.

Sie dürfen sich nicht der Illusion hingeben, dass der Aufbau eines Netzwerks mit etwas Statischem endet. Die technischen Möglichkeiten steigen häufig genauso schnell wie die Wünsche und Bedürfnisse der Benutzer. Es muss jedem klar sein, dass der Weg zum optimalen Netzwerk ein Entwicklungsprozess ist, der im Vorfeld fundiertes Know-how und umfangreiche Planungen erfordert.

Ein optimales Netz kann dabei als Zielvorgabe dienen, wobei optimal nicht nur bedeutet, dass

- ✓ jeder Benutzer problemlos und schnell auf die für ihn wichtigen Arbeitswerkzeuge zugreifen kann,
- ✓ der Datenverkehr in zufriedenstellender Geschwindigkeit verläuft,
- ✓ die Vernetzung in einem finanziell akzeptablen Rahmen bleibt.

Sondern optimal bedeutet in diesem Zusammenhang auch, dass jedes System bei Bedarf mit jedem anderen kommunizieren kann. Darüber hinaus müssen aber auch Kriterien wie Netzwerksicherheit, Netzwerkverfügbarkeit und Wartungskosten berücksichtigt werden.

Eine Herausforderung beim Aufbau von Netzwerken besteht darin, eine kosteneffektive künftige Erweiterung einzuplanen. So sollten beispielsweise Verkabelungen stets mit den besten bezahlbaren Kabeln durchgeführt werden, da eine spätere Veränderung mit erheblichem Mehraufwand verbunden ist.

In gewisser Weise ist diese Aufgabe im Laufe der letzten Jahre einfacher geworden, da viele herstellerspezifische (**proprietäre**) Lösungen aufgegeben wurden und sich in vielen Bereichen firmenübergreifende Standards etabliert haben. Andererseits ist sie schwieriger und aufwendiger geworden, weil die Anforderungen an Netzwerke deutlich gestiegen sind. Dazu zählen der Wunsch nach höheren Geschwindigkeiten und erhöhte Sicherheitsanforderungen genauso wie die immer intensivere Nutzung der Netzwerke bei der täglichen Arbeit.

2.2 Der Weg zu Netzwerken

Ein einfaches Netzwerk

Grundsätzlich ist ein **Netzwerk** eine Gruppe miteinander verbundener Systeme, die in der Lage sind, untereinander zu kommunizieren.

Sobald zwei Rechner per Kabel oder Funk miteinander verbunden sind und Daten austauschen, können Sie bereits von einem Computernetzwerk in der kleinsten Variante sprechen. Die größtmögliche, nämlich weltweite Variante eines Computernetzwerks begegnet Ihnen beim Stichwort Internet.



Zwei Rechner, ein Kabel: ein Netzwerk

Geschichte der Entwicklung von Netzwerken

Die 60er- und 70er-Jahre

Bereits in den 60er- und 70er-Jahren war die Verbindung von Systemen ein wichtiges Thema, damals allerdings in einer recht einseitigen Beziehung. Auf der einen Seite stand in einem abgeschirmten **Rechenzentrum** ein **Zentralrechner** (**Mainframe**, **Großrechner**, **Host**) und auf der anderen Seite befanden sich in den Büros und über Kabel angebunden sogenannte **Terminals** (Tastatur und Bildschirm). Über diese Terminals waren nur Ein- und Ausgaben möglich, die eigentliche Rechenleistung lieferte der Zentralrechner. So gesehen konnte man hier noch nicht von Netzwerken sprechen, da ja nicht zwei Systeme miteinander kommunizierten, sondern eigentlich nur eine Art verlängertes Tastatur- und Bildschirmkabel zum Einsatz kam.

Die 80er- und 90er-Jahre

Mit der zunehmenden Einführung der **Personal Computer** (PC) ab Anfang der 80er-Jahre ging der Wunsch in Erfüllung, kleinere Rechner direkt vor Ort, also auf dem Schreibtisch, zur Verfügung zu haben. Diese konnten mit verhältnismäßig geringem Aufwand selbst gewartet werden und der Benutzer konnte relativ selbstständig über das eingesetzte Programm entscheiden. Die Entwicklung ging weg vom zentralen Rechenzentrum und hin zu mehr Autonomie für den Benutzer. Unterstützt wurde dies im Laufe der Jahre durch immer anwenderfreundlichere und leichter zu bedienende Programme. Mit der zunehmenden Qualität und Quantität von PCs entstand schon bald die Idee, die Einzelplatzrechner in einem Netzwerk zu verbinden. Ein wichtiger Aspekt dabei war unter anderem der Wunsch, durch PC-Netzwerke die kostspieligen Rechenzentren zu ersetzen.

Ab 2000

Obwohl PCs und Vernetzungstechniken in der letzten Zeit immer leistungsfähiger wurden, ist in einigen Branchen auch heute noch der Einsatz von Zentralrechnern unumgänglich. Allerdings ist eine Koexistenz beider Bereiche inzwischen auch unproblematisch, da genormte Übergänge verfügbar sind.

Eine gewisse Renaissance der Idee von Terminals sind **Thin Clients** (z. B. von IGEL, HP, Fujitsu, um nur einige Hersteller zu nennen), die sich vor allem durch Wartungsfreundlichkeit, kleine Baugrößen und einen deutlich reduzierten Stromverbrauch im Vergleich zum PC auszeichnen. Hinzu kommt, dass durch den Verzicht auf lokale Laufwerke und Betriebssysteme erhebliche Kosteneinsparungen möglich werden. Ein Teil dieses Einsparpotenzials geht jedoch für eine leistungsstarke Terminalserverhardware, mehrbenutzerfähige Software und Zugriffslicenzen wieder verloren. Daher rechnet sich der Einsatz von Thin Clients besonders in sehr großen Umgebungen.

Dieses Buch widmet sich in erster Linie der Vernetzung von PCs und behandelt das Thema Rechenzentrum nur dort, wo die Übergänge zwischen PC und Großrechner wichtig sind.

2.3 Grundkonzepte von Netzwerken

Als Erstes werden zwei Grundkonzepte einer Vernetzung im PC-Bereich vorgestellt:

- ✓ Peer-to-Peer
- ✓ Client-Server

Peer-to-Peer

Das Wort **Peer** (engl. Gleichgestellter, Ebenbürtiger) beschreibt den Grundgedanken dieser Art der Vernetzung bereits recht gut. Im lokalen Netzwerk sind damit beispielsweise Drucker- oder Netzlaufwerksfreigaben gemeint, im Internet bezieht sich der Begriff Peer-to-Peer meist auf Filesharing-Netze wie z. B. BitTorrent.

Gleichberechtigung

In einem Peer-to-Peer-Netz sind prinzipiell alle Computersysteme gleichberechtigt. Die Ressourcen im Netz sind auf den beteiligten Rechnern verteilt und jeder Benutzer ist für die **Sicherheit** und Freigabe „seiner“ lokalen Ressourcen verantwortlich. Jeder Rechner kann anderen Rechnern Ressourcen zur Verfügung stellen und umgekehrt auf freigegebene Ressourcen anderer Rechner zugreifen, sofern er dazu berechtigt ist.

Vor- und Nachteile von Peer-to-Peer-Netzwerken

Die Hauptvorteile sind, dass keine Extrakosten für einen Server anfallen und kein spezielles **Betriebssystem** nötig ist, da alle gängigen PC-Betriebssysteme Funktionen für diese Art der Vernetzung bereits integriert haben.

Als Nachteil stellt sich heraus, dass es weder in Bezug auf Ressourcen noch in Bezug auf Benutzer eine zentrale Verwaltung gibt und Sicherheitsrichtlinien im Netzwerk nur sehr eingeschränkt umsetzbar sind.

Peer-to-Peer-Netze werden vorrangig für die Dateiverteilung und das dezentrale Suchen von Dateien genutzt. Dabei wird durch die Verteilung der Daten eine effizientere Auslastung der Verbindungswege erreicht. Ein anderer Aspekt ist das Zusammenschalten von Rechnern mit dem Ziel, die Ressourcen für die Lösung einer gemeinsamen Aufgabe zu nutzen (z. B. Grid- oder Cloud-Computing – Rechenaufgaben oder Daten werden dabei auf mehrere Rechner bzw. Festplatten-Speicher verteilt).

Client-Server

Sobald ein Netzwerk größere Dimensionen annimmt, wird das Peer-to-Peer-Konzept zunehmend unübersichtlich und schwerer zu administrieren. Durch den Einsatz von Servern und Workstations nach dem **Client-Server** Prinzip kann dem entgegengewirkt werden, da technisches Personal sowohl die Server als auch die Workstations verwaltet und die Netzwerksicherheit sicherstellt.

Alle Standard-Betriebssysteme unterstützen das Client-Server-Prinzip. Das Peer-to-Peer-Prinzip kann für einzelne Dienstmerkmale (z. B. Filetransfer) innerhalb von Betriebssystemen weiter genutzt werden.

Client-Server-Prinzip

Das Grundprinzip ist hierbei, dass es auf der einen Seite ein Programm gibt (die **Server-Anwendung** bzw. Applikation), welches über eine Netzwerkverbindung eine Dienstleistung (Service) bereitstellt und passiv auf Anfragen wartet. Auf der anderen Seite fordert die **Client-Anwendung** (Programm auf dem PC des Anwenders) diese Dienstleistung aktiv an.

Das Client-Programm kommuniziert mit dem Server-Programm über eine eindeutige „Sprache“, dem **Protokoll**. Im Protokoll sind alle möglichen Anweisungen und Antworten definiert. Jede Dienstleistung hat in der Regel ein eigenes Protokoll. Beispiel: ein Webserver, von dem ein Webclient (ein Browser wie Internet Explorer oder Firefox) bestimmte Seiten über das HTTP-Protokoll anfordert.

Bei einer Server-Client-Konzeption findet eine Aufgabenteilung statt. Eine oder mehrere Server-Anwendungen stellen zentral Ressourcen und Dienstleistungen zur Verfügung. Die Clients können in der Regel nach erfolgreicher Anmeldung auf diese zugreifen. Oft ist eine Anmeldung nicht erforderlich, wie dies bei Web-, DNS- und DHCP-Servern normalerweise der Fall ist.

Da Server-Programme meist auf besonders gut ausgestatteten Rechnern aktiv sind, hat es sich eingebürgert, auch diese Hardware als „Server“ zu bezeichnen, was mit dem Client-Server-Prinzip nichts zu tun hat. Ebenso werden auch Rechner mit Client-Anwendungen vereinfacht als „Client“ bezeichnet. Dies wird auch in diesem Buch oft übernommen. Generell ist für das Verständnis die Erkenntnis wichtig, dass es sich beim Client-Server-Modell um Programme handelt (oft als Teil vom Betriebssystem), die auf einer Hardware aktiv sind. Auf Server-Hardware und Redundanz wird genauer in Kapitel 8.6 eingegangen.

Es besteht die Möglichkeit, alle gewünschten Dienste von einem einzigen Server anbieten zu lassen. Bei größeren Netzen ist es üblich, die entsprechend anfallenden Aufgaben auf mehrere spezialisierte Server zu verteilen. Neben der effektiveren Ausnutzung der Server-Ressourcen ergibt sich als weiterer Vorteil die Erhöhung der Sicherheit, indem auf dem jeweils spezialisierten Server nur die Dienste laufen, die wirklich benötigt werden. Je weniger Dienste ein einzelner Server anbietet, desto weniger Angriffsfläche bietet er. Viele Dienste können auch redundant auf mehreren Servern installiert werden, wodurch der Dienst bei Ausfall eines einzelnen Servers im Netzwerk erhalten bleibt.

Typische Serveraufgaben

Der Vorteil dieser Vorgehensweise ist, dass jeder Server für seine spezielle Aufgabe optimal ausgerüstet werden kann. Die folgende Tabelle schildert einige der gängigsten Serverdienste:

File-Server	Ein Rechner mit einer oder mehreren schnellen und großen Festplatten dient zum Speichern aller Daten, die von den Benutzern erstellt werden. Für diese Server wird im Normalfall ein eigenständiges Konzept zur regelmäßigen Datensicherung , z. B. auf Bänder, entwickelt.
Print-Server	Print-Server stellen im Netzwerk zentrale Druckdienste bereit. Hierbei können einerseits entsprechend ausgerüstete Computer etliche externe Druckgeräte steuern oder andererseits in Druckgeräte integrierte Print-Server verwendet werden. Zentralisierte Drucklösungen sind gekennzeichnet durch verminderte Druckkosten und effektivere Geräteauslastung.
Application-Server	Ein Application-Server stellt Anwendungsprogramme, die in der ganzen Firma gebraucht werden, zentral zur Verfügung. Die Benutzer starten das gewünschte Programm nicht von einer lokalen Festplatte, sondern von einem Client aus auf diesem Server. Bei Programm-Updates muss die neue Version nur auf dem Server installiert werden und kann danach in dieser aktuellen Fassung in der ganzen Firma genutzt werden. Für den endgültigen Einsatz am Client ist häufig noch ein kleiner lokaler Installationsteil notwendig. Werden die Anwendungen direkt auf dem Server ausgeführt, spricht man entweder von einem Terminal-Server mit Zugriff über spezielle Client-Software (z. B. Remote-Desktop), oder von webbasierten Diensten mit Zugriff über einen beliebigen Webbrowser (z. B. Internet Explorer oder Firefox).

Auf Smartphones, Tablets und ab Windows 8 werden neuerdings „Apps“ angeboten. Eine **App** (die Kurzform von „Application“) stellt dabei für den Benutzer eine **lokale** Anwendung dar, die entweder auf einen Server zugreift (als Client-Programm) oder ein eigenständig ablaufendes Programm ist. Auf einem Application-Server laufen eigene Anwendungen stattdessen über ein Netzwerk gesteuert **remote** (in einer gewissen Entfernung) ab.

Weitere Serveraufgaben

Die folgende Tabelle erhebt keinen Anspruch auf Vollständigkeit, sondern soll einen Eindruck davon vermitteln, wie weit die Palette der möglichen Serveraufgaben bei Bedarf noch ausgebaut werden kann:

DNS-Server	Ein DNS-Server (Domain Name System) ermöglicht im Wesentlichen die Auflösung von Namen zu IP-Adressen in Internet und Intranet.
DHCP-Server	DHCP (Dynamic Host Configuration Protocol) dient dazu, Netzwerk-komponenten (z. B. Rechner, Smartphones etc.) IP-Adressen und Konfigurationen zuzuweisen.
Mail-Server	Für jeden Benutzer kann darüber ein Postfach angelegt werden, sodass z. B. die Firmenmitarbeiter über E-Mail miteinander kommunizieren können.
Webserver	Er stellt im firmeneigenen Netzwerk ähnliche Funktionalitäten zur Ver-fügung, wie sie viele bereits vom Internet gewohnt sind. Auf diese Weise können die Benutzer z. B. über Browser auf Informationen zugreifen.
Datenbank-Server	Mit einem dafür geeigneten Datenbankmanagementsystem (DBMS) kann er große Datenbestände zentral zur Verfügung stellen, sodass mehrere Benutzer gleichzeitig mit diesen Daten arbeiten können.
Proxy-Server	Er kann stellvertretend für andere Client-Programme (nach festlegbaren Regeln) Inhalte aus dem Internet holen und diese für einen erneuten Abruf zwischenspeichern.

Zentrale Benutzerverwaltung

Mit dem Client-Server-Konzept wird häufig eine zentrale Benutzerverwaltung eingeführt. Dabei werden Benutzer verschiedenen Gruppen zugeordnet und diesen Gruppen Berechtigungen eingeräumt oder bestimmte Zugriffe verweigert. Einer der Vorteile davon ist, dass neue Benutzer schnell integriert werden können, indem sie passenden, bereits bestehenden Gruppen zugeordnet werden.

Von einem **serverbasierten Netzwerk** spricht man, wenn mindestens ein zentraler Fileserver im Netzwerk bereitsteht; meistens kommt ein Domänencontroller zur einfacheren Verwaltung der vorhandenen Netzwerk-Ressourcen über eine Windows-Domäne hinzu. Beide zusammen ermöglichen dem Benutzer, dass er sich von jedem beliebigen Rechner aus unter seinem Namen am Netz anmelden und durch seine Zugehörigkeit zu Benutzergruppen auf seine benötigten Ressourcen zugreifen kann.

Nachteile von Client-Server-Techniken

Ein Nachteil sind die höheren Kosten, die für zusätzliche Rechner anfallen, die als Server dienen sollen, sowie für Betriebssysteme und Programme, die für diese Art Verwaltung geeignet sind. Für den Fall, dass ein Server ausfällt, muss ein Ersatz-Server bereitstehen (vgl. Kapitel 2.5, „Absicherung der Verfügbarkeit“). Oft kommen noch Kosten für die Schulung von Mitarbeitern hinzu, die administrative Aufgaben übernehmen sollen.

Total Cost of Ownership (TCO) und Return on Investment (ROI)

TCO ist ein Begriff aus der Wirtschaft. Damit wird versucht, die Gesamtkosten eines Computer-Netzes zu erfassen. Dazu gehören neben den Anschaffungskosten für Hard- und Software auch die Kosten für den laufenden Betrieb bzw. entstehende Kosten durch Ausfall und Instandsetzung von Rechnern.

So sind z. B. die Anschaffungskosten für Betriebssystem-Software meist niedriger als die Kosten, die für die notwendige Schulung der Mitarbeiter aufgewendet werden müssen. Auch muss von Anfang an klar sein, dass der Betrieb eines Netzwerks immer und dauerhaft mit zusätzlichem Personalaufwand verbunden ist.

Ein weiterer Begriff, der in diesem Zusammenhang öfter verwendet wird, ist **ROI**. Hier wird versucht, die Kosten-Nutzen-Relation von Investitionen zu bestimmen. ROI ist das Produkt von Umsatzrendite und Kapitalumschlag. So stehen etwa den Schulungskosten die Zeitersparnisse gegenüber, die sich durch die verbesserte Verwaltbarkeit eines zentralisierten Netzes ergeben.

2.4 Wichtige Netzwerk-Kürzel und deren Bedeutung

Local Area Network (LAN)

Ein **LAN** ist gekennzeichnet durch eine begrenzte geografische Ausdehnung auf ein Firmengelände. (Bei großen Firmen können Entferungen bis ca. 10 km vorkommen.) Im Normalfall werden keine Leitungen öffentlicher Anbieter genutzt, sondern das Netz unterliegt vollkommen der Aufsicht der Firma. Eine Definition der ISO (**I**nternational **S**tandards **O**rganization) beschreibt dies folgendermaßen:

„Ein lokales Netzwerk dient der bitseriellen Informationsübertragung zwischen miteinander verbundenen unabhängigen Geräten. Es befindet sich vollständig im rechtlichen Entscheidungsbereich des Benutzers und ist auf sein Gelände begrenzt.“

Metropolitan Area Network (MAN)

Ein **MAN** zeichnet sich durch die regionale Ausdehnung auf das Gebiet einer Stadt oder eines Ballungszentrums aus. Entferungen bis circa 100 km sind möglich und ausreichend, um den Kommunikationsbedarf in dieser Fläche abzudecken. An manchen Stellen findet sich hierfür auch die Bezeichnung Citynetz.

Wide Area Network (WAN)

Ein **WAN**, auch Weitverkehrsnetz genannt, zeichnet sich durch eine unbegrenzte geografische Ausdehnung aus. In seiner klassischen Form ist ein WAN ein Verbindungsnetzwerk für räumlich getrennte Rechenanlagen. In Bezug auf die Übertragungswege der Daten werden dabei in der Regel Leitungen von externen Firmen angemietet. Unternehmen können ein WAN z. B. als Verbindung zwischen zwei oder mehr LANs nutzen.

Ab und zu taucht auch noch der Begriff **Global Area Network (GAN)** auf. Er beschreibt im Grunde nur die Ausdehnung eines WANs auf eine weltweite und damit globale Dimension.

PowerLAN/Powerline

Ein PowerLAN oder Powerline Communication (PLC) verzichtet auf eine klassische Verkabelung und nutzt als Übertragungsmedium das Stromnetz. Die Informationen werden hier mittels Adapter über die normale Steckdose im Hausnetz übertragen. Das PowerLAN kommt vorzugsweise im privaten Bereich zum Einsatz.

Wireless Local Area Network (WLAN)

Ein **WLAN** ist eine Variante eines LANs und unterscheidet sich von diesem nur durch das verwendete Übertragungsmedium. Anstelle von Kabeln erfolgt der Einsatz von Funktechnologie (vgl. Kapitel 4.5). Gelegentlich wurden in diesem Zusammenhang auch die Begriffe **WaveLAN** und **Wi-Fi** verwendet.

Virtual Local Area Network (VLAN)

Bei einem **VLAN** wird das lokale Netzwerk in logisch voneinander getrennte Netzwerke unterteilt, wobei alle VLANs das gemeinsame physikalische Netz nutzen. Dadurch wird ein flexibles Design, z. B. für Arbeitsgruppen, unabhängig von ihrem physikalischen Standort, gebildet (vgl. Kapitel 12.4).

Network Attached Storage (NAS)

NAS sind Netzwerklaufwerke, die an das lokale Netzwerk angeschlossen werden, um die lokale Speicherkapazität zu vergrößern. Bei NAS erfolgt der Zugriff mit dateibasierten Protokollen, wie z. B. **Network File System (NFS)** oder **Server Message Block (SMB)/Common Internet File System (CIFS)**. Es gibt NAS-Storages für private Anwendungen wie für große Firmen. Sie werden unter Windows über die Netzwerkumgebung eingebunden (vgl. Kapitel 8.7).

Storage Area Network (SAN)

Ein **SAN** dient zur Auslagerung der Datenspeicherung in ein eigenständiges Netzwerk. In einem SAN werden Redundant Array of Independent Disk (RAID) Systeme zur Datenspeicherung über Fibre Channel oder Internet Small Computer System Interface (iSCSI) mit den Servern verbunden. iSCSI verwendet Kommandos des Small Computer System Interface (SCSI) Standards und überträgt diese mit Hilfe des Internet Protocols (IP). Ein SAN arbeitet blockorientiert und erscheint wie ein lokales Laufwerk (vgl. Kapitel 8.7).

Virtual Private Network (VPN)

Ein **VPN** ermöglicht eine verschlüsselte Verbindung zwischen Rechnern und Netzwerken (vgl. Kapitel 18.4).

2.5 Gründe und Ziele einer Vernetzung

Was von Computer-Netzen erwartet wird

Ein Netzwerk bietet Vorteile gegenüber einer Einzelplatzumgebung. Allerdings ist der Einsatz auch mit einem Aufwand verbunden. Umso mehr muss vor der Entscheidung für ein Netzwerk der zu erwartende Nutzen analysiert werden. Der Hauptgrund für die nicht unerheblichen Investitionen liegt letztendlich immer bei den zu erwartenden ökonomischen und unternehmerischen Vorteilen. Die im Folgenden dargelegten Gründe sprechen für eine Vernetzung.

Verbesserte Kommunikation

Netzwerke dienen verstärkt dem Informationsaustausch, der **Kommunikation**. Im abgeschlossenen firmeneigenen Netzwerk werden Neuigkeiten veröffentlicht, die jeder berechtigte Mitarbeiter abrufen kann. Eine Anbindung an das öffentliche Internet kann zentral erfolgen und stellt damit eine Plattform zum weltweiten Austausch von Informationen aller Art dar. Der Einsatz von E-Mails (elektronischer Post), Chat, VoIP oder Videokonferenzen ermöglicht eine gezielte, schnelle und kostengünstige Art der Verbindungsaufnahme zu spezifischen Adressaten.

Steigerung der Effektivität im Datenverbund

Wenn mehrere Personen am gleichen Thema zusammenarbeiten, war früher der Transport von Dateien über Disketten ein häufig benutzer Weg. Heute können Daten über das Netzwerk von einem Rechner auf einen anderen kopiert werden. Als Alternative könnten die Daten auch zentral an einem Ort gespeichert werden und alle Beteiligten erhalten die Erlaubnis, darauf zuzugreifen.

Allgemein wird hier von einem **Datenverbund** gesprochen. Dies bedeutet z. B. den Zugriff auf zentrale Datenbestände von jeder angeschlossenen Station aus und ist ein grundlegendes Ziel jeder Vernetzung.

Es können aber auch Datenbestände, die räumlich getrennt auf verschiedenen Rechnern gespeichert sind, logisch so gekoppelt werden, dass sie einem Benutzer als ein einziger großer Datenpool erscheinen.

Die Effizienz des Netzes hängt stark von der durchdachten Konzeption der Datenablage ab. Das Suchen und Abspeichern der Daten muss einer Logik folgen, die für den Benutzer nachvollziehbar und verständlich ist. Eine besondere Bedeutung kommt in diesem Zusammenhang der Versionierung zu. Dabei werden verschiedene Versionen einer Datei mit unterschiedlichen Zeitstempeln sowie vorgenommene Änderungen an dieser Datei vorgehalten. Im Bedarfsfall kann somit der Besitzer der Datei eine ältere Version dieser Datei wiederherstellen (beispielsweise nach einem versehentlichen Löschen von Inhalten der Datei oder der Datei selbst).

Einfache und effiziente Datensicherung

Ein oftmals unterschätzter Grund für die Vernetzung ist die **Datensicherung**. Wenn alle Daten einer Firma mit einem durchdachten Schema im Netzwerk abgelegt werden, kann ein einfaches Konzept zur automatischen Sicherung (z. B. auf Bänder) entwickelt werden. Da Daten nur auf wenigen Rechnern abgelegt werden, ist es einfacher, die Datensicherung durchzuführen und auf dem aktuellen Stand zu halten. Die Datensicherung ist ein Teilaспект des Datenverbundes. Vor allem NAS und SAN spielen in diesem Zusammenhang eine zentrale Rolle (vgl. Kapitel 8).

Kostensenkung im Funktionsverbund

Am deutlichsten wird dies am Beispiel der gemeinsamen Nutzung von Ressourcen. Wird z. B. ein hochwertiger Drucker angeschafft, kann dieser über das Netzwerk von allen Stationen verwendet werden. Wird z. B. ein neues Programm installiert, kann dies zentral auf einem Rechner geschehen und das Programm für die Nutzung durch angeschlossene Rechner freigegeben werden, wodurch der Wartungsaufwand sinkt.

Allerdings ist es manchmal schwierig, die eingesparten Hardware-Kosten mit den zu erwartenden Administrationskosten zu vergleichen. Denn der Betrieb eines Netzwerks bedeutet auf der einen Seite zusätzlicher Personalaufwand, auf der anderen Seite aber auch den Gewinn zusätzlicher Funktionalitäten für alle Netzwerkeinnehmer.

Allgemein kann bei einem Netzwerk von einem **Funktionsverbund** gesprochen werden. Dies bedeutet, dass verfügbare Ressourcen mithilfe eines Netzwerks allen Beteiligten zur Verfügung gestellt werden können.

Eine Ressource sind Geräte und Systeme zur Realisierung spezieller Funktionen in einem Gesamtnetzwerk, auf die alle autorisierten Benutzer oder Dienste zugreifen können.

Absicherung der Verfügbarkeit

Als **Verfügbarkeitsverbund** soll das Netz auch noch im Falle des Ausfalls einzelner Komponenten arbeitsfähig sein. Diese Anforderung an Netzwerke (**Redundanz**) wird erweitert durch den Anspruch, dass bei Ausfall einzelner Komponenten andere Komponenten deren Funktion übernehmen: so z. B. durch die Bereitstellung eines zweiten Datenbank-Servers, der für den Fall, dass der erste Datenbank-Server ausfällt, sofort die Funktion des ausgefallenen Servers übernehmen kann (Failover).

Darüber hinaus werden auch Teile des Netzwerks selbst sowie bestimmte Netzwerkkomponenten an kritischen Stellen oft redundant ausgelegt. Beispiele sind doppelte Leitungen und Switches etc. bei größeren bzw. wichtigen Installationen. Um Stromausfälle zu überbrücken und Störungen aus dem Stromnetz zu verhindern, sind unterbrechungsfreie **Stromversorgungen (USV)** wichtig.

Auch ist es wichtig, dass bei Ausfall eines Arbeitsplatz-Rechners jederzeit ein Ersatzgerät mit den gleichen Programmen und Daten zur Verfügung steht. Insbesondere dann, wenn Daten und Programme zentral auf einem Server liegen, können einheitliche und standardisierte Arbeitsplatz-Rechner genutzt werden.

Optimierung der Rechner- und Netzwerkauslastung

Dieser Aspekt wird häufig auch als **Lastverbund** (Cluster) bezeichnet und bedeutet, dass Prozesse, die hohe Rechenleistungen (CPU-Zeiten) benötigen, besser ausgestattete Rechner übernehmen. Ein Flaschenhals bei der Datenkommunikation ist häufig die Netzwerkschnittstelle. Indem mehrere Server identische Dienste bereitstellen, kann ein Client an jeweils den Server vermittelt werden, der die geringste Netzwerklast hat (**Network Load Balancing/NLB-Cluster**).

Optimierung der Wartung

Je großflächiger und komplexer die Komponenten des Netzwerks verteilt sind, umso wichtiger wird es, Werkzeuge zu haben, die eine leichte Administration und Wartung aller dezentralen Komponenten über das Netzwerk erlaubt. Die Möglichkeiten eines Netzwerkmanagements mit **Ferndiagnosen und Fernwartung** unterstützen einen schnellen Service in diese Richtung. Dazu kommt die zentrale Verwaltung von Hard- und Software (z. B. durch Einsatz von Gruppenrichtlinien).

Ausblick

Viele, der in den letzten Abschnitten geschilderten Ziele einer Vernetzung, sind inzwischen gelebte Praxis, sodass Raum entsteht, neue Herausforderungen zu integrieren. Im Folgenden seien deshalb exemplarisch drei Stichworte erwähnt, die zeigen, dass die Entwicklung von Netzwerken auf absehbare Zeit kein Ende finden wird.

Hinter dem Begriff **Konvergenz** von Netzen steht der Wunsch nach dem Zusammenwachsen von Daten- und Sprachnetz. Stichworte wie **Voice over IP** (VoIP) oder Telefonieren über das Internet beschreiben die Ansprüche und die erhofften Effekte einer solchen Entwicklung.

Auch der Ruf nach einer allumfassenden **Mobilität** von Mitarbeitern und der damit verbundenen ständigen Verfügbarkeit von Informationen überall auf der Welt stellt für Netzwerke eine große Herausforderung in der Zukunft dar.

Und nicht zuletzt steht das Thema **Sicherheit** in Netzwerken im Mittelpunkt. Dies betrifft den Zugang zu Informationen (z. B. die Vergabe von Zugriffsrechten), die gesicherte Übertragung der Informationen (z. B. mittels VPN und dem Netzwerkprotokoll Internet Protocol Security (IPsec)), die Protokollierung von Informationen (z. B. für die Rechtskonformität von Daten) sowie das Verhindern von Angriffen wie das Ausspionieren von Informationen.

2.6 Vorstellung des Fallbeispiels

Eine Musterfirma als Beispiel für konkrete Überlegungen

So wichtig die Theorie für die Vernetzung auch ist, so sehr steht und fällt das Thema mit praktischen Beispielen. Im Rahmen dieses Buchs wird dazu eine Musterfirma eingeführt, die mit einem kleinen lokalen Netz beginnt, dieses im Laufe der Zeit auf ein größeres zusammenhängendes Gelände ausdehnt und am Ende mehrere Filialen weltweit betreibt.

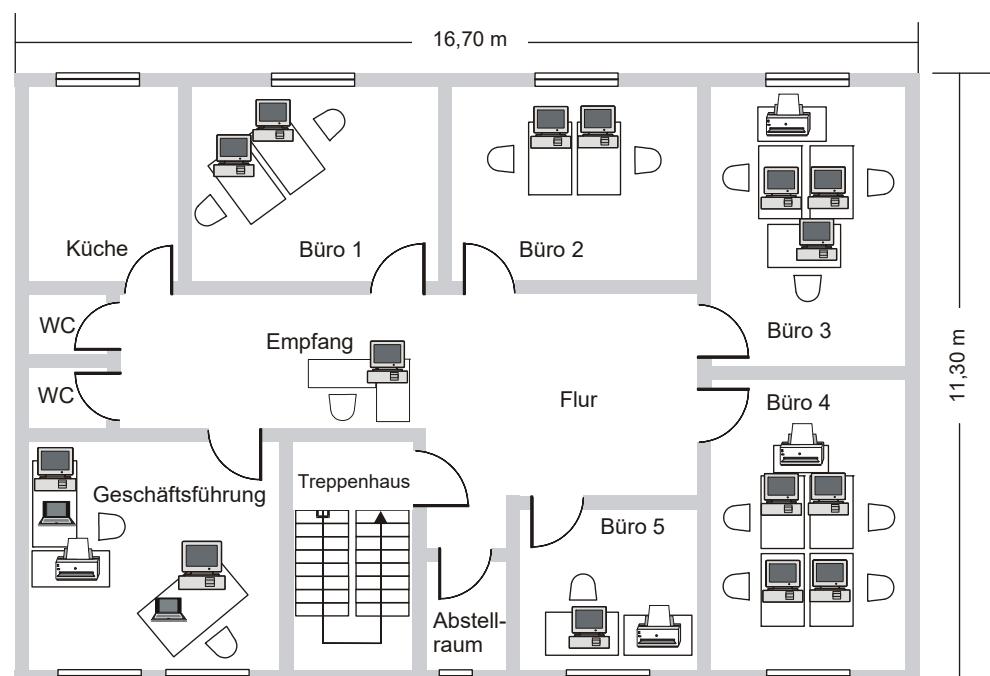
Am Anfang steht eine kurze Beschreibung dieser Firma. Eine Analyse der Ausgangssituation und das Formulieren der Ziele, die mit der Vernetzung erreicht werden sollen, folgen im ersten Praxisteil.

ABC GmbH

Die Firma namens ABC GmbH wurde 2019 gegründet und ist ein Dienstleistungsunternehmen mit Sitz in Deutschland. Für die Einrichtung ihrer neuen Büroräume wurde die komplette erste Etage eines zweistöckigen, frei stehenden Hauses angemietet. In einem zweiten Gebäude auf dem Gelände hat sich ein Start-up niedergelassen. Die Firma beschäftigt derzeit 14 Mitarbeiter, die ganz oder teilweise ihre täglichen Aufgaben am PC erledigen. Da sich das Geschäft im ersten Jahr schneller entwickelte als zunächst angenommen, drängt die Geschäftsführung auf eine Expansion in den nächsten 12 Monaten. Damit verbunden ist die Verdopplung der Mitarbeiterzahl.

Räumliche Aufteilung

Der Etagengrundriss für den Bezug der neuen Räumlichkeiten dokumentiert die geplante Einrichtung der Firma.



Grundriss/Etagenplan

Bevor eine Vernetzung in der Praxis umgesetzt werden kann, müssen zahlreiche Fragen zur Planung und dem späteren Betrieb beantwortet werden. Einige hiervon ergeben sich intuitiv und könnten folgende sein:

- ✓ Welche Kabelwege existieren und wie können die benötigten Kabel verlegt werden?
- ✓ Welche Kabeltypen sollten Verwendung finden?
- ✓ Wie werden die Daten über diese Kabel transportiert und welche Zusammenhänge ergeben sich aus den verwendeten Bestandteilen des Netzwerkes?
- ✓ Mit welchen Betriebssystemen wird derzeit gearbeitet und wie soll der Betrieb zukünftig aussehen?

Andere Fragen stellen sich zwangsläufig, während ein Basiswissen aufgebaut wird. Dabei spielt auch die Wirtschaftlichkeit und Zukunftsträchtigkeit der Planung eine sehr wichtige Rolle. Das Netzwerk soll für viele Jahre den zukünftigen Entwicklungen gewachsen sein. Die nachfolgenden Kapitel beleuchten die notwendigen Aspekte.

3

Topologien

3.1 Der Begriff Topologien

Abgrenzung physikalische – logische Topologien

Topologie ist die griechische Bezeichnung für die „Lehre von Orten“. In der Netzwerktechnik beschreibt der Begriff **physikalische** Topologie den Weg, auf dem Daten durch Kabel transportiert werden. Die **logische** Topologie hingegen beschreibt, nach welchen Regeln diese Daten transportiert werden. Unterscheidungen zwischen physikalischer und logischer Topologie sind teilweise historisch gewachsen.

Physikalische Topologie

Die physikalische Topologie eines Netzwerks bezieht sich auf die Verkehrswege. Hier wird der tatsächliche Aufbau eines Netzes beschrieben, d. h., in welcher Struktur die einzelnen Netzwerkkomponenten miteinander verbunden sind oder einfacher ausgedrückt, in welcher Form z. B. die Kabel verlegt oder an welchen Orten bei drahtloser Übertragung welche Antennen platziert werden.

Die physikalische Topologie ist vergleichbar mit einer Landkarte, auf der die verfügbaren Verkehrswege aufgezeichnet sind. Dieses Kapitel beschreibt die wichtigsten Grundformen von Topologien:

- ✓ Bus
- ✓ Stern
- ✓ Ring

Die Stern-Topologie hat sich im lokalen Netzwerkbereich durchgesetzt.

Logische Topologie

Die logische Topologie des Netzwerks beschreibt die grundlegenden Verkehrsregeln, die auf den Verkehrs wegen gelten. Sie beschreiben, mit welchen Regeln (Netzwerkzugriffsverfahren) auf das Übertragungsmedium zugegriffen werden darf bzw. wie darauf der Datenfluss erfolgt.

Zusammenhang zwischen logischer und physikalischer Topologie

In der praktischen Umsetzung existierte früher ein sehr enger Zusammenhang zwischen beiden Begriffen, sodass im Normalfall eine bestimmte physikalische Topologie eine bestimmte logische Topologie nach sich zog. In Zeiten von **VLANs** müssen jedoch die physikalische und die logische Topologie nicht mehr identisch sein.

Dennoch ist die Auswahl der physikalischen Topologie sehr wichtig, da sie Konsequenzen für etliche weitere Bereiche nach sich zieht. Sie bestimmt, welche Kabel verwendet werden können oder wie flexibel das Netzwerk für weitere Benutzer ausbaufähig ist. Außerdem hängen Aspekte wie Ausfallsicherheit, Geschwindigkeit, verfügbare Bandbreite und nicht zuletzt die anfallenden Kosten ebenfalls eng mit der gewählten Topologie zusammen.

So bietet z. B. ein Hub (vgl. Kapitel 13) physikalisch eine Sternstruktur, logisch aber eine Busstruktur, da alle eingespeisten Daten immer bei allen angeschlossenen Geräten ankommen. Ein Switch (vgl. Kapitel 13) dagegen arbeitet sowohl physikalisch als auch logisch als Sternstruktur, da standardmäßig die von einem Gerät verschickten Daten nur bei dem gewünschten Zielgerät ankommen (Ausnahme: Broadcasts und Multicasts).

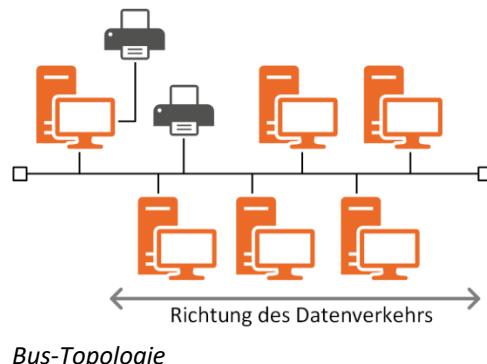
Eine Funkverbindung hat wie ein Hub physikalisch eine Sternstruktur zum Sender (zum zentralen Access Point) und logisch eine Busstruktur (alle verschickten Daten kommen bei allen Geräten an).

3.2 Bus

Alle Geräte nutzen dasselbe Medium

Die **Bus-Topologie** ist gekennzeichnet durch ein einzelnes zentrales Kabel, das als **Bus** bezeichnet wird. An diesen Bus werden alle Geräte angeschlossen und müssen sich dieses Medium teilen (Shared Medium, auch **Shared Media** genannt). Die Bus-Topologie wird auch als Linien- oder Reihennetzwerk bezeichnet.

Die Bus-Topologie ist eine passive Topologie, d. h., die angeschlossenen Stationen führen keine Wiederaufbereitung des Signals durch. Sie greifen die Signale vom Kabel ab oder senden auf das Kabel, wo sich das Signal in beide Richtungen ausbreitet. Hier wird von einem **Diffusionsnetz** gesprochen.



Auf dem Weg über die Kabel werden die elektromagnetischen Signale gedämpft und dadurch schwächer, sodass die mögliche Länge des Busses beschränkt ist. Durch den Einsatz von Signalverstärkern (**Repeater**, vgl. Kapitel 13) kann die Länge erweitert werden.

Die Bus-Enden müssen mit speziellen Abschlusswiderständen (Terminatoren) versehen werden, um ein rücklaufendes Signal, welches das Nutzsignal überlagert, auszuschließen. Terminatoren haben den gleichen Wellenwiderstand wie die Leitung, da ansonsten die Signale und damit die Daten gestört werden. Der **Wellenwiderstand** ist der Widerstand (Impedanz), den eine solche (theoretisch unendlich lange) Leitung einer bestimmten Hochfrequenz bietet.

Der größte Nachteil dabei ist, dass eine Störung des Übertragungsmediums an einer einzigen Stelle im Bus (defektes Kabel, lockere Steckverbindung etc.) den gesamten Netzstrang blockiert und zu einer aufwendigen Fehlersuche führt.

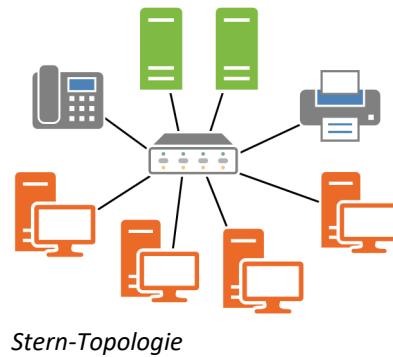
Trotz der Nachteile war die Bus-Topologie bei kleineren lokalen Netzen bis etwa Mitte der 90er-Jahre des letzten Jahrhunderts eine der am häufigsten verwendeten Technologien und ist eng verbunden mit dem Begriff Ethernet in den Formen 10Base5 und 10Base2. Heute spielt diese Art der Verkabelung keine Rolle mehr. Sie wurde weitgehend von der physikalischen Sternstruktur verdrängt.

3.3 Stern

Jedes Gerät nutzt ein eigenes Kabel

Bei einer **Stern-Topologie** wird jedes physikalisch angeschlossene Gerät separat mit einem zentralen Verteiler verbunden.

Als zentrale Komponente ist häufig ein **Switch** im Einsatz, an den die Endgeräte direkt angeschlossen werden. Der Switch realisiert eine Punkt-zu-Punkt-Verbindung zwischen zwei direkt kommunizierenden Endgeräten.



Der Switch (vgl. Kapitel 13.4) ersetzt heute vollständig die früher verwendeten Hubs als zentrale aktive Komponente.

Vorteile der Stern-Topologie

- ✓ Der Ausfall einer Station oder der Defekt eines Kabels hat keine Auswirkungen auf das restliche Netz.
- ✓ Aktive Verteiler wirken gleichzeitig als Signalverstärker.
- ✓ Bei entsprechender Funktionalität des Sternverteilers können zwei Stationen die volle Bandbreite des Übertragungsmediums für ihre Kommunikation nutzen, ohne dabei andere Stationen zu behindern. Dadurch erlaubt diese physikalische Topologie in der Summe höhere Datendurchsatzraten.
- ✓ Weitere Stationen und/oder Verteiler können problemlos hinzugefügt werden.

Nachteile der Stern-Topologie

- ✓ Große Kabelmengen
- ✓ Kosten für den Switch als zentrale Komponente
- ✓ Beim Ausfall des Verteilers ist kein Netzverkehr mehr möglich.

Einsatzgebiet

Die Stern-Topologie stellt die häufigste physikalische Netzwerkstruktur dar. Mit dem Aufkommen von Hub und Switch hat sie den physikalischen Bus komplett verdrängt. Da die Ethernet-Standards jedoch historisch auf dem Bus basieren, besteht hier eine Verknüpfung der physikalischen Stern-Topologie mit der logischen Bus-Topologie. Bei der Neuinstallation auf Etagen- oder Gebäudeebene wird heute neben Funkverbindungen (WLAN) nur noch diese Form der Verkabelung genutzt.

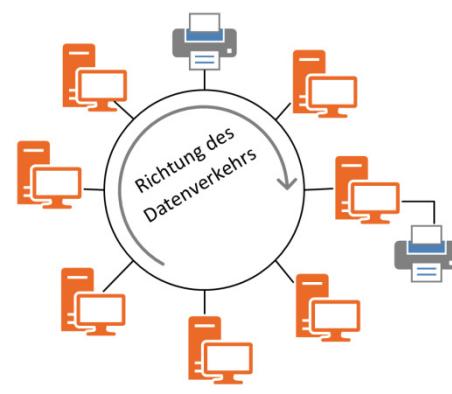
3.4 Ring

Jedes Gerät ist mit zwei Nachbarn verbunden

Bei einer **Ring-Topologie** bilden die Kabel eine geschlossene Form. Es gibt keinen Kabelanfang und kein Kabelende.

Alle Stationen werden als Elemente in diesen Ring aufgenommen, verarbeiten und verstärken die Signale, die auf dem Kabel ankommen, und schicken sie weiter.

Jede Station hat einen eindeutigen Vorgänger und einen eindeutigen Nachfolger. Datenverkehr findet immer nur in eine Richtung statt.



Der Aufwand bei der Kabelverlegung ist höher. Praktisch wurde dieses historische Verfahren im **Copper Distributed Data Interface (CDDI)** und **Fiber Distributed Data Interface (FDDI)** physikalisch umgesetzt. Als logische Topologie kam die Ring-Topologie (basierend auf einer physikalischen Stern-Topologie) zusätzlich im Token-Ring zum Einsatz und löste dabei die zuvor verwendete physikalische Ring-Topologie ab. Ring-Topologien spielen in der heutigen Zeit bis auf die **Automatisierungstechnik** keine Rolle mehr. Dort werden sie wegen ihrer Fehler-Toleranz noch gerne eingesetzt.

3.5 Mischformen

Topologie-Kombinationen

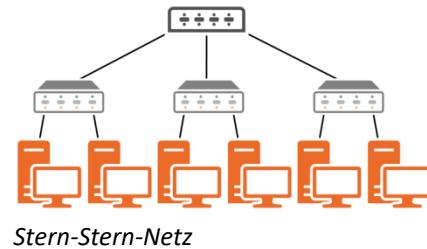
In der Praxis größerer Netzwerke können Kombinationen der aufgeführten Topologien entstehen, z. B. wenn vorhandene (Teil-)Netze beim Aufbau eines sogenannten Backbones zusammengeschlossen werden.

Backbone

Unter einem **Backbone** (Rückgrat) wird die physikalische Verbindung mehrerer Teilnetze verstanden. Es handelt sich damit um ein so genanntes **Hintergrundnetz**, das z. B. die Verbindung verschiedener Gebäude oder Etagen und deren jeweiliger Einzelnetze herstellt.

Stern-Stern-Netz

Ein Stern-Stern-Netz entsteht, wenn Switches jeweils das Zentrum eines Sterns bilden und diese wiederum über Kabel mit einem zentralen Switch oder Multilayerswitch (vgl. Kapitel 13.4) verbunden sind. An diesem werden in der Praxis auch wichtige Server direkt angeschlossen.



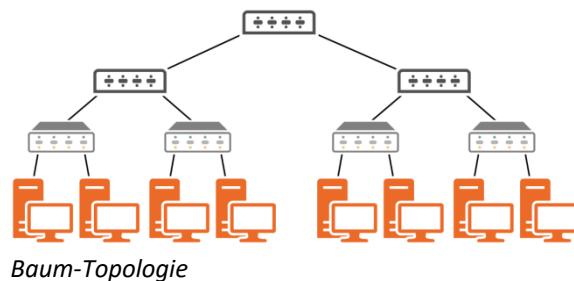
Beispiel: In einem dreistöckigen Bürogebäude ist in jedem Stockwerk ein Etagen-Switch in Stern-Topologie verkabelt. Die Etagen-Switches werden dann zentral (über Lichtwellenleiter) mit dem Backbone-Switch (oder Backbone-Multilayerswitch) verbunden.

Aus Sicherheitsgründen kann dieser Switch auch redundant ausgelegt sein, um beim Ausfall einer Verbindung oder des Gerätes die Kommunikation der Etagen aufrechtzuerhalten.

Baum

Eine **Baum-Topologie** wird so aufgebaut, dass, ausgehend von einer Wurzel, eine Menge von Verzweigungen zu weiteren Verteilungsstellen existiert. Es handelt sich damit um eine Erweiterung eines Stern-Stern-Netzes auf mehrere Ebenen.

Die Baumstruktur eignet sich gut für die Vernetzung eines Firmengeländes, bei dem von einem zentralen Punkt aus die verschiedenen Etagen oder Gebäude miteinander verbunden werden.

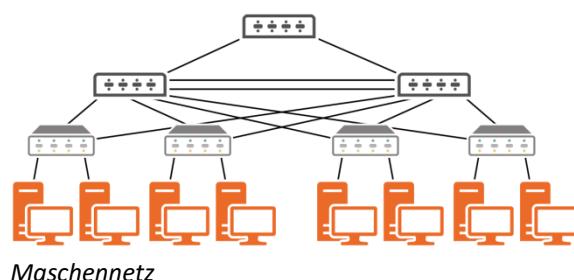


Maschennetz

In einem vermaschten Netz existieren zwischen den einzelnen Netzknoten jeweils mehrere Verbindungen.

Sinn dieser Vernetzung ist es, bei Ausfall einer Verbindung auf eine zweite, redundante Verbindung zurückzugreifen. Diese Art des Netzbaus ist in sicherheitsrelevanten lokalen Netzen und in Weitverkehrsnetzen zu finden.

Des Weiteren kann noch unterschieden werden, ob die redundanten Leitungen aktiv (load sharing, Lastenteilung) oder passiv (standby) eingesetzt werden.



Maschennetze benötigen viel mehr Verkabelung als andere Arten der Vernetzung. Werden sie mit Switchen realisiert, sind das Spanning-Tree-Protokoll bzw. meshing-fähige Switches erforderlich. Auch das Routing kann in solchen Netzwerken erheblich komplizierter werden (vgl. Kapitel 13).

3.6 Wolke (Cloud)

Von einer **Wolke** bzw. der **Cloud** spricht man hauptsächlich bei bestimmten Vernetzungen, wie dem Asynchronous Transfer Mode (**ATM**) u. a. und beim Cloud-Computing. Hier ist von außen nicht zu erkennen, welches Gerät in einem Netzwerk die Daten transportiert oder wo diese gespeichert sind.

Oft wird auch ein Netzwerk als Wolke dargestellt, wenn es sich um eine allgemeine Darstellung von einem Netzwerk handelt oder die interne Topologie nicht bekannt ist.

4

Übertragungsmedien

4.1 Einteilung der Medien

Verkehrswege

Datenverkehr erfolgt über ein Medium. Im Vergleich zum „normalen“ Verkehr, z. B. Güterverkehr, entsprechen diese Medien den Straßen, Luft- oder Wasserwegen, die zum Transport der Güter verwendet werden können. Grundsätzlich stehen für den Datenverkehr die Medien **Kupfer** und **Glasfaser** sowie **drahtlose Übertragung** zur Verfügung. Die ersten beiden lassen sich unter dem Stichwort leitergebundene Übertragungsmedien zusammenfassen, während bei der dritten Variante auch von leiterungsbundenen Systemen gesprochen wird.

Der Aufbau dieser Infrastruktur muss sehr gut geplant werden, da es sich meist um Investitionen mit mehrjähriger Perspektive handelt (Investitionsschutz). Hardware wie Computer oder Switches werden häufiger getauscht als die grundlegende Verkabelung. Dennoch ist z. B. die Verzehnfachung der Übertragungsgeschwindigkeit bei Umstellung von Fast Ethernet auf Gigabit-Ethernet unter Beibehaltung der vorhandenen Verkabelung möglich, wenn die Kabel dem Gigabit-Mindeststandard entsprechen.

Maßeinheiten für Übertragungsgeschwindigkeiten

Bei Angaben zu **Übertragungsgeschwindigkeiten** werden die Werte in **Bit** und kaum in **Byte** pro Sekunde angegeben. In diesem Buch werden dafür die Abkürzungen Bit/s bzw. Kbit/s, Mbit/s etc. verwendet. Für Byte pro Sekunde steht die Schreibweise B/s bzw. KB/s (Kilobyte pro Sekunde), MB/s etc.

Die Handhabung der Einheiten für Übertragungsgeschwindigkeiten sollen folgende Beispiele klären: 1 Kbit/s = 1.000 Bit/s, 1 Mbit/s = 1.000.000 Bit/s. Damit steht Kilo (K) für 10^3 und Mega (M) für 10^6 , was den **SI-Einheiten** (französisch: Système international d'unités, auch SI-Maßeinheiten bzw. SI-Basiseinheiten genannt) entspricht. Die SI-Einheiten gelten seit 1996 auch für die EDV, werden aber sehr zögerlich umgesetzt. Bei Kapazitätsangaben von Festplatten haben sie sich bereits durchgesetzt (die damit bedingten höheren Werte eignen sich besser zur Werbung).

Oft steht noch in der EDV bei der Angabe von Speicherkapazitäten (Arbeitsspeicher, Festplatten) K für 2^{10} und M für 2^{20} . Die Einheit hierfür wäre dann z. B. Kibibyte (KiB), Abkürzung für „Kilo Binär Byte“, Mebibyte (MiB) etc.

Leitergebundene und -ungebundene Übertragung

Für die leitergebundene Übertragung von Informationen werden im Unterschied zur leiterungebundenen (drahtlosen) Übertragung Medien in Form von Kabeln benötigt (metallische Leiter, Fasern aus Glas oder Kunststoff). Ein Kabel besteht dabei aus mindestens einer leitenden **Ader** bzw. **Faser**. Mehrere Adern werden durch entsprechende Isolationsschichten voneinander ge-trennt. Alle Adern eines Kabels werden von einer Schutzhülle, dem **Außenmantel**, umgeben.

Die Daten-Übertragung erfolgt über elektromagnetische Impulse oder Schwingungen (elektromagnetische Wellen, bei Glasfasern über sichtbares oder nicht sichtbares Licht (z. B. Infrarotlicht per Laser etc.) in unterschiedlichen Bereichen des Frequenzspektrums. Auf der Basis bestimmter Trägerfrequenzen werden Daten mit verschiedenen Modulationsverfahren aufbereitet (vgl. Kapitel 18.1). Sender und Empfänger müssen dementsprechend aufeinander abgestimmt sein.

Die leitergebundene Übertragung stellt im lokalen Netzwerk ein wired LAN dar. Die drahtlose Übertragung wird auch als Wireless LAN (**WLAN**) bezeichnet.

Übertragungseigenschaften

Bei der Entscheidung für oder gegen ein Übertragungsmedium sind neben den Kosten vor allem die Übertragungseigenschaften zu bedenken. Das betrifft insbesondere die **Dämpfung** und die **Störempfindlichkeit**.

Dämpfung beschreibt das Abschwächen der Datensignale mit zunehmender Entfernung. Der Sender muss so viel Energie in das Medium abgeben, dass am Empfänger noch hinreichend starke Signale ankommen. Ansonsten erhöht sich die Fehlerrate, bis keine Übertragung mehr möglich ist. Durch fehlende bzw. schlechte Verdrillung zusammengehörender Adern, z. B. bei der Verlegung, steigt die Dämpfung durch Abstrahlung (Antenneneffekt) ebenfalls an.

Die Qualität eines Netzwerkkabels wird insbesondere von der Übersprech- und der Signaldämpfung des Kabels bestimmt. Dämpfungswerte werden in **Dezibel** (dB) angegeben. Dies ist eine logarithmische Maßeinheit, was bedeutet, dass z. B. 10 dB den Faktor 10, 20 dB den Faktor 100 und 30 dB den Faktor 1000 darstellen.

Die **Übersprechdämpfung** gibt an, wie stark sich Signale verschiedener Adern in einem Kabel gegenseitig beeinflussen. Diese Übersprechdämpfung sollte möglichst groß sein und wird durch Isolation der Leitung und andere Maßnahmen (z. B. spezielle Verdrillung der Adernpaare) optimiert. Sie wird auch als Near End Cross Talk (NEXT) bezeichnet. Bei Glasfasern gibt es kein Übersprechen und damit auch keine derartige Dämpfung.

Die **Signaldämpfung** dagegen gibt an, wie stark sich Signale auf einer bestimmten Strecke abschwächen. Die Signaldämpfung sollte möglichst gering sein, um eine große Reichweite des Signals zu erreichen.

Bei Kupferkabeln wird die Dämpfung in drei Werten angegeben: **Dämpfungsmaß**, **NEXT** und **Attenuation To Crosstalk Ratio** (ACR), dem Dämpfungs-Übersprech-Verhältnis. Es bezeichnet die Differenz zwischen NEXT und Dämpfungsmaß.

Störempfindlichkeit beschreibt, wie das Medium auf Störeinflüsse bzw. Störstrahlungen von außen reagiert. Dies betrifft z. B. Störungen durch Elektromotoren, andere elektrische Leiter, die in der Nähe zum Netzwerkkabel verlegt sind oder allgemein Geräte, die elektromagnetische Felder erzeugen. Hier kann eine Verbesserung der Störempfindlichkeit durch eine zusätzliche Abschirmung der Adern und Kabel erreicht werden.

Verlegung

Abhängig von der geplanten Kabelverlegung müssen Außenmantel und Kabelaufbau folgenden Kriterien entsprechen:

- ✓ **Zug- und Abriebfestigkeit:** Wie reagiert das Kabel auf mechanische Belastungen?
- ✓ **Flexibilität:** Wie leicht ist das Kabel zu verlegen? Welcher minimale Biegeradius ist für das Kabel zulässig, wenn es z. B. in Kabelschächten um Ecken herum verlegt werden muss?
- ✓ **Nagetierschutz:** Besonders im Außenbereich wichtig.
- ✓ **Temperaturbeständigkeit, Flammwidrigkeit:** Besonders in Gebäuden zu beachten. Wie verhält sich das Kabel im Brandfall? Werden eventuell giftige Gase freigesetzt?



Aufgrund der steigenden **Anforderungen** beim Brandschutz sollten nur noch Twisted-Pair-Kabel (vgl. Kapitel 4.3) mit **halogenfreiem** (ohne PVC) und flammwidrigem Außenmantel, z. B. definiert als **Low Smoke and Fume (LSF)**, **Low Smoke Zero Halogen (LSOH)** etc. eingesetzt werden. Brennendes PVC erzeugt Salzsäurenebel, dessen Einatmung tödlich ausgehen kann. Zudem wird PVC nur durch umstrittene Weichmacher flexibel.

- ✓ Je nach Einsatzgebiet (Büro, Lagerhalle, Produktionshalle) gibt es sehr unterschiedliche Anforderungen und dementsprechend auch unterschiedliche Ausführungen von Kabeln.
- ✓ Bestimmte Kabeltypen sind eng verbunden mit bestimmten Ausprägungen von Netzwerken. Um Zuordnungen zu vereinfachen, befinden sich in den folgenden Abschnitten jeweils Hinweise auf entsprechende praktische Umsetzungen.



Ergänzende Lerninhalte: *Weiterführende Informationen.pdf*

In diesem Dokument finden Sie u. a. vergleichende Übersicht mit den wichtigsten Kenndaten zu den verschiedenen Kabeltypen.

4.2 Koaxialkabel

Einsatzgebiet und Beschreibung

Koaxialkabel gibt es in unterschiedlichen Ausführungen für verschiedene Einsatzgebiete, wie z. B. im Hochfrequenzbereich oder in der Antennentechnik. Im Bereich von Computernetzwerken spielen die als Koax- oder auch **BNC-Kabel** benannten Übertragungsmedien heute keine Rolle mehr, stellten aber lange Zeit eine weitverbreitete Form der Verkabelung dar. Wegen der unterschiedlichen Außendurchmesser von 10mm und <=6mm, wurden diese u. a. auch als **Thick-Ethernet** (der Norm entsprechend 10Base5) und **ThinEthernet** (10Base2) bezeichnet.

4.3 Twisted-Pair-Kabel (TP)

Einsatzgebiet und Beschreibung

Twisted-Pair-Kabel in der einfachsten Form bestehen aus zwei isolierten Adern, die umeinander gedreht (twisted, geschlungen, verdrillt) sind. Die Verdrillung reduziert die Empfindlichkeit gegen Störstrahlung von außen, von benachbarten Adernpaaren, sowie die Abstrahlung nach außen, indem sich die Wirkung der Magnetfelder, die in einem durchströmten Leiter entstehen, durch die enge Verdrillung gegenseitig aufhebt. Mehrere verdrillte Adernpaare können nun zu einem Kabel zusammengefasst werden, wobei die einzelnen Adernpaare unterschiedlich stark verdrillt werden müssen, um einen gleichmäßigen Durchmesser des Kabels zu erreichen.

Ursprüngliches Einsatzgebiet war der Fernmeldebereich, inzwischen aber ist die Twisted-Pair-Verkabelung auch im LAN das Standardmedium und eng verbunden mit einer physikalischen Stern-Topologie. Die maximal mögliche Distanz zwischen einem Computer und der zentralen Komponente (Switch, Multilayerswitch, Router) kann bis zu 100 Metern bei Übertragungsraten von bis zu 10 Gbit/s betragen.

Unshielded Twisted-Pair (UTP)

Unshielded (ungeschirmt) bedeutet, dass die einzelnen verdrillten Adernpaare keine extra Einzelabschirmung besitzen.



UTP-Kabel sind anfälliger gegenüber elektromagnetischen Störfeldern. Neben möglichen Einstrahlungen von außen, z. B. wenn in einem Kabelschacht mehrere Kabel eng beieinander liegen, ist ein weiteres Problem das Übersprechen zwischen den Adernpaaren eines Kabels, während der Übertragung von sehr hohen Frequenzen. UTP-Kabel ermöglichen dagegen einen geringeren Verlegeaufwand und ein aufwendiger Potenzialausgleich für die Schirmung entfällt.

Shielded Twisted-Pair (STP)

Shielded (geschirmt) bedeutet, dass jedes Adernpaar einzeln abgeschirmt wird. Das Kabel insgesamt (alle Adernpaare) wird durch eine Ummantelung mechanisch geschützt. Dadurch sind STP-Kabel gegenüber elektrischen Störeinflüssen weniger anfällig als UTP-Kabel.



Screened

Sowohl UTP- als auch STP-Kabel gibt es in einer S-Version, bei der zusätzlich die Kabel, bestehend aus mehreren Adernpaaren, durch einen Gesamtmetallschirm (Screen) vor Störstrahlungen von und nach außen abgesichert sind. Die Bezeichnungen für Kabel dieser Art sind S/UTP- bzw. S/STP-Kabel. Dieser Gesamtmetallschirm kann auch als Folie ausgeführt werden. Dann spricht man von F/UTP- bzw. F/STP-Kabel.

Die Bezeichnung der erwähnten Twisted-Pair-Kabeltypen entspricht dem Standard **ISO IEC 11801**.

Litze und Massivleiter

Eine weitere Unterscheidung betrifft die Leiter, die entweder in Litzenform (mehrere verselte Einzeldrähte) oder mit massivem Kern angeboten werden. Verseltes Kabel ist viel flexibler und biegsamer, aber da die Signaldämpfung um einiges höher ist, sollte es nur für kurze Entfernungen zwischen Netzwerkkarte und Wanddose oder innerhalb von Verteilerschränken als Patchkabel (engl. „to patch“ = zusammenschalten, flicken) verwendet werden.

Massivleiterkabel haben eine geringere Dämpfung, dürfen aber nicht geknickt oder zu stark gebogen werden. Sie kommen daher bei dauerhaften Installationen zum Einsatz, z. B. zwischen Verteilern und Anschlussdosen oder im Backbone-Bereich.

Kategorien

TP-Kabel sind in verschiedene, sogenannte Kategorien (1 bis 7) eingeteilt, die Auskunft über die Eigenschaften der Kabel geben. Bei den für die Netzwerktechnik relevanten Kategorien werden vier verdrillte Adernpaare verwendet. Der Wellenwiderstand beträgt überwiegend 100Ω , vereinzelt auch 150Ω .

Zuständig für die Standardisierung sind das Gremium der Electronic Industries Alliance (**EIA**) / Telecommunications Industry Association (**TIA**) und die Internationale Organisation für Normung (ISO). Zuständig für die Ableitung entsprechender nationaler Normen ist das Deutsche Institut für Normung (DIN). Da die Bedeutung der Netzwerktechnik jedoch weiterreichend ist, wurden die Standards u. a. in den Europanormen (EN) DIN EN 50173 und EN 50174 abgefasst.

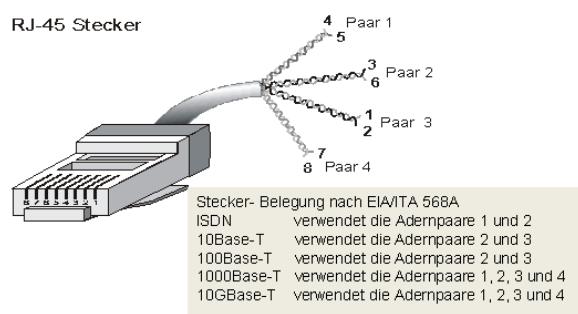
Wurden in der Vergangenheit noch Kategorie-5-Kabel verwendet, sollten heute bei einer Neuvorkabelung im LAN-Bereich die Kategorien 6 und 6A eingesetzt werden, da diese auch 10 Gbit/s unterstützen, bzw. Kategorie 7 und 7A für höhere Übertragungsraten. Die frühere Kategorie 5e ging 2003 in die Spezifikation von Kategorie 5 ein. Die Kategorie 5 (CAT 5 bzw. CAT 5e) reicht für bis zu 1 Gbit/s, für kurze Entfernungen von etwa 20 bis 40 m (je nach Aufbau der Abschirmung) auch für 10-GBit-Ethernet.

Plus **Ergänzende Lerninhalte:** Weiterführende Informationen.pdf

In diesem Dokument finden Sie u. a. eine Übersichtstabelle mit genauen Spezifikationen und Erläuterungen zum Einsatzgebiet der einzelnen Kategorien.

RJ-45/GG-45-Stecker

Für den Anschluss von Twisted-Pair-Kabeln an die Netzwerkkarte bzw. an einer zentralen Komponente wie z. B. einem Switch werden **RJ-45-Stecker** benutzt. Sie ähneln den Telefonsteckern (RJ-11), sind jedoch breiter und besitzen vier Adernpaare. Für Twisted-Pair-Kabel der Kategorie 7 werden dagegen die Steckertypen GG-45 (abwärtskompatibel zum RJ-45-Stecker) und der dazu nicht kompatible TERA-Stecker verwendet.



RJ-45-Stecker mit Belegung nach EIA/TIA 568A

Verteilerschränke/Patch-Panels

Da bei einer sternförmigen Verkabelung jeder Rechner über ein eigenes Kabel mit dem zentralen Verteiler (Switch) verbunden ist, gibt es verschiedene Komponenten, die die Verkabelung vereinfachen:

- ✓ **Verteilerschränke** ① und -einschübe in 19-Zoll-Bauweise (Standard) bieten eine einfache, komfortable und strukturierte Möglichkeit, zentral eine Vielzahl von Verbindungen zu organisieren.
- ✓ Darin installierte **Patch-Panels** ② dienen dazu, eingehende Kabel aufzunehmen und über **Patchkabel** ③ mit den Switches ④ zu verschalten.



Wanddose

Beim Anschluss der Endgeräte in den einzelnen Büros werden häufig Wand- oder Aufputzdosen verwendet.

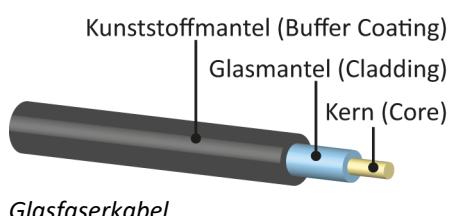
Die Verkabelung von Patch-Panels in Verteilerschränken und in den Wanddosen erfolgt zumeist über eine Schneid-Klemm-Technik, die als **LSA**-Technik (löt-, schraub- und abisolierfreie Technik) bezeichnet wird. Durch ein Anlegewerkzeug (auch Auflegewerkzeug genannt) wird jeder Draht einzeln in Schneidklemmen aus Metall gepresst und mit einer Schneidvorrichtung am Werkzeug meist auch im selben Arbeitsgang abgeschnitten.

Ausführliche Beschreibungen zur Verkabelung finden Sie im HERDT-Buch *Netzwerke – Netzwerktechnik*.

4.4 Glasfaserkabel

Beschreibung

Glasfaserkabel, oft auch **Lichtwellenleiter** (LWL) genannt, bestehen aus einem dünnen zylindrischen Glasfaden (**Kern** oder **Core**), der von einer konzentrischen Glasschicht (**Cladding**) umgeben ist. Das Ganze wird von einem Schutzschirm ummantelt, der für Zugfestigkeit und Bruchsicherheit sorgt.



Die Signalübertragung erfolgt in der Regel über Lichtimpulse unidirektional, d.h. nur in eine Richtung (**Simplex**). Für Datenübertragung in beide Richtungen sind dann zwei Fasern (**Duplex**) pro Kabel notwendig. Eine Ausnahme besteht, wenn die beiden Übertragungsrichtungen unterschiedliche Wellenlängen nutzen. Allerdings ist es üblich, mehrere Fasern in einem Kabel (Mantel) zusammenzufassen (nicht bei Patchkabeln).

Die Fähigkeit, Licht in einem Kabel zu „leiten“, ist dabei durch die Reflexion zwischen Kern und Mantel bedingt. Die Impulse werden mittels einer Laserlichtquelle, einem Vertical Cavity Surface Emitting Laser (VCSEL) oder einer Lumineszenz-Diode (LED = Light Emitting Diode) in den Kern übertragen. Ein Laser nutzt für die Übertragung eine einzelne Wellenlänge (Monomode). Es können auch mehrere Laser mit unterschiedlichen Wellenlängen gleichzeitig über eine Faser senden. Damit ist pro Wellenlänge eine Verbindung möglich. Eine LED oder ein VCSEL benutzt dagegen ein zusammenhängendes Spektrum von Wellenlängen (Multimode) für die Übertragung.

Verwendbare Wellenlängen

Die Dämpfung des Lichts in der Glasfaser fällt sehr unterschiedlich aus und ist abhängig von der Wellenlänge des eingesetzten Lichts. Die besten Werte ergeben sich bei 850 Nanometer (nm), 1310 nm und 1550 nm, sodass diese Wellenlängen auch als Übertragungsfenster verwendet werden.

Monomode und Multimode

LWL werden in zwei Kategorien unterteilt: Monomode-LWL und Multimode-LWL. Der Mode bezeichnet hierbei die Zahl der möglichen unterschiedlichen Ausbreitungswege in der Faser. Ist der Kern klein genug (z. B. 9 µm), dann kann sich nur noch eine Welle in der Faser ausbreiten. Man spricht in diesem Fall von einer Monomodefaser. Im deutlich größeren Kern der Multimodefaser können hingegen mehrere Modes gleichzeitig in unterschiedlichen Winkeln verlaufen.

Monomode-LWL

Der Kerndurchmesser einer Mono- oder **Singlemode**-Faser beträgt 3 µm bis 9 µm. In diesem dünnen Kern verläuft das Licht quasi parallel, wodurch die Dispersion (siehe unten) minimal ausfällt. Ein Injektionslaser bringt das Licht (1310/1550 nm) in die Faser. Mit Monomode-Fasern sind Band-breiten-Längen-Produkte von über 100 GHz x km möglich. Die Eckdaten werden über die Norm OC1 zur Verfügung gestellt.

Der Cladding-Durchmesser beträgt ca. 50 µm bis 150 µm. In Datennetzen kommen in der Regel Fasern mit 9 µm Kern und 125 µm Mantel (Bezeichnung 9/125) zum Einsatz. In einem Kabel können sich viele Fasern befinden (bis zu 144 und mehr).

Da der Einsatz von Monomode-Fasern teuer ist, werden diese im Backbone-Bereich von Telefongesellschaften und großen Netzwerkbetreibern (Primärverkabelung) zur Überbrückung von größeren Entferungen verwendet. Ein wesentlicher Kostenfaktor ist dabei der Einsatz (im Vergleich zu Komponenten der Multimode Technik) teurerer aktiver Komponenten, da diese wegen der geringen Faserdurchmesser, Laser anstelle von VCSEL/LEDs verwenden müssen. Allerdings werden mit steigenden Übertragungsraten Monomode-Kabel vermehrt auch über kürzere Entferungen (ab ca. 500 Meter) eingesetzt.

Multimode-LWL

Multimode-Kabel sind vielseitig einsetzbar (bis hin zum Anschließen einzelner Arbeitsstationen) und werden über die Kategorien OM1-OM5 definiert. Der Kern der gängigen Multimode-Fasern ist mit $62,5 \mu\text{m}$ bzw. $50 \mu\text{m}$ Durchmesser deutlich dicker als der einer Monomode-Faser, wodurch die Streuung der Signallaufzeiten (Dispersion) auch größer wird. Der Cladding-Durchmesser ist mit $125 \mu\text{m}$ in allen Kategorien gleich. Es werden VCSEL/LEDs als Sender eingesetzt.

Mit Multimode-Fasern ist ein Bandbreiten-Längen-Produkt von ca. $1 \text{ GHz} \times \text{km}$ erreichbar. Kabel mit $50 \mu\text{m}$, die bereits Mitte der 70er-Jahre vorgestellt wurden, bieten eine Bandbreite von mindestens $500 \text{ MHz}/\text{km}$ und sowohl bei 850 nm als auch bei 1310 nm eine Reichweite von 500 Metern. Kabel mit $62,5 \mu\text{m}$, die 1986 eingeführt wurden, erreichen $160 \text{ MHz}/\text{km}$ und eine Reichweite von 220 Metern bei 850 nm und ebenfalls 500 Meter bei 1310 nm mit einer Geschwindigkeit von 1 Gbit/s bzw. 2 Kilometer bei einer Geschwindigkeit von 100 Mbit/s .

Die Reichweitenangaben können je nach Kabelqualität stark variieren. Eine Verringerung/Erhöhung der Datenrate bewirkt eine größere/kleinere Reichweite, das gilt es, beispielsweise beim Umstieg auf 10 Gbit/s , zu bedenken.

Tabellarische Darstellungen der Kategorien OM1-OM5 finden Sie unter:

- ✓ <https://www.opternus.de/wissen/om-klassifizierung-der-multimodefasern>
- ✓ <https://de.wikipedia.org/wiki/Lichtwellenleiter>

Dispersion im LWL

Die nutzbare Bandbreite steht in engem Zusammenhang mit der **Dispersion**. Ein Teil des Lichts durchläuft die Glasfaser nahezu geradlinig, während ein anderer Teil zwischen den Leiterwänden hin und her reflektiert wird.

Für diesen Teil des Lichts verlängern sich die Strecke und damit auch die Signallaufzeit, wodurch die Dauer eines beim Empfänger eintreffenden Lichtimpulses zeitlich „gedehnt“ wird. Signale können nur so schnell eingespeist werden, wie sie nach der Übertragung auch wieder sauber voneinander getrennt werden können.



Die obige Grafik zeigt, wie sich ein Signal durch Dispersion verändert, je länger es unterwegs ist. ① zeigt das Ursprungssignal, ② die Auswirkung der Dispersion in einiger Entfernung und ③ die Auswirkung der Dispersion in noch größerer Entfernung.

Gradientenindex/Stufenindex

Monomodefasern sind prinzipiell Stufenindexfasern. Hierbei ist jedoch der Kern so klein, dass der Lichtstrahl kaum einen Zick-Zack-Weg einschlägt und somit Dispersion nicht auftritt, was ideal für lange Wege ist.

Multimodefasern lassen sich weiter aufteilen in Fasern mit **Gradientenindexprofil** bzw. **Stufenindexprofil**.



Um die Dispersion bei Multimode-Fasern zu verringern, wird üblicherweise mit Gradientenindexfasern gearbeitet (auch als **Gradientenprofil** bezeichnet). Bei ihnen fallen die Dichte und damit der Lichtbrechungsindex von der Kernmitte zum Mantel hin parabolisch ab. Dadurch werden die Lichtstrahlen auf ihrem Weg von innen nach außen allmählich gebogen und nicht einfach reflektiert. Da die Strahlen am Rand durch die geringere Dichte schneller vorankommen als diejenigen im Kern, gibt es kaum einen Zeitunterschied (Dispersion), wenn am Ziel die Strahlen ankommen.

Bei den Stufenindexfasern existiert zwischen Kern und Mantel ein abrupter Übergang von einem Brechungsindex zum nächsten.

Bandbreiten-Längen-Produkt

Unter **Bandbreite** wird der Frequenzbereich verstanden, der zwischen der oberen und der unteren Grenzfrequenz liegt, die auf dem entsprechenden Medium übertragen werden kann.

Lichtwellenleiter unterscheiden sich vor allem durch den Kerndurchmesser, welcher wiederum auf die realisierbaren Datenübertragungsraten Einfluss hat. Das sogenannte Bandbreiten-Längen-Produkt gibt an, bei welchen Kabellängen mit welchen Übertragungsraten gearbeitet werden kann. Bei einem Bandbreiten-Längen-Produkt von 1 GHz x km kann z. B.

- ✓ bei 0,5 km Länge mit einer Bandbreite von 2 GHz gearbeitet werden,
- ✓ bei 1 km Länge mit einer Bandbreite von 1 GHz gearbeitet werden,
- ✓ bei 2 km Länge mit einer Bandbreite von 500 MHz gearbeitet werden.

Verbindungselemente

Problematisch und dementsprechend teuer beim Einsatz von Lichtwellenleitern ist das Verbinden bzw. Verlängern der Fasern. Feste Verbindungen werden durch Verschweißen (Spleißen) der Enden der einzelnen Fasern erreicht. Die Qualität der Spleißverbindung ist sehr wichtig, da vor allem an diesen Übergängen eine Signaldämpfung auftritt. Eine zu hohe Dämpfung mindert die Übertragungsqualität und damit auch die Reichweite. Sie kann bis hin zur Unbrauchbarkeit der Kabel führen.



SC-Duplex-, ST-Simplex- und MTRJ-Stecker

Von der Vielzahl an **Steckerverbindungen** für LWL, werden hier nur einige der bekanntesten vorgestellt, wobei die Auflistung auch das Problem deutlich macht. Es gibt keinen einheitlichen Standardstecker:

- ✓ **SC-Duplex-Stecker** (subscriber connector): Normstecker für Glasfaserkabelung bis zum Endgerät mit automatischer Verriegelung und Verdreh sicherung.
- ✓ **ST-Stecker** (straight tip) mit Bajonettschluss waren entsprechend IEEE 802.3 für die Verwendung in 10Base-T-Netzen vorgesehen.

- ✓ **MTRJ-Stecker (mechanical transfer)** sind Duplex-Stecker, die bezüglich ihrer Maße und Verriegelungssysteme vergleichbar mit RJ-45-Steckern sind. Sie lösten den SC-Duplex-Stecker bei der Anbindung von Arbeitsstationen mit Glasfaser (**Fibre to the desk**) ab und wurden inzwischen selbst vom LC-Stecker verdrängt.
- ✓ **LSA-Stecker** werden auch als DIN-Stecker 47256 bezeichnet und vor allem in Deutschland in der WAN-Technologie verwendet.
- ✓ **FC/PC-Stecker (fiber connector)** mit Schraubverschluss ohne Verdrehschutz werden in Europa selten eingesetzt, sind aber Standard in Asien.
- ✓ **LC-Stecker:** kompakter Stecker als Alternative zu MTRJ, inzwischen weitverbreiteter Standard.
- ✓ **E2000:** Die wichtigsten technischen Daten entsprechen denen des SC- oder des LSA-Steckers, der Stecker selbst ist aber kompakter als ein SC-Duplex-Stecker.

Siehe auch:

- ✓ <https://de.wikipedia.org/wiki/LWL-Steckverbinder>
- ✓ <https://www.opternus.de/wissen/kleine-lwl-stecker-lehre>

Vorteile von Lichtwellenleitern

- ✓ Hohe Übertragungsraten (bis zu $n \times 10$ Gigabit) und Reichweiten (technisch über 100 km machbar) durch das Wellenlängenmultiplexverfahren (**Wavelength Division Multiplex, WDM**, paralleles Übertragen von Daten) realisierbar
- ✓ Gute **Sicherheit** sowohl gegen Abhören als auch gegen Störstrahlungen
- ✓ Akzeptable Kabelkosten
- ✓ Galvanische Trennung der Stationen, d. h. keine elektrisch leitende Verbindung und damit Vermeidung von elektrischen Problemen z. B. Potenzialausgleichströme.

Nachteile

- ✓ Teure Gerätetechnik als Hauptnachteil
- ✓ Hoher Konfektionsaufwand (Installation über spezialisierte Firmen)
- ✓ Schwachstelle Steckertechnologie (die Verbindung zweier Kabelstränge ist sehr aufwendig)
- ✓ Relative Empfindlichkeit der Kabel gegenüber mechanischen Belastungen, insbesondere bei den Anschlusskabeln zu Endgeräten

Einsatzgebiet

Die Integration von Daten, Video und Sprache (Voice) in einem Netzwerk erfordert eine einheitliche physikalische Struktur. Eine strukturierte Verkabelung (vgl. Kapitel 12.2) oder universelle Gebäudeverkabelung (**UGV**), stellt das Konzept für eine zukunftsorientierte und anwendungsneutrale Netzwerkinfrastruktur bereit. Damit werden Fehlinstallationen und Erweiterungen vermieden und die Installation neuer Netzwerkkomponenten erleichtert. Als physikalisches Medium kommt u. a. das Twisted-Pair-Kabel zum Einsatz.

Die beschriebenen Kabeltypen werden standardkonform als strukturierte Verkabelung eingesetzt. Bei der strukturierten Verkabelung zwischen Etagen (Sekundärbereich) und Gebäuden (Primärbereich) sollten grundsätzlich Glasfaserkabel verwendet werden. Der Grund dafür liegt in der elektrischen Entkopplung der Signale zwischen den Etagen und den hohen Datenübertragungsraten.

4.5 Drahtlose Übertragung per WLAN

Vielseitiges Einsatzgebiet

Die **Übertragung** von Informationen ohne Kabel ist mittlerweile in vielen Lebensbereichen als praktische Alternative eingezogen. Von der Fernbedienung eines Fernsehers über drahtlose Lautsprecher bis zum Smartphone gibt es viele Beispiele für die Umsetzung dieser Technik. Dabei werden Funksignale in frei verfügbaren Frequenzbändern anstelle von Kabeln für die Datenübertragung verwendet.

Vorteile

- ✓ Es sind keine baulichen Maßnahmen innerhalb eines Gebäudes nötig.
- ✓ Die baulichen Maßnahmen zwischen verschiedenen Gebäuden sind geringer als bei einer Verkabelung.
- ✓ Höhere Mobilität, da theoretisch jeder Punkt eines Firmengeländes drahtlos erreichbar ist.

Nachteile

- ✓ Oft geringere Datenübertragungsraten als bei Kabeln, die abhängig von Hindernissen sind.
- ✓ Anfällig für Störeinflüsse und Abhören durch Unbefugte.
- ✓ Probleme mit Ausleuchtung und Reflexionen.
- ✓ Bei vielen gleichzeitigen Nutzern an einem WLAN-Zugang bricht die Übertragungsrate ein (Shared Media).

Wi-Fi Alliance/WECA

Trotz aller akzeptierten Normen sind die Geräte der unterschiedlichen Hersteller nicht immer hundertprozentig kompatibel. Dies liegt zum Teil an der nicht vollständigen Implementierung der jeweiligen Standards oder an den proprietären Erweiterungen, die Firmen ihren Produkten hinzufügen. Um hier für mehr Klarheit zu sorgen, wurde 1999 die **Wireless Ethernet Compatibility Alliance (WECA)** gegründet.

An dieser Organisation, die inzwischen in Wi-Fi Alliance umbenannt wurde und ein informatives Portal unter <https://www.wi-fi.org/> betreibt, wirken über 200 namhafte Hersteller wie z. B. Apple, Cisco, IBM, Intel, Microsoft oder Sony mit. Ziel ist es, Komponenten auf Kompatibilität zum IEEE 802.11 Standard (vgl. Abschnitt IEEE 802.11) und Interoperabilität in Funknetzen zu testen. Allerdings geschieht dies mit eigenen Testkriterien und mit eigenem Zertifizierungslogo. Das Konsortium arbeitet auch an der Verschlüsselungstechnik **Wi-Fi Protected Access (WPA)** für die drahtlose Übertragung.

Sicherheit von WLANs als kritischer Bereich

Gerade im Bereich Sicherheit gibt es bei WLANs einige Punkte zu beachten, die sich auch in einem etwas größeren Konfigurationsaufwand äußern. Die sogenannte **Service Set Identifier (SSID)** kann eine eindeutige Identifikation (Firmenname etc.) enthalten, damit bei Problemen eine Kontaktaufnahme mit dem Betreiber möglich ist. Ein Verbergen bringt nicht viel, da die SSID in jedem Paket mitgeschickt wird und es Programme gibt, die auch verborgene SSIDs auslesen können.

Eine versehentliche Verbindung durch Unbefugte ist bei verschlüsselten Zugängen nicht zu erwarten. Es gibt auch Empfehlungen, als SSID eine zufällige Zeichenfolge einzugeben, damit die SSID keine Rückschlüsse auf den Betreiber zulässt.

Eine Zugangskontrolle kann auch über Benutzernamen, Passwörter, Zertifikate etc. mit Hilfe von **Remote Authentication Dial-In User Service (RADIUS)** zur Authentifizierung nach **IEEE 802.1x** erfolgen. Besonders im Firmeneinsatz über ein weiträumiges Gelände ist dies eine bewährte Lösung. Bei aktuellen Server-Versionen von Windows ist RADIUS in Form vom Network Policy Server dabei, für andere Systeme gibt es freie Implementierungen.

Letztendlich sollte die Übertragung im WLAN nur **verschlüsselt** erfolgen, wobei die Verschlüsselung mit **Wired Equivalent Privacy (WEP)** unsicher ist. Besser ist der Einsatz von **Wi-Fi Protected Access (WPA)** und der Nachfolgetechnologien **WPA2 / WPA3**. Beide stellen deutlich stärkere Standards für die Verschlüsselung zur Verfügung. WPA2 verwendet den **Advanced Encryption Standard (AES)**. Zusammen mit **Temporal Key Integrity Protocol (TKIP)** sind allerdings nur max. 54 Mbit/s möglich! Höhere Raten erreicht z. B. WPA2 zusammen mit Counter-Mode/CBC-Mac Protocol (**CCMP**).

WPA3 erreicht eine höhere Sicherheit durch **Simultaneous Authentication of Equals (SAE)** und ist dadurch vor dem Durchprobieren von Passwörtern geschützt, wenn der Netzwerkverkehr mitgeschnitten wurde. Der verpflichtende Einsatz bestimmter Verfahren, wie **Protected Management Frames (PMF)**, sorgt für einen sicheren Austausch von Daten in der Anmeldphase. Voraussetzung für den Einsatz von WPA 3 auf Clients, sind aktuelle Betriebssysteme.

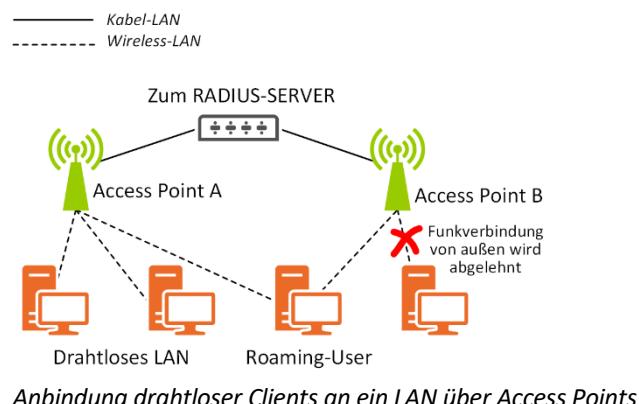
Bauliche Maßnahmen

Gerade die Vermeidung baulicher Maßnahmen ist oft ausschlaggebend für den Einsatz einer drahtlosen Vernetzung. Sie ist oft die einzige realisierbare Lösung, wenn z. B. aus Gründen des Denkmalschutzes keine Veränderungen am Gebäude vorgenommen werden dürfen oder wenn es in einem Kaufhaus darum geht, eine Scannerkasse an das Netzwerk anzubinden, diese Kasse aber nicht fest installiert ist, sondern z. B. auf einem Wagen flexibel durch Sonderaktionsflächen geschoben wird.

Auch bei der Anbindung mehrerer Gebäude, die sich zwar in Sichtweite befinden, aber durch Straßen, Flüsse oder fremde Grundstücke voneinander getrennt sind, ist das Aufstellen von Antennen billiger als eigene Erdarbeiten, um selbst Kabel zu verlegen. Noch dazu würde dies häufig durch langwierige Verhandlungen in Bezug auf Genehmigungen erschwert. Die Alternative, vorhandene Leitungen einer Kabelgesellschaft anzumieten, ist meist mit hohen laufenden Kosten verbunden.

Grundlegende Beschreibung

Kommunikation über WLAN erfolgt entweder als Punkt-zu-Punkt- oder als Mehrpunkt-Kommunikation. Die erste Variante dient z. B. der Überwindung größerer Distanzen durch den Einsatz zweier Richtantennen.



Bei der Mehrpunkt-Kommunikation werden ein oder mehrere sogenannte **Access Points** eingesetzt, die im Prinzip jeweils wie Zentralen (Verteiler) fungieren und die Datenströme mehrerer Clients koordinieren.

Diese (RADIUS-fähigen) Access Points können bei größeren Installationen über Kabel und geeignete Managed Switches (vgl. Kapitel 13.5) eine Verbindung zu einem RADIUS-Server unterhalten, um zwischen berechtigten und nicht berechtigten Sendern zu unterscheiden (Authentifizierung).

Eine Unterscheidung über die **Media Access Control (MAC)-Adresse** (48 Bit große einmalige Identifikationsnummer einer Netzwerkkarte) sollte nur den zum Zugang berechtigten Geräten vorbehalten bleiben, die sich nicht per RADIUS authentifizieren können. Dabei werden in der Zugangsliste (Access Control Table / Access Control List) des Managed Switch die berechtigten MAC-Adressen hinterlegt. Auf einem Access-Point bringt dies keine höhere Sicherheit, da per Funk eine MAC-Adresse unverschlüsselt übertragen wird und somit gefälscht werden kann.

Frequenzspreizungs-Verfahren (Spread-Spectrum)

Dieses Verfahren wird auch Spreiztechnik, Bandspreizung oder Multifrequenz genannt. Der letzte Begriff beschreibt dabei am besten das verwendete Verfahren. Anstelle einer festen Frequenz, wird die Frequenz während der Übertragung permanent gewechselt. Dabei wird ein Signal in einer größeren Bandbreite als nötig (gespreizt) übertragen, damit es weniger störanfällig wird.

Spread-Spectrum-Verfahren arbeiten im Mikrowellenbereich und stellen heute die am weitesten verbreitete Technologie im drahtlosen Bereich dar. Die Einführung von Produkten im 2,4- bzw. 5-GHz-Band ermöglicht es auf einfache Weise, genehmigungsfreie Verbindungen, auch über Grundstücksgrenzen hinweg, herzustellen. Die kleinste Einheit ist dabei eine sogenannte **Funkzelle**, womit der Bereich gemeint ist, der von einem Sender abgedeckt werden kann. Er umfasst im 2,4-GHz-Band je nach baulichen Verhältnissen circa 30 m in Gebäuden und bis zu 300 m im Freien, im 5-GHz-Band erheblich weniger. Mit geeigneten Antennen lassen sich auch mehrere Kilometer erreichen. Die gesetzlichen Bestimmungen sind zu beachten.

Über **Access Points** können zum einen mehrere Funkzellen miteinander verknüpft werden, indem die Access Points per Funk oder über ein kabelgebundenes LAN gekoppelt werden. Zum anderen können Wireless LANs mit herkömmlichen, kabelgebundenen LANs kombiniert werden.

Weitere wichtige derartige Verfahren sind:

Frequency Hopping Spread Spectrum (FHSS)

Zur Datenübertragung werden mehrere Frequenzunterbänder benutzt. Beim 2,4-GHz-Band wurde eine Festlegung auf 79 Kanäle mit je 1 MHz Bandbreite getroffen. Zwei Geräte, die hier miteinander Daten austauschen wollen, einigen sich auf eine zufällige Reihenfolge, in der die Frequenzkanäle bis zu 1.600-mal pro Sekunde gewechselt werden. Während der Übertragung wechseln Sender und Empfänger gleichzeitig die benutzten Frequenzbänder (Hopping).

Der Vorteil ist, dass mehrere Funkzellen parallel betrieben werden können, wenn die Frequenzunterbänder und Hopping-Zeiten entsprechend aufeinander eingestellt werden. Nachteil ist, dass dieses Verfahren relativ unsicher und z. B. in Umgebungen, in denen Reflektionen durch Metall vorkommen, sehr fehleranfällig ist. Es wird noch bei Bluetooth (vgl. nachfolgende Erklärungen) verwendet.

Direct Sequence Spread Spectrum (DSSS)

DSSS wird auch Pseudo-Noise genannt. Die Daten werden so verschlüsselt, dass sie im normalen Rauschen verschwinden. Diese Technik wird vor allem im militärischen Bereich eingesetzt, da sie sehr abhörsicher ist. Die Datenübertragung erfolgt auf dem ganzen Band. So ergeben sich höhere Übertragungsraten bei größeren Reichweiten.

Orthogonal Frequency Division Multiplex (OFDM)

OFDM ist eine äußerst Bandbreiten-effiziente Funktechnik und benötigt ein wesentlich geringeres Frequenzband als Frequenzmultiplex (FDM). Dieses Modulationsverfahren findet bei vielen IEEE 802.11-Normen Anwendung.

Weitere Informationen finden Sie unter <https://de.wikipedia.org/wiki/Frequenzspreizung>.

ISM-Frequenzbänder

In den meisten Fällen wird von den Herstellern ein sogenanntes **ISM-Band** (Industrial, Scientific and Medical) verwendet. Manchmal finden Sie auch die Abkürzung ISMO, wobei der letzte Buchstabe für den Begriff „Office“ (Büro) steht. Der Einsatz dieser Frequenzbänder bietet zwei Vorteile. Sie sind

- ✓ gebührenfrei
- ✓ genehmigungsfrei

! Hierin liegt aber auch gleichzeitig der Nachteil. Sie werden von sehr vielen Herstellern für die unterschiedlichsten Zwecke genutzt, wie z. B. drahtlose Lautsprecher und elektronische Türöffnung bei Autos oder Garagen, und so ist die Gefahr, dass sich Geräte gegenseitig stören, relativ hoch.

Die für WLAN wichtigsten ISM-Bänder sind:

- ✓ das **2,4-GHz-Band** (2,3995 bis 2,4845 GHz) mit max. 13 überlappenden Kanälen von 20 MHz Bandbreite; auch 40 MHz Bandbreite ist möglich, dann aber mit weit weniger nutzbaren Kanälen.
- ✓ das **5-GHz-Band** (5,150 bis 5,350 GHz für Kanalnummer 36–64 und 5,470 bis 5,725 GHz für Kanalnummer 100–140) mit Kanälen von 20, 40, 80 oder 160 MHz Bandbreite, wobei max. 19 Kanäle bei 20 MHz Bandbreite nicht überlappend nutzbar sind. Beim Funken mit 40 MHz Bandbreite sind 2 dieser Kanäle gebündelt erforderlich, mit 80 MHz 4 Kanäle usw. Die Reichweite ist geringer als im 2,4 GHz-Band.
- ✓ zukünftig das **60-GHz-Band** (57 bis 66 GHz) mit vier 2000 MHz breiten Funkkanälen für kurze Distanzen.

Für die Nutzung sind keinerlei Lizenzen erforderlich (im Gegensatz zu den lizenzierten und kostenpflichtigen Frequenzen für das Mobilfunknetz). Nur vor der Installation zum grundstücksübergreifenden Datenverkehr muss in Deutschland der Regulierungsbehörde für Telekommunikation und Post (<https://www.bundesnetzagentur.de>, RegTP) in Mainz eine Mitteilung über die geplante Nutzung einer Frequenz gemacht werden. In Österreich wenden Sie sich an das Ministerium für Verkehr, Innovation und Technologie, <https://www.bmvit.gv.at/> bzw. an die Telekom-Control-Kommission, <https://www.rtr.at/de/rtr/OrganeTKK> und in der Schweiz an das Bundesamt für Kommunikation BAKOM, <https://www.bakom.admin.ch/bakom/de/home.html>.

Entwicklung der Frequenznutzung

In einer **ersten** Stufe der Entwicklung drahtloser Netze wurde das Frequenzband zwischen 902 und 928 MHz mit Geschwindigkeiten bis zu 500 Kbit/s verwendet. Da das Frequenzband durch den zunehmenden Einsatz von Mobiltelefonen überlastet ist, kommt es für die Vernetzung nicht mehr zum Einsatz.

Die **zweite** Entwicklungsstufe setzt auf das 2,4-GHz-Band und erreicht Brutto-Geschwindigkeiten bis 300 Mbit/s. Hier besteht nicht nur die Gefahr der Störung durch andere Geräte (Schnurlos-Telefon, Mikrowelle, Bluetooth, Babyphone etc.), sondern auch der Überlastung durch viele andere Nutzer.

Da im 2,4-GHz-Frequenzband die einzelnen Kanäle sehr nah beieinander liegen, ist ein störungsfreier Betrieb (nicht überlappende Kanäle mit 20 MHz Bandbreite) nur über maximal **3 Kanäle** am selben Ort möglich. Zusätzlich sollten die Kanalnummern entsprechend weit auseinander liegen, also z. B. Kanal 1, 7 und 13 verwendet werden. Einige Geräte können die Kanäle 12 und 13 nicht benutzen, da diese in vielen anderen Ländern nicht erlaubt sind.

In der **dritten** Stufe wird das 5-GHz-Band herangezogen mit Geschwindigkeiten von aktuell bis 600 Mbit/s pro Antenne. Allerdings ist zu bedenken, dass das 5-GHz-Band z. B. in Europa von Flugnavigationsdiensten und vom Wetterradar zusätzlich genutzt wird. Es sind dann nur maximal **16** nicht überlappende Kanäle bei 20 MHz Bandbreite und **7 Kanäle** bei 40 MHz Bandbreite störungsfrei nutzbar.

Viele Hersteller solcher WLAN-Komponenten sperren von Haus aus die Kanäle 120–128 wegen Störungen durch Wetterradar. Eine Verbindung zu anderen Geräten, die keine solche Sperrung haben, ist dann auf diesen Kanälen nicht möglich.

IEEE 802.11

Offiziell ist für die Normung das Institute of Electrical and Electronics Engineers, Inc. (IEEE) zuständig. Im Juni 1997 wurde die Norm 802.11 veröffentlicht, der kleinste gemeinsame Nenner, der für die verschiedenen WLAN-Hersteller gefunden werden konnte. Sie galt zunächst für Übertragungsraten von 1 Mbit/s oder 2 Mbit/s nach dem Spread-Spectrum-Verfahren (sowohl Frequency Hopping Spread Spectrum (FHSS) als auch Direct Sequence Spread Spectrum (DSSS) im 2,4 GHz ISM-Band. Diese Norm sowie die Nachfolger 802.11b und 802.11g gelten heute als veraltet.

Als weitere wichtige Norm wurde 802.11a entwickelt, die im 5-GHz-Bereich arbeitet und im Gegensatz zu 802.11b die Modulationstechnik Orthogonal-Frequency-Division-Multiplexing (OFDM) nutzt. Die Norm 802.11a gilt heute ebenfalls als veraltet. Neuere Normen verwenden zusätzlich Quadratur-Amplituden-Modulation (**QAM**) in den Varianten QAM256 bis QAM1024.

Die folgende Tabelle zeigt einen Ausschnitt wichtiger Varianten von 802.11:

Norm	Beschreibung
802.11a	Max. 54 Mbit/s auf dem 5-GHz-Band mit Verfahren OFDM und 20 MHz breiten Kanälen, nicht kompatibel zu 802.11b.

Norm	Beschreibung
802.11ac	Erweiterung von 802.11n mit bis zu 8 Multiple Input Multiple Output (MIMO)-Streams. Mit 2 Antennen sind derzeit max. 867 MBit/s; mit 3 Antennen 1300 MBit/s brutto im 5-GHz-Band erreichbar. Die Verfahren OFDM und QAM256 finden Verwendung. Mit 802.11ac Wave 2 (früher 802.11ac-2013 genannt) kommen 80 bis 160 MHz breite Kanäle (auch per Kanalbündelung), sowie Multi-User-MIMO (MU-MIMO) im Downstream als Option hinzu. Damit ausgerüstete Geräte sollen max. bis zu 6,9 Gbit/s brutto erreichen können, falls die nötigen Kanäle frei sind. In Europa sind nur 2 Kanäle mit 160 MHz Bandbreite möglich (wegen des Wetterradars ist nur einer störungsfrei) und 4 Kanäle mit 80 MHz (3 störungsfrei).
802.11ad	In Zukunft im 60-GHz-Band mit vier 2000 MHz breiten Funkkanälen auf kurze Distanzen. Erste Geräte wurden zwischen 2016–2018 veröffentlicht. Siehe: ✓ https://wikidevi.com/wiki/List_of_802.11ad_Hardware
802.11ah	Künftiger Kandidat zur Normung von kurzen Übertragungen unterhalb von 1 GHz im „Internet der Dinge“ (IoT) und Smart Home.
802.11ax	Gigabit-WLAN der 2. Generation soll als Nachfolger von 802.11ac Multi-User-MIMO im Upstream bringen. Hinzu kommt das von Long Term Evolution (LTE) bekannte Verfahren Orthogonal Frequency Division Multiple Access (OFDMA), die Multi-User-Version von OFDM, sowie QAM-1024.
802.11ay	Designerter Nachfolger von 802.11ad mit bis zu 4 gebündelten 60 GHz-Kanälen.
802.11b	Max. 11 Mbit/s auf dem 2,4-GHz-Band, nicht kompatibel zu 802.11a. Benutzt das Verfahren DSSS.
802.11g	Max. 54 Mbit/s auf dem 2,4-GHz-Band. Weiterentwicklung von 802.11b. Benutzt OFDM.
802.11n	Kompatibel zu 802.11b+g. Max. 150 Mbit/s bei 20 MHz Bandbreite pro Stream und 300 Mbit/s mit 3 Antennen und 2 Streams; max. 600 Mbit/s bei 40 MHz Bandbreite mit 4 Streams auf den 2,4- und 5-GHz-Bändern (auch gemeinsam bei Einsatz von MIMO). Benutzt OFDM und QAM64.
802.11z	Zum direkten Datenaustausch zwischen Geräten mit „WiFi Direkt“ im 2,4- und 5-GHz-Band über wenige Meter Distanz. Die Übertragungsrate hängt dabei von der Entfernung ab.

Multiple Input Multiple Output (MIMO) ermöglicht die Nutzung mehrerer Sende- und Empfangsantennen für die gleichzeitige Übertragung von mehreren Datenströmen (**Streams**), bei dual-bandfähigen Geräten sowohl im 2,4-GHz als auch im 5-GHz-Band. Mit dem bisherigen Single-User-MIMO können mehrere Empfänger nacheinander bedient werden, mit dem neuen **Multi-User-MIMO** (auch MU-MIMO) mehrere Empfänger gleichzeitig, sofern sowohl der Access-Point als auch das Gerät des Anwenders diese Technik beherrschen.

Dynamic Frequency Selection (DFS) bietet einen automatischen Kanalwechsel im 5-GHz-Band, wenn andere Geräte erkannt werden, die auf denselben Frequenzen funken. Dies soll vor allem Störungen vom Wetterradar verhindern.

Per **Transmit Power Control (TPC)** können Geräte die Sendeleistung im 5-GHz-Band steuern. Sie senden dann bei geringerer Entfernung mit reduzierter Leistung. Können Geräte weder DFS noch TPC, dürfen sie nur auf den unteren Kanälen 36 bis 48 (5150 bis 5250 MHz) mit max. 80 MHz Breite senden.

Die folgende Tabelle zeigt wichtige genormte Erweiterungen für IEEE 802.11:

Norm	Beschreibung
802.11e	Definiert u. a. Quality of Service (QoS) -Erweiterungen
802.11h	Erweiterungen im 5-GHz-Bereich wie z. B. DFS und TPC für 54 Mbit/s mit 20 MHz breiten Kanälen und 108 Mbit/s bei 40 MHz Bandbreite.
802.11i	Regelt Authentifizierung und Verschlüsselung mit TKIP , CCMP , AES und WPA2
802.11s	Legt die Erweiterung der Funkabdeckung in Form eines Mesh-WLAN fest.
802.11w	Sicherheits-Erweiterung (z. B. zur Abwehr von Deauth-Angriffen). Definiert Protected Management Frames und setzt WPA2 mit AES voraus.

WLAN-Standards sind zu den Vorgängerversionen abwärtskompatibel, allerdings mit Einbußen bei Kanalbreite und Übertragungsrate. Dies bedeutet, dass z. B. mit **802.11n** auch Geräte mit 802.11b und 802.11g bedient werden können und auf dem 5-GHz-Band mit **802.11ac** auch 802.11a und 802.11n. Die Abwärtskompatibilität für das 2,4-GHz-Band wird bei 802.11ac durch ein zusätzliches WLAN-Modul erreicht.

Die genannten Übertragungsraten können sich in Zukunft ändern. Sie entsprechen **Brutto**-Raten, die sich aus den Netto-Raten und den Steuerinformationen zusammensetzen. Die möglichen **Netto**-Raten (die übertragenen Nutzdaten) sind selbst bei idealen Empfangsbedingungen je nach Funktechnik oft weniger als halb so groß. Beispielsweise erreicht der Standard 802.11n im 2,4-GHz-Band und mit (selten verfügbaren) 40 MHz breiten Kanälen bestenfalls etwa 10–11 MByte/s, im 5-GHz-Band rund 12–13 MByte/s anstelle der theoretisch möglichen 150 Mbit/s brutto pro Stream. Dies ist etwa das Niveau eines TP-Kabels mit 100Base-TX.

Zudem stellt WLAN wie alle Funkübertragungen (**Universal Mobile Telecommunication System (UMTS)**, **LTE** ...) ein **Shared Media** dar, was bedeutet, dass sich (wie bei einem Hub) alle an der Übertragung beteiligten Geräte die Übertragungsraten innerhalb eines Funkkanals teilen müssen.



Ältere WLAN-Geräte sollten Sie nicht mehr verwenden, wenn Sie die heute erreichbaren Übertragungsraten wünschen. Funken Geräte z. B. mit den veralteten Standards 802.11b oder 802.11g auf dem gleichen oder einem benachbarten Kanal (was Interferenzen ergeben kann), bremst dies die Übertragungen mit 802.11n erheblich. Bei 802.11ac stehen weniger bzw. langsamere Kanäle zur Auswahl, wenn im 5-GHz-Band noch Geräte 20 MHz breite Kanäle mit 802.11n oder 802.11a benutzen. Sind jedoch viele alte Geräte in der Nachbarschaft aktiv, kann meist nur eine Verlegung von Kabeln (TP oder Glasfaser) eine hohe Übertragungsrate sichern.

- ✓ Bei **802.11ac** ist die maximale Übertragungsrates nur mit mehreren parallelen TCP-Streams (**Transmission Control Protocol**) erreichbar, da die standardmäßig eingestellte TCP-Window-Size (mit 256 KB) keine anderen Größen zulässt.
- ✓ Bei **802.11ac Wave 2** kann die Übertragungsrates höher sein als diejenige eines Gigabit-Netzwerkkabels (1000Base-T). Zur Versorgung mit Daten bietet sich daher Port-Bündelung per **Link Aggregation Control Protocol (LACP)** oder auch **NBase-T** nach **IEEE 802.3bz** (vgl. Kapitel 14) anstelle des teuren 10GBase-T an.
- ✓ Die geplante Mobilfunk-Technik **LAA-LTE** (License-Assisted Access-LTE, vgl. Kapitel 19) kann im lizenzierten 5 GHz-Band Störungen bei WLAN-Verbindungen hervorrufen.

- ✓ Die Eignung für IPv6 ist bei etlichen Geräten noch nicht durchgängig vorhanden.
- ✓ Für **Multicast-Übertragungen** (zeitgleiche Übertragung von Datenpaketen an mehrere Empfänger z. B. beim Video-Streaming) ist WLAN schlecht geeignet, da die meisten Access-Points Multicast-Pakete als Broadcasts (Übertragung von Datenpaketen an alle Empfänger) weiterreichen, die Kompatibilität zu langsameren Geräten nur mit 11 Mbit/s bzw. im 5-GHz-Band nur mit 6 Mbit/s verschickt werden. Erst wenn ein Gerät Multicast-Pakete in Unicast-Pakete (Übertragung von Datenpaketen an einen einzelnen Empfänger) umsetzt (**Multicast-to-Unicast, MC2UC**), ist auch Video-Streaming möglich. Ferner müssen die Geräte für Multicast-Übertragungen **IGMP-Snooping** beherrschen. IGMP-Snooping ist eine Erweiterung des **Internet Group Management Protocols (IGMP)**, durch die ein Gerät auf der zweiten Schicht des OSI-Modells erfährt, wohin Multicast-Pakete zu verschicken sind.

Erweiterung von WLAN-Netzwerken

Ein **WLAN-Repeater** vergrößert die Reichweite eines WLAN. Kann er sowohl im 2,4-GHz-Band als auch im 5-GHz-Band senden, ist er dualband-fähig. Die Übertragungsrate sinkt jedoch auf rund die Hälfte, wenn der Repeater die Pakete erst empfangen muss, bevor er sie erneut sendet. Außerdem erhöht sich dabei die Latenzzeit (zeitliche Verzögerung). Neuere WLAN-Repeater können gleichzeitig auf unterschiedlichen Bändern funken (Crossband-Technik), sodass durch den Aufbau einer neuen Funkzelle im jeweils anderen Band kein Verlust an Übertragungsrate entsteht. Bei Anbindung mit einem Netzwerkkabel oder per Powerline (vgl. Kapitel 19) gibt es ebenfalls keinen Verlust.

Die **WLAN-Basis** wird dann zu einem Access-Point. Manche dieser Geräte enthalten zudem eine USB-Buchse für den Anschluss von Druckern, externen Festplatten etc.

WLAN-Router mit Akku bieten sich für die mobile Vernetzung an. Sie stellen die Verbindung mit dem Internet per UMTS oder LTE her und versorgen etliche Client-Geräte per WLAN, indem sie einen eigenen **WLAN-Hotspot** erstellen, oft mit Dualband für das 2,4- und 5-GHz-Band.

WLAN-Adapter (auch als WLAN-Bridge bezeichnet) können Geräte auch dann an ein Netzwerk anschließen, wenn sie keinen WLAN-Anschluss besitzen, indem sie mit dem Access Point eine Verbindung aufnehmen und diese über Ethernet-Kabel zum Gerät weiterreichen. Sie können oft zusätzlich als WLAN-Repeater fungieren.

Wi-Fi Direct nach 802.11z (auch „AD-HOC WLAN“ genannt) ermöglicht eine direkte WLAN-Verbindung, z. B. zwischen 2 Smartphones bzw. zwischen Smartphone und einer WLAN-fähigen Kamera etc. ohne weitere Komponenten (wie einem Access Point), sofern die hierfür nötigen Programme (Apps) vorhanden sind.

Ein **Mesh-WLAN** nach IEEE 802.11s legt eine weitere Art der Übertragung fest, um große Flächen mit WLAN zu versorgen. Ein Mesh-WLAN leitet nur die Pakete weiter, die an den entsprechenden Empfänger gerichtet sind, ähnlich einem Switch. Derartige Mesh-Router verknüpfen sich automatisch zu einem Funknetz. Die Übertragungsrate sinkt dabei jedoch, und die Latenzzeit steigt.

4.6 Bluetooth

Bluetooth stellt keinen Ersatz für WLAN im Sinne von IEEE 802.11 dar, sondern ist in erster Linie gedacht für preiswerte Funkverbindungen im Nahbereich. Für diese Technik werden etliche Geräte angeboten.

Mit **Bluetooth 1** sind Übertragungsraten von 723 KBit/s Downstream (Empfangsrichtung) und 128 KBit/s Upstream (Senderichtung) möglich. **Bluetooth 2.0+EDR** (Enhanced Data Rate) kann bis zu 2,2 MBit/s übertragen. Mit **Bluetooth 3.0** sind netto bis zu 24 MBit/s möglich. Dabei erfolgt nur noch die Aushandlung der Verbindung über Bluetooth-Technik, die Datenübertragung übernimmt ein WLAN-Modul nach IEEE 802.11g. **Bluetooth 4.0** bietet weitere Stromspar-Mechanismen. Die Versionen ab 4.0 werden auch als **Bluetooth Low Energy (BLE)** bezeichnet, die Versionen davor als „Bluetooth Classic“. Alle Versionen sind abwärts kompatibel, sodass diejenige Übertragung erfolgt, die beide beteiligten Geräte mindestens beherrschen.

Es können beispielsweise drei gleichzeitige Sprechverbindungen geführt werden. In einem **Piconet** (einer Funkzelle) können sich maximal acht Geräte gleichzeitig diese Übertragungsrate teilen. Mehrere Piconets lassen sich zu sogenannten Scatternets zusammenschließen.

Verwendet wird das 2,4-GHz-ISM-Band, allerdings mit einer geringeren Sendeleistung als bei 802.11. Eingesetzt wird **FHSS** mit schnellem Frequenzwechsel, wodurch sich eventuelle Stör-einflüsse weniger stark auswirken. Die Sendeleistung ist in drei Leistungsklassen unterteilt. Die höchste Funkklasse (Klasse 1) kann bei einer Sendeleistung von 100 mW eine Reichweite von bis zu 100 m erzielen.

Ein Vorteil von Bluetooth ist, dass bereits im Verfahren sogenannte Profile (anwendungsspezifische Protokolle) definiert sind. Es existieren unter anderem Profile für Audio-Übertragungen, Datei-transfer, Fax, Human Interface Devices (HID, z. B. Maus, Tastatur) und den LAN-Zugriff. Nachteilig ist, dass Bluetooth ohne Verschlüsselung leicht abgehört werden kann.

4.7 Weitere Funktechniken und das Internet der Dinge

NFC und RFID

Mit **Near Field Communication (NFC)** ist auf kurze Entfernungen (wenige Zentimeter bis ungefähr 1 Meter) eine Übertragung von Daten mit maximal **424 kBit/s** möglich. Meist werden die Funk-frequenzen 135 kHz und 13,56 MHz benutzt. Grundlage für diesen Übertragungsstandard bildet die **RFID-Technik (Radio-Frequency-Identification)**, aber auch Bluetooth und WLAN können hierfür eingesetzt werden.

Bereits heute sind etliche Smartphones, Mülltonnen, Preisschilder, Kreditkarten und Wegfahr-sperren sowie Pässe, Personalausweise etc. mit RFID-Transpondern ausgestattet, die eine Ver-bindung per NFC ermöglichen. Wichtige Anwendungen dürften in Zukunft das berührungslose Erkennen von Preisen gekaufter Artikel an Supermarktkassen und Bezahl-dienste sein.

An dem markierten Produkt ist der eigentliche Chip für die Kommunikation (der **RFID-Tag** bzw.-Transponder) ohne Batterie angebracht, der auf die Befehle vom Lesegerät (NFC-Sender) ant-wortet.

Die Stromversorgung des Chips erfolgt bei passiven Tags über die Antenne, über die eine geringe elektrische Leistung vom Lesegerät induziert wird. Ein großes Problem stellt dabei die oft man gelnde Sicherheit dar. So sind z. B. Fälle bekannt geworden, in denen heimlich mit einem geeigneten Smartphone und entsprechender App die Daten von Kreditkarten in der Umgebung ausgelesen wurden, um damit unberechtigte Zahlungen zu tätigen. Weiter ist der Diebstahl von Identitätsdaten im Zusammenhang mit RFID-Transpondern in Reisepässen bekannt geworden.

NFC kann auch die Kontaktaufnahme zwischen WLAN- Smartphone- und Bluetooth-Geräten erleichtern. Da die Reichweite begrenzt ist, reicht es, die Komponenten in die Nähe zueinander zu bringen, um das Pairing (die Übertragung der Einstellungen) zu ermöglichen.

WPAN für kurze Distanzen

Das **Wireless Personal Area Network (WPAN)** ist interoperabel zum Standard IEEE 802.11 und als IEEE 802.15 standardisiert. Es beschränkt sich auf eine kleine Distanz (typischerweise bis 10 m). Hierüber können Mobilfunk-Telefone, **Personal Digital Assistants (PDA)** und Peripheriegeräte miteinander und mit PCs kommunizieren. Dabei werden mit dem Verfahren Bluetooth 3.0 Übertragungsraten bis zu 24 Mbit/s auf der Basis des WLAN-Protokolls erzielt. WPAN bildet die Basis für einige weitere Übertragungsverfahren, die für das **Internet of Things (IoT/Internet der Dinge)** Verwendung finden, wie den herstellerspezifischen Techniken **ZigBee, Z-Wave** etc.

Ein weiteres Verfahren, Ultra Wide Band (UWB), welches höhere Datenraten auf größere Distanzen überträgt, wurde inzwischen aufgegeben.

Internet der Dinge (IoT)

Mit dem Begriff „Internet der Dinge“ bzw. „Internet of Things“ (**IoT**) ist gemeint, dass in naher Zukunft nicht nur Computer, Smartphones, Tablets etc. vernetzt sind und damit eine IP-Adresse erhalten. Geplant und schon teilweise umgesetzt ist, dass nahezu jedes elektrische Gerät über ein Netzwerk erreichbar sein soll. Damit können auch Stromzähler, Kühlschränke, Kameras, Lampen, Heizungsthermostate, motorgetriebene Rollläden und viele weitere Geräte miteinander vernetzt und über entsprechende Programme („Apps“) ausgelesen und gesteuert werden. Ein häufig verwendeteter Begriff für diese Anwendungen in einer Wohnung ist „**Smart Home**“.

Auch kleine Computer, die am Körper getragen werden (sog. „Wearables“) sind bereits käuflich zu erwerben oder befinden sich in der Entwicklung. Beispiele hierfür sind Uhren (Smartwatches), in der Kleidung eingearbeitete Chips und vieles mehr.

Meist wird zur Kommunikation mit diesen Geräten auf Funktechniken gesetzt wie lizenfreie Funkkanäle für kurze Reichweiten (Short Range Networks, **SRN**). Dazu gehören NFC, Bluetooth, WPAN usw. Die Übertragungsraten sind meist relativ gering und die einzelnen Geräte können sich leicht in die Quere kommen.

WLAN nach **IEEE 802.11ah** von 863 bis 886 MHz bietet seit 2016 eine Alternative. Es verwendet Funkkanäle mit 1 bis 16 MHz Breite und Sendeleistungen von 10 mW bis 1 W bei Reichweiten von 100 m bis 1 km. Es verwendet OFDM als Multiplexverfahren. Wegen des Konkurrenzverhaltens zweier Herstellerlager verzögerte sich die Normierung. Ob sich IEEE 802.11ah gegen etablierte Verfahren wie **ZigBee, Bluetooth Low Energy** etc. durchsetzen kann, muss sich zeigen.

Aber auch TP-Kabel oder das Stromnetz (per Powerline-Adapter) ermöglichen einen Zugriff auf viele Geräte. Aktuell gibt es unterschiedliche Protokolle der Hersteller, die meist nicht untereinander kompatibel sind.

Soll eine Steuerung vom Internet her erfolgen, kommen wegen der Knappheit an IPv4-Adressen in der Regel nur IPv6-Adressen in Betracht. Weiter stellt sich die wichtige Frage nach einer guten Sicherheit. Häufig sind Anwendungen und Geräte durch schwere Sicherheitslecks in den Medien aufgefallen. Weitere Forderungen sind stromsparende Geräte und möglichst einfache, effiziente Übertragungsprotokolle.

Das LoRa-Funkverfahren

Das Verfahren **Low power long Range (LoRa)** ist ein Low Power Wide Area Network (**LPWAN**), über das eine deutschlandweite Vernetzung von der Firma Digimondo (eine Tochterfirma von Eon) geplant ist. Damit sollen über eine Entfernung von bis zu 40 km Stromzähler, Straßenlaternen etc. an das Internet angebunden werden. Eine Verbindung erfolgt bidirektional im lizenzenfreien 868 MHz-Band mit 0,3 bis 52 Kbit/s mit max. 25 mW Leistung.

Weitere Informationen zum LoRa-WAN finden Sie unter <https://www.link-labs.com/blog/what-is-lorawan>

4.8 Übertragung per Licht bzw. Laser

Datenübertragung durch Lichtwellen ohne Kabel

Infrarot und Laser sind zwei weitere Möglichkeiten der Übertragung. Allerdings finden beide Methoden kaum oder keine Verwendung im LAN-Bereich.

Infrarot

In manchen Bereichen bietet die Übertragung von Daten mit Infrarot-Technik Vorteile. Bei der Anbindung kleinerer Peripheriegeräte innerhalb von Gebäuden oder auch dem Anschluss von PDAs oder Notebooks kann auf den IrDA-Infrarotstandard zurückgegriffen werden. Hier sind Übertragungsraten von über 1 Gbit/s bei geringer Reichweite (wenige cm) möglich.

Beim Einsatz im Außenbereich erreichen neuere Produkte Geschwindigkeiten von 2 Mbit/s über eine Entfernung von 550 m oder bis zu 10 Gbit/s über maximal 30 m (**Giga-IR**). Allerdings ist die Übertragung empfindlich gegen Sonnenlicht oder Wärmestrahlung, weshalb mit starken Signalen gearbeitet werden muss.

Laser

Laser dienen der Punkt-zu-Punkt-Verbindung. Sie erfordern direkte Sichtverbindung und sind anfällig gegen störende Einflüsse wie Nebel, Schneefall oder Vogelschwärme. Mithilfe von Lasern können Datenübertragungsraten bis 100 Gbit/s erreicht werden.

Beim Einsatz von Laser ist keine Frequenzlizenzierung nötig. Die Übertragung ist nicht anfällig gegenüber elektromagnetischen Interferenzen und relativ abhörsicher. Wenn Streulicht abgefangen werden kann, ist die Abhörsicherheit (wie auch bei Infrarot-Übertragungen) nicht mehr gewährleistet.

4.9 Übung

Fragen zu Übertragung und Eigenschaften von Übertragungsmedien

Übungsdatei: --

Ergebnisdatei: uebung04-E.pdf

1. Beschreiben Sie, mit welchen Maßeinheiten die Übertragungsgeschwindigkeit und die Dämpfung angegeben werden?
2. Warum sollten nur noch halogenfreie Leitungen verlegt werden?
3. Warum sind die Adern in Twisted-Pair-Kabeln verdrillt?
4. Welche Arten von Abschirmungen gibt es und wie werden sie bezeichnet?
5. Welche Kabelkategorie sollte für 10-Gbit-Ethernet verwendet werden?
6. Was ist der Unterschied zwischen Monomode- und Multimode-Fasern?
7. Was ist Dispersion und wie kann sie minimiert werden?
8. Was sollten Sie bei einer drahtlosen Übertragung immer beachten?
9. Welches ist aktuell der WLAN-Standard mit der höchsten Übertragungsrate und was ist dabei zu beachten?

5

Schnittstellen

5.1 Netzwerkkarten

Die Verbindung zwischen PC und Übertragungsmedium

Netzwerkkarten (auch **NIC** für **Network Interface Card**) bzw. Netzwerkadapter stellen eine oder mehrere **Schnittstellen** zwischen dem Computer und Übertragungsmedien (Twisted-Pair, WLAN, LWL etc.) zur Verfügung. Die Datenübertragung auf den Netzwerk-Medien erfolgt seriell, d. h., es wird bitseriell übertragen.

Inzwischen werden Netzwerkschnittstellen für Twisted-Pair-Verkabelung zumeist auf der Hauptplatine von PCs und Notebooks untergebracht. Bei Notebooks, Tablets, Smartphones, etc. findet sich zur Anbindung an ein Netzwerk zusätzlich bzw. stattdessen ein WLAN-Modul. Sollen jedoch in Rechnern spezielle Netzwerkschnittstellen für andere Übertragungsmedien oder zusätzliche Netzwerkkarten eingesetzt werden, z. B. Exemplare mit bis zu vier Anschlüssen, kommen nach wie vor Steckkarten zum Einsatz.

Heutige Netzwerkschnittstellen sind in der Regel bootfähig, d. h., sie bringen eine eigene BIOS-Erweiterung mit, um über das Netzwerk ein Betriebssystem zu booten. Ein Beispiel dafür ist **Preboot Execution Environment (PXE)**.

Aktuelle Netzwerkschnittstellen sind für mehrere Geschwindigkeiten ausgelegt, wie 10/100/1000 Mbit/s oder 10/100/1000/10000 Mbit/s etc. Die Geräte handeln die maximal mögliche Rate untereinander aus (per **Autonegotiation**) und schalten automatisch auf eine niedrigere Rate zurück, wenn die Leitungseigenschaften nicht ausreichen oder ein Gerät mit geringerer Geschwindigkeit angeschlossen ist.

Jede Netzwerkschnittstelle besitzt eine weltweit eindeutige **MAC-Adresse** (nach der OSI-Layer-2-Schicht **Media Access Control**). Bei Netzwerkkarten mit mehreren Anschlüssen hat jede Schnittstelle eine eigene MAC-Adresse. Diese dient als eindeutige Hardware-Adresse, die zur direkten Adressierung von Daten-Frames (auf OSI-Layer 2) innerhalb eines Netzwerksegments benötigt wird (vgl. Kapitel 10.5).

In mobilen Geräten wie Notebooks, Tablets, Smartphones etc. sind bereits **WLAN-Schnittstellen** von Haus aus eingebaut; oft auch solche für Bluetooth, NFC, UMTS, LTE und andere Funktechniken. Viele Notebooks besitzen zusätzlich einen RJ-45-Anschluss für Twisted-Pair Kabel. Möglich ist mitunter auch die Aufrüstung mit Steckkarten nach dem **Personal Computer Memory Card International Association (PCMCIA)** Standard. PCMCIA gilt heute jedoch als veraltet.

Die Funktechniken WLAN und NFC sind in Kapitel 4.7 beschrieben, UMTS und LTE in Kapitel 19.

Steckkarten

NICs können in Form von **Steckkarten** in einen freien Steckkartenplatz eingebaut werden. Je nach Art des vorhandenen Übertragungsmediums sind im Handel dafür passende Karten erhältlich.

Die nebenstehende Abbildung zeigt eine Auto/MDIX-fähige Netzwerk-karte für 10/100/1000 Mbit/s mit einem RJ-45-Anschluss ① für TP-Kabel und einer PCIe-x1-Schnittstelle ② für 1 seriellen Kanal (Lane).

Da heutzutage nur noch Plug-&-Play-Karten erhältlich sind, entfällt zusätzlicher Konfigurationsaufwand bei der Hardware. Heutige Betriebssysteme erkennen Karten dieser Art nach dem Einbau automatisch.



PCIe-Netzwerkkarte

Aktuelle Windows- und Linux-Versionen bringen die Treiber für die meisten Netzwerkkarten mit. Bei speziellen Exemplaren ist Software vom jeweiligen Hersteller erforderlich, die im Normalfall von der Website des Herstellers heruntergeladen werden kann.

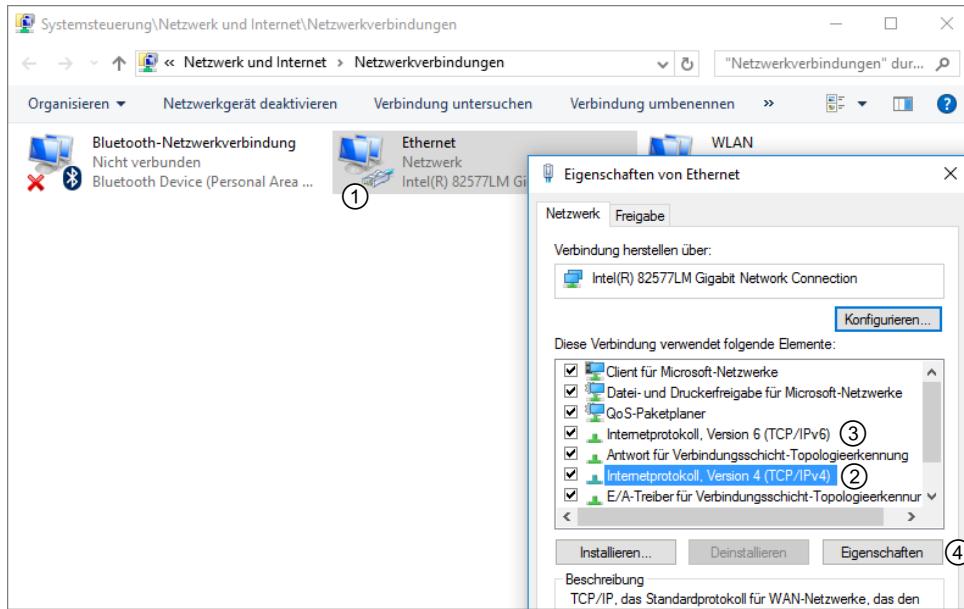
Bindung und Konfiguration einer Netzwerkschnittstelle

Bindung bezeichnet die Anbindung an einen Protokoll-Stack (vgl. Kapitel 11). Eine Protokollfamilie wird dabei an eine Netzwerkschnittstelle (ein Mainboard bzw. eine Netzwerkkarte kann mehrere solcher Schnittstellen haben) gebunden. Dadurch kann diese Netzwerkschnittstelle mit den zugehörigen Schichten des gebundenen Protokoll-Stacks kommunizieren, wodurch der Datenaustausch erst möglich wird.

Es existieren mehrere Realisierungen:

- ✓ **Open Data Link Interface (ODI)** heißt die Entwicklung von Novell und Apple.
- ✓ **Network Device Interface Specification (NDIS)** ist eine Entwicklung von 3Com (inzwischen von HP übernommen) und Microsoft. Aktuell sind die NDIS-Versionen 6.0 von Vista bis 6.5 von Windows 10.
- ✓ Unter Linux erfolgt die Bindung über **Kernel-Module** (nachladbare Gerätetreiber innerhalb des Betriebssystemkerns).

Ein Computer kann mehrere Netzwerkverbindungen ① besitzen. An diese sind unterschiedliche Protokolle und Dienste gebunden, meist IPv4 ② und/oder IPv6 ③, unter der Windows-Einstellung mittels Häkchen vor dem entsprechenden „Element“ (siehe nächste Abb.).



Netzwerkkonfiguration unter Windows

Weitere Einstellungen, wie eine manuelle Konfiguration (beispielsweise mit einer festen IP-Adresse), können unter *Eigenschaften* ④ erfolgen.

Ob die Netzwerkschnittstellen direkt auf dem Mainboard verbaut oder über Steckkarten bzw. externe Adapter (z. B. für USB, Thunderbolt etc.) angeschlossen sind, macht keinen Unterschied.

PCI und PCIe

Der Datenfluss auf der Hauptplatine, also z. B. von einem Steckplatz mit der Steckkarte zum Arbeitsspeicher, erfolgt über ein sogenanntes **Bus-System**. Auf diesem Gebiet gab es im Laufe der letzten Jahrzehnte viele unterschiedliche Entwicklungen, wobei sich für viele Einsatzgebiete **Peripheral Component Interconnect (PCI)** und in neuerer Zeit **PCI Express (PCIe)** durchgesetzt hat.

Der **PCI-Bus** kann auf dem Motherboard mit mehreren Steckplätzen vertreten sein. Die Busbreite beträgt 32 Bit mit meist 33 MHz Taktrate bei PCI und 64 Bit mit 66–133 MHz Taktrate bei Geräten mit **PCI-Extended (PCI-X)**. PCI-X kommt vor allem in Servern zum Einsatz. Bei PCI sind max. 133 MB/s als Übertragungsrate möglich, bei PCI-X bis zu 1067 MB/s.

! PCI-Karten sollten bei Neuanschaffungen nicht mehr verwendet werden, da der PCI-Bus veraltet ist (aktuelle Mainboards haben keine derartigen Steckplätze mehr).

PCI-Express (PCIe, PCI-E) nutzt anstelle eines Bussystems, wie dies noch bei PCI und PCI-X üblich war, sogenannte Lanes. PCI-Express bildet daher keinen Bus, sondern eine Sternstruktur mit einem speziellen internen Switch auf dem Mainboard. Je nach Anzahl der verfügbaren Lanes am Steckplatz, wird der Slot entsprechend bezeichnet (PCIe x16 = 16 Lanes).



Zwei PCIe-Steckplätze (oben x1, darunter x16)

Die Übertragung erfolgt seriell über die Lanes, von denen bis zu 32 gebündelt werden können. Eine **Lane** (x1) kann in Vollduplex mit nominal jeweils 250 MB/s pro Richtung bei PCIe 1.0 übertragen; bei PCIe Version 2.0 mit 500 MB/s und bei PCIe 3.0 mit 1GB/s.

Die Übertragungsrate ist besonders bei schnellen Netzwerkkarten zu beachten, damit sich kein Flaschenhals ergibt. So reicht für Gigabit-LAN oft noch eine PCI-Karte, während bei einer 10 Gigabit Ethernet PCIe-Karte 3 Lanes der Version 3.0 benötigt werden. Auch ist ein schnelles RAID-Array nötig, da einzelne Festplatten dieser Übertragungsrate nicht gewachsen sind.

5.2 Weitere Anschlussmöglichkeiten

Einsatzvarianten für kleinste Netzwerke

Zur Verbindung zweier PCs bei Twisted-Pair-Verkabelung kann ein spezielles, sogenanntes **Cross-Over-Patchkabel** verwendet werden, in dem die signalführenden Adernpaare nicht 1:1, sondern gekreuzt (die Sende-Adern mit den Empfänger-Adern und umgekehrt) verdrahtet sind.

Aktuelle Switches unterstützen **Auto-MDI/MDIX**. Die Abkürzung steht für Medium Dependent Interface (X = „crossover“) und bedeutet die automatische Anpassung der Sende- und Empfangsleitung eines Ports abhängig vom angeschlossenen Kabel (gekreuzt oder nicht gekreuzt). Damit ist es unerheblich, ob Sie einen Rechner per Patch- oder Cross-Over-Kabel an den Switch anschließen.



Cross-Over-Kabel sollten eindeutig **gekennzeichnet** sein, um eine Verwechslung mit normalen Patch-Kabeln oder entsprechenden Kupplungen zu vermeiden. Auch bei ISDN-Kabeln ist dies nötig, da sie zwar RJ45-Stecker benutzen, aber **nicht** für Ethernet-Verbindungen geeignet sind. Bei manchen Geräten, die per **Power over Ethernet (PoE)** mit Strom versorgt werden, können Cross-Over-Kabel Probleme bereiten.

Handelsübliche Gigabit-Netzwerkkarten sowie auf Mainboards integrierte Gigabit-Netzwerkschnittstellen unterstützen ebenfalls Auto MDI/MDIX. Cross-Over-Kabel sind deshalb heute kaum noch gebräuchlich.

Den Zugang zum Internet stellen häufig DSL-Router her. Sie bieten eine Kombination mehrerer Funktionen: eine Switching-Funktionalität für Ethernet, ein Access Point für das WLAN und einen Multiprotokoll-Router für den Transport zwischen LAN und Internet (vgl. Kapitel 19).

Glasfaser-Verkabelung wird bei kleinen Netzwerken standardmäßig nicht verwendet. Wenn doch, dann kann ein normales Glasfaserkabel oder wie bei der TP-Verkabelung eine zentrale Komponente verwendet werden. Allen Varianten gemeinsam ist, dass für jede an der Datenkommunikation beteiligte Komponente eine passende Netzwerkschnittstelle vorhanden sein muss.

USB

Die USB-Schnittstelle (**Universal Serial Bus**) ist ein Bussystem, das fast universell zum Anschluss von Peripheriegeräten einsetzbar ist. Geräte wie z. B. Scanner, Digitalkameras, Memory-Sticks oder Drucker sind in Versionen für diese Schnittstelle am Markt erhältlich.



PCs werden üblicherweise mit mehreren USB-Ports ausgeliefert. Über USB-Hubs oder über Geräte, in denen Verteiler integriert sind, können theoretisch bis zu 127 weitere Geräte mit USB 2.0 angeschlossen werden. Da USB-Verbindungen hot swappable sind, können Geräte angeschlossen oder wieder entfernt werden, ohne dass der Computer heruntergefahren und wieder neu gestartet werden muss. Ein Gerät muss vorher über das Betriebssystem entfernt (ausgeworfen bzw. ungemountet) werden, damit das Dateisystem nicht beschädigt wird und das Schreiben aller vorgenommenen Änderungen sicher erfolgt ist.

Heute relevant ist **USB 2.0** (High Speed) mit einem Nettodurchsatz von bis zu ca. 36 MB/s und **USB 3.0** (Super Speed) mit über 400 MB/s. **USB 3.1** (Super Speed+) kann über besseres Daten-Encoding das Doppelte erreichen. USB ist abwärtskompatibel, sodass auch Geräte mit USB 2.0 an Ports mit USB 3.0 betrieben werden können (dann nur mit High Speed).



Die Übertragungsraten sind zu beachten, wenn Daten über das Netzwerk, z. B. an USB-Festplatten geleitet werden. So eignen sich externe Festplatten, die per USB 3.0 (3.1) angeschlossen sind, sowie über das Netzwerk erreichbare NAS-Systeme gut für Backup-Lösungen, falls auf sicheren Umgang geachtet wird (vgl. Kapitel 8.7).

Bei Geräten, die einen Hub mit **USB-OTG (On The Go)** bieten, können entsprechend ausgerüstete USB-Geräte (USB-Logo mit einem grünen Pfeil) untereinander kommunizieren, ohne dass die Beteiligung eines zentralen Host-Controllers erforderlich wäre.



Für den Anschluss an das lokale Netz kann auch **Wireless USB** verwendet werden, das eine Verbindung über Funk über wenige Meter mit einer Übertragungsrate ermöglicht, die der von USB 2.0 entspricht. Es sollte **nicht** mit WLAN-USB-Sticks verwechselt werden, die eine Verbindung an ein WLAN ermöglichen.



Weitere Informationen über USB finden Sie unter
https://de.wikipedia.org/wiki/Universal_Serial_Bus.

Darüber hinaus stehen auch USB-Adapter für den Anschluss an Twisted-Pair-Netzwerke zur Verfügung (vgl. nebenstehende Abbildung). So können etwa ältere Laptops mit voller Geschwindigkeit in ein Gigabit-Netzwerk eingebunden werden.



Für USB gibt es mehrere Stecker-Arten, die nur in einer Ausrichtung einsteckbar sind. Neu mit der Einführung von USB 3 ist ein weiterer Stecker vom **Typ C**, der unabhängig von der Orientierung einsteckbar (mit 12 Kontakten oben und unten) und für beide Kabelenden gleich ist.

Damit sind auch wesentlich höhere Ströme zum Verbraucher möglich, die untereinander per **Power Delivery** ausgehandelt werden können. Zudem gestattet es **Typ-C-Authentication** bei USB 3.1, die nur Geräte mit signierter Firmware zulässt.

Adapter von Typ C auf etliche andere Verbindungen sind erhältlich, unter anderem auch für eine Anbindung an ein Ethernet-Netzwerk. Auch Thunderbolt 3 kann Stecker und Buchsen vom Typ C benutzen. Bei aktuellen Geräten können einige USB-Buchsen vom Typ C gemeinsam mit USB 3.1 und mit Thunderbolt 3 (siehe unten) beschaltet sein.

Die maximale Länge eines Kabels vom Peripheriegerät zum PC oder zum USB-Hub liegt für USB 2.0 bei 5 Metern; ab USB 3.0 ist keine maximale Länge spezifiziert, sie sollte aber 3 m nicht überschreiten. Es lassen sich mit USB 2.0 maximal sechs Segmente mit USB-Hubs bilden, womit die Reichweite auf 30 Meter ausgedehnt werden kann. Bei USB 3.0 ist dies nicht ratsam, da es dabei wegen der hohen Frequenzen zu Instabilitäten kommen kann.

In den meisten aktuellen Computern sind USB 3.0-Schnittstellen integriert, oft bereits solche mit USB 3.1. Bei älteren Geräten lassen sie sich über entsprechende Schnittstellenkarten nachrüsten.

Firewire

Firewire ist eine serielle Schnittstelle und wurde bereits 1995 als IEEE 1394 standardisiert. Die Grundversion arbeitet mit Übertragungsraten von 100, 200 oder 400 Mbit/s und bietet Anschlussmöglichkeiten für maximal 63 Geräte. Die Spezifikation IEEE 1394b vom April 2002 verdoppelt die Übertragungsrate auf 800 Mbit/s. Im Oktober 2008 wurde unter der Bezeichnung IEEE 1394-2008 die Spezifikation mit einer Datenübertragungsrate von 3,2 Gbit/s verabschiedet.



Ebenso wie bei USB sind IEEE-1394-Verbindungen hot swappable und gedacht für den Anschluss von Geräten wie z. B. Digitalkameras, externe Festplatten oder CD-RW-Brenner. Die maximale Länge eines Kabels ist auf 4,5 Meter begrenzt. Allerdings lassen sich bis zu 16 Kabel miteinander verbinden (daisy chained), sodass eine Gesamtlänge von 72 Metern erreicht werden kann.

Während bei vielen Apple-Rechnern diese Schnittstelle seit Jahren zum Standardumfang gehört, wird sie bei anderen Rechnern selten angeboten. Es gibt auch Adapter von Thunderbolt auf Firewire.

Thunderbolt

Seit Februar 2011 gibt es eine Schnittstellentechnologie, die unter dem Namen Thunderbolt (Blitz) in Zusammenarbeit von Intel und Apple entwickelt wurde. Zusätzlich zu den Möglichkeiten, die auch bei einer USB-Anbindung verfügbar sind, unterstützt Thunderbolt den Anschluss von Monitoren.



Bei Thunderbolt werden auf bidirektionalen Kanälen Transferraten bis zu 40 Gbit/s erreicht. Einige Geräte für die Netzwerkanwendung sind ebenfalls erhältlich. Apple als Mitentwickler von Thunderbolt bietet seit Beginn Computer mit integrierten Schnittstellen an, andere Hersteller haben zwischenzeitlich nachgezogen. **Thunderbolt 2** bietet 2 Kanäle in jeder Richtung mit insg. 20 GBit/s. **Thunderbolt 3** erreicht Übertragungsraten bis 40 GBit/s und kann den von USB 3 bekannten Stecker vom **Typ C** (siehe oben) verwenden. **Thunderbolt 4** wird ebenfalls 40 Gbit/s erreichen.

5.3 Fernwartung bei Büro-Rechnern und Servern

Da Bülorechner für Arbeiten im Büro ausgelegt sind, brauchen sie zumeist keine 3D-Grafik oder andere aufwendige Hardwareausstattung. Deren Hersteller bieten für den Büroalltag bewährte Konstruktionen und schnellen Support, mitunter (gegen Aufpreis) innerhalb von wenigen Stunden. Auch können hier zur Erhöhung der Sicherheit in der Firmware (BIOS) die USB-Ports sowie das Booten von externen Laufwerken deaktiviert werden. In der Regel gibt es ein **Trusted Platform Modul (TPM)**, welches das System um sicherheitsrelevante Funktionen erweitert, sowie eine Überwachung auf das Öffnen vom Gehäuse.

In bestimmten Workstation-Modellen ist auch eine Möglichkeit zur **Fernwartung** eingebaut, die Zugriff über ein Netzwerk bietet – selbst dann, wenn noch kein Betriebssystem aktiv ist oder falls die Maschine ausgeschaltet bzw. abgestürzt ist.

Mit der **Active Management Technology (AMT)** von Intels **vPro**-Plattform (eine Erweiterung der Firmware) ist es dem Support Techniker möglich, über Fernwartung Updates einzuspielen, einen Neustart des Rechners zu veranlassen oder das System zu warten. Die Verbindung erfolgt über das Netzwerk per **Serial over LAN (SoL)**, wobei die IO-Operationen eines internen seriellen Ports über das IP-Protokoll abgebildet werden.

Mainboards für Server benutzen sehr häufig einen separaten Chip für die Fernwartung, den **Baseboard Management Controller (BMC)**. Es können damit über das Netzwerk Messwerte wie Temperatur, Lüfterdrehzahl etc. abgefragt bzw. automatisch verschickt werden. Ebenso ermöglicht der BMC das Ein- und Ausschalten sowie Änderungen an der Firmware.

Der BMC enthält hierzu einen Webserver, der den Zugriff über einen Browser ermöglicht. Viele Server-Brettscheiben bieten für diesen Zweck eine eigene Netzwerkbuchse. Falls diese nicht verwendet wird, erfolgt die Verbindung über die reguläre Netzwerkverbindung. Dies kann die Sicherheit des Servers besonders dann beeinträchtigen, wenn das Gerät über das Internet erreichbar ist, da viele BMC automatisch mit einfachen Standard-User/Passwort-Kombinationen eingerichtet sind. Daher wird die Einrichtung eines separaten Management-Netzwerks dringend empfohlen.

Zugriff zu einem BMC ist ohne Webserver auch über die standardisierte Schnittstelle **Intelligent Platform Management Interface (IPMI)** per serieller Schnittstelle oder Ethernet möglich. Per SoL (siehe oben) auch auf Einstellungen des BIOS, RAID-Controller etc. Über IPMI können ebenfalls Sicherheitslücken auftreten! AMT unterstützt jedoch kein IPMI.

Über **Windows Hardware Error Architecture (WHEA)** werden Fehlermeldungen von Server-Mainboards, wie z. B. Fehler beim Zugriff auf Speichermodule mit **Error Checking and Correction Funktion (ECC)**, an die Ereignisanzeige von Windows weitergeleitet.

6

Zugriffsverfahren

6.1 Zugang zum Übertragungsmedium regeln

Der Begriff Zugriffsverfahren

Nach den Vorüberlegungen zur physikalischen Topologie (Aufbau der Verkehrswege) und den Ausführungen zu den Übertragungsmedien (Zustand der Verkehrswege) wendet sich dieses Kapitel der Frage zu, wie der Datenverkehr auf den jeweiligen Übertragungswegen geregelt wird (Verkehrsregeln). Der wichtigste Aspekt dabei ist, mit welchem Verfahren auf das Medium zugegriffen wird, oder anders ausgedrückt, wie der Zugang zum Übertragungsmedium geregelt wird.

Ein **Zugriffsverfahren** ist ein Regelwerk, das festlegt, wie die Netzwerkknoten das Übertragungsmedium gemeinsam nutzen. Es bestimmt, wer wann in welcher Form senden darf. Häufig wird auch von einem Zugangsverfahren gesprochen.

Datenpakete

In Netzwerken ist es üblich, Daten in kleine Einheiten zu unterteilen und getrennt zu übertragen. Die Begrifflichkeit Daten wird meist stellvertretend gewählt für von Benutzern erstellte Dateien (z. B. Dokumente, E-Mails, Bilder) und Audio- bzw. Video-Informationen. Netzwerke müssen die Möglichkeit haben, diese unterschiedlichen Informationsarten auch unterschiedlich in ihrer Wichtigkeit zu werten, also zu priorisieren.

Als Bezeichnung für diese kleinen Einheiten werden Begriffe wie Paket, Rahmen oder **Frame** verwendet. Insgesamt wird bei dieser Art von Übertragung von **Paketvermittlung** gesprochen. Eine andere Art der Übertragung, nämlich die Leitungsvermittlung, wird im Bereich der Weitverkehrsnetzwerke eingesetzt und dementsprechend auch dort besprochen.

Shared Media

Existiert nur ein einziges gemeinsames Übertragungsmedium für alle Anwender (**Shared Media**, auch Shared Medium genannt), muss der Zugriff darauf geregelt werden. Damit eine Kommunikation zwischen den einzelnen Stationen möglich ist, müssen in einem Netzwerk alle beteiligten Knoten das gleiche Zugriffsverfahren verwenden.

Im LAN-Bereich haben sich für die Regelung dieses Zugriffs auf ein gemeinsames Medium im Laufe der Zeit zwei unterschiedliche Verfahren etabliert, nämlich **Carrier Sense Multiple Access with Collision Detection** (CSMA/CD) und **Carrier Sense Multiple Access with Collision Avoidance** (CSMA/CA). Beide Verfahren werden in den nächsten Abschnitten grundlegend erläutert. Netzwerke mit Switchen stellen **kein** Shared-Media dar, wenn sie im Vollduplex arbeiten, was heute Standard ist. Ein Funknetz (WLAN, UMTS ...) ist immer ein Shared Media im gleichen verwendeten Kanal.

Problem Broadcast/Multicast

In Shared-Media-Netzwerken ist es normalerweise sehr einfach, Nachrichten von einem Rechner an einen anderen (**Unicast**), an einige (**Multicast**) oder an alle Teilnehmer des Netzwerks (**Broadcast**) zu senden.

Allerdings kann dieser Vorgang auch zum Problem werden, wenn in kurzer Zeit sehr viele dieser Broadcasts erfolgen. Es kann z. B. zu einer drastischen Steigerung des Netzverkehrs kommen, sodass schließlich kein Datenaustausch mehr möglich ist (Broadcast Sturm).

- ✓ <https://de.wikipedia.org/wiki/Broadcast-Sturm>

Eine gängige Möglichkeit, dieses Problem zu verringern, ist die Aufteilung eines großen Netzes in mehrere Teilnetze, um diese danach mit geeigneten Geräten wieder miteinander zu koppeln (vgl. Kapitel 11/Kapitel 13).

6.2 CSMA/CD

Das ursprüngliche Zugriffsverfahren des Ethernets

Die Grundidee von **CSMA/CD** ist, dass jede Station zu senden beginnen kann, wenn das Medium nicht belegt ist (**Carrier Sense**). Dieses Verfahren ist nur bei Ethernet-Netzen mit logischer Bus-topologie erforderlich, wie bei Hubs und bei Switchen, die mit Halbduplex arbeiten.

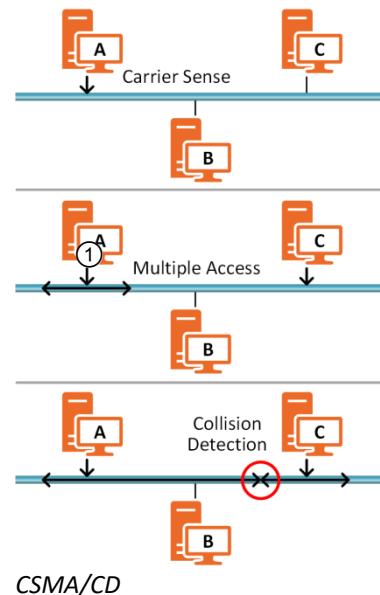
Die Stationen haben Zugang (**Multiple Access**) zum gemeinsamen Übertragungsmedium. Wenn Stationen das Medium als frei erkennen und gleichzeitig zu senden beginnen, treten Kollisionen auf, die von den Stationen erkannt werden (**Collision Detection**). Dabei spielt es grundlegend keine Rolle, ob auch physikalisch eine Bus-Topologie vorliegt oder ob die Verkabelung sternförmig realisiert wurde. Der Unterschied betrifft nur den konkreten Ort, an dem mit Kollisionen zu rechnen ist.

Vorgehen

Bei einer physikalischen Bus-Topologie (siehe Skizze) hängen die Stationen direkt am Kabel und die Signale der sendenden Station werden in beide Richtungen über das Kabel ausgestrahlt ①. Im Falle einer physikalischen Stern-Topologie würde dies erst im Verteiler stattfinden, da bis dorthin eine Station nur in eine Richtung sendet.

Der erste Teil der Abkürzung von CSMA/CD (Carrier Sense) ist dabei auch schon der erste Schritt, um Kollisionen zu verhindern. Dieser Schritt besteht darin, dass eine Station vor einer geplanten Sendung das Übertragungsmedium abhört, ob dieses zurzeit überhaupt frei ist.

Wenn sich auf dem Kabel aktuell bereits Signale befinden, unterlässt die Station einen Sendeversuch. Dies wird auch mit „listen before talking“ umschrieben.



Erkennen von Kollisionen

Kommt es zu einer Kollision, weil zwei Stationen das Kabel als frei vorfinden und gleichzeitig zu senden beginnen (Multiple Access), dann muss diese Kollision erkannt (Collision Detection) und darauf reagiert werden.

Zum Erkennen einer Kollision hören alle Stationen weiterhin das Übertragungsmedium ab. Die Station, die als Erste eine Kollision erkannt hat, sendet ein sogenanntes JAM-Signal aus (Der Begriff Jam kann mit Stau, Verstopfung, Gedränge, u. a. übersetzt werden). Jede Station, die dieses JAM-Signal registriert, stoppt unverzüglich die Sendung von Daten. Ist die Leitung wieder frei, können neue Sendeversuche gestartet werden. Dies kann auf zwei Arten geschehen:

Neuer Sendeversuch

Entweder wird nach einer zufällig gewählten Verzögerungszeit ein neuer Sendeversuch unternommen (non persistent CSMA, Standardeinstellung) oder aber die sendewillige Station hört weiter das Medium ab und sendet sofort, wenn sie das Medium als frei erkennt (1-persistent CSMA).

Wenn viele Stationen nach einer Kollision auf eine freie Leitung warten und sofort wieder zu senden beginnen, ist die nächste Kollision bereits vorprogrammiert. Daraus ergeben sich unter anderem folgende Nachteile:

Nachteile

- ✓ Je mehr Stationen angeschlossen sind und senden wollen, desto häufiger treten **Kollisionen** auf und desto geringer wird der effektive Datendurchsatz.
- ✓ Der Zeitpunkt einer Sendung kann nicht berechnet oder festgelegt werden, sondern ergibt sich zufällig (stochastisch oder nicht deterministisch).

Vorteil

Demgegenüber steht aber nach wie vor als hauptsächlicher Vorteil, dass eine Station rein theoretisch jederzeit senden kann, da nicht auf ein spezielles Signal des Netzwerks gewartet werden muss. Allerdings muss zum Senden die Leitung frei sein. Ist dies nicht der Fall, können sich Verzögerungen ergeben.

6.3 Von Shared Media zu Switched Networks

In modernen Netzen werden Sie, mit Ausnahme von Funktechniken (WLAN, Bluetooth etc.), keine Shared Media vorfinden, wo alle User an einem einzigen Medium angeschlossen sind. Vielmehr ist jeder User dediziert über ein Medium mit dem Switch verbunden. Die Kommunikation erfolgt im Vollduplexmodus (fdx), die Station kann somit gleichzeitig Daten senden und empfangen. Durch diesen Modus gibt es keine Kollisionen, da eine Funktion (Flow-Control) dies überwacht. Bei Switches ist CSMA/CD daher überflüssig (vgl. Kapitel 13).

Bei 10-Mbit- und 100-Mbit-Ethernet werden auf dem Twisted-Pair-Kabel im Halbduplexbetrieb ein Adernpaar und im Vollduplexmodus zwei Adernpaare verwendet. Ab 1-Gbit-Ethernet werden alle vier Aderpaare genutzt.

In einem Switched Network steht damit dem User die maximale Bandbreite zum Switch zur Verfügung.

Gigabit-Ethernet

Gigabit-Ethernet (auch 1000-Mbit-Ethernet, GbE oder GigE genannt) hat zusätzliche Mechanismen für die Fehlerreduzierung auf dem TP-Kabel integriert. Da ist einerseits die Trelli-Kodierung für die Fehlerkorrektur und andererseits das Verwürfeln (Scrambling) der Informationen, um die gegenseitige Beeinflussung (Übersprechen) der einzelnen Adernpaare zu verhindern. Neben der Übertragung auf TP-Kabeln (1000Base-T), die im Standard IEEE 802.3 Clause 40 hinterlegt sind, ist auch ein Lichtwellenleiter (1000Base-SX, 1000Base-LX/LH) nutzbar. Dies wird im Standard IEEE 802.3 Clause 38 dokumentiert.

Mit der Einführung von Gigabit-Ethernet ist es möglich, Jumbo-Datenframes, die größer als 1518 Bytes sind, zu übertragen. Dadurch wird die verfügbare Bandbreite effizienter genutzt.

! Jumbo-Datenframes sind allerdings nicht nach IEEE 802.3 standardisiert, so dass es damit zu Inkompatibilitäten kommen kann. Sie werden daher nur selten bzw. wenn, dann meist nur bis zu einer **Maximum Transmission Unit (MTU)** von 9000 Byte eingesetzt.

10-Gigabit-Ethernet

10-Gbit-Ethernet (auch als 10GE/10GbE oder 10 GigE bezeichnet) arbeitet nur noch im Voll-duplexmodus und wird oft über Lichtwellenleiter (Standard IEEE 802.3ae) angebunden, obwohl es auch für Twisted-Pair-Kabel der Kategorie 6 (Standard 802.3ak-2004 und IEEE 802.3an-2006) spezifiziert ist. Es wird vorrangig für die Anbindung schneller Server oder für das Clustering von Servern im LAN und für SAN-Lösungen angewendet.

Im Metropolitan Area Network (MAN) und Wide Area Network (WAN) haben Internet Service Provider (ISPs) inzwischen eigene 10GE-Backbones für die Kommunikation aufgebaut.

100-Gigabit-Ethernet

Mitte 2010 wurde der Standard IEEE 802.3BA verabschiedet, welcher eine Datenübertragung von 40 Gbit/s als auch 100 Gbit/s über Kabel und Lichtwellenleiter beschreibt. Dieser Standard ist vorrangig für den Einsatz in Rechenzentren und im WAN-Bereich vorgesehen.

6.4 CSMA/CA

Das Zugriffsverfahren des WLANs

Das Wireless Local Area Network (**WLAN**, vgl. Kapitel 4.5) arbeitet mit dem **CSMA/CA**-Netzwerk-zugriffsverfahren (**Carrier Sense Multiple Access with Collision Avoidance**), das auch beim Wired AppleTalk-Protokoll angewendet wird. Es ist eine Modifikation des CSMA/CD-Verfahrens.

Genau wie bei CSMA/CD hören die Stationen physikalisch den Verkehr auf dem Medium ab (**Carrier Sense**). Will eine Station senden (**Multiple Access**), wartet sie auf das freie Medium. Wenn das der Fall ist, wird ein Zeitzähler mit einer fest vorgegebenen Wartezeit und einer Zufallszeit gestartet und erst dann das Datenframe übertragen.

Sendet in dieser Gesamtwartezeit eine andere Station, wird der Zeitzähler gestoppt und nach deren Übertragungsende erneut gestartet. Damit wird die Priorität des Übertragungswunsches erhöht. Da die Stationen unterschiedliche Zeitzählerstände aufweisen, werden Kollisionen weitestgehend vermieden (**Collision Avoidance**).

Nach erfolgreicher Übertragung antwortet der Empfänger mit einer Bestätigung (ACK-Frame) und eine andere Station kann nun ihr Datenframe übertragen.

Die Funktion von WLAN wird im Standard IEEE 802.11 und deren Untergruppen beschrieben (vgl. Kapitel 4).

6.5 Zusammenfassung und Ausblick

Etablierte Netzwerkzugriffsverfahren

In lokalen Netzwerken haben sich heute Switches mit Vollduplex und bei WLANs das Zugriffsverfahren CSMA/CA durchgesetzt.

Vor- und Nachteile von Ethernet

Ethernet bietet eine breite Auswahl an hohen Datenübertragungsraten. Neben Gigabit-Ethernet existieren Standards von 10 Gbit/s, 40 Gbit/s und 100 Gbit/s. Die nächste Ethernet-Evolution wird bei 1Tbit/s (1 Terabit per second) liegen und in den nächsten Jahren zur Verfügung stehen. Bei diesen Übertragungsraten kommen ausschließlich Lichtwellenleiter als Medium zu Einsatz.

Somit migrieren lokale Zugriffsverfahren in den WAN-Bereich und ersetzen klassische WAN-Verfahren. In diesem Zusammenhang wird auch der Begriff Carrier Ethernet oder Metro Ethernet genannt. Das Standardisierungsgremium für Carrier Ethernet ist das **Metro Ethernet Forum (MEF)**.

In großen lokalen Netzen sind hohe Bandbreiten für den Primärbereich (Backbone) interessant. Sie können damit Gebäude mit einer hohen Bandbreite anbinden.

Ein weiterer Aspekt ist die Anbindung von im Netzwerk integrierten **SAN**-Systemen. Die bisherige Anbindung dieser Systeme über Fibre Channel und iSCSI wird zunehmend in Ethernet integriert. Beispiel hierfür ist **Fibre Channel over Ethernet (FCoE)**. Dieser Aspekt wird bei der Virtualisierung von Speichersystemen in Rechenzentren und großen Netzwerken umgesetzt (vgl. Kapitel 8).

Echtzeit-Ethernet

Ethernet garantiert keine festen Zeiten für die Ankunft eines Frames beim Empfänger. Für einige Anwendungen, wie in der Automatisierungstechnik, bei Audio- und Video-Systemen etc. sind jedoch konstante Laufzeiten sehr wichtig. Die Norm **IEEE 802.1as** (Timing and Synchronisation for Timing-Sensitive Applications in Bridged Local Area Networks) stellt eine Echtzeit-Erweiterung für Ethernet dar. Dabei kommen Synchronisationsmechanismen nach **IEEE 1588** (Precision Time Protocol) zum Tragen.

Vor- und Nachteile von WLAN

WLAN hat als größten Vorteil den flexiblen Standort der Nutzer und Geräte. Für die Inbetriebnahme eines WLANs sind wenige bauliche Maßnahmen erforderlich. Beispiele sind öffentliche Bereiche und denkmalgeschützte Gebäude. In der Öffentlichkeit haben sich kommerzielle **Wireless Internet Service Provider (WISP)**, z. B. Mobilfunkbetreiber, Swisscom Eurospot, ISIS Arcor Hot Spot etc., öffentliche WLAN-Projekte (z. B. in Hamburg, Bochum und Düsseldorf) oder kleine Hotspot-Anbieter (z. B. in Cafés und Hotels) etabliert.

Der Vorteil der Flexibilität wird jedoch durch die zumeist geringere Übertragungsrate relativiert (die sich alle angeschlossenen Geräte teilen müssen und die zudem abhängig von Umgebungs-Hindernissen ist) und stellt somit eine Ergänzung und keine Alternative zur Verkabelung dar.

Ein weiterer Vorzug von WLAN liegt in der kostengünstigen Vernetzung zwischen Gebäuden, sofern keine Kabelinfrastruktur vorhanden ist.

Als großes Risiko stellte sich vor einigen Jahren die sogenannte Störerhaftung dar, nach der ein Betreiber eines Hotspots für rechtliche Verfehlungen der Nutzer haftbar ist (z. B. Filesharing, beleidigende E-Mails). Dies ist nach aktueller Rechtsprechung nicht mehr der Fall. Dennoch bleibt es bei der dringenden Empfehlung, private WLANs grundsätzlich verschlüsselt zu betreiben, da dies auch andere rechtliche Auswirkungen haben kann und der Zugang zum Internet über freie WLAN-Netze auf die grundsätzlichen Dienste beschränkt sein sollte. Weitere Informationen zur Störerhaftung finden Sie hier:

- ✓ <https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/stoererhaftung-besserer-schutz-fuer-wlanbetreiber-19261>
- ✓ <https://www.handelsblatt.com/unternehmen/it-medien/bgh-bestaeigt-haftung-fuer-freie-wlans-wird-abgeschafft/22846910.html?ticket=ST-5472892-7cLMfNRffie6V0F1sblr-ap5>
- ✓ <https://www.ihk-nuernberg.de/de/Geschaeftsbereiche/Recht-Steuern/Rechtsauskuenfte/Recht-des-E-Commerce-Internetrecht/haftung-von-wlan-anbietern/>

7

Arbeitsweise lokaler Netze

7.1 Umsetzung im LAN

Nach all den Vorüberlegungen der letzten Kapitel kann nun mit einer konkreten Planung für die Umsetzung des Netzwerks begonnen werden. In den folgenden Abschnitten werden die Informationen zu den Themen Topologie, Übertragungsmedien und Zugriffsverfahren zusammengefasst und die wichtigsten Realisierungen in der Praxis aufgeführt.

Die beiden Hauptrichtungen in Bezug auf den Aufbau lokaler Netze, die sich im Laufe der Jahre herausgebildet haben, sind Ethernet und ergänzend WLAN.

7.2 Ethernet

Die Entwicklung von Ethernet

Ethernet wurde über die Jahrzehnte hinweg in vielen Belangen, unter anderem in Bezug auf die Geschwindigkeit, weiterentwickelt. Dieses Kapitel beschreibt die Varianten ab 10 Mbit/s, da sie in der Praxis z. T. noch vorkommen. Neue Netze sollten dagegen mindestens mit Gigabit-Ethernet eingerichtet werden. Eine genauere Beschreibung erfolgt im weiteren Verlauf dieses Buchs zusammen mit 10-Gigabit-Ethernet bei größeren lokalen Netzen (vgl. Kapitel 14).

Geschichte

Die Geschichte des Ethernets geht zurück bis in die 70er-Jahre und ist eng verbunden mit dem Namen Robert Metcalfe, der damals für die Firma Xerox am Palo-Alto-Forschungszentrum (PARC) in Kalifornien erste Netze dieser Art realisierte.

Im Laufe der Weiterentwicklung wurde dann Mitte der 70er-Jahre von den Firmen DEC, Intel und Xerox (DIX) Ethernet II mit einer Übertragungsrate von 1 Mbit/s bis 10 Mbit/s als Standard definiert, der auch unter dem Namen „Blue-Book-Standard“ bekannt wurde.

Weitere, zum Teil von diesem ersten Standard abweichende Normierungen wurden danach von den dafür zuständigen nationalen oder internationalen Gremien durchgeführt. In erster Linie ist dies das **IEEE** (Institute of Electrical and Electronic Engineers) und hier vor allem die Projektgruppe 802, die seit Februar 1980 den verabschiedeten Normen auch die entsprechende Nummerierung gibt. Unter der Bezeichnung IEEE 802.3 sind wichtige Vorgaben für Ethernet festgeschrieben.



Ergänzende Lerninhalte: *Weiterführende Informationen.pdf*

In diesem Dokument finden Sie u. a. eine detaillierte Aufstellung der Standards dieser Projektgruppe.

Kennzeichen

Ethernet bezeichnet Netze, die sich unter anderem durch folgende Kennzeichen beschreiben lassen:

- ✓ Der logische Aufbau entspricht einer Bus-Topologie.
- ✓ Bei der Verwendung von UTP, STP oder Glasfaser wird physikalisch eine Stern-Topologie eingesetzt.
- ✓ Der logische Aufbau über Switches entspricht ebenfalls einer Stern-Topologie.
- ✓ Die Verkabelung erfolgt heute nur noch mit Switches als zentralen Verbindungselementen.
- ✓ Das Zugriffsverfahren CSMA/CD ist bei Koax-Kabeln sowie Hubs erforderlich und damit veraltet.

10Base-T (Ethernet)

Die Abkürzung beschreibt eine Vernetzung mit 10 Mbit/s mit **Twisted-Pair-Kabel**. Die Norm IEEE 802.3 wurde 1991 um 10Base-T erweitert und schreibt UTP oder STP der Kategorie 3, 4 oder 5 mit RJ-45-Steckern vor. Dieser Standard wird nun unter IEEE 802.3 Clause 14 geführt.

10Base-F (Ethernet)

10Base-F beschreibt eine Vernetzung mit 10 Mbit/s über Glasfaserkabel. Im Unterschied zu 10Base-T ergeben sich höhere Kosten für die aktiven Komponenten (Verteiler), aber eine deutlich größere Reichweite. Dieser Standard ist unter IEEE 802.3 Clause 16-18 hinterlegt.

100Base-TX (Fast Ethernet)

Die Bezeichnung **100Base-T** steht für mehrere Arten von **Fast Ethernet**. Davon hat sich in der Praxis **100Base-TX** durchgesetzt. Sie definiert eine Datenübertragung von 100 Mbit/s auf einem Twisted-Pair-Medium der Kategorie 5 (IEEE 802.3 Clause 25). Niedrigere Übertragungsraten sind heute bedeutungslos.

100Base-FX

Definiert eine Datenübertragung von 100 Mbit/s über Lichtwellenleiter (IEEE 802.3 Clause 26).

1000Base-T (Gigabit-Ethernet)

Kennzeichnet eine Datenübertragung von 1000 Mbit/s (1 Gbit/s) auf einem Twisted-Pair-Medium, wobei alle 4 Adernpaare benutzt werden und das Kabel mindestens Kategorie 5 (5e) entsprechen muss (IEEE 802.3 Clause 40). Alternativ können Lichtwellenleiter verwendet werden. Es kommt nur Vollduplex zum Einsatz.

10GBase

Insgesamt 10 Standards definieren 10 Gbit/s für verschiedene Medien. Der gebräuchlichste ist dabei **10GBase-T**. Er klassifiziert eine Datenübertragung von 10 Gbit/s auf einem Twisted-Pair-Medium, wobei für die Kabel mindestens Kategorie 6A für die maximale Länge von 100 m Anwendung findet (IEEE 802.3an), bei kurzen Entfernung (ca. 20–40 m je nach Art der Kabelabschirmung) auch Kategorie 5 (5e).

100GBase-SR10

Beschreibt eine Datenübertragung von 100 Gbit/s auf Multimode-Lichtwellenleiter nach der Norm IEEE 802.3BA.

100GBase-LR4 (100GBase-ER4)

Festlegung für eine Datenübertragung von 100 Gbit/s über Singlemode-Lichtwellenleiter (IEEE 802.3BA).

Ausdehnung

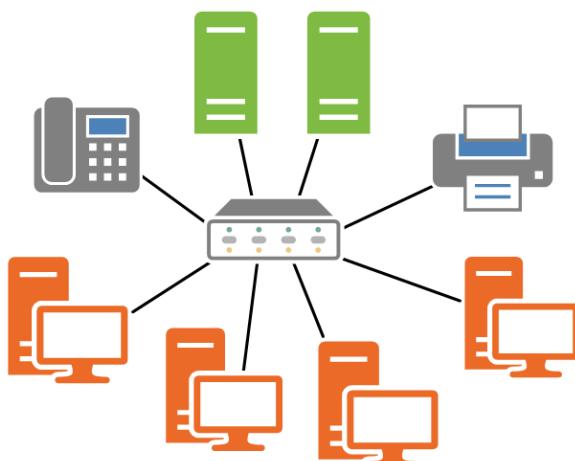
Den beschriebenen Verfahren liegt bei der Verwendung von Twisted-Pair-Kabeln eine maximale Ausdehnung zwischen zwei aktiven Komponenten von 100 m zugrunde. Mit Lichtwellenleitern lassen sich (je nach Medium) deutlich größere Ausdehnungen realisieren.

Hub und Switch

Die Verlegung erfolgt physikalisch als Stern-Topologie, was auch bedeutet, dass hier erstmals ein weiteres Gerät als zentrale Steuereinheit integriert werden muss. Früher wurde hierfür ein Hub (englisch für „Nabe“) eingesetzt, heute werden dazu Switches verwendet. In den folgenden Kapiteln erfahren Sie mehr zur Arbeitsweise von Switches.

Praxiseinsatz

Viele kleinere LANs verwenden noch 100Base-TX. Bei Neuinstallationen kommt fast nur noch 1000BaseT (Gigabit) und höher zum Einsatz. Ältere Geräte mit geringerer Übertragungsrate werden dabei von einem Switch ebenfalls akzeptiert, sofern die Steckverbindungen zusammenpassen (nicht RJ-45-Stecker auf Lichtleiter-Buchse und umgekehrt). Die Kabeldistanz zwischen den Komponenten und dem Switch darf dabei nicht mehr als 100 m betragen, bezogen auf Twisted-Pair-Kabel. Bei Lichtwellenleitern ist die Entfernung vom Typ (Singlemode oder Multi-mode) abhängig. Jede Station ist dabei dediziert angebunden.



Beispiel-Netzwerk mit Geräten, die 100Base-TX, 1000Base-T und 10GBase-T verwenden

Der eingesetzte Switch im Zentrum ermöglicht im Normalfall die Ausnutzung der verfügbaren Bandbreite zwischen zwei kommunizierenden Endgeräten.

Dazu sollten die Server mit einer höheren Bandbreite (z. B. 10GBase-T) angeschlossen werden, damit die von den angeschlossenen Stationen angeforderten Daten vom bzw. zum Server zügig übertragen werden können, z. B. mit dem Verfahren Store-and-Forward bei Switchen (vgl. Kapitel 13).

Daneben können Server auch mit mehreren Netzwerkadapters angeschlossen werden, um so mehrere Clients insgesamt mit hoher Bandbreite bedienen zu können (**Link Aggregation Control Protocol**, LACP; vgl. Kapitel 14). Ein weiterer Vorteil dieses Verfahrens ist die erhöhte Ausfallsicherheit, wenn die Verbindungen über mehrere Server und Switches verlegt sind.

Mehrere Switches können auch problemlos hintereinandergeschaltet (kaskadiert) werden, um flexibel weitere Stationen in ein bestehendes Netz einzufügen.

Normung

Sowohl der Einsatz für Twisted-Pair-Kabel als auch für Glasfaser wurde geregelt und in folgenden Variationen genormt. Hier ein Auszug:

- ✓ **100Base-TX:** vieradrige Leitungen mindestens der Kategorie 5 bzw. 5e (von den vorhandenen 8 Adern werden nur 4 Adern benutzt)
- ✓ **100Base-T4:** achtadrige Leitungen mindestens der Kategorie 3 oder höher; wird bei Neuverkabelungen nicht mehr benutzt
- ✓ **100Base-FX:** Multimode-Glasfaserkabel mit zwei Fasern
- ✓ **1000Base-T:** achtadrige Leitungen mindestens der Kategorie 5 oder höher
- ✓ **1000Base-SX:** Multimode-Glasfaserkabel für eine maximale Distanz bis 550 m
- ✓ **1000Base-LX:** Multimode-Glasfaserkabel (bis 550 m) bzw. Singlemode-Glasfaserkabel (bis 5 km)
- ✓ **1000Base-ZX:** Singlemode-Glasfaserkabel für eine maximale Distanz bis 100 km
- ✓ **10GBase-T:** achtadrige Leitungen mindestens der Kategorie 6A oder höher
- ✓ **10GBase-SR:** Multimode-Glasfaserkabel für eine maximale Distanz bis 300 m
- ✓ **10GBase-LR:** Singlemode-Glasfaserkabel für eine maximale Distanz bis ca. 25 km
- ✓ **100GBase-SR10:** Multimode-Glasfaserkabel mit zehn WDM-Pfaden und maximale Distanz bis 100 m
- ✓ **100GBase-LR4:** Singlemode-Glasfaserkabel mit vier DWDM-Pfaden und maximale Distanz bis 10 km

Der Vorteil der Normung liegt in der Möglichkeit, bestehende Implementierungen Zug um Zug an die höhere Geschwindigkeit anzupassen. Das ist für den Umstieg von Fast Ethernet zu Gigabit-Ethernet bzw. von Gigabit-Ethernet zu 10-Gigabit-Ethernet relativ einfach, da bei vielen Installationen bereits Kabel der Kategorie 5/6 und höher bzw. entsprechende Lichtwellenleiter vorhanden sind.

8

Betriebssysteme und Server

8.1 Einteilung von Betriebssystemen

Arten von Betriebssystemen

Die Auswahl des am besten geeigneten Betriebssystems für das Netzwerk sowie die Ausstattung und Positionierung des Servers bzw. der Server im LAN sind keine einfachen Aufgaben. Das ideale Betriebssystem wird es nie geben, und die immer höheren Anforderungen an ein Netzwerk fordern eine fast permanente Erweiterung der Hardware.

Dieses Kapitel gibt eine kurze Übersicht über den aktuellen Stand der Dinge in Bezug auf Betriebssysteme.

Client-Server

Im Folgenden werden hauptsächlich Betriebssysteme betrachtet, die auch aus einem normalen PC einen Server machen können, der allen angeschlossenen Systemen Dienste zentral zur Verfügung stellt. Diese werden dann von den Clients abgerufen (vgl. Kapitel 2.3).

Mainframe (Großrechner)

Im Mainframe-Bereich werden meist herstellerspezifische Betriebssysteme verwendet. So liefern auf diesem Gebiet führende Hersteller wie IBM, HP, Fujitsu, Sun (Oracle) und andere jeweils eigene Betriebssysteme mit, wie z. B. IBM i (vormals i5/OS bzw. OS/400) und AIX, HP-UX, BS2000/OSD oder Solaris. Häufig sind diese Entwicklungen vergleichbar mit UNIX, aber den speziellen Gegebenheiten des jeweiligen Rechners angepasst.

Mainframes werden sukzessive von Server-Clustern abgelöst und damit durch Standard-Betriebssysteme ersetzt. Dennoch sind sie für spezifische Applikationen bzw. für die Migration auf Standardapplikationen unentbehrlich (z. B. POWER8 von IBM).

Wo es dagegen auf Zuverlässigkeit und hohen Datendurchsatz ankommt (Banken, Versicherungen, große Unternehmen oder die öffentliche Verwaltung), sind Mainframes unverzichtbar.

Im Gegensatz zu Mainframes sind sogenannte Supercomputer oder Superrechner auf maximale Rechenleistung ausgelegt. Es werden dabei zunehmend Cluster von normalen Servern verwendet, die jedoch für bestimmte Prozesse optimiert sind (z. B. Fließkommaberechnung). Eingesetzt werden diese z. B. bei meteorologischen Berechnungen, naturwissenschaftlichen Simulationen und dem Militär.

Bladeserver

Ein Bladeserver besteht aus einer Reihe von Hauptplatten mit Prozessoren und Hauptspeicher, die in einem gemeinsamen Gehäuse verbaut sind. Netzteile und Speichermedien werden von den Rechnern gemeinsam verwendet. Dies bringt Vorteile bei der Skalierbarkeit, dem Platzbedarf, den Kosten und dem Verwaltungsaufwand, vor allem bei der Bereitstellung von Windows-Servern.

Nachteilig wirkt sich die hohe Wärmeentwicklung aus, die bei der Planung ebenso wie der Strombedarf berücksichtigt werden muss.

Bei der Konsolidierung von Serverfarmen haben Bladeserver die Mainframes inzwischen oft verdrängt.

8.2 Aufgabengebiete von Betriebssystemen

Basisaufgaben

Betriebssysteme werden allgemein als **OS (Operating System)** oder oft auch einfach nur als „System“ bezeichnet, wenn der Zusammenhang klar ist. So steht z. B. der Begriff **DOS** für Disk Operating System.

Ein Betriebssystem besteht grundsätzlich aus zwei Teilen, dem Betriebssystemkern (Kernel) und den installierten **Applikationen**. Der Kernel hat dabei die Aufgabe, den Applikationen Ressourcen der Hardware, z. B. Speicherbereiche, IRQs und Prozessorleistung, zur Verfügung zu stellen. Den Applikationen stehen einerseits eine Schnittstelle zum Kernel und andererseits eine Verbindung zum Benutzer über ein **Command-Line Interface (CLI)** oder **Graphical User Interface (GUI)** zur Verfügung. Die CLI besteht aus einer textbasierten Oberfläche ohne Mausunterstützung, z. B. UNIX- oder DOS-Shell (Eingabeaufforderung). Sie kann, muss aber keine grafischen Elemente haben. Dagegen bietet eine GUI grafische Elemente (**Widgets**), mit der über Maus, Touchpad oder Touchscreen das System bedient werden kann.

Unterteilung von Betriebssystemen

Jedes aktuelle Betriebssystem kann über ein Netzwerk kommunizieren. Die Bezeichnung „Netzwerk-Betriebssystem“ ist daher kaum noch gebräuchlich. Ausnahmen stellen **Embedded-Systeme** dar. Hier wird ein Betriebssystem auf die minimal nötigen Funktionen reduziert, um z. B. eine Waschmaschine oder eine Kaffeemaschine zu steuern. In Zukunft sollen weitere Geräte ebenfalls Internetzugang erhalten (Internet of Things, vgl. Kapitel 4.7).

Die Bezeichnung „Server-Betriebssystem“ wird zwar oft benutzt, aber eher künstlich, da es von der Firmenpolitik abhängt, welche Funktionen ein derartiges Betriebssystem bietet. So sind z. B. bei den Desktop-Versionen von Windows die maximalen Zugriffe vom Netzwerk her limitiert. Bei den Server-Versionen von Windows gibt es diese Grenze nicht, jedoch sind für den Betrieb bestimmte Zugriffslizenzen zu erwerben.

Der Begriff „Server-Betriebssystem“ soll zum Ausdruck bringen, dass ein Betriebssystem viele Server-Anwendungen enthält. Bei Windows-Server-Systemen ist heute vor allem der **Domänencontroller** (DC) für diese Namensgebung ausschlaggebend. In den 90er Jahren stellte ein Novell-Server noch ein reines Server-Betriebssystem dar, welches keine Client-Programme enthielt. Aus dieser Zeit stammt noch, dass unter dem Begriff „Server“ in der Regel ein **File-Server** gemeint ist. Zum Client-Server-Prinzip siehe auch Kapitel 2.3.

Core Services

Neben der Kommunikation über ein Netzwerk ergeben sich weitere Aufgaben, die mittlerweile als Standard angesehen werden. Diese oft auch als **Core Services** bezeichneten Dienste sind u. a.:

- ✓ **File Service:** Dateien im Netz zur Verfügung stellen,
- ✓ **Print Service:** Drucker im Netz zur Verfügung stellen,
- ✓ **Authentification:** einzelne Benutzer eindeutig identifizieren,
- ✓ **Directory Service:** alle Netzwerkressourcen zentral verwalten.

Moderne Betriebssysteme für Serveranwendungen haben diese Core Services bereits integriert und verzichten hierbei meist auf eine klare Trennung der einzelnen Dienste.

Directory Service

Mit dem Begriff Directory Service (Verzeichnisdienst) ist gemeint, die Vielzahl der Einzelkomponenten eines Netzwerks übersichtlich und skalierbar (flexibel erweiterbar) zu organisieren. In erster Linie geht es dabei um die zentrale Verwaltung von Benutzern und deren Ressourcen. Zu diesem Zweck wurde das Protokoll X.500 definiert. Mit dem **Lightweight Directory Access Protocol (LDAP)** gibt es eine vereinfachte Implementierung davon, die die Basis heutiger Verzeichnisdienste darstellt.

! Der Begriff Directory Service hat nichts mit dem Begriff Directory im Sinne von Ordnern bzw. Verzeichnissen bei Betriebssystemen zu tun, sondern ist eher im Sinne eines Telefonbuchs (engl. telephone directory) zu verstehen, in dem zentral alle für das Netzwerk relevanten Daten zusammengefasst sind.

Benutzerverwaltung

Die Benutzerverwaltung regelt, welcher Benutzer Zutritt zum Netzwerk hat und was er dort tun darf. Dabei bringt eine zentrale Verwaltung der Benutzer u. a. folgende Vorteile mit sich:

- ✓ Ein Benutzer kann sich nur mit gültigem Namen und Kennwort am Netzwerk anmelden und erhält dann dediziert Zugriff auf die benötigten Applikationen.

- ✓ Benutzer mit gleicher Aufgabenstellung können zu Gruppen zusammengefasst werden und erhalten über ihre Gruppenzugehörigkeit ihre Rechte im Netzwerk.
- ✓ Ein oder mehrere Administratoren verwalten Benutzer und Gruppen zentral.

Insgesamt lässt sich so eine systematischere und damit auch übersichtlichere Struktur des Netzwerks aufbauen. Auch unter dem Aspekt der Sicherheit ist es vorzuziehen, dass Administratoren festlegen, auf welchem Weg auf die Ressourcen zugegriffen werden darf.

Ressourcen-Verwaltung

Darunter fallen z. B. Ressourcen wie Drucker oder Speicherplatz auf Festplatten. Für den Anwender soll der Zugriff auf diese Ressourcen transparent erfolgen, d. h. der Benutzer soll komfortabel mit diesen Ressourcen arbeiten können, ohne weitere technische Details zu kennen. Auch dies lässt sich effektiver erreichen, wenn eine zentrale Verwaltung des gesamten Netzwerks existiert.

Erweiterung der Aufgabenbereiche

Etliche Erweiterungen der Standardaufgaben eines Betriebssystems hängen deutlich mit dem Thema Internet zusammen und betreffen Dienste wie z. B. Webserver, DNS-Server, Proxy-Server oder die Sicherheit über eine Firewall zzgl. eines Virenschutzes.

Während ein Webserver Informationen firmenintern oder für externe Nutzer zum Abrufen per Browser bereitstellt, kümmert sich ein Proxy-Server stellvertretend für die Benutzer des LANs um einen zentralen Zugang zum Internet. Eine **Firewall** schließlich steht zwischen LAN und Internet oder zentral im LAN und soll unbefugten Datenzugriff verhindern. Die meisten Hersteller bieten hier eigene oder über Fremdanbieter geeignete Lösungen an.

Darüber hinaus gibt es etliche weitere Themen, die eine Ausweitung der Aufgabenbereiche des Betriebssystems deutlich machen. Exemplarisch dazu folgende Stichworte:

- ✓ Anbindung an eine **Datenbank**,
- ✓ Anbindung eines LANs an Mainframe,
- ✓ Zusammenfassung mehrerer Server zu sogenannten **Clustern**,
- ✓ Optimierung der Replizierung von Daten zwischen verschiedenen Standorten.

8.3 Microsoft Windows

Betriebssysteme in Server- und Clientversionen

Seit der Markteinführung von Windows NT (New Technology) im Jahr 1993 hat Microsoft eine ganze Reihe von darauf aufbauenden Betriebssystemen im Client- und Serversegment veröffentlicht. Aktuell unterstützt, wenn zum Teil auch nur im Rahmen des erweiterten Supports, werden die nachfolgend aufgelisteten OS Versionen:

- ✓ Windows 7, 8.1, 10, 11
- ✓ Windows Server 2008, 2008R2, 2012, 2012R2, 2016, 2019, 2022

Das Client-Betriebssystem Windows XP war im Oktober 2021, laut Erhebung der Firma Net Market-share, nur noch mit 0,27 % im Einsatz, obwohl der Support und damit auch die Verfügbarkeit von Sicherheitsupdates im April 2014 auslief. Windows 8.1 war im gleichen Zeitraum zu 2,21 % vertreten. Den Rest des circa 87,56 % Markanteils teilen sich Windows 7 (19,77 %) und Windows 10 (67,65 %). Die verbleibenden 12,44 % sind von anderen Betriebssystemen wie macOS, Linux und anderen Windows-Versionen belegt.

Veraltete Betriebssysteme sollten nicht mehr benutzt werden, sobald ein Rechner mit dem Internet verbunden ist, da neben einem tagesaktuellen Antivirenschutz auch die Herstellerupdates zur Sicherheit des Gesamtsystems beitragen.

Windows 10 sollte nach Aussage von Microsoft die vorerst letzte Desktop-Windows Version sein. Durch halbjährliche Updates, die für den am meisten verbreiteten „Semi Annual Channel“ (einer der möglichen Updatekanäle für Windows 10) gelten, sollte es unbegrenzten Support und neue Funktionen erhalten. Mit der Veröffentlichung von Windows 11 und der Ankündigung, Windows 10 nur noch bis 2024 bzw. 2025 zu unterstützen, sind diese Pläne von der Realität überholt worden. Windows 11 wird als kostenloses Update an alle Windows-10-Anwender verteilt, deren Hardware über die erforderlichen Voraussetzungen (Intel Prozessor Gen. 8 / TPM 2.0) verfügt.

Die Betriebssystemlizenz ist an die verwendete Hardware gebunden, wodurch die Weiterverwendung von Windows 10/11 auf einem neuen Rechner nicht mehr möglich ist. Auch sind die Lizenzinstellungen für Windows zunehmend im BIOS untergebracht. Derzeit steht der Rollout der Windows Version 21H2 an. Nach einem Upgrade auf Windows 11 trägt dieses die gleiche Versionsnummer. Windows Server 2022, als Nachfolger von Windows Server 2019, wurde im August 2021 veröffentlicht. Windows Server unterstützt bereits seit seiner Version 2000 die Einrichtung und den Betrieb von Netzwerkinfrastrukturen mit einer zentralen Benutzer-, Ressourcen- und Rechteverwaltung. Außerdem stellt es Standarddienste und Anwendungen für das Netzwerk bereit. In den letzten Versionen zeigt sich deutlich eine Entwicklung in Richtung Cloud-Computing und deren Absicherung mit Cloud-Diensten wie Microsoft Azure.

Während Windows traditionell als System mit einer grafischen Benutzeroberfläche verstanden wird, ist es seit Server 2012 auch möglich, sogenannte Core Installationen durchzuführen, die auf diesen „Aufsatz“ verzichten. Ähnlich wie bei Unix oder Linux Systemen erfolgt die Systemverwaltung über die Kommandozeile. Zu diesem Zweck steht eine leistungsstarke Befehlsverarbeitung, die Power Shell, zur Verfügung. Ein weiterer Vorteil der Core Installation ist der Wegfall aller GUI-Updates und Anwendungen, die reduzierte Systemanforderung und vor allem eine verkleinerte Angriffsfläche. Jede Software kann potenzielle Fehler oder andere Unzulänglichkeiten aufweisen, die durch den Wegfall der grafischen Oberfläche minimiert ist.

Auch scheint sich Microsoft der Open Source Welt gegenüber weiter zu öffnen, da beispielsweise nun auch Linux als Installationsplattform für den SQL Server verwendet werden kann und der hauseigene Hypervisor Hyper-V verschiedene Linux Derivate direkt unterstützt.

Zusätzliche Produkte

Windows-Server bilden oft die Basis für weitere Microsoft-Produkte, mit denen spezialisierte Serverdienste installiert werden können. Die folgende Tabelle nennt zwei bekannte Beispiele dazu:

Produkt	Beschreibung
MS Exchange Server	Server für E-Mail, Gruppenterminplanung, elektronische Formulare usw. zur Nutzung auf einer gemeinsamen Plattform
MS SQL Server	Relationales Datenbank-Management-System, das den Zugriff von vielen Clients auf zentrale Datenbestände ermöglicht und regelt

8.4 UNIX

Herstellerunabhängige Entwicklung

Die Entwicklung von **UNIX** reicht zurück bis zum Ende der 60er Jahre und ist dort eng verbunden mit den Namen Ken Thompson und Dennis Ritchie, die damals in den AT&T Bell Laboratories arbeiteten. Die leichte Portierbarkeit des Betriebssystems auf unterschiedliche Hardware-Plattformen führte im Laufe der Zeit zur Entstehung von unzähligen Varianten. In letzter Zeit wird UNIX immer mehr von Linux-Systemen und Server-Versionen von Windows abgelöst.

Vorteile

Hauptgründe, warum UNIX auch heute noch eine sehr große Bedeutung im Netzwerkbereich hat, sind die leichte Portierbarkeit auf verschiedene Plattformen und die Unterstützung von TCP/IP bereits von Anfang an. Damit stellt es quasi eine Referenz für die Netzwerktechniken im Internet dar. Es ist zudem skalierbar (vom PC bis zum Großrechner), sehr stabil und kaum von Viren bedroht. Daher werden auch heute noch viele wichtige Server im Internet mit UNIX oder dessen Varianten Linux, Solaris u. a. betrieben.

UNIX ist nicht nur ein Multitasking-, sondern auch ein Multiuser-Betriebssystem, d. h., auf einem UNIX-Rechner können gleichzeitig unterschiedliche Programme ausgeführt werden und auch verschiedene Personen angemeldet sein. UNIX kann sowohl als Client- als auch als Server-Betriebssystem eingerichtet werden.

Varianten

Die leichte Portierbarkeit des Betriebssystems auf unterschiedliche Hardware-Plattformen führte im Laufe der Zeit zur Entstehung von unzähligen Varianten. Von einem Standard-UNIX konnte nicht mehr die Rede sein. Es etablierten sich schließlich diese 2 Hauptzweige: **System V** von AT&T und **BSD (Berkeley Software Distribution)** von der Berkeley Universität in Kalifornien.

Einige der aktuellsten Varianten davon sind:

- ✓ Solaris von SUN (Oracle)
- ✓ AIX von IBM
- ✓ mAC OS X
- ✓ HP-UX von Hewlett-Packard
- ✓ OpenBSD
- ✓ Linux

Linux

Linux ist ein UNIX-ähnliches Betriebssystem, das auf die Initiative des Entwicklers Linus Torvalds zurückgeht. Linux ist, genauso wie UNIX, multiuser- und multitaskingfähig. Seit 1992 ist Linux im Internet kostenlos erhältlich. Auch vertreiben verschiedene Distributoren das Linux-Betriebssystem inklusive Handbüchern und weiteren Zugaben zu einem sehr günstigen Preis.

Der Source-Code (Quell-Text) wird von vielen unabhängigen Programmierern weiterentwickelt. Dadurch ist die Wahrscheinlichkeit sehr hoch, dass eventuell auftretende Programmierfehler nach kurzer Zeit entdeckt, beseitigt und die Korrekturen über das Internet verbreitet werden. Ein Verschieben von Updates bis zu einem bestimmten „Patchday“ gibt es hier nicht. Damit ist das Risiko für **Zero-Day-Exploits** (für Anti-Viren-Lösungen noch unbekannte Angriffe) erheblich geringer.

GNU

GNU (GNU's Not UNIX) oder **GPL** (GNU General Public License) sind Kürzel, mit denen wohl die meisten PC-Benutzer schon einmal konfrontiert wurden. Dahinter steht das Konzept der **Free Software Foundation (FSF)**, das freien Zugang zum Source-Code eines Programms erreichen will. Die Software kann geändert, erweitert oder verbessert werden, allerdings ist der Entwickler wieder auf die GPL festgelegt. Er kann seine Software nur wieder inklusive Source-Code weiterverbreiten.

Linux-Distributionen

Der Markt bietet eine große Anzahl von Linux-Distributionen und deren Derivaten. Hier die wichtigsten Linux-Distributionen:

- ✓ Red Hat Enterprise Linux (RHEL)
- ✓ Debian
- ✓ Knoppix
- ✓ Ubuntu
- ✓ Android (z. B. Smartphones, Tablets)
- ✓ openSUSE (aktuell: Tumbleweed und Leap)
- ✓ SUSE Linux Enterprise
- ✓ Gentoo
- ✓ Fedora (Red Hat Linux)
- ✓ Linux Mint

Ein bekanntes Derivat ist z. B. CentOS, das auf RHEL basiert. Von manchen Distributionen stehen Versionen für unterschiedliche Kategorien zur Verfügung, beispielsweise für Desktops oder Server (z. B. Ubuntu und SUSE). Des Weiteren gibt es Distributionen, die auf spezielle Anforderungen hin optimiert wurden, z. B. für den Einsatz als Firewall, für das Clustering oder für professionelle Anwendungen (Enterprise Versionen). Jeder, der über das dafür erforderliche Know-how verfügt, kann sich aber auch seine eigene Distribution zusammenbauen.

Etliche Linux-Distributionen benutzen als Unterbau Teile einer anderen Distribution, wie z. B. Knoppix und Ubuntu, welche beide auf Debian basieren. Knoppix kam als erste Distribution als Live-System heraus und ist auf diese Art immer noch nutzbar, also ohne Installation direkt von CD oder DVD startbar. Dies vereinfacht auch Reparaturen und Änderungen an installierten Systemen.

X Window System

UNIX und Linux waren anfangs kommandozeilenorientierte Betriebssysteme. Erst durch Zusatzprogramme erhalten sie eine grafische Oberfläche. Unter dem Stichwort **X Window System** wurde Mitte der 80er-Jahre am **Massachusetts Institute of Technology** (MIT) ein solches Fenstersystem entwickelt. Es wurde unter Linux abgelöst von XFree86. Aktuell ist X.Org und zukünftig Wayland bzw. Mir (unter Ubuntu) im Einsatz.

Das zugrunde liegende X-Protokoll ist netzwerkfähig, sodass Lösungen nach dem Client-Server-Prinzip erstellt werden können. Der X-Server stellt Ressourcen in Form von Tastatur, Bildschirm und Maus zur Verfügung, die am Client im Rahmen von Anwendungen genutzt werden können. Unter Linux werden als grafische Oberfläche unter anderem KDE, Gnome oder Xfce eingesetzt.

8.5 Interaktion in heterogenen Netzen

Kommunikation zwischen verschiedenen Betriebssystemen

Die Kommunikation zwischen verschiedenen Betriebssystemen erfordert Dienste, die bestimmte Protokolle eines anderen Betriebssystems verstehen, um Daten oder Verwaltungsinformationen austauschen zu können. Diese Situation kann sich ergeben, wenn ehemals getrennte einzelne Netze zusammenwachsen, z. B. bei der Fusion zweier Firmen. Heterogen bedeutet dann, dass auf den vernetzten Servern unterschiedliche Betriebssysteme zum Einsatz kommen oder dass Clients unter verschiedenen Betriebssystemen auf dieselben Server zugreifen.

Server-Lösungen

Auf den Servern müssen die notwendigen Dienste für die Kommunikation mit dem Client implementiert werden. Hierzu gehören die Festlegung von Nutzerkonten für den Zugriff und die Bindung der notwendigen Ressourcen zu den Konten.

Um z. B. den Anwendern im lokalen Netzwerk den Zugriff auf einen Mailserver auf einem Windows-Rechner zu ermöglichen, müssen dort erst die notwendigen Programme installiert, konfiguriert und gestartet werden. Die Benutzer können dann mit dem entsprechenden Client-Programm auf den Mailserver zugreifen.

Einen anderen Ansatz verwendet **Docker-Container**. Hier sind fertig installierte und konfigurierte Anwendungen (wie Webserver, Datenbank, Mailserver etc.) in einer Datei (dem fertigen Image) enthalten. Sie können einfach aus dem Internet geholt und gestartet werden und laufen dann in einem gekapselten Prozess ab, der nur solche Zugriffe auf die Umgebung erlaubt, die er für seine Arbeit braucht. Dies ist vergleichbar mit einer Chroot-Umgebung bei Linux, bei der nur Zugriffe auf einen vorgegebenen Bereich möglich sind.

Im Vergleich zu einer **Virtualisierung**, bei der ein oder mehrere komplett Betriebssysteme auf einem Gastsystem laufen und oft als virtuelle **Root-Server** vermietet werden, sind mit Docker-Containern wesentlich mehr Anwendungen gleichzeitig startbar und manageable. Im neuen Windows Server 2022 wurde die Container-Lösung weiter ausgebaut.

Verzeichnisdienste

Die grundlegende Kommunikation zwischen Computern mit verschiedenen Betriebssystemen ist heutzutage kein Problem mehr, da fast ausnahmslos TCP/IP als Übertragungsprotokoll eingesetzt wird und für viele Einsatzgebiete häufig mehrere Programme zur Auswahl stehen.

Gelöst werden muss weiterhin, wer welche Ressourcen im Netzwerk verwaltet bzw. wie sich die unterschiedlichen Verzeichnisdienste zueinander verhalten. Am deutlichsten sichtbar wird diese Problematik bei Benutzer- und Gruppenkonten und den dazugehörigen Berechtigungen. Daraus ergeben sich beispielsweise folgende Fragen:

- ✓ Wie erkennt der Linux-Server, dass der Windows-Domänenbenutzer sich schon als legitimes Mitglied im Netz angemeldet hat?
- ✓ Wie kann ein Benutzer, der sich erfolgreich unter Linux angemeldet hat, einfach auf einen Windows-Rechner zugreifen?

In solchen Fällen kann es nötig sein, für einzelne Benutzer mehrere Benutzerkonten auf verschiedenen Systemen anzulegen, was aber einer zentralen Verwaltung in einem Client-Server-Netzwerk widerspricht. Als Lösung bietet sich hier die Verwendung eines Identitäts-Managers oder eines Metadirectories an.

Über **Samba** Version 4 kann unter Linux ebenfalls eine Windows-Domäne bereitgestellt werden, die bereits die wichtigsten Funktionen der Microsoft-Implementierung bietet. Eine weitere Möglichkeit ist die direkte Nutzung von **LDAP** (Lightweight Directory Access Protocol) bzw. der Open-Source-Variante (OpenLDAP), die auch im Bereich von Benutzerkonten im Netzwerk verwendet werden kann. Werden solche Produkte nicht eingesetzt, bedeutet dies letztendlich, dass versucht werden muss, entweder die Betriebssystemlandschaft zu homogenisieren oder die Ressourcenverwaltung sehr strikt zu planen.

8.6 Kennzeichen der Hardware eines Servers

Unterschiede zu einem normalen PC

Theoretisch lässt sich jeder PC, der die grundlegenden Leistungsmerkmale erfüllt, als **Server** aufbauen. In kleineren Netzwerken ist das mitunter noch zu verantworten, nicht mehr jedoch für Firmen, die z. B. durch Stillstandzeiten des Netzwerks hohe finanzielle Verluste zu befürchten haben. Dementsprechend muss ein Server besser als ein normaler PC ausgestattet und gesichert werden und in jedem Fall folgende Kriterien erfüllen:

- ✓ **zuverlässig**, z. B. darf er nur wenige Stunden (oder gar nur Minuten) im Jahr ausfallen;
- ✓ **integer**, z. B. müssen Datenfehler (im Hauptspeicher, in der Festplatte etc.) auf jeden Fall erkannt und behoben werden;
- ✓ **leistungsfähig**, z. B. in Bezug auf Prozessoren, Geschwindigkeit und Kapazität der Speicher;
- ✓ **skalierbar**, z. B. in Bezug auf eine flexible Erweiterbarkeit durch Aufstockung einzelner Komponenten.

Das wichtigste Kriterium ist dabei die **Zuverlässigkeit**. Laut etlichen Untersuchungen ist das Überleben einer Firma schon nach wenigen Tagen Ausfall der EDV gefährdet, ganz abgesehen vom Imageschaden.

Von der korrekten Umsetzung der dahinter stehenden Konzepte in die Praxis hängt viel von der Stabilität eines Netzwerks ab.

Hochverfügbarkeit

In Bezug auf die Ausfallsicherheit ist das Stichwort **Hochverfügbarkeit** ein wichtiger Begriff. Manche Hersteller nennen für ihre Systeme Prozentwerte, die angeben, wie hoch die Ausfallzeiten, umgerechnet auf ein Jahr, sind. Zur Ausfallsicherung können dabei grundlegend zwei verschiedene Ansätze verfolgt werden:

- ✓ **Redundanz im Server selbst**
- ✓ **Redundanz der Server**

Redundanz im Server selbst

Deshalb besteht solche Hardware meist aus Komponenten, die im laufenden Betrieb austauschbar sind (**Hot Swapping** bzw. **Hot Plugging**), wie Gehäuse-Lüfter, Festplatten im Hardware-RAID, doppelt vorhandene Netzteile und sogar Hauptspeicher- und CPU-Module bei Multi-Prozessor-Architekturen. Auch beim Arbeitsspeicher können mit Error detection and Correction Code (**ECC**) Einbitfehler korrigiert werden (Mehrbitfehler werden erkannt). Neuere Verfahren wie **Chipkill** bzw. **Single Device Data Correction (SDDC)** kompensieren den Ausfall eines kompletten Speicherchips. Daher sollte ein gesicherter Hauptspeicher selbstverständlich sein, ebenso eine unterbrechungsfreie Stromversorgung (**USV**).

Server-Festplatten sind für Anwendungen gedacht, die 24 Stunden am Tag 7 Tage die Woche (24/7-Betrieb) ununterbrochen auf die Platte zugreifen. Desktop-Festplatten mit **Parallel Advanced Technology Attachment (PATA)** bzw. **Serial Advanced Technology Attachment (SATA)** sind meist **nicht** für einen derartigen Dauerbetrieb ausgelegt und können überhitzen.



Hot-Swap-Festplatte eines IBM-Servers

Zum Anschluss von Server-Festplatten wird heute anstelle von SCSI meist **Serial Attached SCSI (SAS)** benutzt. SAS-Platten bieten meist zwei serielle Anschlüsse mit zusammen bis zu 12 Gbit/s (seit 2017 auch mit bis zu 22,5 Gbit/s).

Darüber hinaus werden die Umgebungsdaten (Temperatur, Luftfeuchtigkeit, CPU-Kühlung etc.) elektronisch überprüft. Ebenso können Festplatten mit **Self-Monitoring, Analysis and Reporting Technology (SMART)** auf wichtige Parameter geprüft werden, wie auf Temperatur, ausgelagerte Sektoren, Fehlerrate beim Schreiben bzw. Lesen etc. Ein kritischer Zustand kann damit in vielen Fällen erkannt werden, bevor eine Platte endgültig defekt ist. Ein entsprechender Hintergrundprozess verschickt beim Erreichen bestimmter Grenzwerte automatisch Meldungen an das administrative Personal.

Viele Hersteller bieten Server im 19-Zoll-Format mit 1 oder 2 **Höheneinheiten (HE)** an. Diese Geräte haben den Vorteil, dass sie übersichtlich und in großer Stückzahl in 19-Zoll-Schränken untergebracht werden können. Bei einer Höhe von 2 HE passen bis zu 21 Server in einen Schrank. Mit sogenannten Blade Servern lassen sich kostenoptimiert auf kleinem Raum komplettete **Cluster-Lösungen** aufbauen.

Redundanz der Server

In diesem Zusammenhang sind **Server-Farmen** und **Cluster** wichtig. In beiden Fällen wird das Zusammenwirken mehrerer Server angedeutet.

Eine Absicherung erfolgt z. B. dadurch, dass Spiegel-Server existieren, die so konfiguriert werden, dass sie beim Ausfall die vollständige Funktionalität des ausgefallenen Rechners übernehmen. Diese Lösung heißt Active/Passive- oder Active/Standby-Redundanz oder -Cluster. Bei einem Active/Active-Cluster arbeiten dagegen ein oder mehrere Rechner ständig parallel. Solche Cluster-Lösungen haben den Vorteil, dass sich die beteiligten Rechner die Aufgaben teilen können (z. B. über Load Balancing).

Bei Hochverfügbarkeit-Lösungen (**High-Availability**) benutzt man mindestens zwei Switche, die zwei oder mehr Server mit mehreren Storages (Netzwerkspeichern wie NAS oder SAN) verbinden. Dann kann ein Switch bzw. Server ausfallen, ohne dass die Datenverarbeitung zusammenbricht. Das intakte Gerät übernimmt jeweils bei Ausfall (Failover) den Betrieb. Bei allen Geräten sollte zudem die Stromversorgung per USV gestützt sein.

Unterbrechungsfreie Stromversorgung (USV)

Auch eine unterbrechungsfreie Stromversorgung (**USV**) für den Fall eines Stromausfalls oder bei Störungen im Stromnetz gehört zu professionellen Installationen. Werden im Netzwerk noch andere aktive Komponenten wie z. B. Switche oder Router eingesetzt, sollten diese ebenfalls mit einer USV versehen werden. Im Extremfall besteht sogar die Möglichkeit, mit Notstromgeneratoren einem Ausfallszenario entgegenzuwirken.

Mit einer USV kann der Betrieb auch bei unsicheren Stromnetzen bzw. bei Stromausfall weitergeführt werden, solange deren Akku nicht entladen ist. Stützzeiten von einigen Minuten bis zu mehreren Stunden sind üblich. Der wichtigste Vorteil einer USV ist, dass der Administrator und die angeschlossenen Geräte bei Stromausfall zum geordneten Herunterfahren bewegt werden können.

Die USV informiert hierzu einen Server z. B. per USB-Kabel oder per Software, wenn deren Akku einen kritischen Zustand erreicht hat. Über ein spezielles Protokoll kann dieser Server die Information an weitere Rechner leiten, damit alle geordnet ihre Systeme herunterfahren, bevor der Akku einen bestimmten Ladungszustand unterschreitet. Ein NAS bzw. SAN sollte als letztes Gerät abschalten, damit darauf eventuell offene Dateien vorher geschlossen werden können.

Preis

Die oben aufgelisteten höheren Anforderungen an einen Server erklären, warum der Preis dafür höher liegen muss als der für einen Standard-PC. Bei der Suche nach dem geeigneten Anbieter sollten nicht alleine die Kosten ausschlaggebend sein, sondern auch die Bedingungen in Bezug auf Service und Wartung berücksichtigt werden. Im Notfall zahlen sich die höheren Preise für einen funktionierenden, kompetenten und zeitnahen Service aus.

Leistungsdaten

Die Leistungsdaten eines Servers hängen grundlegend und ähnlich wie bei einem PC von der Auswahl und dem Zusammenspiel von Komponenten wie Prozessor, Chipsatz, Taktfrequenz oder RAM ab. Allerdings gibt es für die meisten Bauteile spezielle Komponenten, die leistungsfähiger sind als die von Standard-PCs.

Dieses Buch kann nur dazu anregen, sich mit der jeweils aktuellen Entwicklung auf den entsprechenden Hardware-Gebieten detaillierter auseinanderzusetzen. Dazu gehören z. B. die Neuerungen auf dem Gebiet der Prozessoren oder aktuelle Trends bei Mainboards.

Allgemein lässt sich sagen, dass ein Server zumindest einen Prozessor vom Typ Xeon (Intel), EPYC (AMD), SPARC (Oracle), Power8 (IBM) usw. mit mehreren Kernen bzw. mehrere derartige Prozessoren eingebaut hat und dass so viel durch ECC etc. vor Speicherfehlern gesicherter Arbeitsspeicher wie nur irgendwie möglich vorhanden sein sollte, allerdings relativiert durch die Aufgabe, die ein Server jeweils leisten soll.

Skalierbarkeit

Die Aufgaben an einen modernen Server können mittlerweile sehr breit gefächert sein. Angefangen von einem File- und Print-Server über Applikation-Server bis hin zum Web- und Proxy-Server. Sie können auch als virtuelle Server (mehrere Betriebssysteme sind auf derselben Hardware gleichzeitig aktiv) eingerichtet sein, auf die bestimmte Aufgaben verteilt sind.

Betrachten Sie diese Anforderungen genauer und versuchen Sie, sich alle diese Funktionen auf einem Gerät vorzustellen, so wird klar, dass ein System dieser Art Stabilitätsprobleme haben kann. Beispielsweise gibt es Vorgaben der Firma Microsoft, welche Dienste von Windows Servern auf mehrere Rechner aufzuteilen sind.

Die Entwicklung geht dahin, nicht mehr einen PC als Ausgangsbasis zu benutzen, sondern bereits vom Hardware-Hersteller ausgewählte Geräte auszuliefern, die für einen bestimmten Zweck optimal zugeschnitten sind. Oft gebräuchliche Bezeichnungen für diese Art Server sind **Appliance Server** bzw. **Thin Server**. Solch ein Server zeichnet sich durch zwei Merkmale aus, nämlich durch eine für den gewünschten Zweck passende Hardware und die dafür abgespeckte Software. Heraus kommen hier am Ende spezialisierte Geräte, was sich auch in der englischen Übersetzung Appliance (Gerät/Vorrichtung/Apparat) widerspiegelt.

Neben dem Aspekt, dass diese Geräte die nach wie vor nötigen Haupt-Server von vielen Routinearbeiten entlasten können, sprechen weitere Gründe für einen verstärkten Einsatz in Zukunft. Dazu zählt neben einer einfachen Installation und Wartung oder einem standardisierten Zugang über Web-Browser auch der Sachverhalt, dass keine extra Lizenzen für das Betriebssystem nötig sind.

8.7 Exkurs: Speichern von Daten

Festplatten-Systeme

Ein extrem wichtiges Thema in vielen Firmen ist die sichere Speicherung und die hohe Verfügbarkeit der Datenbestände. Drei Ansätze müssen in diesem Zusammenhang angesprochen werden:

- ✓ RAID
- ✓ NAS
- ✓ SAN

Unabhängig davon, für welche der hier aufgeführten Lösungen sich eine Firma entscheidet, gehört grundlegend die Sicherung (**Backup**) der Firmendaten mit zu den wichtigsten Aufgaben im Alltag einer Netzwerkverwaltung. Das bedeutet neben einem sinnvollen Sicherungskonzept auch die regelmäßige Sicherung der kritischen Daten auf externe Medien, wie z. B. auf Bandlaufwerke, Disc-Storages, Blu-ray-Medien, USB-Festplatten etc.

Eine erhebliche Bedrohung unter Windows stellen aktuell **Erpressungs-Trojaner** dar, die sämtliche Daten auf der Festplatte verschlüsseln und für ein Lösegeld (bei viel Glück) den Schlüssel zum Entschlüsseln verkaufen. Es werden dabei auch **alle** Daten verschlüsselt, an die diese Trojaner herankommen, also auch auf allen Medien, die per Netzwerk, Funk, USB etc. am befallenen Windows-Rechner mit Schreibrechten angeschlossen sind. Nicht immer erkennt Antiviren-Software eine Bedrohung.

Bei der Erstellung von Backups sollte daher beachtet werden:

- ✓ Backup-Medien dürfen nicht permanent erreichbar sein, da sie sonst gegen Fehlbedienung (versehentliche Löschung), Schädlingsbefall (Trojaner) etc. nicht schützen. Es sollten mehrere Medien abwechselnd (je nach Backup-Strategie) zum Einsatz kommen und ansonsten sicher aufbewahrt werden.
- ✓ Einmal beschreibbare Medien (DVD, Blu-ray etc.) können die wichtigsten Daten optimal sichern.
- ✓ Falls ein Backup über ein Netzwerk auf einen Backup-Server erfolgen soll, sollte unbedingt ein eigenes Benutzer-Konto für den Zugriff darauf verwendet werden.
- ✓ Im professionellen Bereich haben sich Lösungen bewährt, bei denen ein Backup-Server (z. B. ein NAS, siehe unten) sich nach dem **Pull-Prinzip** die zu sichernden Daten selbstständig holt.

Eigenständige externe Datenspeicher (außerhalb eines Rechners) werden oft als **Storage** bezeichnet.

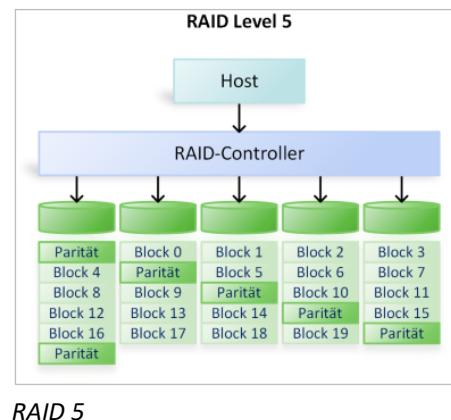
RAID

RAID steht für **Redundant Array of Independent Disks**, wobei gelegentlich statt des Begriffs **Independent** auch **Inexpensive** benutzt wird. In der Ursprungsidee verfolgt RAID zwei Ziele, nämlich die Steigerung der **Performance** und die Erhöhung der **Datensicherheit**. RAID-Systeme gibt es als Soft- oder Hardware-Lösungen, zumeist auch als Basis für NAS- und SAN-Installationen.

Implementierung von RAID

RAID gibt es in verschiedenen Stufen, wobei die höhere Nummer nicht automatisch die bessere Lösung bedeutet, denn bei der Implementierung eines RAID-Systems spielt neben Performance und Datensicherheit auch immer die Wirtschaftlichkeit eine Rolle.

Es werden zwei oder mehr Festplatten so miteinander kombiniert, dass sie eine große Plattenstruktur bilden. Bei RAID 5 zum Beispiel werden die Daten blockweise auf mehreren Festplatten abgelegt und zusätzlich die entsprechende Paritätsinformation davon auf den Platten verteilt. Aus diesen Paritätsinformationen, die meist über die boolesche Funktion XOR (eXclusiv OR) ermittelt werden, können dann beim Defekt **einer** der Festplatten alle Daten wiederhergestellt werden.



Bei Laufwerkszugriffen kann auf mehrere Festplatten gleichzeitig geschrieben bzw. von ihnen gelesen werden, was den Datendurchsatz bei den meisten RAID-Leveln erhöht (nicht bei RAID 1). Oft ist eine Reserve-Platte (Spare-Disk) mit eingebaut, die beim Ausfall einer Platte automatisch die ausgefallene Platte ersetzt.

Im Folgenden werden einige Umsetzungen aufgelistet:

- ✓ **RAID 0:** Stripe-Set, Daten werden abwechselnd auf die beteiligten Festplatten geschrieben (Performance-Gewinn, **keine** Fehlerabsicherung, da die Daten nicht redundant gespeichert werden).
- ✓ **RAID 1:** Mirroring (Festplattenspiegelung), Daten werden parallel auf ein zweites Laufwerk geschrieben (hohe Fehlertoleranz, kein Performancegewinn, es wird die doppelte Plattenkapazität benötigt).
- ✓ **RAID 4:** Block-Striping mit Parity-Disc, auf einer der – mindestens drei – Festplatten. Fällt eine Festplatte aus, können aus den Paritätsinformationen die fehlenden Daten wiederhergestellt werden.
- ✓ **RAID 5:** Wie RAID 4, aber die Paritätsinformationen werden auf alle beteiligten Festplatten geschrieben. RAID 5 wird häufiger eingesetzt als RAID 4. Die Kapazität von einer Platte ist redundant.
- ✓ **RAID 6:** Wie bei RAID 5 werden Paritätsinformationen auf alle Festplatten verteilt, benutzt werden aber 2 Prüfsummen (meist per XOR + Reed-Solomon-Code), daher ist eine zusätzliche Festplatte erforderlich. Damit ist die Kapazität von 2 Platten redundant, und die Schreibleistung verringert sich.
- ✓ **RAID 10:** Kombination aus RAID 1 und RAID 0, bei der ein bestehendes Stripe-Set gespiegelt wird. Wird meist als Hardware-Lösung realisiert und ist dementsprechend teuer.
- ✓ **RAID 15:** Diese Kombination aus RAID 1 und 5 stellt Mirroring mit Parität dar.
- ✓ **RAID DP:** Ein RAID-System mit doppelter Parität(2 mal XOR). Beispielsweise ist RAID 5 DP ein RAID 5, bei dem die Kapazität von 2 Platten redundant für die Paritätsinformationen verwendet wird. Ein gleichzeitiger Ausfall von mehr als einer Platte kann damit verkraftet werden (ähnlich RAID 6).

Weitere Kombinationen sind die RAID-Level 50, 51, 60, 61 etc.

- ✓ Ein RAID ist **kein** Ersatz für eine Backup-Lösung. Das heißt, ein RAID sichert die Daten gegen den Ausfall einer Festplatte zwischen den Backups.
- ✓ Es schützt nicht vor schlechendem Datenverfall (**Silent Data Corruption**, Bitfäule oder Bit-Rot).
- ✓ Entdeckt es eine fehlerhafte Platte, sollte ein RAID-System den Administrator sofort alarmieren.
- ✓ RAID-Systeme sollten wie andere wichtige Komponenten auch, wie z. B. Server, Switch, Router, NAS etc., immer über eine USV (unterbrechungsfreie Stromversorgung) betrieben werden!

NAS

Network Attached Storage lässt sich mit ans Netz angeschlossener Speicher übersetzen und suggeriert das Bild einer Festplatte mit eingebautem Netzwerkanschluss. Ein solches Gerät stellt damit einen File-Server mit eigenem Betriebssystem dar. Es kann somit auch spezielle Programme für Backups etc. ausführen.

Der Zugriff erfolgt **dateibasiert** über Protokolle wie CIFS (SMB), NFS, FTP etc. Eine gleichzeitige Bearbeitung der Daten von mehreren Clients aus wird in der Regel über Mechanismen des Betriebssystems ermöglicht, bereits geöffnete Dateien zu sperren (Lock = Sperre).

Einfachere NAS-Geräte sind wie Standard-PCs in einer Blackbox aufgebaut. Es bietet im Wesentlichen eine Netzwerk-Schnittstelle mit hoher Bandbreite zum Anschluss an das LAN und ggf. Einschübe zur Erweiterung der Plattenkapazität. Einige Systeme haben auch ein Hardware-RAID integriert. Die Verwaltung der Geräte erfolgt meist webbasiert über Browser zur einfachen Wartung und Pflege. Große Lösungen für professionelle Anwendungen können den Midrange- und Enterprise-Bereich bei Firmen abdecken.

Wenn Sie einen DSL-Router für den Zugang zum Internet benutzen (z. B. eine Fritz!Box), können Sie mit vielen derartigen Geräten relativ einfach einen günstigen und sparsamen Netzwerkspeicher (NAS) aufbauen, indem Sie ein Speichermedium (USB-Memorystick, USB-Festplatte etc.) anschließen und über die Netzwerkschnittstellen vom DSL-Router freigeben. Die entsprechende Konfiguration von Firewall, DynDNS und VPN gestattet dann auch einen sicheren Zugriff vom Internet aus. Der Durchsatz ist dabei meist relativ gering.

SAN

Ein **Storage Area Network** (SAN) bietet die Möglichkeit, eine noch größere räumliche Trennung von Daten- und Anwendungsservern durchzuführen, wie sie durch Server-Cluster bereits eingeleitet worden ist. So entsteht neben dem LAN des bzw. der Server auf der einen Seite ein SAN als eigenständiges Netzwerk zum Speichern der Daten auf der anderen Seite.

Ein Zugriff erfolgt hier nicht dateibasiert wie bei NAS, sondern **blockbasiert**. So kann ein Server z. B. den Datenblock 2011 anfordern und ändern. Ein SAN wird wie eine große Festplatte eingebunden.

Soll mehr als ein Server gleichzeitig zugreifen, ist ein geeignetes **Cluster-Dateisystem** erforderlich, wie **Cluster Shared Volumes** ab Windows Server 2008 R2, oder **GlusterFS**, **Ceph**, **Oragefs** etc. von Linux.

Möglich wird dies nur, wenn Hochleistungsübertragungsmedien (siehe unten) zum Einsatz kommen, die erstens eine bestimmte Datentransferrate zur Verfügung stellen und zweitens in Bezug auf die möglichen Distanzen zwischen Server und SAN keine engen Beschränkungen haben. Die zugrunde liegenden Übertragungs-Protokolle sind **Fibre Channel (FC)** und **SCSI über TCP/IP (iSCSI)**.

! Auch auf NAS bzw. SAN ausgelagerte Daten sind regelmäßig zu sichern. Dass viele dieser Storages auf RAID-Systemen aufgebaut bzw. über mehrere Systeme gespiegelt sind, schützt nicht vor Datenverlust, z. B. durch Unachtsamkeit, mutwillige Beschädigung, Viren etc.

Fibre Channel

Fibre Channel (FC) nutzt das SCSI-3-Protokoll und lässt sich über einen FC-Switch mit bestehenden Plattsystemen kombinieren. Die erreichbare Bandbreite liegt inzwischen bei 16 Gbit/s vollduplex, wobei vielerorts auch mit 2, 4 oder 8 Gbit/s gearbeitet wird.

Bei FC gelten folgende Längenrestriktionen:

- ✓ 30 m mit STP-Kupferkabel und speziellen HSSDC- bzw. Sub-D-Steckern
- ✓ 500 m mit Multimode-Glasfaser (50 µm)
- ✓ 10 km mit Monomode-Glasfaser (mit Extended-Distance Transceiver bis zu 120 km)

Fibre Channel Arbitrated Loop

Eine einfache Einsatzmethode nennt sich **Fibre Channel Arbitrated Loop (FC-AL)** und erlaubt den Anschluss von 127 Geräten an einem logischen Bus. Die Verkabelung selbst erfolgt meist sternförmig über einen Fibre Channel Hub, wobei sich die angeschlossenen Geräte die verfügbare Bandbreite teilen. Es ist eine maximale Übertragungsrate je nach eingesetzter Hardware bis zu 16 Gbit/s erzielbar.

Fibre Channel Switch

Die Implementierung als **Fibre Channel Switch (FC-SW)** ist leistungsfähiger, aber auch teurer als FC-AL. Als Zentrale fungiert ein Fibre Channel Switch. Werden mehrere FC-SW verwendet, spricht man von Fibre Channel Fabric. Über diesen werden alle anderen Geräte zusammengeschlossen. So ermöglicht der Switch oder die Switch Fabric direkte Punkt-zu-Punkt-Verbindungen zwischen zwei angeschlossenen Geräten.

Fibre Channel over Ethernet

Anstelle von Glasfasern können auch Ethernet-Leitungen für FC benutzt werden, die eine Verbindung zu den SAN-Speichern über das Protokoll **Fibre Channel over Ethernet (FCoE)** nutzen. Dieses benötigt weniger Protokoll-Overhead als iSCSI, da es direkt auf Ethernet aufsetzt, ohne Netzwerk-Protokolle wie IP und TCP zu verwenden. Es hat damit aber die Nachteile von Ethernet, wie den Rahmenverlust bei Überlast, welche Erweiterungen des Ethernet-Protokolls (Data Center Bridging) erfordern.

iSCSI

Bei **iSCSI** (SCSI über TCP/IP nach RFC 3720; meist über TCP-Port 3260) sind wie bei FCoE keine speziellen und damit teuren Glasfaser-Kabel erforderlich, es sind übliche Ethernet-Kabel und -Switches benutzbar. Damit sind mit CAT-6A-Kabeln Übertragungsraten von 10 Gbit/s erreichbar, mit CAT-7 oder Glasfasern entsprechend mehr (vgl. Kapitel 7).



Der Datenaustausch zu dem bzw. den SAN-Geräten muss der iSCSI-Verkabelung separat vorbehalten bleiben; jeder sonstige Datenverkehr im Netzwerk ist über andere Leitungen zu führen.

Einsatz

Über ein SAN-System werden die benötigten Speichermedien miteinander verbunden. Die Massenspeicher bilden eine eigene logische Einheit, getrennt von den Servern. Das SAN verwaltet den gesamten Speicher zentral, unabhängig von seinem physikalischen Standort.

Die Speichermedien im SAN können dabei virtuelle Einheiten bilden, unabhängig von ihrer Lokation. Redundante Wege zwischen den Servern, Switchen und Speichermedien erhöhen die Verfügbarkeit und die Performance des SAN-Systems.



Wissenstest: Lokale Netzwerke

8.8 Übung

Fragen zu Betriebssystemen und Diensten

Übungsdatei: --

Ergebnisdatei: uebung08-E.pdf

1. Was ist unter einem Dienst bzw. Service gemeint?
2. Nennen Sie die Core-Services in einem Netzwerk.
3. In welchem wesentlichen Punkt unterscheiden sich die Server-Versionen der Windows-Betriebssysteme von den Desktop-Versionen von Windows?
4. Welches sind die Hauptaufgaben von einem Directory Service?
5. Welches sind die Vorteile eines Live-Systems und nennen Sie einen bekannten Vertreter?
6. Welches sind die wichtigsten Kennzeichen der Hardware eines Servers?
7. Wie können Speicherfehler im laufenden Betrieb erkannt werden?
8. Welches RAID-Level ermöglicht eine Spiegelung von Festplatten?
9. Wie erfolgt ein Zugriff auf ein SAN?

9

Praxis 1

9.1 Planung

Vorarbeiten zur Umstellung

Die im Rahmen der Vorbemerkungen erwähnte Musterfirma kann nun konkrete Schritte unternehmen, um mit der Planung der Vernetzung zu beginnen. Ziel dieses Praxisteils ist die grundlegende Vernetzung der Firma in Bezug auf die eingesetzte Hardware.

Die nachfolgende Arbeit, nämlich die Installation und Konfiguration der benötigten Software, sollte in ihrer zeitlichen Dimension nicht unterschätzt werden, ist aber nur teilweise Bestandteil dieses Buchs.

Für beide Bereiche müssen zu Beginn der Planung eine Analyse der augenblicklichen Situation, eine Auflistung der kurzfristigen Ziele und, soweit möglich, eine Prognose über zukünftige Anforderungen stehen.

Bestandsaufnahme

Vor Einzug in die neuen Räumlichkeiten erfolgte die Entwicklung der ABC GmbH heterogen, d. h., je nach Bedarf wurden neue Mitarbeiter eingestellt und PC Systeme mit den jeweils aktuellen Betriebssystemen gekauft. Die meisten Mitarbeiter erledigten ihre Aufgaben in kleinen Teams und tauschten Daten über Cloudspeicher im Internet aus, daher spielte die Vernetzung der Firma bisher nur eine untergeordnete Rolle. Dies soll sich mit dem Einzug in die neuen Räume ändern.

Die meisten der 15 PCs, die die Firma aktuell besitzt, sind mit Microsoft Windows 10 Home oder Pro ausgestattet, einige jedoch auch mit Microsoft Windows 8.1. Pro. Die Geschäftsführer besitzen neben ihren PC-Systemen je ein unvernetztes Notebook mit Windows 10 Home, die sie zu Kundenterminen mitnehmen. Alle PC-Systeme, bis auf die zwei Notebooks, verfügen über interne Netzwerkadapter. Ein spezialisiertes Team betreibt für Tests der firmeneigenen Web-Applikation im Büro 4 einen eigenen Datenbankserver. Die bisher verwendeten Internetzugänge werden zukünftig durch einen zentralen DSL-Anschluss ersetzt.

Insgesamt stehen vier Druckgeräte zur Verfügung: zwei Laserdrucker mit Netzwerkanschluss, ein USB-Farbintenstrahldrucker und ein Nadeldrucker mit paralleler Schnittstelle, der Lieferscheine mit Durchschlägen druckt. Des Weiteren sind noch ein Kopiersystem und ein Faxgerät verfügbar.

Bedarfsanalyse

In einer ersten Bedarfsanalyse wurden die nachfolgenden Wünsche geäußert:

- ✓ Alle Mitarbeiter sollen einfach und direkt miteinander kommunizieren können.
- ✓ Die Drucker sollen auf allen PCs verfügbar sein.
- ✓ Eine zentrale Kundendatenbank soll unter Berücksichtigung unterschiedlicher Zugriffsrechte für alle Mitarbeiter verfügbar sein.
- ✓ Der Schulungs- und Verwaltungsaufwand bei der Umstellung sollte gering sein.
- ✓ Die Sicherung der Daten einer Arbeitswoche soll zentral, möglichst automatisch erfolgen.
- ✓ Die Mitarbeiter wollen intern sowie extern Mails mit einheitlicher Notation verwenden.
- ✓ Der Internetzugang wird von mehreren Personen gleichzeitig genutzt.

Häufig tritt bei einer Bedarfsanalyse folgendes Problem auf: Die Bedürfnisse der Endbenutzer sind geprägt von dem Wunsch, möglichst sorgenfrei mit dem Netzwerk arbeiten zu können, während die Wünsche der Geschäftsführung die Umsetzungsmöglichkeiten, oft aufgrund der entstehenden Kosten, wieder einschränken. Hier muss ein vernünftiger Kompromiss gefunden werden oder ein externer Berater beauftragt werden, der passende Lösungsmöglichkeiten vorschlägt.

Prognose

Die Firma geht davon aus, weiter zu wachsen. Der Mietvertrag des Start-ups in der zweiten Etage des aktuellen Gebäudes läuft demnächst aus. Im Fall der Expansion soll das gesamte Gebäude genutzt werden. Eine Option ist mit dem Vermieter besprochen. Ein weiterer Umzug in neue Räume muss unbedingt vermieden werden.

9.2 Allgemeine Abschätzung

Wichtige Punkte bei der Planung

Ein wichtiger Aspekt, der sich durch alle Phasen einer Vernetzung zieht, sind die entstehenden Kosten. Sie verteilen sich unter anderem auf folgende Posten:

- | | |
|------------------------------------|---------------------------|
| ✓ Baumaßnahmen | ✓ Einweisung und Schulung |
| ✓ Material- und Anschaffungskosten | ✓ Wartung und Pflege |
| ✓ Zeitaufwand der Installation | |

Baumaßnahmen

Die Kosten für eventuelle bauliche Maßnahmen (inklusive Kabelverlegung) variieren sehr stark und in Abhängigkeit von der vorhandenen Gebäudesituation. In jedem Fall sollte hierzu eine spezialisierte Firma beauftragt werden. In Zusammenarbeit mit dieser Firma müssen einige wichtige Fragen geklärt werden.

- ✓ Wo werden die Kabel verlegt? Sind verwendbare Kabelschäfte bzw. Installationskanäle vorhanden?
- ✓ Sind Mauer- oder Deckendurchbrüche notwendig? Gibt es abgehängte Decken oder ist eine Unterbodenverkabelung (auch Unterflurverkabelung) vorbereitet?
- ✓ Sind spezielle Rahmenbedingungen zu beachten, wie z. B. Denkmal- oder Brandschutzbestimmungen?
- ✓ Wie viele Anschlüsse werden pro Raum benötigt?



*Unterbodenversorgung
(Strom und Netzwerk)*

Als Anhaltspunkt für eine flexible Erweiterbarkeit kann davon ausgegangen werden, dass pro vorhandenem Arbeitsplatz mindestens zwei Anschlüsse gelegt werden, besser vier, da weitere Gerätschaften wie IP-Telefone, Drucker, Testsysteme, etc. eigene Anschlüsse benötigen.

Material- und Anschaffungskosten

Dieser Posten betrifft Punkte wie z. B. Kabel, Stecker, Netzwerkkarten, Server und weitere Hardware genauso wie die Auswahl und die benötigten Lizenzen für Betriebssysteme.

In Bezug auf die Hardware ist es jedoch selten der richtige Weg, nur nach dem Preis zu urteilen. Ein Netzwerk ist ein System vieler Einzelkomponenten, und wie in jedem System orientiert sich das Zusammenspiel der Einzelteile an dem schwächsten Glied in der Kette. Langfristig gesehen ist es deshalb sinnvoll, gleichzeitig mit der Vernetzung einen Schnitt zu vollziehen und die bereits vorhandene Hardware zu überprüfen, um z. B. eventuell veraltete Computer zu ersetzen.

Zeitaufwand der Installation

Hier ist zu klären, wie lange die Installationsarbeiten dauern und wie sie organisiert sind. Wenn Baumaßnahmen nötig sein sollten, kann meist in den Büros während dieser Zeit nicht gearbeitet werden. Auch muss geprüft werden, welchen Zeitaufwand die Aufrüstung und Konfiguration der vorhandenen Rechner erfordert.

Einweisung und Schulung

Dieser Bereich betrifft sowohl die Personen, die in Zukunft in der Firma das Netzwerk verwalten sollen (Administratoren), als auch die Personen, die das Netzwerk nur benutzen. Besonders Letzteren muss gezeigt werden, welche neuen Möglichkeiten sich durch die Vernetzung ergeben. Außerdem muss ihnen Zeit gegeben werden, diese neuen Möglichkeiten zu üben, da ansonsten die Gefahr besteht, dass von den Neuerungen kein Gebrauch gemacht wird.

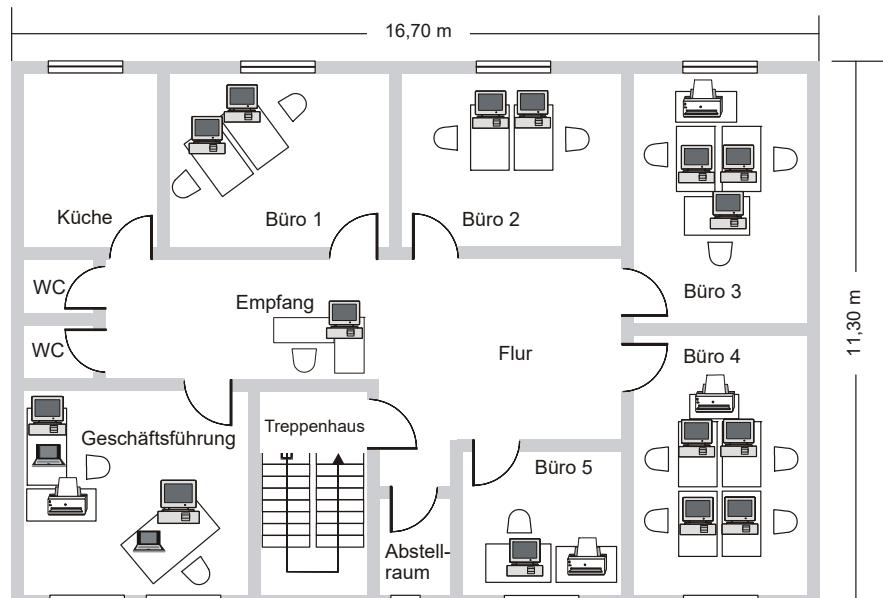
Wartung und Pflege

Je mehr eine Firma auf ein funktionierendes Netzwerk angewiesen ist, desto wichtiger ist ein Wartungsvertrag. Meistens besteht die Auswahl zwischen einer monatlichen Pauschale oder einer Abrechnung nach Arbeitsstunden. Bei der Auswahl der Firma, mit der hier zusammen-gearbeitet wird, sollte die Qualität des Services höher eingestuft werden als der Preis.

9.3 Realisierung

Gewählte Umsetzungsvariante und Alternativen

Bevor im Kern dieses Praxisteils die verschiedenen Varianten ausführlicher angesprochen werden, sollen noch einige Aspekte erwähnt werden, die die allgemeine Konzeption betreffen. Um die Einordnung in Bezug auf die Musterfirma zu erleichtern, zeigt die Skizze noch einmal den Grundriss der vorhandenen Räumlichkeiten.



Grundriss/Etagenplan

Anschlüsse

Prinzipiell sollen Netzwerk-Anschlussdosen mit Doppelanschlüssen verlegt werden. Im Büro 5 und beim Empfang sollen vier Anschlüsse, im Büro 1 und 2 und bei der Geschäftsleitung sollen je sechs Anschlüsse, im Büro 3 und 4 jeweils acht Anschlüsse vorhanden sein.

! Sie müssen berücksichtigen, dass an jedem Arbeitsplatz mindestens zwei Anschlüsse für PCs und zwei als Reserve vorhanden sein sollten. Hier können weitere Gerätschaften wie IP-Telefone, Drucker und andere netzwerkfähige Systeme angeschlossen werden. Anschlüsse für herkömmliche Telefone sind in der Regel anders beschaltet als Netzwerk-Anschlussdosen und verwenden andere Kabel und Buchsen. IP-Telefone benötigen jedoch eine entsprechende Konfiguration. Bei Schnurlos-Telefonen ist die Verwendbarkeit der Mobilteile von der Verbindungsqualität zur Basisstation abhängig.

Telefone

Die in der Firma vorhandenen klassischen analogen Telefone, die entweder über eine Verkabelung mit der Telekommunikationsanlage (TK-Anlage) oder schnurlos mit einer Basisstation verbunden werden, können auf das Verfahren VoIP (**Voice over IP**) umgestellt werden. Infrage kommen auch Internettelefone (vgl. Kapitel 19).

Gerade für Telefone bietet sich heutzutage bei Verwendung von VoIP der Einsatz schnurloser Geräte an.



Diese werden über Funk per **DECT** (Digital Enhanced Cordless Telecommunications) mit einer Basisstation bzw. einem geeigneten DSL-Router (z. B. einer Fritz!Box) verbunden. Die Telefonate können dann über einen bestehenden DSL-Anschluss per VoIP geführt werden. Dadurch lassen sich die benötigten Kabel und Anschlussdosen reduzieren und gleichzeitig die Telefonkosten senken.

Server

Auch wenn es sich hier noch um ein kleines Netzwerk handelt, sollte im Rahmen der Neuplanung, eine Client-Server-Struktur aufgebaut werden. Der anfängliche Aufwand ist höher, da mehr Zeit in die Planung und den Aufbau investiert werden muss, aber jede spätere Änderung und Erweiterung wird schneller umsetzbar sein. Der Server sollte in einem speziell präparierten Raum untergebracht werden, wobei sich hier der Abstellraum anbietet, in dem auch ein Datenschrank stehen wird. Dieser Raum sollte wegen der zu erwartenden Wärmeentwicklung klimatisiert werden. Um unbefugtes Betreten und Manipulationen am Server zu verhindern, sollte solch ein Raum verschließbar sein.

Der Server und weitere wichtige Geräte sollten zusätzlich mit einer unterbrechungsfreien Stromversorgung (USV) ausgestattet sein. Gerade beim Thema **USV** darf nicht vergessen werden, dass dann auch aktive Netzwerkkomponenten (z. B. Switches) vor Stromausfall gesichert sind.

Austausch der Windows Home-Betriebssysteme

Da Windows-Systeme mit Home-Versionen keine Mitglieder einer Windowsdomäne sein können, wird es notwendig, die Maschinen mit diesen Betriebssystemen neu zu lizenziieren und zu installieren. Nur innerhalb einer Windows-Domäne können einheitliche und verbindliche Einstellungen über Gruppenrichtlinien für Computer und Benutzer vorgenommen und erzwungen werden. Auch die Verteilung von Updates und Software bleibt bei entsprechender Konfiguration konsistent.

Die Maschinen mit Windows 8.1 Pro können mit den vorhandenen Lizenzschlüsseln als Windows 10 Pro neu installiert und anschließend auf Windows 11 aktualisiert werden, vorausgesetzt, es sind unterstützende Prozessoren (Intel 8. Generation) und TPM (Trusted Platform Module) Baugruppen vorhanden oder können nachgerüstet werden. Dies gilt auch für die Windows Home-Geräte. Diese müssen mit neuen Windows 10/11 Pro-Lizenzen reinstalliert werden.

Weiter bietet es sich an, die zwei Notebooks im Büro der Geschäftsführer mit USB-Netzwerkadapters auszustatten, damit eine einfache Datensynchronisation mit den Netzlaufwerken der Geschäftsführer ermöglicht wird. Andernfalls wird ein WLAN-Access Point (mit all seinen Einschränkungen und Problemen) in diesem Bereich benötigt. Wegen der Gefahr des Verlustes eines Notebooks sollen die Festplatten mit BitLocker verschlüsselt werden.



Die USV ① versorgt neben den beiden Switches ② auch eine USB-Backup-Platte ③ sowie eine (nicht auf der Abbildung sichtbare) FRITZ!Box

Server-Betriebssystem und Office-Paket

Bei der Auswahl eines geeigneten Betriebssystems für den Server kommen mehrere Varianten in Betracht. Hier ist zunächst zu entscheiden, ob die Datenhaltung ausschließlich lokal in der Firma erfolgen soll oder auch Cloud-Technologien genutzt werden dürfen. Bei rein lokalen Lösungen kommen auch Linux-Server in Betracht, die überwiegend kostenlos zur Verfügung stehen, jedoch ein höheres Fachwissen bei der Einrichtung und im Betrieb erfordern.

Microsoft Office-Dateiformate sind häufiger Standard für den Austausch von Daten mit Kunden, daher muss überlegt werden, ob eine 100%ige Kompatibilität benötigt wird oder auch alternative Office Suiten wie LibreOffice oder Apache OpenOffice den Anforderungen genügen.

Auswahl einer passenden Lösung

Trotz der nicht unerheblichen Kosten fällt die Wahl auf Windows Server 2022 Essentials als lokalen Datenspeicher und Microsoft 365 Business Standard (im Jahresabo) als Office-Lösung. Neben den Standardanwendungen wie Word, Excel und PowerPoint kann Outlook auf allen Arbeitsplätzen mit einer firmeneigenen E-Mail-Domäne konfiguriert werden, sodass der Wunsch nach einem einheitlichen Namensschema für die Mailadressen gegeben ist. Zusätzlich erhält jeder Mitarbeiter Zugriff auf Microsoft Teams, womit auch Gruppen-Chatnachrichten, Gespräche mit anderen Anwendern und die Arbeit an gemeinsamen Dateien ermöglicht werden. Wegen der Cloud-Anbindung besteht auf alle persönlichen Dateien via OneDrive ortsunabhängig Zugriff, was ein flexibles Arbeiten unterwegs oder im Homeoffice erlaubt.

Microsoft garantiert seinen Geschäftskunden eine DSGVO-konforme Speicherung ihrer Daten, womit große Bedenken der Geschäftsführer ausgeräumt werden können. Die Serverlizenz unterstützt bis zu 25 Benutzer und 50 Geräte. Alle Zugriffe auf den Server, inklusive Terminalserver-Dienste, sind lizenziert, wodurch auch dem erwarteten Wachstum der Firma Rechnung getragen wird. Ein weiteres Argument für diese Entscheidung ist die Verfügbarkeit eines „echten“ Active Directories, der die Benutzerkonten organisiert und in das Azure AD synchronisiert wird. Als Gerät ist eine Serverhardware aus dem Bestand geeignet. Die benötigten Datenbanken können auf der gleichen Hardware als virtuelle Maschinen bereitgestellt werden.

Drucker

Der Wunsch, dass jede Person auf jedem Drucker drucken kann, wird für die netzwerkfähigen Geräte über die Windows-Serverrolle Druckserver gelöst. Die an lokalen Schnittstellen installierten Drucker (Nadel- und Tintenstrahldrucker / Parallelport und USB) sind im Netzwerk freigegeben. Da das Faxaufkommen und die Anzahl von Fotokopien kontinuierlich gesunken ist, wird ein netzwerkfähiges Business All-in-One-Gerät mit ADF (Automatic Document Feeder) an der Anmeldung aufgestellt. Hiermit können auch Dokumente digitalisiert und in einem Archiv auf einem Netzlaufwerk abgelegt werden.

Datenablage

Die Datenablage wird zentralisiert. Bearbeitete Daten werden nicht mehr lokal auf den Einzelplatz-PCs gespeichert, sondern jede Person erhält einen persönlichen Ordner auf dem Server, in dem die Daten abgelegt werden. Dadurch wird eine zentrale Datensicherung erleichtert.

Wichtiger als die Auswahl des Mediums zur Datensicherung (z. B. **DAT**- oder **LTO**-Bandlaufwerke oder im Fall der Firma ABC GmbH eine externe Festplatte) ist die Erarbeitung einer Strategie, was, wann und in welchen Intervallen gesichert werden soll. Ebenso sollte bereits im Vorfeld geklärt werden, wer die Datensicherung letztendlich durchführt und dafür verantwortlich ist. Die Medien mit den gesicherten Daten sollten an einem sicheren Ort verwahrt werden. Auch im Hinblick auf Schadsoftware, die einen permanent verbundenen Sicherungsdatenträger ebenfalls verschlüsseln würde, ist der Einsatz von Offline-Sicherungsdatenträgern erforderlich.

Einheitliche Hardware

Bei der Anschaffung neuer Hardware sollte in jedem Fall auf Einheitlichkeit geachtet werden. Je homogener die Ausstattung, desto leichter ist die Pflege der angeschafften Hardware. Das beginnt mit Rechnern, Festplatten, Netzwerkkarten, Druckern usw. und geht bis hin zur tatsächlichen (Rechner-)Konfiguration, d. h. einheitlichen Verzeichnisstrukturen, einheitlichen Schemata für die Vergabe von Rechner- und Benutzernamen u. v. m.

Entstehen in solch einem Netz Probleme, muss die Lösung nur einmal gefunden werden. Ein Beispiel wären Probleme mit Druckertreibern. Arbeitet die gesamte Firma mit identischen Druckern, kann beim zweiten Auftauchen des gleichen Problems bereits auf eine Lösung zurückgegriffen werden.

Telefonie

Da auf eine eigenständige Verkabelung für Telefone verzichtet werden soll, wird das bestehende Netzwerk für den Anschluss von IP-Telefonen genutzt. In den Büros 1 und 2 teilen sich die Mitarbeiter einen Anschluss, Büro 3 und 4 erhalten je 2 Telefone, jeder Geschäftsführer 1 Telefon und die Anmeldung ein Festnetzgerät mit zusätzlichem Mobilteil. Büro 5 wird wegen der Lärmbelastung durch den Nadeldrucker ausgelassen. Die Bereitstellung einer virtuellen VoIP TK-Anlage übernimmt ein externer Provider.

Twisted-Pair-Verkabelung

Sie führt zu einer Stern-Topologie, d. h., zu jedem TP-Anschluss führt ein Kabel. Je nachdem, wie bzw. wo die Kabel verlegt werden können, ergibt sich ein unterschiedlicher Kabelbedarf.

Können die Kabel direkt zu den Anschlussdosen geführt werden (z. B. über abgehängte Decken), ist der Bedarf deutlich geringer, als wenn sie in neuen Kabelkanälen verlegt werden müssen.

Posten	Anzahl
Kabel	ca. 450 bis 650 Meter
Anschlussdosen	42 oder 21 Doppel-dosen
Netzwerkkarten	2 x USB für Notebooks
Switch	1

Es wird mit einem zentralen Switch gearbeitet, der sich im Serverraum (ehemaliger Abstellraum) befindet. Als Kabeltyp wird Kategorie 6a (CAT 6a) gewählt. Die PCs sind per 100Base-T bzw. 1000Base-T über den Switch mit dem, im LAN Schrank zu platzierenden, Server und dem DSL-Router verbunden. Außerdem werden ein 19-Zoll-Schrank sowie Patch-Panel und Patch-Kabel eingesetzt.

Glasfaser-Verkabelung

Lichtwellenleiter bis zum Arbeitsplatz sind heute eher selten anzutreffen. Für den aufgezeigten Bedarf dieser Firma rechtfertigen sich die Kosten nicht. Auch diese Verkabelung führt zu einer Stern-Topologie, d. h., zu jeder Anschlussdose führt ein Kabel. Die weitere Aufzählung entspricht derjenigen für Twisted Pair.

Drahtlose Vernetzung

Der Aufbau eines drahtlosen Netzwerks ist eine Alternative für mobile Geräte, wobei geeignete Sicherheitsmaßnahmen gegen das Abhören durchzuführen sind. Die benötigten Antennen und Access Points liegen inzwischen preislich in einem vertretbaren Rahmen und sie haben den Vorteil, dass weder Kabel noch nennenswerte bauliche Maßnahmen notwendig sind.

Vor allem durch die zunehmende Bedeutung von Notebooks, Smartphones, Tablets etc. ist ein WLAN über einen Access Point eingerichtet, der meist im DSL-Router integriert ist. Darüber sind diese mit WLAN ausgestatteten Geräte an das restliche verkabelte Netzwerk angebunden. Der Vorteil ist, dass Sie sich dann mit diesen Geräten völlig frei innerhalb der bestehenden Büroräume bewegen können. Dabei müssen jedoch die baulichen Gegebenheiten überprüft werden, um die optimale Ausleuchtung der WLAN-Funkzelle zu ermitteln.

Trotz der höheren Mobilität wurde in diesem Szenario die verkabelte Lösung per USB-Netzwerkkarte für die Notebooks bevorzugt, da im Falle einer Mitnahme des Geräts zu einem Außentermin die Synchronisation der Netzwerkspeicher deutlich schneller zu bewerkstelligen ist.

9.4 Auswirkungen

Investitionsschutz

Die folgenden Bemerkungen dienen einer abschließenden Gegenüberstellung der vorher geschilderten Varianten. Das Hauptaugenmerk gilt dabei einem der wichtigsten Aspekte jeder grundlegenden Vernetzung, nämlich dem Investitionsschutz bzw. der Investitionssicherung in die Zukunft.

Twisted-Pair-Verkabelung mit CAT 6 oder 7 entspricht inzwischen auch für kleine Netzwerke dem Stand der Technik. Damit kann Fast Ethernet und Gigabit-Ethernet mit Übertragungsraten von 100 Mbit/s bzw. 1Gbit/s aufgebaut werden. Einem späteren Umstieg auf 10-Gigabit-Ethernet steht nichts im Wege. Gerade unter Berücksichtigung des Themas Investitionsschutz wird viel Wert darauf gelegt, die Leistungsfähigkeit eines Netzwerks unter Beibehaltung möglichst vieler bereits vorhandener Komponenten auszubauen.

Glasfaser bis zum Arbeitsplatz bietet zwar hohe Datenübertragungsraten und wäre auch ein Investitionsschutz für die Zukunft, allerdings zu einem relativ hohen Preis.

Bei drahtloser Vernetzung sind die oft niedrigeren Übertragungsraten und extra Maßnahmen zur Absicherung des Datenverkehrs zu überdenken. Selbst bei Einsatz von Geräten, die der Norm IEEE 802.11ac entsprechen, kommt in der Praxis an den damit verbundenen Geräten unter Laborbedingungen kaum mehr an als mit Gigabit-Ethernet (1300 Mbit/s). Tritt viel Verkehr auf, teilt sich die gesamte Übertragungsrate auf alle Nutzer auf (Shared Media), über Kabel und einen Switch nicht (vgl. Kapitel 13).

Auch wenn die vollständig drahtlose Vernetzung in diesem Szenario nicht gewünscht wird, kann deren Einsatz in Teilen eines lokalen Netzes, zur Erhöhung der Mobilität einzelner Benutzer, durchaus sinnvoll sein.

	Twisted Pair	Glasfaser	Drahtlos
Kosten	Mittel	Hoch	Mittel
Zukunftsinvestition	Ja	Ja	Ja
Übertragungsraten	Hoch	Hoch	Mittel

Preise

Entscheidungen für oder gegen eine bestimmte Lösung sind immer mit den dabei entstehenden Kosten verbunden. Eine nicht zu unterschätzende Aufgabe für Beschäftigte in diesem Bereich ist es, über Neuerungen und aktuelle Preise auf dem Laufenden zu bleiben. Allerdings sind die Bewegungen auf diesem Markt sehr schnell und die Preise unterscheiden sich je nach Anbieter und Produkt teilweise gravierend. Da sich darüber hinaus Preise innerhalb kurzer Zeit oft stark ändern, wurde in diesem Buch bewusst auf die Angabe von Preisen verzichtet.



Ergänzende Lerninhalte: Weiterführende Informationen.pdf

In diesem Dokument finden Sie auszugsweise Internetadressen von einigen Anbietern und Herstellern, die Sie bei der Suche nach Informationen über Produkte und Preise unterstützen.

IP-Konzept

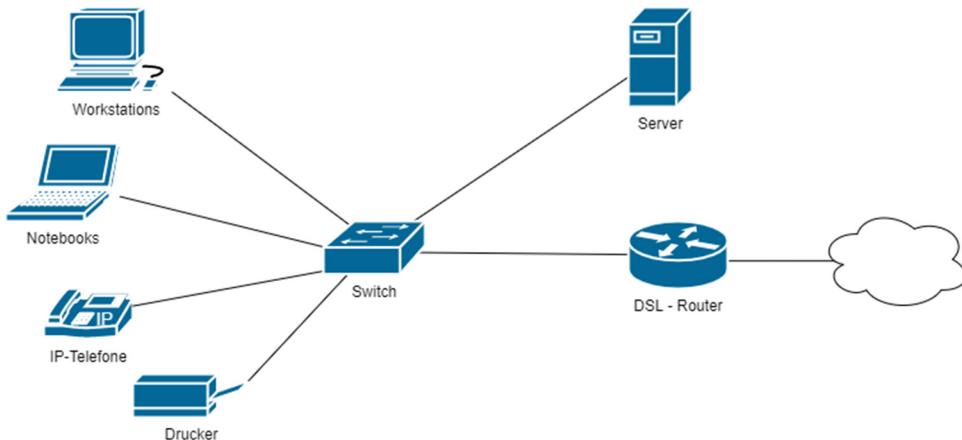
Wie in Kapitel 11 thematisiert wird, existiert für die Adressierung privater, nicht öffentlicher Netzwerke innerhalb der Netzwerkklassen A–C je ein IP-Bereich, der kostenlos und registrierungsfrei von der ABC GmbH genutzt werden kann (vgl. Private IP-Netze). Hiermit können die firmeneigenen Rechner mit IP-Adressen versorgt werden. Der Transport von Anfragen nach außen erfolgt über den geplanten zentralen DSL-Router, der mit der Funktion NAT Anfragen aus dem privaten Netz zur öffentlichen IP-Adresse übersetzt (vgl. *Direkte Verbindung zum Internet per NAT/PAT*).

Die Wahl fällt auf ein Klasse C-Netz, da diese Klasse am besten zu den wenigen benötigten Adressen passt (vgl. *IP-Adressklassen*).

Das gewählte IP-Netz 192.168.0.x verwendet die Standard-Subnetzmaske 255.255.255.0 und stellt die Adressen 192.168.0.1 – 192.168.0.254 bereit. Für unterschiedliche Einsatzzwecke wird das IP-Netz in mehrere Blöcke (mit Reserven) aufgeteilt:

IP-Bereich	Einsatzzweck
192.168.0.1 – 192.168.0.50	Client-Computer
192.168.0.100 – 192.168.0.120	Drucker
192.168.0.140 – 192.168.0.160	IP-Telefone
192.168.0.200 – 192.168.0.230	Verwaltbare Netzwerkgeräte (Switche, Kameras)
192.168.0.250 – 192.168.0.254	Server, Gateway (DSL-Router)

Die IP-Adresse 192.168.0.0 ist für die Netzwerkadresse (NetID). Gleicher gilt für die IP-Adresse 192.168.0.255, die als Broadcast-Adresse (Nachricht an alle Geräte im Netzwerk) fungiert.



Schematische Darstellung des Netzwerkes der ABC GmbH

Umsetzungsdetails

Der IP-Bereich für die Client-Computer wird automatisiert per DHCP an die Clients verteilt. Zu diesem Zweck wird die Serverrolle DHCP Server auf dem Windows Server installiert und ein entsprechender Scope eingerichtet. Die Drucker, IP-Telefone, der Server und der DSL-Router erhalten statische IP-Adressen. Beim Einrichten einer Windows-Domäne ist bei dieser Konfiguration dringend darauf zu achten, dass auf dem Domänencontroller für eine korrekte Funktion der Internetverbindung der Clients eine DNS-Weiterleitung zum Router eingerichtet wird.

Gerät(e)	IP-Adressen
DSL-Router	192.168.0.254
Windows Server	192.168.0.253
Drucker (Laser 1, Laser 2, All-in-One)	192.168.0.100 - 192.168.0.102
IP-Telefone (9 St.)	192.168.0.140 - 192.168.0.148
Admin Interface (Switch)	192.168.0.200

Teststrategie

- ✓ Überprüfen der IP-Konfiguration an den PC-Systemen mit dem Befehl ipconfig

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address.....: FE80::260:70FF:FECE:CA73
IPv6 Address.....: :::
IPv4 Address.....: 192.168.0.1
Subnet Mask.....: 255.255.255.0
Default Gateway.....: :::
                                         192.168.0.254
```

- ✓ Überprüfung der eigenen Netzwerkverbindlichkeit mit dem Befehl PING

Erhalten Sie keine Antworten auf den Ping-Befehl, müssen Sie ggf. eine Ausnahme in den Firewall-Regeln vornehmen.

```
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time=2ms TTL=128
Reply from 127.0.0.1: bytes=32 time=3ms TTL=128
Reply from 127.0.0.1: bytes=32 time=2ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

- | Name | Gruppe | Profil | Aktiviert | Aktion | Außer Kraft setzen | Programm | Lokale Adresse | Remoteadresse | Protokoll |
|---|----------------------------|----------|-----------|----------|--------------------|----------|----------------|-----------------|-----------|
| • Datei- und Druckerfreigabe (Echoanforderung - ICMPv4 eingehend) | Datei- und Druckerfreigabe | Privat.. | Ja | Zulassen | Nein | System | Beliebig | Lokales Subnetz | ICMPv4 |
- ✓ Überprüfen der Netzwerkverbindlichkeit zum **Server** mit dem Befehl ping

```
C:\>Ping 192.168.0.253

Pinging 192.168.0.253 with 32 bytes of data:

Reply from 192.168.0.253: bytes=32 time<1ms TTL=128
Reply from 192.168.0.253: bytes=32 time=3ms TTL=128
Reply from 192.168.0.253: bytes=32 time<1ms TTL=128
Reply from 192.168.0.253: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

- ✓ Überprüfen der Netzwerkverbindlichkeit zum **Gateway** mit dem Befehl ping

```
C:\>Ping 192.168.0.254

Pinging 192.168.0.254 with 32 bytes of data:

Reply from 192.168.0.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- ✓ Überprüfen der Netzwerkverbindlichkeit zum **Internet** mit dem Befehl ping (hier einer der Google DNS-Server)

```
C:\>ping 8.8.8.8

Ping wird ausgeführt für 8.8.8.8 mit 32 Bytes Daten:
Antwort von 8.8.8.8: Bytes=32 Zeit=31ms TTL=111
Antwort von 8.8.8.8: Bytes=32 Zeit=29ms TTL=111
Antwort von 8.8.8.8: Bytes=32 Zeit=30ms TTL=111
Antwort von 8.8.8.8: Bytes=32 Zeit=29ms TTL=111

Ping-Statistik für 8.8.8.8:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 29ms, Maximum = 31ms, Mittelwert = 29ms
```

- ✓ Überprüfen der Konnektivität zum Internet inklusive Prüfung der DNS-Namensauflösung

Der Schalter -4 erzwingt die Verwendung von IPv4.

```
C:\>Ping -4 dns.google

Ping wird ausgeführt für dns.google [8.8.4.4] mit 32 Bytes Daten:
Antwort von 8.8.4.4: Bytes=32 Zeit=30ms TTL=111

Ping-Statistik für 8.8.4.4:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 30ms, Maximum = 30ms, Mittelwert = 30ms
```

10

Normen und Modelle

10.1 Gremien

Notwendigkeit von Normierungen

Der IT-Bereich ist geprägt von einer enormen Herstellervielfalt. Auch beim Thema Netzwerke finden sich viele Kombinationsmöglichkeiten von Hard- und Software-Produkten unterschiedlichster Hersteller.

Um die Kompatibilität von Produkten gewährleisten zu können, ist es für die Hersteller unumgänglich, Normen als Richtlinien zu erhalten. Genauso verhält es sich für den Endverbraucher, der sich auf Standards verlassen können muss, da er nicht jedes Produkt einzeln testen kann.

De facto versus de jure

An vielen Stellen ist die Entwicklung der Vernetzung geprägt von Firmen, die Neuentwicklungen so schnell wie möglich umsetzen wollten. Häufig hat der Markt solche Entwicklungen angenommen, und es wurden dadurch De-facto-Standards (lat. für „aufgrund der Tatsache“) geschaffen.

Beispiele: IBM mit dem Konzept der **Systems Network Architecture (SNA)**, eine hierarchische Netzwerkarchitektur für Großrechner und DEC mit **Digital Network Architecture (DAN)**, eine Protokollsammlung für lokale Netze).

Bei einem komplexen Thema wie Vernetzung können proprietäre Lösungen aufgrund von Inkompatibilität Probleme verursachen. Deswegen sind internationale De-jure-Standards (lat. für „von Rechts wegen“) wichtig. Viele Standardisierungsgremien sind jedoch starr strukturiert und brauchen oft lang, um einen Standard zu definieren.

Die folgenden Abschnitte schildern die wichtigsten Gremien.

International Organization for Standardization (ISO)

Die ISO (<https://www.iso.org/home.html>) ist eine Dachorganisation von 163 nationalen Normungsausschüssen, darunter z. B. American National Standards Institute (ANSI) oder Deutsches Institut für Normung (DIN). Die ISO selbst ist Mitglied bei der International Telecommunication Union-Telecommunication (ITU-T). Aufgabe der ISO ist es, die von den einzelnen Ländern vorgeschlagenen Standardisierungen abzustimmen, zu vereinheitlichen und dann den nationalen Ausschüssen als Empfehlungen weiterzugeben. Zwei der bekanntesten Beispiele dürften der **American Standard Code for Information Interchange (ASCII)** -Zeichensatz sein, der 1968, 1977 und 1986 Thema war, und der Begriff „Qualitätsmanagement“, der unter dem Kürzel ISO 9000 publik wurde.

Institute of Electrical and Electronics Engineers (IEEE)

Dieser Fachverband (<https://www.ieee.org/>) bemüht sich in mehrmaligen Treffen pro Jahr hauptsächlich um die Normierung auf dem Gebiet der Elektrotechnik.

Die Projektgruppe 802, deren Name sich auch gut mit dem Datum ihres ersten Treffens, dem 29-2-1980, in Verbindung bringen lässt, hat etliche Standards definiert, die für lokale Netze weltweite Gültigkeit erlangten. Innerhalb dieser Projektgruppe (häufig auch 802-Komitee genannt) gibt es mehrere Arbeitsgruppen, die sich um die einzelnen Normierungen kümmern. Die folgende Tabelle zeigt eine Liste wichtiger Themenbereiche im Detail und schildert in der Spalte „Status“ den aktuellen Zustand der entsprechenden Gruppe:

Nummer	Beschreibung	Status
802.1	Internetworking	aktiv
802.2	Logical Link Control (LLC) -Teilschicht	inaktiv
802.3	CSMA/CD, Ethernet	aktiv
802.10	Netzwerksicherheit	aufgelöst
802.11	Drahtlose Netzwerke	aktiv
802.12	Demand Priority Access, 100VG AnyLAN	inaktiv
802.15	Wireless Personal Area Network (WPAN)	aktiv
802.16	Broadband Wireless Access Working Group	aktiv
802.17	Resilient Packet Ring Working Group	aktiv
802.18	Radio Regulatory TAG (Technical Advisory Group)	aktiv
802.19	Coexistence TAG	aktiv
802.20	Mobile Broadband Wireless Access (MBWA), drahtlose Breitbandnetze	aktiv
802.21	Media Independent Handoff Working Group	aktiv
802.22	Wireless Regional Area Networks, drahtlose Regionalnetze	aktiv

Die Standards des IEEE werden von der ISO unter dem Kürzel 8802 übernommen, z. B. ist IEEE 802.3 identisch mit ISO 8802-3.

In einigen Arbeitsgruppen gibt es noch weitere Unterteilungen in Einzelthemen. So kümmert sich z. B. 802.1 mit 802.1b um Netzwerk-Management, mit 802.1d um den Spanning-Tree-Algorithmus, mit 802.1p um die Priorisierung von Frames, mit 802.1q um VLANs und mit 802.1x um die Authentifizierung im Netzwerk.

International Telecommunication Union (ITU)/Comité Consultatif International Télégraphique et Téléphonique (CCITT)

Die ITU (<https://www.itu.int>) besteht aus drei Hauptsektoren:

- ITU-R Radiocommunication befasst sich mit der weltweiten Zuteilung von Radiofrequenzen.
- ITU-D Developement befasst sich mit Entwicklungsaufgaben.
- ITU-T Telecommunication befasst sich mit Telefon- und Datenkommunikationssystemen, löste unter dem Kürzel ITU-TSS (Telecommunication Standard Sektor) seit 1988 schrittweise die CCITT als beratendes Gremium ab. Die ITU-T ging aus der ehemaligen CCITT hervor. Die endgültige Umstrukturierung war im März 1993 abgeschlossen.

Es wurden viele „Empfehlungen“ herausgegeben, die allerdings für die meisten Länder verpflichtend wirkten, sofern sie sich nicht vom internationalen Standard abkapseln wollten.

Die Empfehlungen werden in sogenannten Serien herausgegeben, wobei jeweils ein bestimmter Anfangsbuchstabe einem bestimmten Bereich zugeordnet wird. Innerhalb dieser Bereiche werden die Empfehlungen dann durchnummeriert. Viele Normen, zum Beispiel bezüglich Modems oder Telefaxübertragung, wurden von CCITT (heute ITU-T) festgelegt. Die folgende Tabelle zeigt eine Liste wichtiger Empfehlungsserien:

Serie	Thema
A	ITU-interne Organisation, Verfahrensabläufe, Gremien
B	Ausdrucksmittel (Definitionen, Vokabular, Symbole, Abkürzungen)
E	Betrieb von Telefonnetzen, Adressierung, Nummerierung
F	Telegrafendienste, Telematikdienste, Mitteilungs- und Verzeichnisdienste
G	Telefonübertragung über drahtgebundene Verbindungen, Satelliten- und Funkverbindungen
I	Dienste integrierendes digitales Netzwerk (ISDN)
J	Fernsehübertragungen
T	Endgeräte und Protokolle für Telematikdienste
V	Datenübertragung über das Telefonnetz, Normen für Modems
X	Datenübermittlungsnetze

International Engineering Task Force (IETF)

Diese Organisation (<https://www.ietf.org>) ist eine offene internationale Gemeinschaft von Herstellern, Netzwerktechnikern, Netzbetreibern, Anwendern und Forschern, die die technische Entwicklung des Internet koordiniert und standardisiert.

Die Request For Comment (**RFC**) Dokumente der IETF enthalten ausführliche Beschreibungen zu Internetprotokollen, der Vernetzung, uvm. Sie können direkt im Browser unter dem Internetlink <https://www.ietf.org/standards/rfcs/> eingesehen werden.

Internet Corporation for Assigned Names and Numbers (ICANN)

Sie (<https://www.icann.org>) ist für die Vergabe von eindeutigen Namen (hauptsächlich der Top-Level-Domains) und IP-Adressen im Internet verantwortlich und koordiniert die Strukturierung vom Dienst DNS. Die Vergabe von IP-Adressen wird an die Unterorganisation **Internet Assigned Numbers Authority (IANA)** delegiert. Das Handelsministerium der USA hat seit der Gründung die Aufsicht über die ICANN, die es aber in nächster Zeit aufgeben will.

Internet Assigned Numbers Authority (IANA)

Eine Abteilung der ICANN mit Namen IANA (<https://www.iana.org>) ist verantwortlich für die Vergabe von IP-Adressen, Portnummern und Namensvergaben im Internet.

Plus  **Ergänzende Lerninhalte:** *Weiterführende Informationen.pdf*
In diesem Dokument finden Sie u. a. eine Auflistung weiterer wichtiger Gremien.

10.2 Schichten-Modelle

Der Sinn von Schichten-Modellen

Netzwerke bestehen nicht nur aus einer Architektur (Topologie, Übertragungsmedium, Zugriffsvorfahren), wie dies in den vorherigen Kapiteln beschrieben wurde. Es bedarf auch einer Reihe von Regeln zur Steuerung der Kommunikation zwischen den verschiedenen Systemen.

Da Kommunikation überall, z. B. auch im zwischenmenschlichen Bereich, ein sehr komplexes Thema ist, ist es nur verständlich, dass zu einer funktionierenden Kommunikation viele Komponenten zusammenwirken müssen. Diese vielen verschiedenen Bestandteile können und werden in der Praxis meist nicht von einem Hersteller komplett angeboten, sondern verteilen sich auf viele verschiedene Firmen.

Um eine nahtlose Zusammenarbeit der unterschiedlichen Einzelkomponenten verschiedener Hersteller zu gewährleisten, gibt es Gremien, die Normen und Standards veröffentlichen. Firmen, die sich bei der Entwicklung einer neuen Teilkomponente an diese Normen halten, können relativ sicher sein, dass ihre Neuentwicklung problemlos mit Komponenten anderer Hersteller zusammenarbeiten wird.

Neben diesen sehr wichtigen Normen gibt es für Hersteller und Benutzer noch eine zweite große Orientierungshilfe, über die versucht wird, alle für den Netzwerkverkehr relevanten Teilkomponenten in ein einziges Schema zu bringen, nämlich sogenannte Schichten-Modelle.

Allgemeine Beschreibung von Schichten-Modellen

Ein Schichten-Modell stellt den Netzwerkverkehr als eine Reihe aufeinander folgender Schichten dar. Es wird davon ausgegangen, dass zwischen zwei Systemen eine Kommunikation stattfindet und dass es dementsprechend einen Sender und einen Empfänger gibt, die über ein bestimmtes Medium miteinander verbunden sind. Möchte der Sender eine Nachricht versenden, sind bei komplexen Systemen viele Komponenten und Medien involviert, so dass eine Aufteilung der Übertragung auf mehrere Bereiche (Schichten) sinnvoll ist. Während der Übertragung durchläuft die Nachricht auf dem Sendersystem mehrere Schichten, in denen die Nachricht Stück für Stück für die Übertragung präpariert wird. Nach der Übertragung durchläuft die Nachricht beim Empfänger die gleichen Schichten in umgekehrter Reihenfolge und wird wieder Stück für Stück zurücktransformiert.

Komplexität reduzieren

Modelle werden unter anderem deshalb entworfen, um die Komplexität von Systemen auf allgemeine Standards zu reduzieren. Solche Modelle entsprechen nie exakt der Wirklichkeit, was in Kauf genommen wird, denn sie sollen eine Übersicht über die Zusammenhänge vermitteln.

Datenverkehr in Netzwerken ist ein komplexes und vielschichtiges Thema. Eine brauchbare Methode, diese Komplexität zu verringern, besteht darin, Netzwerke als eine Reihe von imaginär übereinander liegenden Schichten aufzubauen, von denen jede einzelne für bestimmte Aufgaben zuständig ist. Die Schnittstellen und Übergänge zwischen den einzelnen Schichten regeln die Kommunikation zwischen diesen.

10.3 Das OSI-Referenz-Modell allgemein

Wichtige theoretische Grundlage

Das Open-System-Interconnection-Modell, kurz OSI-Referenz-Modell, ermöglicht, den komplexen Ablauf bei der Übermittelung von Daten zwischen zwei Systemen logisch aufzuteilen. Der Blick auf das Netzwerk als Gesamtsystem wird vereinfacht. Jede Definition eines Netzwerkdienstes bezieht sich auf das OSI-Schichten-Modell bzw. auf das TCP/IP-Referenzmodell, welches ein noch weiter vereinfachtes Modell darstellt.

Herleitung und Übersicht

Mit der Zielsetzung, einen einheitlichen Standard zu schaffen, entwickelte die ISO ab 1977 ein abstraktes, logisch-funktionelles Architekturmodell, das die Datenkommunikation in offenen Systemen beschreibt. 1978 wurde dieses Modell (ISO 7498) erstmalig veröffentlicht. 1984 wurde die heutige, überarbeitete Version unter dem Namen OSI-Modell (Open System Interconnection) veröffentlicht.

Überblick über das OSI-Referenz-Modell

Die gesamte Netzwerkkommunikation wird in ein Modell aus sieben Schichten eingeteilt. Die folgende Tabelle gibt, von oben nach unten, einen Überblick über die englischen und deutschen Bezeichnungen der einzelnen Schichten sowie eine kurze Beschreibung der jeweiligen Aufgabe.

Nr.	Layer	Schicht	Aufgaben
7	Application	Anwendung	Schnittstelle der Anwendungen auf das Netzwerk
6	Presentation	Darstellung, Präsentation	Protokolle für die Syntax der Daten
5	Session	Sitzung	Funktionen für den Auf- und Abbau einer Sitzung, Festlegen von Synchronisationspunkten
4	Transport	Transport	Ende-zu-Ende-Kommunikation
3	Network	Vermittlung, Netzwerk	Routing der Pakete
2	Data-Link	Sicherung, Datenverbindung	Festlegung des Zugriffsverfahrens, Fehlererkennung der Frames oder Zellen
1	Physical	Bitübertragung	Definition von Aspekten für die Bitübertragung auf dem Medium

Eine detaillierte Erklärung der Arbeitsweise in den einzelnen Schichten erfolgt im weiteren Verlauf dieses Kapitels. Folgende zwei Sätze erleichtern es, sich die Reihenfolge der Schichten anhand der englischen Bezeichnung einzuprägen:

Von Schicht 1 bis 7:

Please Do Not Throw Sausage Pizza Away

Von Schicht 7 bis 1:

All People Seem To Need Data Processing

Ziele des Modells

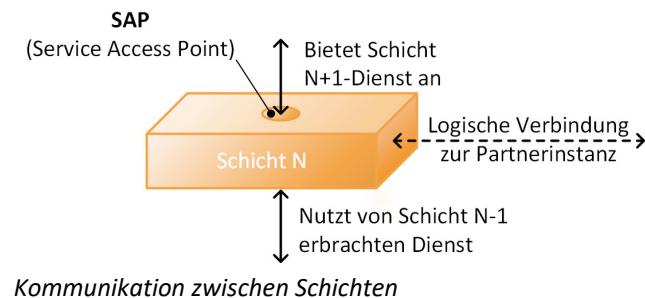
Ziel war ein standardisierter Formalismus zur Beschreibung und zum Vergleich der Kommunikation in vorhandenen Architekturen sowie ein konzeptioneller Rahmen zur Ausarbeitung künftiger Standards. Folgende Entwurfskriterien wurden zugrunde gelegt:

- ✓ Jede Schicht entspricht einer genau definierten Funktion.
- ✓ Zwischen den Schichten soll der Informationsfluss so gering wie möglich sein.
- ✓ Eine Schicht kann nur mit der Schicht darüber oder darunter kommunizieren.
- ✓ Die Anzahl der Schichten soll möglichst gering sein.
- ✓ Neue Schichten stellen einen neuen, höheren Abstraktionsgrad dar.

Funktionsprinzip des Modells

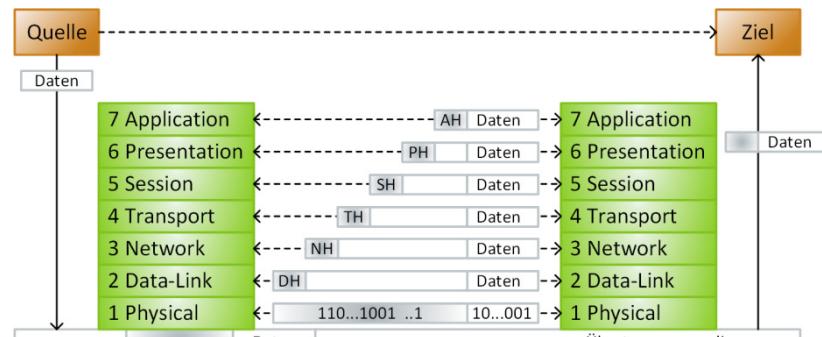
Über eine definierte Schnittstelle, den sogenannten **Service Access Point (SAP)**, stellt jede Schicht der nächsthöheren eine Gruppe von Methoden (Dienste bzw. Primitive) zur Verfügung.

Mit steigender Schicht nimmt die Komplexität der Aufgaben zu. Die Funktionalität jeder Schicht baut auf die Standards der darunter liegenden auf.



Es interagieren immer nur Schichten, die direkt beieinander liegen, d. h., einzelne Schichten können nicht übersprungen werden.

Während des Datenverkehrs agieren die einzelnen Schichten der beteiligten Netzknoten so, als ob sie mit der jeweiligen Schicht des anderen beteiligten Netzwerk-knotens kommunizieren würden (horizontale Kommunikation über eine logische Verbindung).



Schematische Interaktion der einzelnen Schichten

Tatsächlich aber durchlaufen alle Daten immer alle Schichten (vertikale Kommunikation). Angefangen beim Sender von Schicht 7 abwärts zur Schicht 1 auf das Übertragungsmedium (physische Verbindung) und beim Empfänger dann vom Übertragungsmedium zur Schicht 1 aufwärts zur Schicht 7. Die Antworten durchlaufen die Schichten wiederum alle Schichten in umgekehrter Reihenfolge zurück.

Der wirkliche Weg der Nachricht führt **vertikal** durch alle Schichten, wobei nicht unbedingt in jeder Schicht eine Aktion erfolgen muss. Virtuell jedoch kommunizieren die Schichten auch **horizontal** miteinander. Das bedeutet, dass die Schichten der jeweils gleichen Ebene aufeinander abgestimmt sein müssen. Dabei sind die Schichten 1–4 transportorientiert und die Schichten 5–7 anwendungsorientiert.

Header

Beim Weiterreichen stellt jede involvierte Schicht des Senders (mit Ausnahme von Schicht 1) den erhaltenen Daten einen **Header** voran, der von der entsprechenden Schicht auf der Seite des Empfängers interpretiert und wieder entfernt wird. Der Header enthält die vom Kommunikationspartner in der jeweiligen Schicht benötigten Steuerinformationen und stellt den wesentlichen Teil der virtuellen Kommunikation zwischen den Instanzen gleicher Schichten her. Zum Beispiel ist dieser in Schicht 2 in der Abbildung oben mit DH bezeichnet (Header der Schicht Data-Link) usw.

Vorteile des Schichten-Modells

Obwohl das Schichten-Modell sehr abstrakt ist, ergeben sich daraus für Hersteller und Entwickler etliche Vorteile. Realisiert werden einzelne Schichten durch entsprechende Protokolle, die bei der Kommunikation zwischen einzelnen Netzwerkkomponenten spezifische Aufgaben übernehmen.

In Netzwerken wirken viele einzelne Komponenten zusammen. Solange sich alle Hersteller an die Definition der Übergänge zwischen den Schichten und an die Protokolle in den Schichten halten, hat der Anwender eine hohe Sicherheit, dass neu gekaufte Produkte mit Produkten anderer Hersteller zusammenarbeiten.

Der wohl wichtigste Vorteil des OSI-Schichtenmodells ist, dass das Verfahren innerhalb einer Schicht (z. B. das Internet Protokoll IPv4 in Schicht Nr. 3) durch ein anderes ausgetauscht oder ergänzt werden kann (z. B. durch IPv6), ohne dass Änderungen auf anderen Schichten vorgenommen werden müssen.

Unabhängigkeit der einzelnen Schichten voneinander

Die eigentliche Umsetzung des Inhalts einer Schicht ist unerheblich. Wichtig sind nur die Dienste, die an den Schnittstellen zur Verfügung stehen. So können einzelne Schichten unabhängig von einander z. B. durch unterschiedliche Institutionen entwickelt werden.

Flexibilität

Änderungen an einzelnen Schichten wirken sich nicht auf darüber oder darunter liegende Schichten aus, solange die definierten Schnittstellen erhalten bleiben.

Physikalische Trennung der Schichten

Jede Schicht kann in der für ihre Aufgabenstellung günstigsten Technik entwickelt werden.

Vereinfachte Standardisierung

Die genaue Festlegung der Funktion einer Schicht erlaubt es, Standardschichten zu entwickeln.

Einfache Wartung und Implementation

Die Entwicklung komplexer Systeme wird durch die Modularität mit klar definierten Schnittstellen vereinfacht.

Nachteil

Der Nachteil dieses Schichten-Konzepts besteht in dem Aufwand an Steuerinformationen. Nahezu jede Schicht schreibt ihren eigenen Header und fügt dadurch Overhead der zu transportierenden Information hinzu, wodurch sich der effektive Datendurchsatz verringert.

10.4 Die sieben Schichten des OSI-Modells

1. Physical Layer (Bitübertragungs-Schicht)

Der **Physical Layer** definiert alles, was für die direkte Übertragung (Senden und Empfangen) einzelner Bits über ein Medium notwendig ist.

Dazu werden im mechanischen Teil die physikalischen Eigenschaften des Interface zu einem Übertragungsmedium (z. B. Steckergeometrie, Pinbelegung) spezifiziert.

Der elektrische bzw. optische Bereich definiert, wie die Datenbits auf dem Medium dargestellt werden. Daraus ergibt sich eine maximal erreichbare **Datenübertragungsrate**.



Die funktionalen Spezifikationen befassen sich mit dem Aufbau von Verbindungen, wie z. B. der Unterscheidung zwischen Datenleitung – Steuerungsleitung oder Taktgebung.

Die verfahrenstechnischen Spezifikationen definieren u. a. den **Übertragungsmodus** (Halb-, Vollduplex).

2. Data Link Layer (Sicherungs-/Datenverbindungs-Schicht)

Der **Data Link Layer** transformiert die Daten des Network Layers in **Frames** (Datenrahmen unterschiedlicher Größe) oder **Zellen** (Datenrahmen fester Größe) und reicht sie an die Bitübertragungs-Schicht weiter bzw. umgekehrt.



Das Zerlegen von Frames in einzelne Bits für die Bitübertragungs-Schicht bzw. das Zusammensetzen empfangener Bits zu Frames gehört ebenfalls zu den Aufgaben dieser Schicht. Der **Data Link Layer** verbindet somit zwei an ein gemeinsames Medium angeschlossene Teilschichten (**Network Layer/Physical Layer**).

Ein Frame besteht bei Ethernet aus einem **Header** (den Adressen von Empfänger und Sender sowie Steuerinformationen), den **Daten** sowie einem angehängten **Trailer**. Ebenfalls darin enthalten ist die **Frame Check Sequence (FCS)**, um zu erkennen, ob die Daten fehlerfrei übertragen wurden. Für die Berechnung der Frame Checksum wird in der Regel ein **Cyclic Redundancy Check (CRC)** Algorithmus verwendet.

3. Network Layer (Vermittlungs-/Netzwerk-Schicht)



Die als **Network Layer** bezeichnete Schicht dient zur Wegfindung (**Routing**) der Pakete über verschiedene Netzwerkknoten. Weitere Aufgaben sind die Kontrolle der Pakete und letztlich der Transport der Pakete zu den Zielknoten (**Messages Forwarding**). Auf Layer 3 finden sich u. a. wichtige Protokolle für die Wegefindung (**Internet Protocol Version 4 und 6 (IPv4/IPv6)**) und Statusmitteilungen (**Internet Control Message Protocol (ICMP/ICMPv6)**).

4. Transport Layer (Transport-Schicht)

Der **Transport Layer** realisiert eine Kopplung von Endsystemen über eine transparente Verbindung (Ende-zu-Ende-Kommunikation). Weitere Aufgaben sind die **Segmentierung** (Zerstückelung/Vereinigung) des Datenstroms, die Initiierung des erneuten Sendens von fehlenden Datensegmenten anhand der **Sequenznummer**, falls keine Empfangsbestätigung vom Empfänger eintrifft (nur bei Verwendung des **Transmission Control Protocols (TCP)**) und die Überwachung der Netzlast (Congestion Control) zwischen den benachbarten Netzknoten.



Die Transport-Schicht vermittelt zwischen den darüberliegenden, anwendungsorientierten Schichten und den darunterliegenden, transportorientierten Schichten.

5. Session Layer (Kommunikationssteuerungs-/Sitzungs-Schicht)

Der **Session Layer** liefert Funktionen zur Eröffnung bzw. Beendigung einer geordneten und logischen Kommunikationsbeziehung (Session/Sitzung), die zwischen zwei Systemen auf- bzw. abgebaut werden soll.

Hierzu gehören die **Namensauflösung** (Umwandlung von Namen zu IP-Adressen und umgekehrt) von Netzwerkressourcen sowie das Aushandeln von Parametern für die Flusskontrolle (wer darf wann und wie lange wie viele Daten auf einmal senden). Sie stellt einen universalen Transportservice (Prozess-zu-Prozess-Verbindung) dar.



Zur Sitzungsverwaltung gehört vor allem auch die **Synchronisation**. Bei kurzfristigen Netzausfällen muss es möglich sein, fehlende Daten erneut zu übertragen. Um dies zu gewährleisten, werden entsprechende Prüfpunkte in die Daten eingefügt. Reißt der Datenstrom ab, müssen nur die Daten nach dem letzten empfangenen Prüfpunkt erneut übertragen werden.

6. Presentation Layer (Darstellungs-/Präsentations-Schicht)

Der **Presentation Layer** konvertiert die Daten in ein allgemeines, vereinbartes und für die beteiligten Computer verständliches **Standardformat (Abstract Syntax Notation One (ASN.1))**. Dies ist notwendig, da sich die interne Darstellung von Daten (z. B. in den Zeichencodes **ASCII**, **ANSI**, **EBCDIC**) je nach eingesetztem System unterscheidet.



Weitere Aufgaben dieser Schicht sind die Datenkodierung sowie Komprimierung zur Reduzierung der zu übertragenden Datenmenge und die Verschlüsselung.

7. Application Layer (Anwendungs-Schicht)

Der **Application Layer** bildet die Schnittstelle zwischen den Anwendungen (Programmen) und dem darunterliegenden Netzwerk. Zu diesem Zweck stehen den Anwendungen diverse Protokolle zur Verfügung. Zwei der bekanntesten sind das **Hypertext Transfer Protocol (HTTP)** und das **Simple Mail Transfer Protocol (SMTP)**.



Mehrfache Kontrolle

Verschiedene Mechanismen, wie z. B. die Fehler- oder Flusskontrolle, sind mehrfach den verschiedenen Schichten zugeordnet, andere findet man nur in bestimmten Schichten. Jede Schicht regelt dabei „ihren“ Teil der Kontrolle. Erst wenn eine Schicht nicht mehr weiterkommt, wird eine entsprechende Meldung an die übergeordnete gegeben. Diese verwendet dann einen anderen Mechanismus, um das Problem zu umgehen.

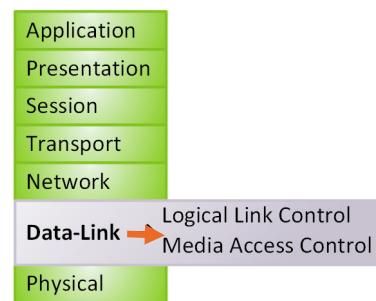
10.5 Das OSI-Modell und IEEE 802

Erweiterung des Data Link Layers

Die Projektgruppe 802 des IEEE setzt ausschließlich bei den beiden unteren Schichten des OSI-Modells an. Einfluss auf das OSI-Modell hatte 1985 der Vorschlag, die Sicherungs-Schicht in zwei Teilschichten zu gliedern.

Logical Link Control (LLC)

Die LLC-Teilschicht leistet die Flusskontrolle (Sequenzierung und Bestätigung von Rahmen). Hier wird sichergestellt, dass eine Station nur so viele Daten sendet, wie der Empfänger auch verarbeiten kann. Ziel ist es, eine Station nicht mit Daten zu überfluten. Sie definiert die Schnittstellen für die darüberliegende OSI-Schicht (Network).



Die entsprechenden Standards sind in IEEE 802.2 definiert.

Media Access Control (MAC)

Die MAC-Teilschicht kommuniziert direkt mit dem **Network Layer**. Sie steuert den Sendevorgang und ist für die Adressierung der Datenframes zuständig. Von dieser Teil-Schicht hat die Adresse ihren Namen, die für eine Netzwerk-Schnittstelle auf Layer 2 benötigt wird: die **MAC-Adresse** (in Ethernet-Netzwerken auch Ethernet-Adresse genannt, vgl. Kapitel 11.3).

Durch die Aufteilung des Data-Link-Layers wurde eine stärkere Hardware-Unabhängigkeit erreicht, da quasi alle Hardware-Spezifika in der MAC-Teilschicht behandelt werden. So sind z. B. die Treiber von Netzwerkkarten auf dieser Schicht angesiedelt.

10.6 Exkurs: Frames

Der Aufbau eines Ethernet-V2-Rahmens (nach IEEE 802.3)

Im Folgenden wird dargestellt, wie in einem Ethernet-Netzwerk auf den Schichten 1 und 2 Daten übertragen werden. Am bekanntesten ist die Definition des heute noch gültigen Ethernet-V2-Rahmens für den Layer 2 (Data-Link-Layer).

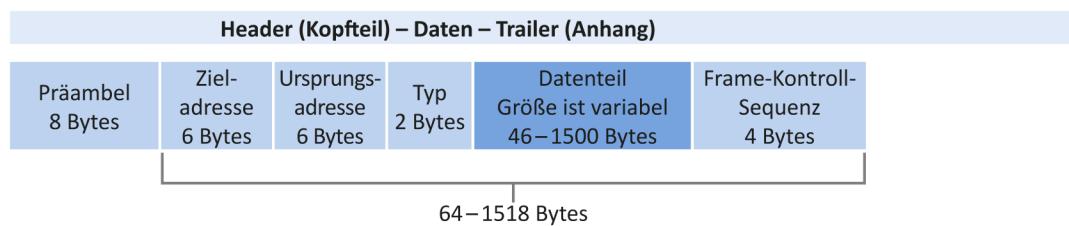
Frames

Grundsätzlich werden größere Datenmengen nicht in einem Stück verschickt. Zum einen würde dieses Vorgehen zeitweise die gesamte Bandbreite des Netzes beanspruchen und den Netzwerkzugriff für alle anderen Teilnehmer sperren. Zum anderen müssten bei einem Übertragungsfehler die gesamten Daten erneut übertragen werden.

Um dieses Problem zu umgehen, werden größere Datenmengen in kleinere Einheiten, sogenannte **Frames**, **Rahmen** oder **Datagramme**, zerlegt. Dadurch müssen bei Fehlern nur die entsprechenden Rahmen neu übertragen werden. Außerdem können mehrere Benutzer abwechselnd Rahmen verschicken, wodurch ein nahezu zeitgleicher Netzwerkgzugriff möglich wird.

Bei der Konfiguration eines Netzinterfaces kann eine sogenannte **Maximum Transmission Unit (MTU)** angegeben werden. Sie definiert die maximale Größe eines Datagramms. Daten, die diese Länge überschreiten, werden immer in mehrere Frames aufgeteilt bzw. fragmentiert und danach über das Netzwerk versendet.

Um sicheren Datenverkehr zu gewährleisten, müssen die Daten mit entsprechenden Informationen versehen werden. Der prinzipielle Aufbau eines Rahmens nach IEEE 802.3 ist dabei immer:



Ethernet-V2-Frame

Wie sich die einzelnen Teile zusammensetzen, ist abhängig vom verwendeten Übertragungsverfahren.

Ein Ethernet-V2-Rahmen hat (ohne VLAN-Tag) eine Rahmengröße zwischen 64 und 1518 Bytes und folgenden Aufbau:

- ✓ Die **Präambel** enthält ein Bitmuster, das es den Netzwerkkarten ermöglicht, ihre Empfangselektronik zu synchronisieren. Sie endet mit dem sogenannten **Start Frame Delimiter (SFD)**, der den Beginn des eigentlichen Frames anzeigen. Diese 8 Bytes werden bei den Größenangaben eines Rahmens nicht mit gerechnet.
- ✓ Als Ziel- und Ursprungs-Adresse werden die **MAC-Adressen** der beteiligten Netzwerkschnittstellen eingetragen.
- ✓ Im **Typ-Feld** wird die Art des darüberliegenden Protokolls angegeben, z. B. ob es für IPv4 oder IPv6 bestimmt ist.
- ✓ Der Daten-Teil hat eine Größe zwischen 46 und 1500 Bytes. Hier sind die Nutzdaten (inklusive der Header der höheren Schichten) enthalten.
- ✓ Als Frame-Kontroll-Sequenz (**Frame Check Sequence, FCS**) wird ein **CRC**-Algorithmus eingesetzt. Anhand der FCS kann erkannt werden, ob der Rahmen korrekt übertragen wurde.

Es ist möglich, dass sich höhere Schichten auf größere Paketgrößen geeinigt haben, die dann hier in Schicht 2 auf mehrere kleinere Frames aufgeteilt (fragmentiert) werden.



Es existieren neben dem Ethernet-V2 (auch **Ethernet-II** genannt) noch andere Frame-Definitionen, die mittlerweile veraltet sind. Ethernet-V2 besitzt kein Längenfeld, dafür ein Typfeld mit Informationen über das Protokoll der Nutzdaten im Datenteil. Größere Datenanteile mit mehr als 1500 Byte (Jumbo-Frames) sind möglich, jedoch nicht in der IEEE 802.3 spezifiziert.

- ✓ Ist ein Netzwerk über einen oder mehrere Switches in virtuelle Netzwerke aufgeteilt, erhält jeder Frame im Datenteil zur Identifizierung der VLANs zusätzlich ein 4 Byte großes Feld, das **VLAN-Tag** (vgl. Kapitel 12.4).
- ✓ Unter IPv6 gibt es keine Fragmentierung mehr. Ist ein Frame zu groß, erhält der Absender eine Fehlermeldung per ICMPv6, damit er die MTU reduziert.

10.7 Übung

Fragen zu Schichtenmodell und Übertragung

Übungsdatei: --

Ergebnisdatei: uebung10-E.pdf

1. Welches ist der wichtigste Vorteil eines Schichtenmodells?
2. Wie werden die Verbindungspunkte zwischen den Schichten bezeichnet?
3. Über welche Schicht erfolgt die Übertragung per Ethernet?
4. Welcher Schicht gehören Verteilerschränke mit Patchpanels an?
5. Wie wird bei der Übertragung die maximale Größe eines Rahmens (Frames) definiert?
6. Welche Adressierung gibt es bei Ethernet und wie viele Bytes beansprucht eine Adresse?

11

Protokolle

11.1 Der Begriff Protokolle

Der Begriff **Protokolle** taucht im Umgang mit Computernetzen immer wieder auf, wird dabei aber sehr uneinheitlich benutzt. Allgemein betrachtet bezeichnen Protokolle Kommunikationsregeln zwischen Systemen und die darauf zugreifenden Prozesse. Dementsprechend lassen sich die Protokolle auch konkret den einzelnen Schichten des OSI-Modells zuordnen.

Protokoll-Stack

Da sich ein einzelnes Protokoll immer nur um eine Teilaufgabe im Rahmen der Kommunikation kümmert, werden mehrere Protokolle zu Protokollfamilien, den sogenannten **Protokoll-Stacks**, zusammengefasst. Die wichtigsten Einzel-Protokolle werden dann oft stellvertretend als Bezeichnung des gesamten Protokoll-Stapels genutzt.

Kommunikation zwischen Netzwerkkomponenten funktioniert nur dann, wenn sie denselben Protokoll-Stack benutzen oder wenn Geräte eingesetzt werden, die zwischen verschiedenen Stacks vermitteln können. Hierzu dienen **Gateways**. Spätestens bei der Installation eines Netzwerks bzw. bei der Konfiguration einer **Netzwerkarte** müssen Netzwerkprotokolle angegeben und ggf. konfiguriert werden.

Dabei ist zu unterscheiden zwischen Netzwerk- bzw. **Übertragungsprotokollen** (wie Ethernet-Protokoll, PPP, IP, TCP, UDP etc.), die als Träger für weitere Protokolle dienen (**vgl. Ende dieses Kapitels**), und **Anwendungs-Protokollen** (wie FTP, HTTP, SMTP etc.). Für Switches und Router sind in der Regel nur die Übertragungsprotokolle, nämlich für die Wegfindung, interessant. Die enthaltenen Anwendungs-Protokolle werten sie nicht aus (außer Layer-7-Switches bzw. Gateways).

Die folgenden Abschnitte geben einen Überblick über die gängigsten Protokoll-Stacks und schildern die jeweiligen Vor- und Nachteile.

Routing-Fähigkeit

Ein sehr wichtiges Kriterium für die Auswahl eines Protokoll-Stacks ist dessen Routing-Fähigkeit. Routing bezeichnet eine Vermittlungsfunktion, die notwendig wird, wenn Daten von einem Netzwerknoten oder einem LAN zu einem fremden LAN oder ins WAN übertragen werden müssen und dabei ggf. mehrere Übertragungswege zur Verfügung stehen.

Routingfähige Protokolle liefern dazu Informationen, die es einem Router ermöglichen, eine Entscheidung über den passenden Weg (Route) zu diesem Ziel zu treffen. Alle gängigen Protokoll-Stacks sind auf dem Layer 3 routingfähig.

11.2 TCP/IP

Die wichtigsten Protokolle: TCP/IP

Transmission Control Protocol/Internet Protocol ist der Standard des Internets. Der Begriff **TCP/IP** steht dabei nicht für ein einzelnes Protokoll, sondern für eine Vielzahl von Netzwerk-Protokollen, welche die Grundlage des Internets darstellen und dieses standardisieren.

Die Entwicklung von TCP/IP ist dabei eng verbunden mit der Entwicklung von UNIX und der Entwicklung des Internets. Die Normung der einzelnen Protokolle lag beim Internet Architecture Board (**IAB**) und hier vor allem bei der Abteilung Internet Engineering Task Force (**IETF**). Die Veröffentlichung der genormten Definitionen erfolgt dann in Form von durchnummerierten Request for Comment (**RFCs**).

Hinter TCP/IP steht kein einzelner Hersteller, sondern weltweit anerkannte Gremien. Heute wird TCP/IP von jeder Rechnerplattform (auch Smartphones, Tablets etc.) unterstützt und ist damit geeignet, auch heterogene Systeme zu vernetzen. Aufgrund seiner enormen Bedeutung wird TCP/IP hier ausführlicher behandelt als alle anderen Protokoll-Stacks.

Geschichte

Seinen Ursprung hat TCP/IP als Entwicklung für das Advanced Research Projects Agency Network (ARPANet), den Vorgänger des heutigen Internets. TCP/IP entstand zur Zeit des Kalten Krieges. Ziel der Entwicklung war es, eine Netzarchitektur zu entwickeln, die auch dann noch funktioniert, wenn große Teile des bestehenden Netzes zerstört werden. Finanziert wurde das Projekt durch das US-amerikanische Department of Defense (**DoD**).

Wichtig in diesem Zusammenhang ist das Thema Routing. Anhand der Informationen im IP-Header kann ein Router entscheiden, auf welchem Weg das Paket weitergeleitet werden soll. Fällt dieser Weg aus, erfährt der Router dies und wählt einen anderen Weg.

Einordnung

TCP/IP geht von einem vierstufigen Architekturmodell aus und lässt sich folgendermaßen in Einklang mit dem OSI-Referenz-Modell bringen:

TCP/IP-Schicht	TCP/IP	OSI	OSI-Schicht
4	Anwendungs-Schicht	Application Layer	7
		Presentation Layer	6
		Session Layer	5
3	Transport-Schicht (TCP)	Transport Layer	4
2	Internet-Schicht (IP)	Network Layer	3
1	Netzwerk- und Link-Schicht	Data Link Layer	2
		Physical Layer	1

Wichtige Protokolle

Neben den beiden Protokollen TCP und IP, die der Protokollfamilie den Namen geben, gibt es noch eine Vielzahl weiterer Protokolle. Der Ausdruck „IP“ steht hier stellvertretend für die beiden Versionen IPv4 und IPv6 des Internetprotokolls. Die folgende Tabelle listet einige dieser Protokolle auf und ordnet sie dem OSI-Modell zu.

Protokoll	OSI-Schicht	Name	Beschreibung
FTP	7	File Transfer Protocol	Dateitransfer Protokoll
SMTP	7	Simple Mail Transfer Protocol	Versenden von E-Mails
HTTP	7	Hypertext Transfer Protocol	Übertragen von HTML-Seiten (Hypertext Markup Language)
HTTPS	7	HTTP over TLS/SSL	Sicheres HTTP-Protokoll für verschlüsselte Verbindungen
RPC	5	Remote Procedure Call	Dient zur Interprozess-Kommunikation
TCP	4	Transmission Control Protocol	Aufbau logischer Verbindungen zwischen Applikationen; verbindungsorientiertes Übertragungsprotokoll zur gesicherten Datenübertragung
UDP	4	User Datagram Protocol	Verbindungsloses Übertragungsprotokoll, welches schnellere Übertragungen als mit TCP ermöglicht, die aber ungesichert sind (z. B. bei Video-Streaming)
IP	3	Internet Protocol	Verbindungsloses Protokoll (in Version IPv4 und IPv6) zur Paketlenkung und Paketvermittlung über IP-Adressen

Zu beachten ist, dass z. B. hinter einem Begriff wie „FTP“ sowohl ein Protokoll als auch ein Dienst bzw. eine Anwendung (FTP-Server oder FTP-Client) stehen kann.

Portnummer

Da unterschiedliche Protokolle, wie z. B. FTP, HTTP oder HTTPS, bei einem Rechner über dieselbe IP-Adresse angesprochen werden können, muss über eine zusätzliche Kennung deutlich gemacht werden, welcher dieser Dienste konkret gewünscht wird. Dies geschieht über sogenannte **Portnummern**, die im TCP- oder UDP-Header eingetragen sind.

Ein Webserver beispielsweise könnte auch eine andere Nummer als den üblichen Port 80 verwenden, jedoch müsste dies beim Aufruf der Webseite im Browser explizit angegeben werden (*IP-Adr.:Port*). Ist ein Dienst (Server-Anwendung) an einen Port gebunden, kann das Betriebssystem keinen weiteren Dienst über die gleiche Portnummer bereitstellen. Umgangssprachlich „lauscht der Server bereits auf diesem Port“.

Verschiedene Dienste könnten sich daher in die Quere kommen. Einzige Ausnahme sind Dienste, die verschiedene Schicht 3 Protokolle wie (TCP/UDP) verwenden. Somit wäre es möglich, Dienst A per TCP an eine bestimmte Portnummer zu binden und für Dienst B per UDP die gleiche Nummer zu verwenden. Tatsächlich verfügen TCP sowie UDP über zwei getrennte Sätze von Portnummern, wodurch diese hypothetische Konfiguration nur wie eine Doppelbelegung aussieht.

In der Praxis sind die Portnummern der wichtigsten Dienste (Server-Anwendungen) weltweit genormt. Die Tabelle zeigt auszugsweise einige Nummern von Diensten.

Port-Nummer	Bedeutung
20	FTP-Daten
21	FTP-Befehle
25	SMTP
80	HTTP
110	POP3
443	HTTPS

Eine vollständige Liste aller Portnummern kann auf der Website der IANA (<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>) abgerufen werden.

Während die IP-Adresse also eindeutig einen Rechner identifiziert, kennzeichnet die Portnummer den Dienst, der auf dem Rechner angesprochen wird. Beide Informationen zusammen werden auch als **Socket** bezeichnet.

Allgemein lassen sich die Portnummern in verschiedene Bereiche einteilen, wie die nebenstehende Tabelle zeigt. Hersteller von Applikationen können Portnummern bei der IANA registrieren lassen, was zur Konsequenz hat, dass Anwendungen anhand ihrer dann weltweit bekannten Portnummer identifiziert werden können.

Bereich	Beschreibung
0 bis 1023	Well Known Ports
1024 bis 49151	Registered Ports
49152 bis 65535	Dynamic/Private

11.3 IP-Adressierung

IPv4-Adresse und MAC-Adresse

IP-Adressen in der Version IPv4 sind **32 Bit** lange Binärzahlen (4 Byte), die zur besseren Lesbarkeit im sogenannten **Dotted-Decimal-Format** (oder Dotted-Quad-Notation) angegeben werden: Jedes der vier Bytes wird als Dezimalzahl mit Werten von 0 bis 255 angegeben, jeweils durch einen Punkt getrennt (Oktette = Bytes), wie z. B. 193.96.1.200. Die Punkte haben also nichts zu tun mit dem üblichen Tausendertrennzeichen.

Bei Verwendung von TCP/IP muss jeder Netzwerk-Schnittstelle innerhalb eines Netzwerkverbunds eine eindeutige IP-Adresse zugewiesen werden. Dadurch wird der physikalischen 48-Bit langen Hardware-Adresse (**MAC-Adresse**) eine logische IP-Adresse zugeordnet.

Um ansprechbar zu sein, besitzt jede einzelne Netzwerk-Schnittstelle auf einer Netzwerkkarte oder auf einem Mainboard (auch bei WLAN) eine eingebrannte weltweit eindeutige MAC-Adresse. Bei dualband-fähigen WLAN-Geräten haben die Schnittstellen für das 2,4 GHz- und für das 5 GHz-Band jeweils eine eigene MAC-Adresse.

! Eine **MAC-Adresse** (unter Windows „**Physische Adresse**“ genannt) kann per Software verändert werden. Allerdings ist davon dringend abzuraten, da dies gravierende Auswirkungen auf das korrekte Zusammenspiel aller Netzwerkkomponenten haben kann!

Die weltweit eindeutigen Adressen werden in hexadezimaler Form angegeben und haben einen einheitlichen Aufbau. Die ersten drei Bytes kennzeichnen den Hersteller (Vendor) und die zweiten drei Bytes sind die fortlaufende Nummer der Netzwerkkarte. Die folgende Tabelle zeigt zwei Beispiele zu Produkten der Firmen ASUS und Intel. Ein Hersteller kann auch mehrere Vendor-codes besitzen.

Die Kennziffern des Herstelleranteils werden von der IEEE zentral vergeben. Die Kennung der einzelnen Karten wird dann von den Herstellern selbst vorgenommen.

Hersteller			Fortlaufende Nummer		
10	BF	48	E2	B1	B7
00	27	10	15	40	5E

Für die erwartete hohe Anzahl von Geräten beim Internet der Dinge (IoT) wird die Länge von 48 Bit für die MAC-Adresse auf Dauer nicht reichen. Nach RFC 4291 soll in Zukunft für IPv6 die Länge auf 64 Bit erweitert werden.

Vergleich IP-Adresse – Telefonnummer

Netze setzen sich meistens aus mehreren Segmenten (Teilabschnitten) zusammen. Eine Telefonnummer besteht beispielsweise aus einer Vorwahl und einer Teilnehmernummer. Eine **IP-Adresse** ist ähnlich aufgebaut und besteht aus den folgenden zwei Teilen, wobei die Abkürzung ID für Identifikation steht:

- ✓ Die **Netzwerk-ID** (bzw. Netz-ID) im vorderen linken Teil entspricht der Vorwahl und kennzeichnet das entsprechende Netzwerk.
- ✓ Die **Host-ID** im hinteren rechten Teil kennzeichnet eine einzelne Netzwerk-Schnittstelle und entspricht der Teilnehmernummer im Ortsnetz. Bei einer **Netzwerk-Adresse** enthält sie nur Nullen.

Entsprechend können Rechner im selben Netzwerk direkt miteinander kommunizieren. Dagegen erfordert Kommunikation zwischen Netzwerken einen Vermittler (Router oder Gateways). Auf den Rechnern ist dafür die Adresse des Vermittlers als Standardgateway (auch Default-Route) angegeben. Um zu erkennen, wo die Netzwerk-ID endet und die Host-ID beginnt, muss bei der Bezeichnung von Netzwerken zusätzlich zur IP-Adresse zwingend eine sogenannte **Subnetzmaske** (auch Netzmaske) angegeben werden. Diese legt die Größe eines Netzwerk-Segments fest.

Subnetzmaske

Die Subnetzmaske ist ein Bitmuster, das (von links nach rechts) Teile der IP-Adresse maskiert, um den Übergang zwischen Netz-ID und Host-ID zu kennzeichnen. Binär betrachtet besteht eine Netzmaske aus einer Folge von Einsen, die ab einer bestimmten Stelle zu einer Folge von Nullen wechselt. Dieser Wechsel gibt an, wie viele Bits zur Netzwerk-ID (Einsen) und zur Host-ID (Nullen) gehören. Die Schreibweise erfolgt dabei ebenfalls im Dotted-Decimal-Format. Hier ein Beispiel für IP-Adresse 192.168.10.1 und der Subnetzmaske 255.255.255.0:

	Netz-ID (24 Bits)			Host-ID (8 Bits)
IP-Adresse (dezimal)	192	168	10	1
Binär	1100 000	1010 1000	0000 1010	0000 0001
Netzmaske (dezimal)	255	255	255	0
Binär	1111 1111	1111 1111	1111 1111	0000 0000

Die Maskierung ergibt, dass sich der Computer mit der IP-Adresse 192.168.10.1 im Netzwerk (Net-ID) 192.168.10 befindet und die Nummer (Host-ID) 1 besitzt.

Netzmasken werden oft auf der Basis von ganzen Oktetten gesetzt, was die folgenden Beispiele zeigen:

	Beispiel 1	Beispiel 2	Beispiel 3
IP-Adresse	120.96.1.200	172.96.1.200	193.96.1.200
Netzmaske	255.0.0.0	255.255.0.0	255.255.255.0
Netz-ID	120	172.96	193.96.1
Host-ID	96.1.200	1.200	200

- ✓ Eine **Netzwerk-Adresse** stellt die erste Adresse in einem Netzwerk-Segment dar. Die Host-ID besteht dabei nur aus Nullen. Die letzte Adresse ist die **Broadcast-Adresse**, deren Host-ID nur Einsen enthält.
- ✓ Ein **Netzwerk** wird durch die Netzwerk-Adresse **zusammen** mit der **Netzmaske** definiert. In einem IPv4-Netzwerk kennzeichnet die Netzwerk-Adresse die erste IP-Adresse, die Netzmaske legt dessen Größe fest.
- ✓ Im Grunde ist auf IP-Ebene jedes andere Netzwerk ein Subnetz (Erläuterungen siehe unten) des Internets.

IP-Adressklassen

Früher wurden zu vergebende IP-Adressen in verschiedene Adressklassen aufgeteilt. Für die Adressierung von Rechnern waren die Klassen A, B und C vorgesehen. Heute ist die klassenbasierte Vergabe vom **Classless Inter-Domain Routing (CIDR)** abgelöst. Die nachfolgende Tabelle zeigt die Aufteilung:

Class	Netzwerk-ID	Netzmaske	Anzahl Netzwerke	Anzahl Netzwerknoten
A	1 bis 126	255.0.0.0	126	16.777.214 ($2^{24}-2$)
B	128.0 bis 191.255	255.255.0.0	16.384	65.534 ($2^{16}-2$)
C	192.0.0 bis 223.255.255	255.255.255.0	2.097.152	254 (2^8-2)
D	224 bis 239	240.0.0.0	-	nur für Multicast-Anwendungen
E	240 bis 254	240.0.0.0	-	reserviert, experimentell

Einige Adressbereiche dürfen nicht vergeben werden:

- ✓ die mit **0** beginnen (wegen der Default-Route)
- ✓ die mit **127** beginnen (sie sind reserviert für interne Funktionen, wie z. B. die **Loopback**-Adresse 127.0.0.1, die auf jedem Rechner konfiguriert ist und die die eigene Adresse für das virtuelle Netzwerkinterface des IP-Stacks darstellt)
- ✓ die mit **255** beginnen (für Broadcasts).

Jedes IPv4-Netzwerk verwendet die erste Adresse (0) für die Adressierung des Netzwerks (Netzwerk-Adresse) und die letzte Adresse (255) als **Broadcast-Adresse**. Ein Class-C-Netz kann daher keine 256 Hosts beinhalten.

Subnetze (Subnetting)

Die Netzmaske kann zur Aufteilung bestehender Netzwerke in Subnetze benutzt werden (auch **Subnetting** genannt). Das größte Netz ist das Internet selbst, welches über Netzmasken in viele weitere Netzwerke aufgeteilt wird. Das **gesamte Internet** hat die Netzwerk-Adresse **0.0.0.0** und die Netzmaske **0.0.0.0**. Diese Angaben sind Teil der **Default-Route** (vgl. Kapitel 13), die in der Regel den Weg zu demjenigen Router zeigt, der die Verbindung eines Netzwerks (oder Subnetzes) zu allen vorkommenden IP-Adressen (also dem Internet) ermöglicht.

Soll etwa das bestehende Netz mit der Netzwerk-Adresse **172.96.0.0** in 4 Teilnetze segmentiert werden, so kann die Netzmaske um 2 Bits erweitert werden (in der Tabelle unten in eigener Spalte dargestellt). Diese zwei Bits gehen dann für die Adressierung von Host-IDs verloren. Das Resultat wären vier Netzwerk-IDs, bestehend aus je 18 Bits mit der zugehörigen Netzmaske **255.255.192.0**. Die folgende Tabelle gibt die möglichen IP-Adressen für die einzelnen Subnetze an und zeigt den binären Aufbau (Subnetze in CIDR-Notation, siehe weiter unten):

172.96er-Netz	Netz-ID (18 Bits)			Host-ID (14 Bits)
Netzmaske (binär)	1111 1111	1111 1111	11	00 0000 0000 0000
1. Subnetz (172.96.0.0/18) (172.96.0.1–172.96.63.254)	1010 1100	0110 0000	00	00 0000 0000 0001– 11 1111 1111 1110
2. Subnetz (172.96.64.0/18) (172.96.64.1–172.96.127.254)	1010 1100	0110 0000	01	00 0000 0000 0001– 11 1111 1111 1110
3. Subnetz (172.96.128.0/18) (172.96.128.1–172.96.191.254)	1010 1100	0110 0000	10	00 0000 0000 0001– 11 1111 1111 1110
4. Subnetz (172.96.192.0/18) (172.96.192.1–172.96.255.254)	1010 1100	0110 0000	11	00 0000 0000 0001– 11 1111 1111 1110

CIDR

Der rasante Zuwachs an Internetknoten und die Praxis, ganze IP-Adressklassen zu vergeben, führte schnell zu der Einsicht, dass die IPv4-Adressen schnell zu Ende gehen werden. Eine Abschwächung des Problems wurde mit der RFC 1519 und der Abkürzung **CIDR** (Aussprache: caidar) für **Classless Inter-Domain Routing** angeboten.

Der Grundgedanke war, dass durch die Vergabe von ganzen Adressblöcken in Form von Class A, B oder C etliche Einzeladressen nicht genutzt und dadurch verschwendet werden. So erwarben viele Firmen ein oft viel zu großes Class-B-Netz, da ein Class-C-Netz mit 254 adressierbaren Hosts zu klein gewesen wäre.

Der Lösungsansatz von CIDR ist, die verfügbaren Adressen in Blöcken variabler Größe anzubieten. Benötigt eine Firma z. B. 2000 Adressen, dann wird nicht mehr ein Class-B-Bereich mit ca. 65.000 Adressen vergeben, sondern ein Adressbereich zur Verfügung gestellt, der acht aufeinanderfolgenden Class-C-Bereichen entspricht (also 2.048 Adressen). Dennoch gingen bereits 2015 die neu zu vergebenden IPv4-Adressen aus.

Bei der **CIDR-Schreibweise** (CIDR-Notation) steht die Netzmaske nicht einzeln, wie 255.255.255.0, sondern durch einen Schrägstrich getrennt als Anzahl von Einsen hinter der Netzwerk-Adresse. In diesem Beispiel sind **24** Einsen in der Netzmaske, die somit das Netzwerk **220.78.168.0/24** darstellen.

Das Zusammenschließen von Netzen wird durch **Supernetting** (umgekehrtes Subnetting) möglich. Dazu wird nicht, wie im Beispiel oben, die 24-Bit-Netzmaske 255.255.255.0 gesetzt. Mit z. B. drei Bits weniger ergibt sich die Netzmaske 255.255.248.0. Ein solches Netzwerk hätte die achtfache Größe vom vorherigen und damit die Bezeichnung **220.78.168.0/21**. Dieses umfasst die Adressen von 220.78.168.0 bis 220.78.175.255.

In diesem Netzwerk ist dann z. B. die IP-Adresse 220.78.169.0 **keine** Netzwerk-Adresse mehr. Sie kann somit die Adresse von einem Rechner sein!

IPv6

Obwohl die Vergabe der Adressen inzwischen restriktiver gehandhabt wurde als in den Anfangszeiten des Internet, war bei den Zuwachsraten an Internetknoten absehbar, dass bald keine freien IPv4-Adressen mehr verfügbar sein werden. Bereits Anfang der 90er-Jahre initiierte deshalb die IETF ein Projekt zu dieser Thematik und forderte im Dezember 1993 mit RFC 1550 unter dem Kürzel **IP next generation (IPnG)** alle Beteiligten auf, Vorschläge für die Umstrukturierung der Adressen und notwendige Änderungen am Protokoll IP zu machen.

Im Dezember 1995 folgte mit RFC 1883 (Kürzel **IPv6**) die Veröffentlichung eines Diskussionspapiers, das seither noch mehrfach überarbeitet wurde. Die gravierendste Änderung betrifft die Erweiterung der Adressgröße von 32 auf **128 Bit**, sodass jeder denkbare Host eine offizielle IP-Adresse erhalten kann. IPv6 ist nicht kompatibel zur Version des IPv4-Protokolls auf der gleichen Schicht, aber konform zum darüberliegenden **Transport Layer**. IPv4 und IPv6 (Dual Stack) können gleichzeitig auf einem System genutzt werden. Das Internet ist bereits in weiten Teilen auf die zusätzliche Unterstützung von IPv6 neben dem weiter bestehenden IPv4 umgestellt. Die **Internet Service Provider (ISP)** sind ebenfalls in der Umstellungsphase oder haben diese abgeschlossen.

Vorteile von IPv6

- ✓ Stark erweiterter Adressraum (10^{12} Hosts und 10^9 Netzwerke)
- ✓ Vereinfachte Header für IPv6, jedes Protokoll (ICMP, TCP, UDP usw.) erhält ein eigenes Format.
- ✓ Das Routing zwischen IPv6-Netzen ist effizienter als bei IPv4-Netzen.
- ✓ Verbesserung des Managements durch das Protokoll ICMPv6
- ✓ Ein spezieller Multicast ersetzt den bisherigen Broadcast der IPv4 Netze.
- ✓ Sicherheit: Mechanismen zur Authentizität (Authentication Header(AH)) und Verschlüsselung (Internet Protocol Security (IPsec)) sind integriert.
- ✓ Multicast: echtes Video- und Audiostreaming
- ✓ **Quality of Services (QoS):** verbesserte Dienstgüte gegenüber IPv4
- ✓ Mobilität: Der User ist weltweit über seine IPv6-Adresse erreichbar.

Adressaufbau von IPv6

IPv6-Adressen werden nicht in dezimaler Schreibweise notiert wie IPv4-Adressen, sondern mit Hilfe von Hexadezimalzahlen. Dabei wird eine komplette Adresse von 128 Bit Länge in acht Blöcke aufgeteilt. Die Trennung der Blöcke erfolgt nicht über einen Punkt, sondern über einen Doppelpunkt. Sofern sich in mehreren aufeinanderfolgenden Blöcken nur Nullen befinden, kann die Darstellung dieser Blöcke **einmalig** durch die Zeichenfolge :: verkürzt werden. Bei nur einem Block muss „0000“, „00“ oder auch nur „0“ geschrieben werden.

Beispiele: 2001:0:0:fe72::1234

::1 Adresse des eigenen Rechners bzw. Gerätes (localhost bzw. Loopback)

Bei der Angabe einer Portnummer wird die gesamte IPv6-Adresse in eckige Klammern gesetzt und die Portnummer, durch einen Doppelpunkt getrennt, hinzugefügt.

Beispiele: [2001:ab13:4412:0000:ca11:4545:0000:1234]:80
[http://\[2001:2498:7654::654:3210\]](http://[2001:2498:7654::654:3210])

Je nach Netzwerk und Provider (Provider Aggregated) bilden die ersten 48 Bit (für bis zu 65535 öffentliche Subnetze), 56 oder 64 Bit die Netzwerk-ID bzw. den **Präfix**. Die letzten 64 Bit sind die **Host-ID**. Ähnlich den Netzmasken bei IPv4 wird die entsprechende Anzahl der Bits, die die Netzwerk-ID bilden, als Zahl hinter einem Schrägstrich ans Ende der IPv6-Adresse angefügt.

Beispiel für ein IPv6-Netzwerk: 2001:ab13:4412:0000:ca11:4545:0000:1234/48

Eine besondere Rolle spielen die ersten 16 Bits einer IPv6-Adresse, da hier einige Kennziffern bereits genormt wurden, so z. B. die hexadezimale Angabe 2001 für europäische Provider oder fe80 als sogenannte Local Link Unicast (oft auch Link-Local-Unicast). Jedes IPv6-Interface erhält eine solche linklokale Adresse, die nur im lokalen Netzwerk gültig ist.

Der Eintrag für eine **Default-Route** zeigt auch unter IPv6 auf das gesamte Internet, also auf das Netzwerk ::/0.

Weitere Informationen zu IPv6 finden Sie im HERDT-Buch *Netzwerke – IPv6*.

11.4 Umsetzung der IPv4-Addressierung in der Praxis

Offizielle IP-Adressen

Internetanschlüsse werden durch ihre IP-Adresse weltweit eindeutig identifiziert. Die Eindeutigkeit wird durch zentrale Vergabestellen gesichert, bei denen IP-Adressen beantragt werden müssen. Die oberste Vergabestelle ist die **Internet Assigned Numbers Authority (IANA)**, dahinter folgen fünf regionale Registrare (**Regional Internet Registry(RIR)**). Für Europa ist dies das **Réseaux IP Européens Network Coordination Centre (RIPE NCC)**. Den regionalen Registraren wiederum folgen die **Local Internet Registries (LIRs)**, die letztendlich die IP-Adressen für Endkunden bereitstellen. LIRs sind meist ISPs oder auch Unternehmen sowie akademische Institutionen.

Diese Stellen vergeben jedoch keine einzelnen Adressen, sondern verwalten ganze Adressgruppen (Blöcke), die dann von anderen Providern an ihre Kunden weitergegeben werden. Die Endkunden können je nach Anzahl der Rechner in ihrem Netz eine gewisse Anzahl von IP-Adressen beantragen. Heute erfolgt die Vergabe von Adress-Gruppen grundsätzlich anhand von **CIDR**.

Für die Vergabe von Adressbereichen wurde die Welt von der IANA in Zonen unterteilt. Eine geografische Zuordnung von Internetadressen ist über Tabellen möglich, die von den Registraren bzw. Providern geführt werden.

Den ungefähren geografischen Ort einer vergebenen IP-Adresse zeigen auch Formulare in Webseiten wie <http://www.utrace.de> oder <http://www.ip-adresse-ermitteln.de>.

Angaben über den Besitzer einer IP-Adresse oder einer Internetdomain in Deutschland können über die Webseite der Denic ermittelt werden (<https://www.denic.de/service/whois-service/>). Der Dienst **whois** ist auch direkt benutzbar, wenn er auf einem Rechner installiert ist. Es ist dabei die Domain allein (ohne „www“) einzugeben.

Private IP-Netze

Für die Erstellung privater IP-Netze, und das betrifft auch viele kleine LANs, wurde aus den drei benannten Netzklassen je ein Bereich ausgeschlossen. Die Adressen dieser drei Bereiche werden niemals als öffentliche Internetadressen vergeben und von Routern im Internet generell nicht weitergeleitet. Jeder darf sie in seinem eigenen Netz verwenden. Sie sind in der RFC 1918 (Address Allocation for Private Internet) hinterlegt. Dadurch sind diese Adressen prädestiniert für den Einsatz in privaten Netzwerken.

Es handelt sich um die Bereiche:

- ✓ 10.0.0.0 bis 10.255.255.255 entspricht ca. 16,8 Millionen Hosts (1 Class A Netz)
- ✓ 172.16.0.0 bis 172.31.255.255 entspricht ca. 1 Millionen Hosts (16 Class B Netze)
- ✓ 192.168.0.0 bis 192.168.255.255 entspricht ca. 65 500 Hosts (255 Class C Netze)

Soll ein LAN allerdings an ein WAN angeschlossen werden und damit z. B. über das Internet ansprechbar sein, muss sichergestellt sein, dass diese Systeme eine weltweit eindeutige offizielle IP-Adresse besitzen. Dies kann durch die Nutzung einer eigenen offiziellen Adresse oder für Rechner in internen Netzen über **Network Address Translation (NAT)/Port and Address Translation (PAT)** erfolgen.

Für die vollautomatische IP-Konfiguration in kleinen Netzen ohne DHCP-Server hat Microsoft ein Verfahren namens **Automatic Private IP Addressing (APIPA)** () entwickelt, das Adressen im Bereich 169.254.0.1 bis 169.254.255.254 mit der Netzmaske 255.255.0.0 verwendet. Auch diese Adressen können nicht für Verbindungen zum Internet benutzt werden.

Address Resolution Protocol (ARP)

Wenn ein vernetztes Gerät mit einem anderen vernetzten Gerät eine Verbindung aufnehmen will, muss es erst die **MAC-Adresse** bzw. **Ethernet-Adresse** der Netzwerk-Schnittstelle des Gerätes ermitteln, zu dem ein Frame (Paket) verschickt werden soll. Allerdings ist dies nur innerhalb des **gleichen** Netzwerk-Segmentes möglich. Bei Verbindungen zu anderen Netzwerken müssen daher die Frames an die MAC-Adresse der passenden Netzwerk-Schnittstelle des Routers zur Weiterleitung verschickt werden.

Für IPv6 findet nicht ARP, sondern **Neighbor Discovery Protocol (NDP)** Verwendung.

Internet Control Message Protocol (ICMP)

Die Aufgabe vom Protokoll **ICMP** ist auf OSI-Layer 3 der Transport von Diagnose- und Fehlermeldungen, die in einem Netzwerk anfallen können. Wenn z. B. eine IP-Adresse nicht erreichbar ist, erhält der Absender darüber eine entsprechende Fehlermeldung. Unter IPv6 ist das Protokoll **ICMPv6** hierfür zuständig.

Domain Name Service (DNS)

Der **Domain Name Service (DNS)** erlaubt es, statt der unhandlichen numerischen IP-Adressen einen Computer mit einem Namen anzusprechen. Hier wird einer IP-Adresse ein DNS-Name zugeordnet. Die Auflösung der Namen erfolgt über einen DNS-Server Dienst, der auch zusätzlich zu anderen Funktionen auf einem Server im Netzwerk installiert werden kann. Ein Beispiel für die Zuordnung wäre der DNS-Name *www.herdt.com*, für den die IP-Adresse 195.243.78.74 ermittelt wird.

Diese Namen werden von rechts nach links aufgelöst. Sie beginnen (rechts) mit einer sogenannten Top Level Domain, hier *.com* für eine kommerzielle Organisation. Auch sind zweistellige Kürzel für Länder, z. B. *de* für Deutschland oder *at* für Österreich gebräuchlich. Es folgen, je durch einen Punkt getrennt, ein Domain-Name und möglicherweise Subdomain-Namen. Der letzte Eintrag (links) entspricht einem Host-Namen. Einem Host können auch mehrere Namen zugeordnet werden. Der allgemeine Aufbau ist:

rechner-name.[subdomain.]domain.top-level-domain

Domain-Namen müssen ebenso wie IP-Adressen eindeutig sein, beantragt und genehmigt werden. Für die **Top-Level-Domain (TLD)** *de* ist das **Deutsche Network Information Center (Denic)**, <https://www.denic.de/> zuständig. Für den privaten Gebrauch im internen LAN ist eine Registrierung nicht erforderlich.

Verwendung finden solche Namen auch als Bestandteil einer **Uniform Resource Locator (URL)** z. B. für die Webseite <https://cms.hertd.com/de/>

Dynamic Host Configuration Protocol (DHCP)

In größeren Netzwerken wird eine manuelle IP-Konfiguration der Clients sehr aufwendig. Neben den IP-Adressen sind weitere Informationen, wie Standardgateway, DNS-Server usw. anzugeben. Weiter muss protokolliert werden, welche IP-Adressen bereits vergeben sind. Solche Tätigkeiten sind sehr fehleranfällig. Spätestens, wenn das Netz in verschiedene Subnetze aufgeteilt ist und sich beispielsweise ein Notebook-Benutzer an verschiedenen Stellen mit dem Netzwerk verbindet, ist dies nicht mehr praktikabel. Netzwerk-Schnittstellen konfigurieren sich daher, falls sie nicht auf manuelle Konfiguration umgestellt werden, generell automatisch. Hierzu dient DHCP.

Ein **DHCP-Server** ist bereits häufig im DSL-Router enthalten oder kann als Server-Dienst nachinstalliert werden. Über ihn werden sogenannte IP-Bereiche (zu vergebende IP-Adressen) definiert und mit weiteren Konfigurationseinstellungen, wie z. B. Standardgateway (Router) oder DNS-Server verschickt. Beim Starten fragt ein Client beim DHCP-Server nach einer IP-Konfiguration, die er dann für eine bestimmte Zeit (Lease-Dauer) nutzen kann. Beim Herunterfahren meldet sich der Client beim DHCP-Server ab, woraufhin dieser die IP-Adresse, bei entsprechender Konfiguration, an einen anderen Client vergeben kann.

Unter IPv6 ermitteln normalerweise die Netzwerk-Schnittstellen automatisch deren IPv6-Adressen per Autokonfiguration. Ein DHCP-Server (DHCPv6) stellt weitere Einträge zur Verfügung, wie die Adressen von DNS-Servern und mitunter zusätzliche Konfigurationsinformationen.

Verbindung zum Internet per Proxy-Server

Ein **Proxy-Server** (Proxy = Stellvertreter) bedient nur bestimmte Protokolle, typischer Weise HTTP, HTTPS und FTP. Im Grunde könnte man auch DNS- oder einen Zeit-Server (**Network Time Protocol (NTP)**) als eine Art Proxy bezeichnen, da sie einem im Internet stehenden Rechner die internen Anfragen weiterleiten, ohne dass eine direkte Verbindung zwischen dem Rechner im LAN und dem WAN vorhanden sein muss. Diese Art der Anbindung, die das Gegenteil zu Routern oder NAT (siehe weiter unten) bildet, wird mitunter zur Erhöhung der Sicherheit im internen Netzwerk vorgenommen. Man spricht dabei auch von einer Application Level Firewall (vgl. Kapitel 13).

Ein Proxy kann grundsätzlich auf jedem geeigneten Rechner im internen oder externen Netzwerk (oft beim Provider) installiert werden. Soll er die Verbindung zum Internet bereitstellen, muss er auf dem Rechner laufen, der über eine Internetverbindung verfügt. Ein Router ist dann nicht erforderlich. In den Webbrowsers auf den Client-Rechnern müssen die IP-Adresse und der Port vom Proxy eingetragen werden. Ein HTTP-Proxy kann für Clients auch **transparent** eingerichtet sein – dann sind diese Einstellungen nicht nötig.

Viele angeforderten Daten speichert ein Proxy in einem **Cache**, damit die erneute Belieferung eines Clients schneller geht und die Belastung der Leitung zum Internet sinkt. Zeitlich abgelaufene (expired) Webseiten und per HTTPS verschlüsselte Seiten sind nicht darunter.

Zudem ist über einen Proxy-Server die **Kontrolle** des Internetverkehrs möglich, beispielsweise durch die Vergabe von Benutzernamen und Passwörtern. Es können Zugriffsbeschränkungen verhängt werden, z. B. durch das Sperren bestimmter Websites (Nutzung von Webmail-Accounts während der Arbeitszeit etc.). Dies wird vor allem auch bei Internetzugängen über öffentliche WLAN-Access-Points (Hotspots) praktiziert.

Ein bekannter Proxy im Windows-Umfeld war das **Threat Management Gateway** (früher ISA Server), welches aus dem Microsoft Vertriebsprogramm genommen wurde. Daher muss unter Windows auf eine Drittherstellerlösung ausgewichen werden. Diese sind unterschiedlich stark und in unterschiedlichen Preislagen verfügbar. Im Linux- bzw. UNIX-Umfeld wird meist **Squid** verwendet.

Die Adress-Umsetzung mit NAT/PAT ermöglicht im Gegensatz dazu eine direkte Verbindung zum Internet für **alle** IP-Pakete (die Änderungen im Header zulassen) und damit auch für alle übergeordneten Protokolle. Dann kann z. B. ein Ping (über das Protokoll ICMP) zu einem Rechner im Internet von jedem Rechner im internen Netz aus abgesetzt werden, trotz privater IP-Adressen.

Direkte Verbindung zum Internet per NAT/PAT

In der Regel sind in einem internen Netzwerk private IP-Adressen vergeben. Da diese im Internet nicht weitergeleitet werden (wohin auch, da sie beliebig oft vorkommen können), ist für eine direkte Verbindung ins Internet das Abbilden von privaten IP-Adressen auf offizielle IP-Adressen erforderlich.

Hierzu wird in IPv4-Netzen **Network Address Translation (NAT)** meist zusammen mit **Port and Address Translation (PAT)** verwendet, welches in der Regel auf dem Rechner bzw. dem Router zum Internet aktivierbar ist. Ein Zugriff vom Internet her auf das interne Netzwerk ist dann nicht möglich. Mit IPv6 ist zwar NAT nicht mehr erforderlich, wird aber nach RFC 4864 (Local Network Protection for IPv6) in einigen Fällen dennoch empfohlen, beispielsweise um die interne Netzwerkstruktur zu verbergen (vgl. Privacy Extentions in Kapitel 17).

Die ursprüngliche Bedeutung von **NAT** ist die Umsetzung jeweils **einer** internen IP-Adresse in eine jeweils andere offizielle Adresse; es stellt damit eine 1:1-Adressbeziehung zwischen interner und offizieller Adresse dar. **PAT** kann zusammen mit NAT **viele** interne IP-Adressen in eine einzige offizielle Adresse umsetzen, wobei zusätzlich die Quell-Portnummern ersetzt werden. Dies wird auch **Masquerading** genannt.

Heute wird **NAT** als Sammelbegriff für alle Arten der Umsetzung einer Adress-Information in Datenpaketen verwendet. Es ist für die meisten Protokolle ab OSI-Level 3 problemlos verwendbar.



Protokolle, die keine Änderungen im Header zulassen, sind mit NAT schwierig einsetzbar. So ist z. B. beim Einsatz von IPsec (vgl. Kapitel 18) die Protokollerweiterung NAT-Traversal erforderlich.

Alle Clients verschicken dabei ihre Internetanfragen über den Router, der als Standard- (Default-) Router eingetragen ist (z. B. ein DSL-Router), wo sie mittels NAT (und PAT) entsprechend verändert und ins Internet weiterleitet werden. Dabei ersetzt er im ankommenden IP-Paket des Clients zwei Informationen:

- ✓ auf Layer 3 die private Quell-IP-Adresse des Clients mit der öffentlichen Adresse des Routers,
- ✓ auf Layer 4 den Quell-Port des Paketes einer Anwendung mit einer nicht genutzten Portnummer.

Der Router führt dazu eine Tabelle, in die er speichert, welche Kombination er aus interner Client-IP und Client-Port auf welche offizielle Client-IP und Quell-Port umgesetzt hat.

Der Ziel-Rechner im Internet sieht nun als Absender die öffentliche IP-Adresse des Routers und wird seine Antwort an diese Adresse zurückschicken. Anhand der Portnummer in der Antwort kann dieser in seiner internen Tabelle nachprüfen, an welche IP-Adresse und unter welcher Portnummer er die Antwort zurück ins lokale Netz schicken soll, indem er diese Einträge im ankommenden IP-Paket entsprechend zurück ändert.

- ✓ Eine spezielle Konfiguration der Client-Anwendungen ist nicht nötig, da NAT generell **transparent** wirkt (ohne dass ein Anwender dies bemerkt).
- ✓ Bei Protokollen, die keine Portnummern verwenden, wie z. B. bei ICMP (Ping), wird anstelle der Portnummer ein anderer Wert ausgetauscht, im Beispiel die ICMP Query ID nach RFC 3022.
- ✓ Beim Zugang zum Internet über Funkverbindungen wie UMTS oder LTE bekommen Sie in der Regel (je nach Anbieter) ebenfalls eine private IP-Adresse, die per NAT beim Provider umgesetzt wird.

 **Ergänzende Lerninhalte:** Weitere Protokolle.pdf

11.5 Zuordnung zum OSI-Modell

Protokolle im OSI-Referenz-Modell

Die verschiedenen Protokolle eines Protokoll-Stacks erfüllen bei der Datenkommunikation unterschiedliche Aufgaben. Als Zuordnung kann am einfachsten das OSI-Modell dienen und so die Basis für eine Einteilung in **Anwendungs-Protokolle** auf Layer 7 und **Netzwerk-Protokolle** auf unteren Layern, die als Träger für weitere Protokolle bzw. von Diagnose- und Fehlermeldungen dienen (Transport- und Verbindungs-Protokolle). Die folgenden Abschnitte sollen auf diese Weise noch einmal ein anderes Licht auf die Protokolle werfen.

Protokolle der Anwendungs-Schicht

Anwendungs-Protokolle arbeiten auf der obersten Schicht **7** des OSI-Modells und ermöglichen den Informationsaustausch zwischen Anwendungen. Beispiele aus den verschiedenen Protokollfamilien dazu sind:

- ✓ FTP, SMTP und HTTP für den Austausch von Daten
- ✓ DHCP bzw. DHCPv6 u. a. für die automatische Netzwerk-Konfiguration bei IPv4 bzw. IPv6
- ✓ DNS für die Namensauflösung.

Protokolle der Transport-Schicht

Transport-Protokolle stellen eine Verbindung zwischen zwei Netzwerknoten her. Sie liegen auf der OSI-Schicht **4** und sind letztlich für die Datenübertragung zuständig. Beispiele sind:

- ✓ TCP aus TCP/IP für die gesicherte Datenübertragung
- ✓ UDP aus TCP/IP für die ungesicherte Datenübertragung.

Protokolle der Verbindungs-Schicht

Verbindungs-Protokolle sind auf Schicht **3** im OSI-Modell angesiedelt. Hier werden die Adress- und Routing-Informationen sowie die Meldung von Ereignissen (z. B. Fehlermeldungen) realisiert. Beispiele sind:

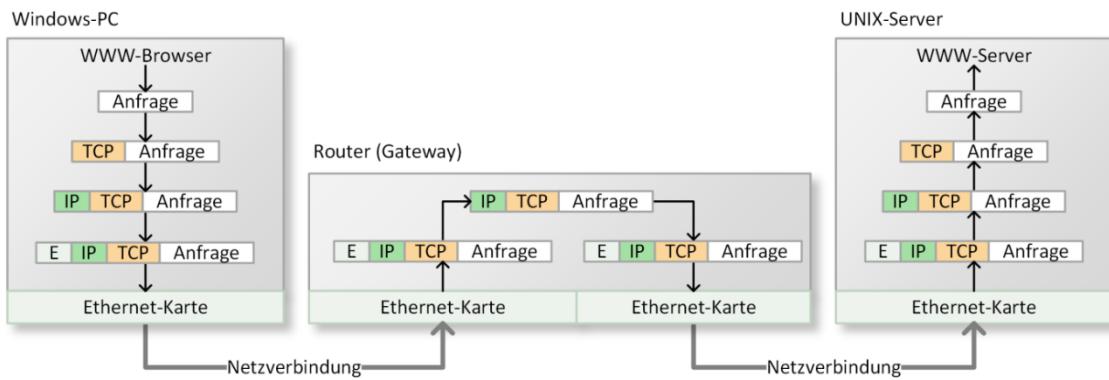
- ✓ IPv4 (**Internet Protocol Version 4**) zur Adressierung in IPv4-Netzwerken
- ✓ ICMP (**Internet Control Management Protocol**) für Meldungen in IPv4-Netzen
- ✓ IPv6 als nächste Version vom IP-Protokoll
- ✓ ICMPv6 (**Internet Control Management Protocol**) für Meldungen in IPv6-Netzen.

Beispiel

Das folgende vereinfachte Beispiel soll zum Abschluss die Zusammenarbeit der verschiedenen Protokolle eines Protokoll-Stacks über die verschiedenen Schichten des OSI-Modells hinweg verdeutlichen. Als Ausgangspunkt dient die Eingabe der Adresse www.herdt.com in einen Browser und die Verwendung von TCP/IP.

- ✓ Die Anwendung (Browser) schickt eine HTTP-Anforderung.
- ✓ Über eine Namensauflösung muss die zu www.herdt.com passende IP-Adresse gefunden werden.
- ✓ Das Anwendungs-Paket (HTTP) wird erst in ein Transport-Paket (TCP) gepackt, dieses in ein Verbindungs-Paket (IP) und dieses schließlich in einen Ethernet-Frame.
- ✓ Anhand der Netzmaske ist bekannt, dass das Ziel sich nicht im eigenen Netzwerk befindet und damit nicht direkt erreichbar ist. Daher wird per ARP die MAC-Adresse der internen Netzwerk-Schnittstelle des Default-Routers (Gateway) ermittelt und als Empfänger-Adresse im Ethernet-Frame eingetragen.
- ✓ Der Default-Router packt das IP-Paket um und übergibt es dem Internet. Anhand der Informationen im IP-Header (unter anderem der IP-Adresse vom Ziel) wird das IP-Paket von weiteren Routern von Zwischenstation zu Zwischenstation weitergereicht (routing). Ob, wie schnell und auf welchem Weg es ankommt, ist weder gesichert noch festgelegt.
- ✓ Am Ziel kann festgestellt werden, ob das angekommene IP-Paket korrekt ist. Wenn ja, wird der IP-Header entfernt und es wird über das Protokoll TCP weitergereicht.
- ✓ TCP stellt sicher, ob alle Pakete in der richtigen Reihenfolge korrekt angekommen sind, und fordert verlorene Pakete erneut an.
- ✓ Nachdem der TCP-Header entfernt wurde, wird die HTTP-Anforderung zum Webserver-Prozess weitergereicht.
- ✓ Dieser kann reagieren und seinerseits die angeforderten Daten auf umgekehrtem Weg zurücksenden.

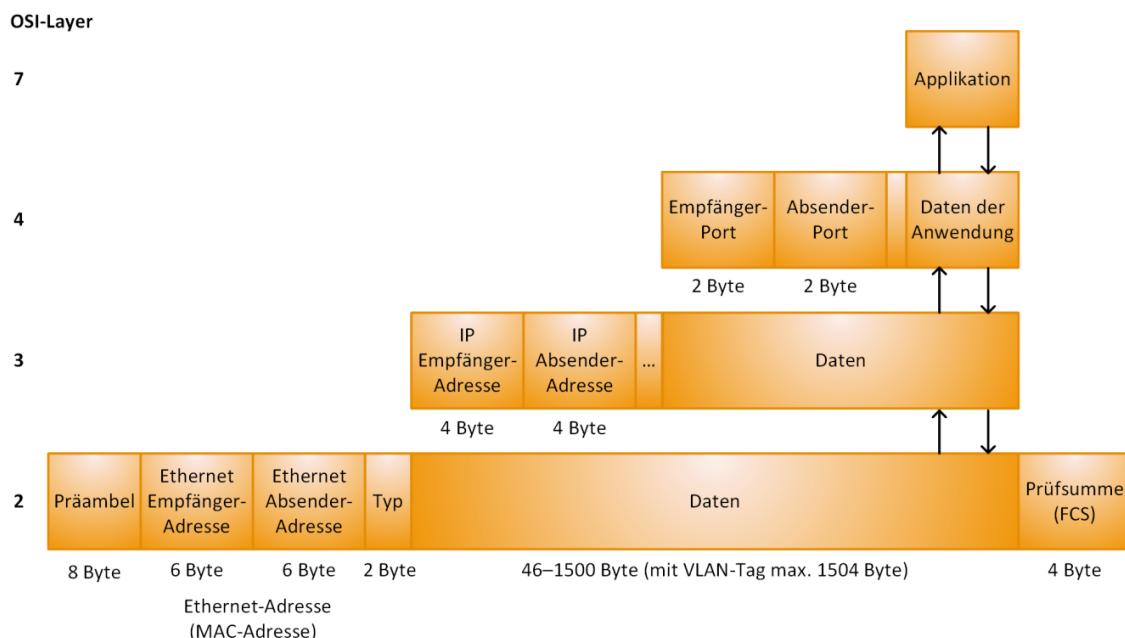
Die folgende Grafik stellt diese Kommunikation nochmals vereinfacht dar:



Schematische Abfolge einer WWW-Anfrage (vereinfacht)

Datenübertragung anhand des OSI-Modells

In folgender Abbildung ist schematisch die Art und Weise gezeigt, mit der Daten einer Server- bzw. Client-Applikation (Anwendung) im Netzwerk über die einzelnen OSI-Layer hinweg in verschiedenen Paketen verpackt verschickt werden. Der Übersicht halber sind nur die zum Verständnis nötigen Elemente gezeigt.



Die eigentlichen Daten vom Anwendungs-Protokoll befinden sich hier auf Layer 4 in einem Paket, welches das TCP- oder UDP-Protokoll zur Verfügung stellt. Damit die Daten der Anwendung zum richtigen Dienst auf Layer 7 verschickt werden, ist der Port des Empfängers und für die Antworten der Port des Senders wichtig. Diese befinden sich neben weiteren Flags im Header des Transportpakets.

Das Paket auf Layer 4 ist wiederum in einem IP-Paket verpackt (darunter auf Layer 3), damit es über das IP-Protokoll verschickt werden kann. Hierzu ist im Header neben weiteren Flags die IP-Adresse des Empfängers und wiederum für die Antwort die IP-Adresse des Senders erforderlich. Damit das IP-Paket über ein Ethernet-Netz verschickt werden kann, muss es in einem Ethernet-Frame (auf Layer 2) eingepackt sein, denn hier gelten nur Ethernet-Adressen. Diese befinden sich neben dem Typ-Feld im Header des Ethernet-Frames.

11.6 Übung

Fragen zu Protokollen

Übungsdatei: --

Ergebnisdatei: uebung11-E.pdf

1. Was ist ein Protokoll und welchen Zweck hat es?
2. Auf welchen OSI-Schichten kann es Protokolle geben?
3. Nennen Sie mind. drei typische Anwendungs- und mind. drei Übertragungsprotokolle.
4. Welches ist der wichtigste Unterschied zwischen TCP und UDP?
5. Wozu werden Portnummern benötigt und wo gibt es eine Liste davon?
6. Welche Portnummern benötigen Sie zum Surfen im Internet und wo geben Sie diese an?
7. Ergänzen Sie die folgende Tabelle von IPv4-Netzwerken um die fehlenden Angaben:

Netzwerkadresse	Netzmaske	CIDR-Schreibweise	Anzahl möglicher Hosts
		192.168.0.0/16	
		172.20.30.0/24	
67.23.155.64			62
205.117.200.0	255.255.255.254		
198.17.20.0	255.255.252.0		
78.56.23.16			6

8. In welchem Netzwerk mit Broadcast-Adresse 22.175.16.63 liegt die IP-Adresse 22.175.16.35?
9. Sie hatten bisher die Netzwerke 10.20.0.0/16 und 10.30.0.0/16, die Sie nun in ein einziges Netzwerk zusammenfassen wollen. Welches kleinstmögliche Netzwerk benötigen Sie hierzu?
10. Können alle Rechner/Geräte in einem Netzwerk die IP-Adresse per DHCP erhalten? Begründen Sie Ihre Aussage.
11. Tragen Sie in der Tabelle ein, wann es vorteilhafter ist, entweder mit einem Proxy oder per NAT für eine Firma eine Verbindung ins Internet einzurichten:

Verbindung per Proxy	Verbindung per NAT

12

Erweiterung der Netzwerkstruktur

12.1 Überlegungen zur Vergrößerung eines Netzwerks

Wenn ein kleines Netzwerk wächst

Bisher ging es hier um kleine Netzwerke mit einer überschaubaren Anzahl von Arbeitsstationen und moderaten Ansprüchen bezüglich der Geschwindigkeit, Bandbreite und Zuverlässigkeit des Netzwerks.

Spätestens, wenn die Anzahl der Arbeitsstationen weiter steigt und mehr Netzbürger eine umfangreichere oder schnellere Vernetzung benötigen, müssen Fragen bezüglich der vorhandenen Struktur, der verfügbaren Bandbreite des Netzwerks und der Netzwerksicherheit neu beantwortet werden. Die Planung soll längerfristig sicherstellen, dass Bedürfnisse der Netzbürger auch in Zukunft so flexibel wie möglich realisiert werden können.

Integration von Diensten

Ein weiterer Aspekt ist die Integration unterschiedlichster Dienste (Voice, Video, Daten) über eine physikalische Struktur (Medium). Dazu benötigen Sie eine dienstneutrale Netzinfrastruktur. Man spricht hier von Konvergenz (Übereinstimmung) der Dienste. Hierzu zählen neben der Kabelinfrastruktur auch die benötigten Netzwerkkomponenten, die diese Merkmale unterstützen müssen. Die Netzwerkkomponenten müssen die Dienste priorisieren können, d. h., Voice muss vor Video und Daten übertragen werden.

Welche Aspekte müssen bei der Vergrößerung eines Netzwerks berücksichtigt werden?

Bei der weiteren Ausdehnung eines LANs kommen zu den bisherigen Überlegungen neue Aspekte hinzu und es müssen etliche Fragen neu beantwortet werden. Einige der wichtigsten davon sind folgende:

- ✓ Soll das bestehende Netz in mehrere Einzelnetze unterteilt werden? Welche Möglichkeiten gibt es, um diese Einzelnetze dem Endbenutzer wieder als ein Netz erscheinen zu lassen?
- ✓ Welche Geräte werden benötigt, um die Netze physisch zu erweitern bzw. bestehende Netzwerk-Segmente miteinander zu verbinden?

- ✓ Welche Änderungen der Topologien sind eventuell nötig, um Netzverkehr effektiver zu strukturieren?
- ✓ Welche zusätzlichen Maßnahmen müssen getroffen werden, um die gestiegenen Sicherheitsanforderungen zu erfüllen?

80/20-Regel

Auch die Gültigkeit und Relevanz der früheren 80/20-Regel, nämlich dass 80 Prozent des Netzwerkverkehrs segmentintern und nur 20 Prozent segmentübergreifend stattfindet, muss für größere Netzwerke überdacht werden und führt häufig zu Konsequenzen in Bezug auf die Bildung von Teilnetzwerken. Der Trend verschiebt sich eindeutig in Richtung segmentübergreifender Verkehr, d. h., man greift zunehmend auf Ressourcen zu, die sich nicht im eigenen Segment befinden.

Verkabelung

Spätestens dann, wenn Netzwerke eine bestimmte Dimension übersteigen und es vorher noch nicht in ausreichendem Maß getan worden ist, muss noch einmal intensiv über die Verkabelung nachgedacht werden. Das betrifft sowohl die Prüfung der bestehenden Übertragungsmedien als auch Überlegungen bezüglich einer neuen Verkabelung.



Da die Verkabelung eine längere zeitliche Perspektive aufweist als die Programme, die darauf aufsetzen, muss diese Frage zukunftsträchtig gelöst werden. Die Verkabelung wird nicht alle fünf Jahre erneuert, aber die verfügbaren Technologien, die über diese Kabel realisiert werden, kann sich innerhalb von fünf Jahren zum Teil erheblich verändern.

Anforderungen an eine neue Grundstruktur

Letztendlich ist es unumgänglich, sich eine vernünftig und flexibel erweiterbare Grundstruktur zu überlegen, die im Bedarfsfall ausreicht, eine prognostizierte maximale Anzahl an Benutzern mit einem hochgerechneten Bedarf an Netzkapazität bedienen zu können. Dazu sollten gewisse Installationsreserven von Anfang an mit eingerechnet werden.

Möglichkeiten der Verkabelung

Eine unstrukturierte Verkabelung, die sich an den momentanen Bedürfnissen orientiert, führt über kurz oder lang zu einer Kostenexplosion, vor allem dann, wenn Erweiterungen Änderungen an den bereits bestehenden Strukturen notwendig machen.

Als Unterstützung der Planung für die praktische Umsetzung der Verkabelung von Gebäuden stehen zwei unterschiedliche Ansätze zur Verfügung:

- ✓ Strukturierte Verkabelung
- ✓ Collapsed Backbone

Beide Konzepte werden in den folgenden Abschnitten vorgestellt. Obwohl namentlich nur im zweiten Konzept erwähnt, spielt der Begriff **Backbone** in beiden Strategien eine Rolle und wird deshalb vorab kurz definiert.

Definition Backbone

Ein Backbone (Rückgrat) ist ein Hochleistungsnetz, welches verschiedene Teilnetze miteinander verbindet. Es ist der Teil der Kabelinfrastruktur, der z. B. als verbindendes Glied der einzelnen Gebäudeverkabelungen dient. Ein Anschluss von Endgeräten, Terminalnetzen, Telefonanlagen usw. an den Backbone ist zwar auch möglich (Collapsed Backbone), wird aber kaum noch durchgeführt. Durch die Vielzahl der Kombinationsmöglichkeiten haben sich für die unterschiedlichen Bereiche (LAN, MAN, WAN) unterschiedliche Techniken herausgebildet.

12.2 Strukturierte Verkabelung

Internationaler Standard

Amerikanische, europäische und internationale Gremien bemühten sich um Standards bezüglich der Verkabelung. Der Standard 568 Custom Premises Wiring von der EIA/TIA lieferte als Commercial Building Telecommunication Standard die Grundlage für die strukturierte Verkabelung. Unter der Bezeichnung ISO/IEC DIS 11801 findet dieser Standard internationale Anerkennung. In Deutschland geschieht dies nach der Norm DIN EN 50173 (Österreich: ÖN EN 50173 und Schweiz: EN 50173).

Generell werden in dieser Norm Topologie und übertragungstechnische Kenndaten definiert. Ausgehend von den gängigen Übertragungsraten und den verfügbaren Kabeltypen bilden diese bestimmte, sogenannte Link-Klassen. Die Ende-zu-Ende-Verbindungen werden den Link-Klassen A, B, C, D, E und F zugeordnet.

Der Standard wurde anfangs für folgende Eckdaten optimiert:

- ✓ geografische Ausdehnung bis 3000 m,
- ✓ Bürofläche bis zu 1 Mio. m²,
- ✓ Anzahl der Benutzer zwischen 50 und 50000.

Vorteile der strukturierten Verkabelung

- ✓ Die Verkabelung ist anwendungsneutral, d. h., jede Information (Voice, Video, Daten) kann über das gleiche Medium übertragen werden.
- ✓ Sie gewährleistet den Betrieb aktueller und zukünftiger Kommunikationssysteme (Investitionsschutz).
- ✓ Sie ist flexibel erweiterbar und durch die sternförmige Topologie ausfallsicher angelegt.

EN 50173

In Europa wurde diese Norm im März 1994 unter der Bezeichnung EN 50173 als strukturierte, anwendungsneutrale Gebäudeverkabelung veröffentlicht. Da bis zum damaligen Jahreswechsel kein Widerspruch einging, wurde diese Norm im Juli 1995 von der CENELEC verabschiedet.

Bedingt durch Weiterentwicklungen im Bereich Ethernet (Stichwort Gigabit) war bereits Ende 1999 absehbar, dass Erweiterungen der Norm nötig werden würden. Dies führte im Juli 2000 zur Veröffentlichung von EN 50173:2000 und im November 2002 zur aktuellen Version EN 50173-1 bzw. EN 50173 2. Ausgabe.

Im Wesentlichen wurde dabei die Link-Klasse D (bis 100 MHz) überarbeitet und die Link-Klassen E (bis 250 MHz) und F (bis 600 MHz) wurden modifiziert. Parallel dazu wurden die Anforderungen an Kabel der Kategorie 6 und 7 festgelegt sowie neue LWL-Kabel in die Norm integriert. Die aktuelle Normung der Kategorie 6 und 7 liegt bei 600 MHz bzw. 1000 MHz. Detaillierte Informationen dazu sind auf der CENELEC-Website (<https://www.cenelec.eu>) erhältlich.

Allgemein soll diese Norm eine Planungssicherheit für mehrere Jahre und für alle gewünschten Dienste liefern. Im Kern beinhaltet sie dabei eine Dreiteilung der Verkabelungsstruktur in einen **primären, sekundären und tertiären** Bereich.

Primärverkabelung (zwischen Gebäuden)

Diese Stufe wird als **Campus Backbone** bezeichnet. Sie beschreibt die Verbindung zwischen Gebäudeverteilern und Standortverteilern über Lichtwellenleiter in Ring- oder Stern-Topologie. Dieser Bereich kümmert sich um die Verkabelung der einzelnen Gebäude und stellt das Bindeglied zwischen den einzelnen Sekundärbereichen dar.

Als weitere Aufgabe wird hier oft auch die Anbindung an ein WAN realisiert.

Die wichtigsten Anforderungen sind:

- ✓ hohe Datenraten über große Entfernung,
- ✓ redundante Verbindungen,
- ✓ eine sichere und gut dokumentierte Trassenführung.

Die oben genannten Punkte gewährleisten eine hohe Ausfallsicherheit. Weitere Punkte betreffen die hohe Abhörsicherheit von Glasfaserkabeln.

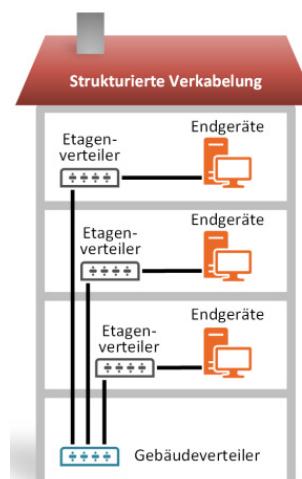
Sekundärverkabelung (zwischen Etagen)

Gemeint ist damit die Verkabelung der Etagen ausgehend von dem Gebäudeverteiler. Jede Etage erhält dabei einen Etagenverteiler. Auch hier sollten Lichtwellenleiter verwendet werden. Die maximale Länge sollte laut Norm nicht über 500 m hinausgehen.

Ein wichtiger Aspekt ist auch hier die problemlose Begehbarkeit der Gebäude- und Etagenverteilerverbauteile, um so eine schnelle Fehlersuche und Wartung zu ermöglichen.

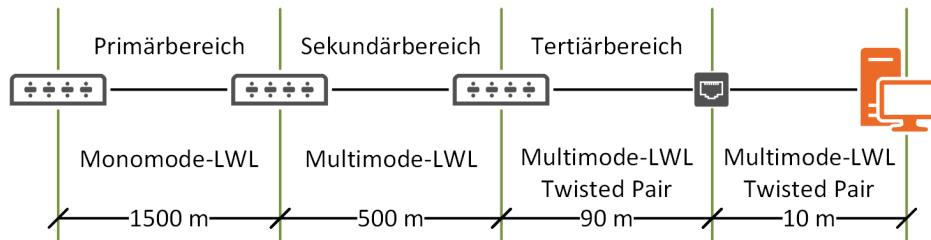
Tertiärverkabelung (auf der Etage)

Diese Stufe beschreibt die Verbindung vom Etagenverteiler zu den einzelnen Arbeitsstationen über Twisted-Pair- oder Glasfaserkabel in Stern-Topologie. Die Norm empfiehlt hier mindestens zwei Anschlüsse pro Arbeitsplatz.



Als weitere grobe Richtdaten können genannt werden, dass dieser Bereich für Etagen mit maximal 900 bis 1000 m² gedacht ist, wobei die maximale Länge des fest verlegten Kabels zur Arbeitsstation 90 m (+ 10 m für Rangier- und Geräteanschlusskabel) nicht überschreiten darf.

Die maximale Distanz im Tertiärbereich zum Endgerät darf bei Twisted-Pair-Kabeln 100 m betragen, bei Einsatz von Glasfaserkabeln entsprechend mehr. Weitere Einschränkungen zur Kabellänge können Sie der nachfolgenden Grafik entnehmen.



Verkabelungsstruktur der strukturierten Verkabelung

Die Längenangaben der Kabel im Tertiärbereich gelten nur für **Twisted-Pair-Kabel**.

Überschneidungen

Es gibt Situationen, in denen der sekundäre und tertiäre Bereich nicht klar zu trennen sind. So kann bei günstigen räumlichen Gegebenheiten ein Verteilerraum z. B. für drei Etagen mit insgesamt 2000 m² sinnvoll sein. Andererseits kann bei großen Gebäuden ein einziger Verteiler pro Etage nicht ausreichen.

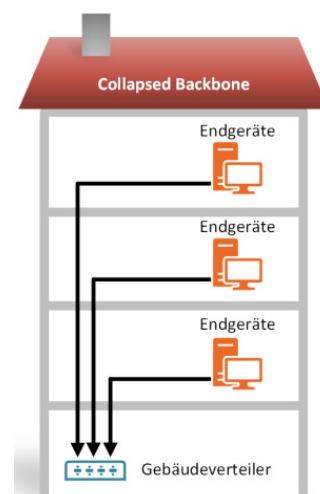
12.3 Collapsed Backbone

Bündelung in einem Gerät

Bei einem Collapsed Backbone erfolgt die Bündelung aller Netzsegmente in einem einzigen Gerät. Alle Segmente werden in diesem Gerät zusammengefasst, das seinerseits damit selbst die Rolle des Backbone übernimmt. Ein Collapsed Backbone entspricht nicht der Norm zur strukturierten Verkabelung.

Vorteil/Nachteil

Der hauptsächliche Vorteil liegt im einfacheren Netz-Management, das zentral in einem einzigen Gerät durchgeführt werden kann, und in der Flexibilität bei der Netzwerkstrukturierung, da diese unabhängig von Standorten oder Etagen stattfinden kann.



Ein weiterer Vorteil des Collapsed Backbone wären die geringeren Kosten, da eben nur ein zentraler Verteiler nötig ist. So können Platz in den Etagen und Kosten für Klimatisierung, Zugangskontrollen usw. gespart werden.

Aber zumindest bei größeren Gebäuden bedeutet Collapsed Backbone aufgrund der Reichweiten fast zwangsläufig Glasfaser-Kabel, womit die aktiven Komponenten wieder teurer werden.

Ein gravierender Nachteil liegt genau darin, dass nur eine Zentrale das gesamte Netz steuert. Wenn diese Zentrale ausfällt, ist kein Netzverkehr mehr möglich. Aus diesem Grund wird solche Zentrale oft redundant ausgelegt (teilweise oder vollständig).

Weiterhin muss erwähnt werden, dass sich bei größeren Teilnehmerzahlen ein Collapsed Backbone mit einem Gerät als Verteiler nicht realisieren lässt, da die Anschlussmöglichkeiten begrenzt sind. In diesem Fall wird man auch hier zusätzliche Verteiler integrieren müssen.

Distributed Backbone

Bei einem Distributed Backbone erfolgt eine Dezentralisierung, indem z. B. pro Etage oder pro Gebäude ein Gerät zur Zusammenfassung zur Verfügung steht. Diese einzelnen Geräte koordinieren dann die Kommunikation der angeschlossenen Systeme. In gewisser Weise findet damit eine Annäherung an die strukturierte Verkabelung statt.

Randbemerkung

Die Entscheidung für eine strukturierte Verkabelung oder für einen Collapsed Backbone ist wichtig, da sie große Auswirkungen auf die Gebäudeinfrastruktur hat (Kabelschächte, Brandschutzrichtlinien).

Die Hersteller von Twisted-Pair-Kabeln unterstützen die strukturierte Verkabelung, da die Längen von Kupferkabel ohne Etagenverteiler für viele Gebäude nicht ausreichen würden. Die Hersteller von Glasfaserkabeln tendieren zum Collapsed Backbone, da hier größere Reichweiten problemloser umzusetzen sind.

12.4 VLAN (Virtual Local Area Network)

Logische Netzwerkstrukturen aufbauen

Neben den Versuchen, durch neuere Entwicklungen bei den Geräten eine Steigerung der Bandbreite im Netz zu erreichen, gibt es auch im konzeptionellen Bereich Möglichkeiten, Netzverkehr zielgerichtet zu steuern. Daraus ergibt sich die Notwendigkeit zur Strukturierung von Netzwerken. Dies kann physikalisch in die Praxis umgesetzt werden, indem für jedes (Teil-) Netz ein eigener Verteiler eingesetzt wird. Ein anderer Ansatz ist, die Strukturierung des Netzwerks virtuell zu erreichen. Unter dem Begriff **Virtual Local Area Network (VLAN)** wird dieses Vorhaben in mehreren Varianten umgesetzt.

Definition

Ein VLAN ist eine in sich geschlossene logische Gruppe innerhalb eines physikalischen Netzwerkes. Ein VLAN wird durch eine eindeutige Nummer (**VLAN-ID**) gekennzeichnet. Ein VLAN kann sowohl auf einem Switch angelegt werden als auch über mehrere Switches hinweg.

Bei einem virtuellen LAN ist es somit nicht mehr primär wichtig, wie und mit welchem Verteiler eine Arbeitsstation physikalisch verbunden ist, sondern welchem Teilnetzwerk sie logisch zugeordnet wird. VLANs sind daher durch eine mögliche Trennung zwischen der physikalischen und der logischen Anbindung der einzelnen Stationen gekennzeichnet.

So können z. B. Arbeitsstationen, die physikalisch an verschiedenen Verteilern liegen, logisch in einem separaten Netzwerk zusammengefasst werden.

Vorteile

Einerseits wird damit eine hohe Flexibilität erreicht, d. h., eine Arbeitsstation kann umziehen und ist immer noch Mitglied in dem angelegten VLAN. Auf der anderen Seite wird damit grundlegenden Sicherheitsaspekten Rechnung getragen, da Verkehr nur noch innerhalb des VLANs stattfindet. Es entsteht eine in sich geschlossene Benutzergruppe. Durch die Segmentierung der einzelnen Nutzer in VLANs wird auch der Verkehr in den VLANs reduziert, weil weniger Teilnehmer auch weniger Broadcast- und Multicastverkehr je Segment erzeugen.

Und letztlich kann durch die Mechanismen des VLANs (IEEE 802.1P) der Netzwerkverkehr (Voice, Video, Daten) priorisiert werden.

Normierung durch IEEE 802.1Q

Die Normierung von VLAN erfolgte durch IEEE 802.1Q. Ein Teil dieser Norm betrifft auch IEEE 802.3 (Ethernet), da 802.1Q eine Verlängerung des Ethernet-Frames um vier Byte vorsieht. In diese vier Byte werden zusätzliche Informationen gespeichert, die den Datenaustausch in einem VLAN regeln. Dies wird als **Tagging** bezeichnet.

Das **Tagging** dient dazu, eine VLAN-ID im Header der Datenpakete unterzubringen, um den Vermittlungsgeräten eine Entscheidung zu ermöglichen, in welches VLAN das zu vermittelnde Frame weitergeleitet werden soll.

Ebenfalls in 802.1Q wird das VLAN Registration Protocol **GARP VLAN Registration Protocol (GVRP)** spezifiziert. Dieses Protokoll leistet eine dynamische Konfiguration von VLANs auf Switchen und arbeitet auf der Basis des **Generic Attribute Registration Protocols (GARP)**, welches durch IEEE 802.1d definiert ist.

Auf diese Weise lässt sich die Konfiguration der VLANs zentral verwalten und über GVRP im LAN umsetzen. Gerade in größeren Netzwerken ist dies eine große Erleichterung gegenüber der statischen VLAN-Konfiguration auf jedem der beteiligten Switches.

Die Nachfolger dieses Protokolls sind das **Multiple Registration Protocol (MRP)** und das **Multiple VLAN Registration Protocol (MVRP)**, welche im Standard IEEE 802.1ak hinterlegt sind.

Innerhalb eines VLANs können Switches definiertem Verkehr Vorrang gewähren. Dazu müssen die Switches auf den **Uplinkports** (das sind die Verbindungsports zwischen den Switchen) den Standard IEEE 802.1Q unterstützen und die Pakete mit entsprechenden Tags versehen.

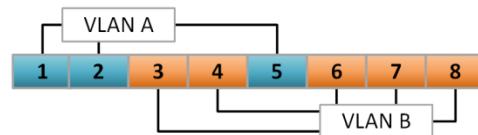
Stacking bezeichnet das Parallelschalten mehrerer gleichartiger Switches. Mehrere Switches können dabei nach IEEE 802.1Q miteinander über spezielle Stacking-Ports und mit speziellen Stack-Kabeln verbunden werden. Damit erhalten Sie einen einzigen Switch mit hoher Portanzahl. Da dies nur bei manageable Switches geht, haben diese Switches ein gemeinsames Management, mit dem sich ein VLAN switchübergreifend erweitern lässt.

Verschiedene Varianten

Da das VLAN eine in sich geschlossene Benutzergruppe darstellt, ist es prinzipiell egal, wie Sie diese definieren. Sie können diese auf der Basis der physikalischen Ports, der Adressierung, des Protokolls oder anwenderbasiert festlegen.

Statisches oder portbasiertes VLAN

Die Bildung des virtuellen LANs entsteht hier durch die Zusammenfassung einzelner physikalischer Ports am Switch oder an den miteinander verbundenen Switchen zu verschiedenen Gruppen. Im folgenden Beispiel gehören die Geräte an Port 1, 2 und 5 zum VLAN A und die Geräte an Port 3, 4, 6, 7 und 8 zum VLAN B.



Die Ports eines VLANs können nun nicht mehr mit den Ports des anderen VLANs kommunizieren, da sie in ihrem VLAN isoliert sind. Das dient einerseits der Sicherheit und andererseits wird damit der Broadcastverkehr reduziert.

Dynamisches VLAN

Bei einem **dynamischen VLAN** ist im Gegensatz zur statischen Portzuordnung die Gruppe der Mitglieder eines VLAN durch den Inhalt der Frames definiert. Dynamische VLANs sind zwar flexibler, sollten aber nur in sicheren Bereichen eingesetzt werden.

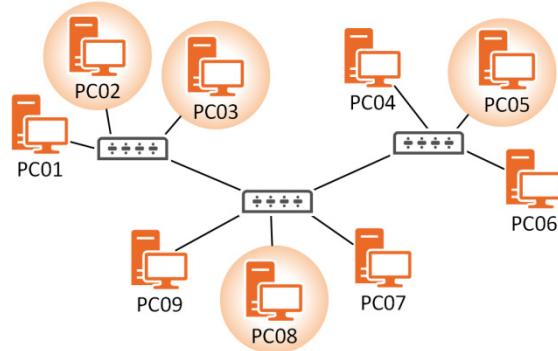


Eine dynamische Zuordnung ist **unsicher** und daher für sicherheitsrelevante Einsatzbereiche nicht geeignet.

MAC-Adressenbasierte VLANs

In Gegensatz zu einem portbasierten VLAN werden hier die Nutzer anhand der MAC-Adresse ihres Computers zu einer Gruppe zusammengefasst. Sie sind somit nicht mehr statisch fest an einen physikalischen Port gebunden.

Die Skizze rechts soll dies verdeutlichen. Wenn eine mit einem Kreis gekennzeichnete Station an einen anderen Switch umzieht, muss nicht mehr der Port für dieses VLAN konfiguriert werden, da die Station anhand ihrer MAC-Adresse erkannt wird.



Diese auch Layer-2-VLANs genannten Konfigurationen werden hauptsächlich bei Nutzern, die sich ständig an anderen Orten eines LANs aufhalten, angewendet. Die Sicherheit leidet in dieser Konfiguration durch den Umstand, dass MAC-Adressen gefälscht bzw. verändert werden können.

Protokollbasierte VLANs

Bei diesem Typ von VLAN werden die Gruppen anhand von Protokolltypen gebildet, z. B. vom Protokoll IP. Jedes Frame, das nicht der Protokolltypdefinition entspricht, wird ausgeschlossen. Wurden zwei protokollbasierte VLANs des gleichen Typs gebildet, können sich diese trotzdem nicht überschneiden.

Anwendungsbasierte VLANs

Bei einem anwendungsbasierten VLAN wird jeweils eine Gruppe von Anwendern, die die gleiche Applikation nutzen, in einem VLAN abgebildet. Diese Art von VLANs erfordert im Netzwerk Multilayerswitche.

Die Zugehörigkeit einer Station zu einem bestimmten VLAN wird z. B. über IP-Adresse und Portnummer der gewünschten Anwendung geregelt. Die physikalische Anbindung der Station an das Netzwerk spielt auch hier keine gravierende Rolle mehr, sondern es können logische Arbeitsgruppen innerhalb eines Netzes gebildet werden.

Layer-3-VLAN

Erfolgt die Zuordnung über die IP-Adresse, wird es als Layer-3-VLAN bezeichnet. Dann kann sich ein derartiges VLAN auch über Subnetze erstrecken.

12.5 Industrie-LAN

Ein Industrie-LAN ist die Vernetzung innerhalb einer industriellen Fertigung. Neben hersteller-spezifischen Lösungen sind, wie beim Ethernet, allgemeine und weitergehende Standards für den industriellen Einsatz implementiert, wie die auf dem **Feldbus** (IEC 61158) basierenden Standards **EtherNet/IP** bzw. **EtherNet Industrial Protocol (EIP)**, **Process Field Bus (PROFIBUS)** und **EtherCAT** sowie **Process Field Network (PROFINet)**.

Ethernet ist das Standardprotokoll im LAN-Bereich, daher ist es zur Kompatibilität der Netzstrukturen und -übergänge notwendig, um den Produktionsbereich in das vorhandene LAN einzubeziehen. Damit sind alle Informationen für die Steuerung und Kontrolle der Produktionsprozesse verfügbar. Wegen der Sensibilität der Anlagen ist immer auf eine ausreichende Absicherung (z. B. über Firewalls) der Industrie-LANs zu achten.

Heute existieren z. B. neben Switchen und Medienkonvertern auch Komponenten, die im WAN eingesetzt werden. Solche Gerätschaften müssen natürlich an die industriellen Umgebungsbedingungen angepasst sein. Dies betrifft beispielsweise:

- ✓ die Gleichstrom-Spannungsversorgung (24 V DC)
- ✓ einen erweiterten Betriebstemperaturbereich
- ✓ die Schutzart (Schutz gegen Staub, Spritzwasser, Schmutz, usw.)
- ✓ Vibrationsfestigkeit
- ✓ erhöhte Verfügbarkeit der Komponenten

In Industrie-LANs wird aus Redundanzgründen häufig eine physikalische Ringstruktur verwendet. Im Falle eines Ausfalls einer Verbindung oder einer Komponente kann das Netzwerk weiter arbeiten.

12.6 Übung

Fragen zur Netzwerkstruktur und zur strukturierten Verkabelung

Übungsdatei: --

Ergebnisdatei: uebung12-E.pdf

1. Nach welcher Norm ist die strukturierte Verkabelung definiert?
2. Nach welcher Norm ist ein Collapsed Backbone definiert?
3. Wann sollten Sie eine strukturierte Verkabelung verwenden?
4. Welche Vorteile bietet ein Collapsed Backbone im Vergleich zur strukturierten Verkabelung?
5. Welche Vorteile kann ein VLAN bringen?
6. Welche grundsätzlichen Varianten von VLANs gibt es in Bezug auf Sicherheit?

13

Kopplung von Netzwerken

13.1 Aktive Komponenten

Geräteübersicht

Zur Vergrößerung von Netzwerken bzw. zur Überwindung vorhandener Einschränkungen wie Längen oder Bandbreitenengpässe gibt es verschiedene Geräte unterschiedlicher Funktionalität.

Je höher die Einbindung eines Gerätes im Referenzmodell erfolgt, desto komplexer ist die in ihm realisierte Funktionalität. Das reicht von der physischen Kopplung mit den Medien über die Steuerung der Wegwahl (Routing) bis hin zur Zugangskontrolle und zur Umsetzung von Protokollen.

Angelehnt an das OSI-Modell zeigt die folgende Tabelle eine Übersicht von aktiven Netzwerkkomponenten, auch wenn diese z. T. nicht mehr marktüblich sind.

OSI-Schicht	Netzwerkkomponenten	Kennzeichen
7	Gateway, Proxy, Application-Layer-Firewall	Protokollumsetzung auf Applikationsebene
4	Layer-4-Switch, Stateful-Inspection-Firewall	Segmentierung, Fehlerkorrektur (TCP), Portfilterung
3	Router, Multilayerswitch (Layer-3-Switch), Paketfirewall	Routing, IPv4/IPv6-Adressierung, IP-Filterung
2	Bridge, Switch, Access Point, Netzwerkadapter	Switching, MAC-Adressierung. Daten werden zur Übertragung in Frames (Datagramme) gepackt.
1	Repeater, Hub, Medienkonverter	Signalregenerierung, Autonegotiation, Autosensing

Sie können Netzwerkkomponenten unterschiedlicher Hersteller miteinander kombinieren. Bei den genormten Standardfunktionen der verwendeten Protokolle sind sie untereinander vollständig kompatibel. Einige Hersteller haben jedoch zusätzliche proprietäre Erweiterungen implementiert, um sich im Netzwerkmarkt abzugrenzen.

Deshalb sollten Sie vor Einsatz prüfen, ob die Netzwerkkomponenten in Ihrer Netzwerkinfrastruktur zusätzliche Funktionen beinhalten, die sie weiter benutzen möchten. Des Weiteren sollten Sie darauf achten, wie sich proprietäre Funktionen bei der Erweiterung Ihres Netzwerkes auswirken können. Dadurch stellt sich die Frage, ob man ein **homogenes Netzwerk** (alle Komponenten von einem Hersteller) oder ein **heterogenes Netzwerk** (Komponenten von verschiedenen Herstellern) aufbaut.

Den ersten Punkt sollten Sie in Betracht ziehen, wenn Sie Netzwerke konzipieren und einen einheitlichen Standard für die Wartung und das Management bevorzugen. Der zweite Punkt findet Anwendung, sofern Sie in Teilbereichen Ihres Netzwerkes besondere (manchmal nicht standardkonforme) Lösungen benötigen.

13.2 Repeater und Hub (Schicht 1)

Repeater

Ein **Repeater** verbindet physikalische Medien (auf Layer 1 des OSI-Referenzmodells), um die vorgegebenen Längenbeschränkungen des Mediums zu erweitern. Er verstärkt dabei die ankommenden Signale am Ausgangsport auf das erforderliche (ursprüngliche) Signalniveau. Er ist ein **Signalregenerator** zwischen Ein- und Ausgangsport. Repeater werden auch als **Link Extender** bezeichnet. Sie sind in Einzelfällen, z. B. für die Überbrückung von Längenrestriktionen, durchaus noch gebräuchlich.

Verbindet ein Repeater unterschiedliche Medien (z. B. Twisted-Pair-Kabel mit Lichtwellenleitern), spricht man von einem **Medienkonverter**.

Hub (veraltet)

Ein **Hub** (englisch für „Nabe“, „Mittelpunkt“) ist ein zentraler Verteiler, basierend auf einer klassischen Bus-Topologie. Er wird auch als Kabelkonzentrator bezeichnet. Ein Hub arbeitet wie ein Repeater auf der Schicht 1 des OSI-Modells und wird deshalb auch **Multiportrepeater** genannt. Er ist für andere Systeme vollkommen transparent. Die einzelnen Endgeräte werden mit jeweils einem eigenen Kabel an den Hub angeschlossen. Eine solche Anschlussstelle wird als **Port** bezeichnet.



8-Port-Hub

- ✓ Ein derartiger Port hat allerdings nichts mit den Ports zu tun, die bei Transportprotokollen (TCP, UDP) Verwendung finden.
- ✓ Hubs finden in aktuellen Netzwerken keine Anwendung mehr, da sie vollständig durch Switches ersetzt wurden. Zudem müssen sich bei Hubs alle angeschlossenen Geräte die verfügbare Bandbreite teilen; es handelt sich bei dieser Art des Transportmediums um ein **Shared Media**, wie auch bei Funknetzen, z. B. bei WLAN, UMTS, LTE ...

OSI-Einordnung und Beschreibung

Repeater und Hubs arbeiten auf der Schicht 1 des OSI-Modells, d. h., sie regenerieren nur die Bitströme, die über die Medien gesendet werden, haben aber keinen Einblick in den Inhalt der Informationen. Repeater und Hubs können deshalb nicht als Koppelement zwischen Ethernet- und Fast Ethernet verwendet werden (ausgenommen von dieser Regel sind Dual-Speed-Hubs).

Die Segmente von Repeatern und Hubs bilden eine sogenannte Kollisionsdomäne, d. h., Kollisionen auf dem Medium wirken sich auf jeden angeschlossenen Ausgangsport aus. Es können bei hoher Last derart viele Kollisionen auftreten, dass die Übertragungsrate komplett zusammenbricht.

13.3 Bridge (Schicht 2)

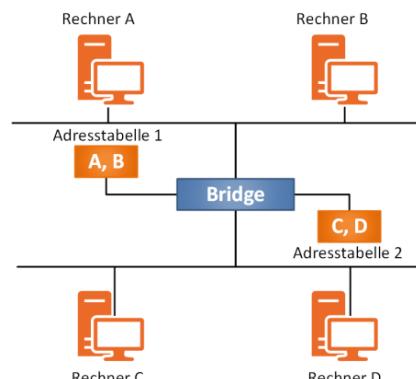
Definition

Eine **Bridge** verbindet lokale Netzwerk-Segmente miteinander. Sie verfügt über zwei Ports und arbeitet auf der Schicht 2 des OSI-Modells. Dabei leitet sie die Frames anhand der MAC-Adresse Informationen weiter.

Durch die Einordnung auf der Schicht 2 ist eine Bridge für höhere Protokollsichten transparent. Das bedeutet, dass sämtliche Protokolle, die auf Schicht 2 aufsetzen, von der Bridge unbearbeitet weitergeleitet werden. Im Unterschied zu Repeater oder Hub kann eine Bridge unterschiedliche Übertragungsraten und unterschiedliche Zugriffsverfahren auf den Ports umsetzen.

! Eine Bridge kann die Übertragung von Broadcasts- oder Multicast-Paketen **nicht** auf ein Netzwerk-Segment begrenzen, d. h., alle Stationen, die an einer Bridge angeschlossen sind, bilden eine Broadcastdomäne.

Durch Zwischenspeichern und Aufbereiten der Frames erhöht eine Bridge die Latenzzeit (Verzögerungszeit) im Netzwerk. Durch geeignete Verschaltung der Leitungen werden Segmente gebildet, in der sich möglichst die Systeme befinden sollten, die regelmäßig miteinander kommunizieren, z. B. könnten alle Rechner einer Arbeitsgruppe in einem eigenen Segment zusammengefasst werden, während andere Rechner, auf die von dieser Gruppe selten zugegriffen wird, in einem anderen Segment liegen.



Segmentierung mit einer Bridge

Arbeitsweise

Eine Bridge transportiert Datenframes anhand ihrer **MAC-Adressen** zwischen den angeschlossenen Segmenten. In der Abbildung oben rechts sieht man die Aufteilung eines Netzwerkes in zwei Segmente (eines mit Rechner A und B und ein weiteres mit Rechner C und D).

Die MAC-Adresse bzw. die Ethernet-Adresse ist die Adresse der Netzwerk-Schnittstelle (vgl. Kapitel 11). Für diese Aufgabe verwaltet die Bridge für jeden Port Adresstabellen (**Forwarding Database, FDB**), in denen die MAC-Adressen der angeschlossenen Stationen eingetragen sind. In den Segmenten sind theoretisch so viele Stationen möglich, wie viele MAC-Adressen die Bridge für den entsprechenden Port speichern kann. In der Praxis wird allerdings kaum noch eine Bridge verwendet, da ein Switch (vgl. Kapitel 13.4) flexibler ist.

Learning Bridge

Als „**Learning Bridge**“ wird eine Bridge bezeichnet, die ihre Adresstabellen automatisch aufbaut und während des Betriebs selbstständig aktualisiert. Die Bridge lernt die Adressen durch Mitlesen der Absenderadressen (Quell- oder Source-Adresse) aller ankommenden Frames und ordnet diese dem entsprechenden Port zu.

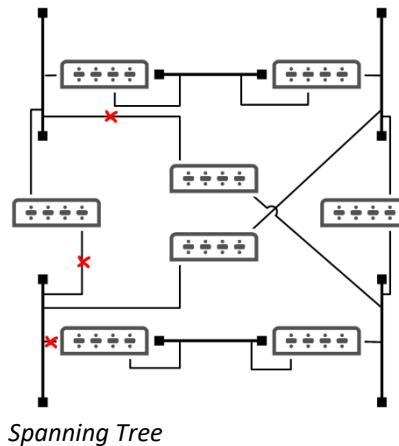
Mit diesen Adresstabellen trägt eine Bridge dazu bei, den Netzverkehr zwischen den einzelnen Segmenten zu reduzieren. Eine Bridge unterscheidet zwischen lokalem Verkehr in einem Segment und Verkehr von einem zum anderen Segment. Nachrichten, die für eine Station im gleichen Segment bestimmt sind, werden damit nicht in das andere Segment übertragen. Sie trägt zur Entlastung des Gesamtnetzes bei.

Spanning-Tree-Algorithmus

Bei Bridges wird sehr häufig das **Spanning-Tree-Protokoll (STP)** eingesetzt. **Spanning Tree** ist ein Verfahren zur Unterdrückung von Schleifen in Netzwerken, die sich ergeben, wenn redundante Wege zu gleichen Netzwerkzielen existieren. Dies ist oft beabsichtigt, um alternative Wege für den Fall des Ausfalls einer Bridge vorzuhalten.

Gibt es mehrere Wege zwischen Sender und Empfänger, können Frames, wie in einer Schleife (**Loop**), immer wieder von einer Bridge zur nächsten weitergereicht werden. Dieses x-malige Weiterreichen führt dazu, dass das Netz durch Überlastung zum Stillstand kommt.

Spanning Tree legt in einem Netz einen **eindeutigen** Weg zwischen Sender und Empfänger über Bridges fest und blockiert redundante Verbindungen innerhalb des Normalbetriebs. Dadurch sind die MAC-Adressentabellen auf jeder Bridge eindeutig und es können keine Loops mehr entstehen. Fällt die aktive Verbindung zwischen den Bridges aus, schaltet Spanning Tree eine blockierte Leitung frei, um den alternativen Pfad zu verwenden.



Dieses Protokoll findet auch bei Switches Anwendung. Neben dem Protokoll Spanning Tree (IEEE 802.1D) gibt es die beschleunigten Versionen Rapid Spanning Tree (IEEE 802.1W) und Multiple Spanning Tree (IEEE 802.1S).

Beim **Meshing** (nach IEEE 802.1aq) definieren geeignete Switches dennoch Schleifen zur Redundanz und für höhere Übertragungsraten. Ein Beispiel ist die Topologie Maschennetz.

13.4 Switch (Schicht 2)

Definition

Ein **Switch** (engl. für „Schalter“) ist quasi eine Multiport-Bridge, welche die Vorteile einer Bridge auf mehrere Ports überträgt. Er arbeitet ebenfalls auf der Schicht 2 des OSI-Modells. Durch Schalten („switchen“) von Verbindungen ist es für miteinander kommunizierende Geräte so, als ob sie direkt miteinander verbunden wären.



Desktop-Switch

Per **Kaskadierung** lässt sich mit Switchen eine Vergrößerung der Gesamtportanzahl ermöglichen. Dabei bilden diese Verbindungen einen Flaschenhals für den Datenverkehr, und die Latenzzeit erhöht sich. Dieses Problem wird mit **Stacking** gelöst (vgl. Kapitel 12.4). Vor allem bei einer Kaskadierung können sehr viele Geräte miteinander verbunden sein, daher verfügen bereits einfache Desktop-Switches über internen Speicherplatz für 1000 und mehr MAC-Adressen.



19"-Switches: Managed ①, Unmanaged ② und Webinterface des Managed Switches ③

Sogenannte **Managed Switches** können konfiguriert werden (meist per Webinterface). Desktop-Switches sind in der Regel unmanaged und damit nicht konfigurierbar, aber dafür sofort einsetzbar. Managed Switches benötigen eine eigene IP-Adresse zur Konfiguration.

Arbeitsweise

Damit ein Switch schnell die Frames zwischen den Ports vermitteln kann, muss er über eine interne Verdrahtung (**Backplane**) mit sehr hoher Geschwindigkeit verfügen. Je nach Gerät werden hier mittlerweile interne Übertragungsraten von 100 Gbit/s oder mehr realisiert, womit problemlos mehrere Ports, die mit 100 Mbit/s, 1 Gbit/s oder 10 Gbit/s arbeiten, gleichzeitig bedient werden können.

Ein Switch kann im Prinzip mit einer Telefonanlage verglichen werden, bei der zeitlich begrenzt zwischen kommunizierenden Telefonen eine exklusive Verbindung besteht. Die für diese Verbindung benutzten Ports können so mit ihrer maximalen Geschwindigkeit arbeiten.

Bei **serverbasierten Netzwerken**, bei denen nahezu alle Arbeitsstationen Daten vom gleichen Server benötigen, ist dies für die Verbindung zum Server nicht mehr der Fall. Kollisionen werden dabei durch die Flusskontrolle der Übertragung vermieden.

Es kann immer nur **ein** Frame auf denselben Leitungs-Adern in einer Richtung zur gleichen Zeit übertragen werden. Bei Duplex-Verbindungen gilt dies gleichermaßen für jede der beiden Richtungen. Bei Switches spielt heute Halbduplex und damit auch CSMA/CD keine Rolle mehr.

Flusskontrolle der Übertragung

Im Duplexmodus wird durch **Pause-Frames** den sendewilligen Geräten signalisiert, eine Pause per **Flow-Control** nach IEEE 802.3x einzulegen, falls der Port mit der Leitung zum Empfänger bereits mit der Übertragung von einem anderen Frame belegt ist. Ein Zusammenbruch der Übertragungsrate bei hoher Auslastung, wie dies bei Hubs der Fall sein kann, ist dann nicht möglich.

Ob ein Download ein paar Sekunden mehr oder weniger dauert, stellt heute kein Problem dar. Dagegen gibt es vor allem bei Sprachübertragungen (wie bei VoIP, Voice over IP) strikte Anforderungen an die Verzögerungszeit (Latenz), damit eine gute Verständigung möglich ist. Solche Pakete sollten daher in einem Netzwerk bevorzugt (priorisiert) werden.

Bei **Priority Flow Control (PFC)** nach IEEE 802.1p von 1998, bzw. Priority based Flow Control nach IEEE 802.1Qbb ab 2008) wird auf OSI-Layer 2 von einem Switch ein 3 Bit großes Feld (**PCP, Priority Code Point**) in das 4 Byte lange **VLAN-Tag** des Ethernet-Frames eingefügt. Es können Prioritätswerte von 0 (niedrigste) bis 7 (höchste) für die **Quality of Service (QoS)** definiert werden. Sie werden allerdings nur von Switches ausgewertet, die VLAN-fähig sind und das PCP-Feld lesen. Etliche Switches haben die Funktion **Auto-VoIP**, mit der sie automatisch VoIP-Pakete erkennen und passende VLAN-Tags generieren.

Prioritäten können auch von Einträgen im IP-Header auf **Layer 3** stammen, die dort als **Differentiated Service Codepoint (DSCP)-Flag** bzw. **Type of Service (ToS)** bekannt sind. Diese Einstellungen bleiben auf dem gesamten Weg bis zum Empfänger erhalten. Ein derartiger Switch (**Layer-3-Switch** bzw. **Smart-Switch** genannt) kann daher Ethernet-Frames bis zum IP-Header auf Layer 3 auspacken, um die eingebetteten Information auszuwerten.

Bei einer weiteren Art der Flusskontrolle, dem **Traffic Shaping**, wird in das Bandbreiten-Management eingegriffen. Nach bestimmten Kriterien erfolgt hier die Steuerung des Datenflusses, indem z. B. ACK-Pakete (Acknowledge- bzw. Bestätigungs-Pakete) bevorzugt behandelt sowie bestimmte Protokolle bei hoher Übertragungsrate zur Stau-Vermeidung verzögert werden.

Mit **Traffic Shaping** beschleunigt sich die gesamte Übertragung, und damit verbessern sich auch Verbindungen von sensiblen Anwendungen wie VoIP. Etliche Managed Switches und DSL-Router (z. B. viele Fritz!Boxen) verwenden diese Technik, die auf VLAN-Tags verzichtet.

Die verschiedenen Modi der Weiterleitung

Sowohl bei einem Switch als auch bei einer Bridge haben sich grundsätzlich folgende drei Verfahren etabliert, wobei die Ports zwischen den Verfahren nach Bedarf umschalten können. Dies hängt von den angeschlossenen Stationen und der Ausstattung der Komponente ab.

Cut-Through

Beim **Fast-Forward-Modus** beginnt der Switch sofort mit dem Weiterleiten (Forward) der Daten zur Ziel-MAC-Adresse, nachdem er die Zieladresse gelesen hat. Diese befindet sich am Anfang des Ethernet-Frames.

Beim **Fragment-Free-Modus** prüft der Switch erst, ob der Frame die minimale Länge von 64 Byte hat, indem er die ersten 64 Bytes liest. Erst danach leitet er den Frame weiter (Forward). Kürzere Frames verwirft er.

In beiden Modi von **Cut-Through** müssen die Ports gleiche Übertragungsraten und Übertragungsmedien haben. Andernfalls weicht der Switch auf **Store-and-Forward** aus (wie z. B. beim Übergang von Twisted-Pair auf Glasfaser).

Der Nachteil dieser beiden Modi ist, dass bei der Übertragung nicht auf fehlerhafte oder unvollständige Frames geprüft wird. Dafür ist die Geschwindigkeit höher als im Store-and-Forward-Modus.

Store-and-Forward

Bei diesem Modus **speichert** der Switch den Frame vollständig zwischen, bevor er ihn zum Zielport weiterschickt. **Store-and-Forward** muss verwendet werden, wenn zwischen Quell- und Zielport unterschiedliche Übertragungsraten verwendet werden, z. B. von 1 Gbit/s nach 100 Mbit/s. Beim Zwischenspeichern überprüft der Switch die Daten auf Fehler anhand der im Ethernetframe vorhandenen FCS-Prüfsumme. Somit werden fehlerhafte Frames nicht weitergeleitet, was jedoch eine längere Latenzzeit zur Folge hat.

Der Store-and-Forward-Modus ist der kleinste gemeinsame Nenner aller Switches, allerdings auch der langsamste.

Error-Free-Cut-Through

Dies ist eine Mischform aus den vorgenannten Modi, zwischen denen der Switch je nach Qualität der Datenübertragung (Fehlerrate etc.) wechselt kann. Somit können je nach Situation die Vorteile aller oben genannten Modi kombiniert werden. Diesen Modus nennt man auch **Adaptive Switching**.

Interne Switcharchitektur

Auch bei der internen Behandlung der Frames gibt es bei Switches unterschiedliche Methoden. So bestehen bei einem **Cross-Bar-Switch** dedizierte Verbindungen zwischen allen Ports, was einen maximalen Datendurchsatz garantiert. Sobald der Weg zwischen Quelle und Ziel bekannt ist, werden die Daten über die entsprechende Verbindung weitergeleitet, ohne von anderem Datenverkehr behindert oder blockiert zu werden. Ein Nachteil dieser Methode liegt in der schlechteren Skalierbarkeit bei steigender Portzahl.

Beim **Cell-Backplane-Switch** kommunizieren alle Ports über einen schnellen internen Bus. Der Switch zerlegt die Frames in kleinere Zellen und fügt jeder Zelle einen Header mit der Adresse des Zielports hinzu. Dort werden die Zellen zwischengespeichert, zum Ausgangsframe zusammengesetzt und endgültig an das Ziel weitergeleitet.

Zusammenfassung

Hier zusammengefasst die wichtigsten Vorteile von Switches allgemein:

- ✓ Ein Zusammenbruch der Übertragungsrate bei hoher Auslastung ist nicht möglich.
- ✓ Es ist eine höhere gesamte Übertragungsrate durch Vollduplex erreichbar.
- ✓ An jedem Port kommen nur die Daten an, die für das angeschlossene Gerät bestimmt sind.
- ✓ Geräte mit unterschiedlichen Übertragungsraten sind anschließbar.

Managed Switches ermöglichen weitere Funktionen, wie zum Beispiel:

- ✓ die Aufteilung eines Netzwerkes in VLANs (siehe Kapitel 12.4),
- ✓ eine priorisierte Übertragung per PFC bzw. Layer-3-basierte Priorisierung (DSCP),
- ✓ eine Portbündelung über **LACP** zur Erhöhung der Übertragungsrate (siehe Kapitel 14.2),
- ✓ die Einspeisung einer Versorgungsspannung (Power over Ethernet (**PoE**)) für angeschlossene Geräte,
- ✓ eine Authentifizierung des Netzwerkzugangs nach **RADIUS 802.1x** (siehe Kapitel 4.5),
- ✓ eine Überwachung und Administration per **SNMP** (siehe Kapitel 15.1),
- ✓ die Überwachung des Datenverkehrs auf einzelnen Ports durch **Port-Mirroring** (siehe Kapitel 15.2),
- ✓ eine Skalierung durch **Uplinkports** und **Stacking** (siehe Kapitel 12.4).



Der größte Nachteil eines Switchs soll dabei nicht verschwiegen werden: Fällt ein Switch aus, ist in dem von ihm abgedeckten Netzsegment keine weitere Übertragung mehr möglich. Bei wichtigen Netzwerken werden daher mehrere Server und Switches zur Ausfallsicherheit bereitgestellt.

Ein weiterer Nachteil ist, dass das Umstecken eines bereits angeschlossenen Gerätes von einem Port an einen anderen eine gewisse Zeit lang dieses Gerät nicht erreichbar werden lässt. Der Switch spricht dieses Gerät so lange an dem alten Port an, bis die Position der MAC-Adressen neu erlernt ist.

Weitere Entwicklungen

Etliche Hersteller bieten Hochleistungs-Switches an, die nicht nur auf der Schicht 2 des OSI-Modells arbeiten, wie dies bei einem klassischen Switch der Fall ist, sondern auf Schicht 3 und höher, d. h., dass sie für die Entscheidung über die Paketweiterleitung Informationen der höheren Schichten berücksichtigen. Hier handelt es sich um **Multilayer-Switches**.

Layer-3-Switching

In einem Netzwerk ohne Priority Flow Control sind prioritätsgesteuerte Übertragungen nur dann auf Layer 2 möglich, wenn der Switch nicht nur die ankommenden Frames weiterleitet, sondern zusätzlich auf Layer 3 die IP-Header analysiert und sie auf **ToS**-Attribute bzw. das **DSCP**-Flag untersucht (siehe „Flusskontrolle“ weiter oben). Von daher kommt der Ausdruck Layer-3-Switch.

Routing kommt erst dann hinzu, wenn ein zusätzliches Routermodul in ein derartiges Gerät eingebaut ist. In diesem Fall handelt es sich um ein Multifunktionsgerät. Ein Switch allein verbindet keine unterschiedlichen Netzwerke. Dennoch wird der Ausdruck „**Layer-3-Switch**“ oft fälschlicherweise als Synonym für Router benutzt.

Andere Argumente für die Weiterentwicklung waren die Segmenttrennung (VLAN-Bildung auf Basis von Layer-3-Merkmalen) und das Schaffen von Redundanz ohne das **Spanning-Tree-Protokoll (STP)**.

Layer-4-Switching

Auf der Schicht 4 des OSI-Modells sind die Portnummern angesiedelt (vgl. Kapitel 11.2). Beim Layer-4-Switching stehen somit die Paket-Informationen der Schicht 4 zur Verfügung, sodass z. B. ein Administrator über Zugriffsregeln (**Access Control List (ACL)**) festlegen kann, welcher Verkehr vom Switch behandelt wird. Der Switch kann damit, abhängig von der Anwendung (deren Portnummer), eine Entscheidung über den Weitertransport eines Datenpaketes treffen und damit Datenverkehr filtern oder priorisieren. Damit können Sie eine einfache Paketfirewall einrichten.

Layer-7-Switching

Switches, die bis hinauf zur Schicht 7 arbeiten, können neben der Portnummer weitere Angaben, wie z. B. eine Web-Adresse, für die Steuerung des Datenverkehrs nutzen. Insbesondere auf dem Gebiet der Bereitstellung von Daten für Webanfragen werden solche Geräte eingesetzt.

Sie dienen im Rahmen von Serverfarmen dazu, gleichzeitige Anfragen von Tausenden von Clients per Load Balancing (Lastverteilung) auf die Server zu verteilen. Häufig finden sich daher für Layer-7-Switches auch die Begriffe Load-Balancer, Web-Switches oder Content-Switches.

13.5 Router (Schicht 3)

Definition

Ein **Router** ist ein Gerät, das getrennte Netzwerke mit unterschiedlichen Adressräumen oder verschiedenen Netzwerktechnologien koppelt oder Netzwerke in **Subnetze** aufteilen kann. Diese Kopplung kann eine Verbindung zwischen zwei oder mehr lokalen Netzen oder die Verbindung zwischen LAN und WAN bzw. WAN und WAN sein. Die wesentliche Funktion ist die „**Vermittlung**“, oder anders gesagt, die Kenntnis der verschiedenen Netze und der Wege zu diesen Netzen.

Einordnung und Arbeitsweise

Die einfachste Form eines Routers ist ein PC mit mehreren Netzwerkadapters, die jeweils Kontakt zu unterschiedlichen Netzwerken haben. Die Funktion „**IP Forwarding**“ muss dabei aktiviert sein, sonst erfolgt keine Weiterleitung der Pakete.



SOHO-Router (Vorder- und Rückseite)

Die Vielfalt an eigenständigen Geräten dieser Art reicht vom **Small Office, Home Office (SOHO)**-Router für kleinere Installationen bis hin zur Verbindung von internationalen Backbones. Besonders leistungsfähige Geräte lassen das Routing nicht von einer „langsam“ Software, sondern von Hardware in Form von **Application Specific Integrated Circuit (ASIC)**-Bausteinen durchführen. Durch das Implementieren von Routing-Entscheidungen innerhalb dieser Hardware-Chips wird der Netzwerkverkehr deutlich beschleunigt.

Router arbeiten auf der **Schicht 3** (Network/Vermittlung) des OSI-Modells. Das bedeutet, dass sie Netzwerke mit unterschiedlichen **Topologien** der darunter liegenden Schichten 1 und 2 verbinden können. Allerdings müssen alle beteiligten Netzwerke die gleiche Art der Adressierung ihrer Datenpakete verwenden, d. h. die gleichen Protokolle auf Schicht 3. Ist dies der Fall, z. B. beim Einsatz von IP-Adressen im Netzwerk, dann kann ein Router ankommende Frames bearbeiten und an ein anderes Netzwerk übergeben.

Dazu muss ein Router das IP-Paket des empfangenen Frames auf Schicht 3 auspacken, um aus dem IP-Header die IP-Adresse des Ziels zu ermitteln. Das IP-Paket selbst packt er nach der Ermittlung des weiteren Weges in einen neu erstellten Frame und schickt diesen über die entsprechende Schnittstelle in ein anderes Netzwerk weiter. Dieser Vorgang kostet Zeit, und so ist der Router im Normalfall langsamer als Switch oder Bridge.

Multiprotokollfähig

Ein wichtiges Unterscheidungskriterium von Routern ist die Frage, ob es sich bei dem Gerät um einen **Einzelprotokoll-** oder **Multiprotokoll-Router** handelt. Ein Router, der nur ein Protokoll kennt, ist lediglich in der Lage, Netzwerke mit gleichem Protokoll zu verbinden. (z. B. IPv4).

Ist der Router multiprotokollfähig, beherrscht er mehrere Protokolle, ohne diese zu vermischen (z. B. IPv4 und IPv6). Dies heißt aber nicht, dass ein Multiprotokoll-Router ein Protokoll direkt in ein anderes umwandeln kann, sondern nur, dass er in der Lage ist, unterschiedliche Protokolle weiterzuleiten.

Tunneling

Mittels Tunneling können die Datenpakete eines Protokolls in den Nutzdaten (**Payload**) eines anderen Protokolls transportiert werden. Dies wird nötig, wenn ein Netzwerk überbrückt werden muss, welches das Zielprotokoll nicht direkt transportieren kann. Am Ende der Übertragung bzw. am Ende des „Tunnels“ wird der Transportrahmen entfernt, wodurch das Paket wieder in seinen ursprünglichen Zustand gebracht wird. Ein Beispiel für solch ein Verfahren könnte der Transport von IPv6-Paketen über ein reines IPv4-Netzwerk sein. Damit können zwei IPv6-Netzwerke über ein IPv4-Netz gekoppelt werden. Beispiele für solche Verfahren sind **4in6, 6in4, Teredo**. Weitere Informationen finden Sie im Internet unter: <https://www.elektronik-kompendium.de/sites/net/1904031.htm>

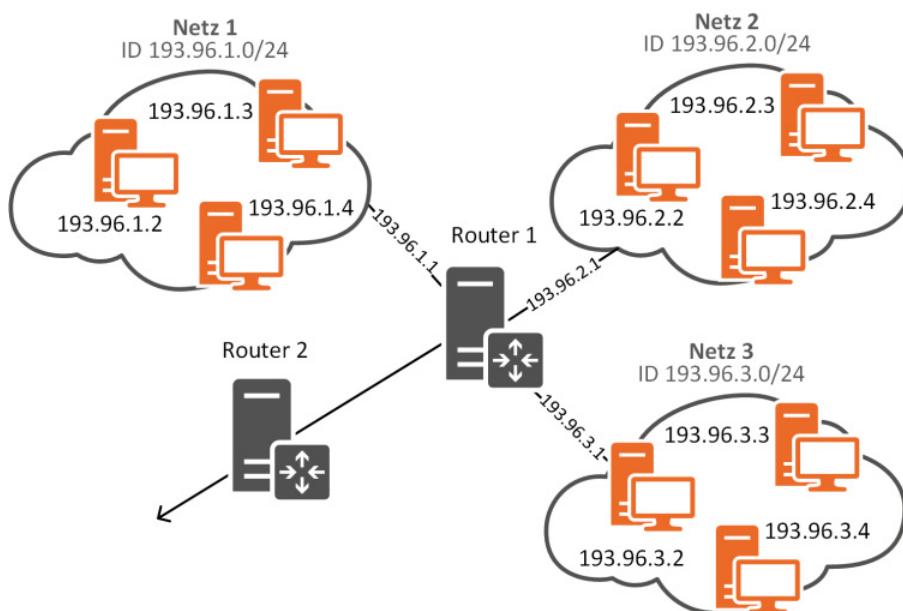
Tunneling-Protokolle ermöglichen grundsätzlich nur eine erhöhte Sicherheit während der Übertragung, wenn sie auf Tunnel-Kryptografie aufsetzen. Hierzu werden u. a. die Protokolle **Layer 2 Tunneling Protocol (L2TP) / IPsec, OpenVPN**, und weitere verwendet.

Routing-Tabellen

Die Hauptfunktion eines Routers besteht in der Pfadbestimmung (**Routing**) für IP-Pakete zum Zielnetzwerk. Dazu verwenden Router sogenannte Routing-Tabellen (eine für jedes Routing-protokoll), in denen die an dem Router direkt angeschlossenen Netzwerke (inkl. Netzmasken) und Wege zu benachbarten Netzen hinterlegt sind. Empfängt der Router ein IP-Paket und hat die geforderte Zieladresse ermittelt, muss er den weiteren Weg bestimmen.

Der Router prüft erst anhand der Einträge in den Routing-Tabellen, ob das Gerät mit der Ziel-Adresse direkt angeschlossen ist. Dann kann der Router das IP-Paket in einen neuen Frame packen und diesen **direkt** zum Ziel weiterleiten. Andernfalls wird er das Paket an einen anderen Router weiterschicken. Dieser nächste Router, der auch als „**Next Hop**“ bezeichnet wird, versucht dann auf seine Weise das Paket weiter zuzustellen. Eine wichtige Voraussetzung dafür ist, dass die **Time to live (TTL)** des Pakets noch nicht den Wert 0 erreicht hat. Bei der TTL handelt es sich um einen Zähler, der von jedem Router reduziert wird, nachdem das Routing stattgefunden hat.

In der Abbildung unten hat Router 1 direkten Kontakt zu den Netzwerken 193.96.1.0/24, 193.96.2.0/24 und 193.96.3.0/24. Wird von Rechner 193.96.1.4 ein Paket an 193.96.2.4 gesendet, kann der Router das Paket direkt ins richtige Netzwerk 193.96.2.0/24 weiterleiten, da er dieses Netzwerk kennt und dieses mit seiner Schnittstelle 192.96.2.1 verbunden ist.



Schematische Darstellung von Netzwerken mit Routern

Default-Router

Nicht jeder Router kann die Wege zu allen Netzen kennen. Die Größe der Routing-Tabelle wäre nicht mehr handhabbar, bzw. die Zeitdauer, bis jeder Router alle Wege gelernt hat, würde ein großes Problem darstellen. Daher wurde als Lösung der **Default-Router** eingeführt. Alle Pakete, für die das Zielnetz unbekannt ist, werden stets an den Default-Router weitergeleitet.

Jedes IP-fähige Gerät besitzt intern eine statische Routing-Tabelle. Dort ist in jedem Fall das eigene Netzwerk mit dessen Netzmase eingetragen. Ein Router hat entsprechend mehr Netzwerk-Einträge. Zusätzlich gibt es in der Regel einen Eintrag (die **Default-Route**) für unbekannte Wege zum Ziel. So ist im obigen Beispiel in Rechner 193.96.1.4 der Router 1 über seine hier passende IP-Adresse 193.96.1.1 als Default-Router eingetragen. Ohne Default-Route wäre keine Verbindung mit dem Internet nicht möglich.

Alle Einträge von den direkt angeschlossenen Netzwerken schreibt das Betriebssystem (des Routers) während der Konfiguration der Netzwerkeinstellungen in seine Routing-Tabelle. Alle weiteren Einträge müssen beim **statischen** Routing manuell (z. B. vom Administrator) angelegt werden. Beim **dynamischen** Routing tauschen die Router ihre Routeninformationen miteinander aus und generieren die entsprechenden Tabellen selbst.

Wird z. B. von 193.96.1.4 ein Paket an die IP-Adresse 193.96.4.4 gesendet (und beide Adressen liegen in unterschiedlichen Netzwerken, wie dessen Protokoll-Stack anhand der Netzmasken herausfindet), dann schickt der Rechner sein Paket an Router 1. Dieser schickt es weiter an Router 2 (seinen Default-Router), da er zum gewünschten Zielnetzwerk 193.96.4.0/24 keine Verbindung hat und daher die gesuchte Zieladresse nicht kennt. Falls auch Router 2 das Zielnetzwerk nicht kennt, schickt er das Paket ebenfalls an seinen Default-Router weiter.

Ein Router trifft seine Routingentscheidung in folgender Reihenfolge:

1. Er prüft zunächst anhand der Einträge in den Routing-Tabellen und den dazugehörigen Netzmasken, ob sich die Zieladresse in einem **direkt** angeschlossenen Netzwerk befindet. Falls ja, ermittelt er die MAC-Adresse (Ethernet-Adresse) des Ziels über das Protokoll ARP und erzeugt ein Paket mit der MAC-Adresse des gewünschten Geräts.
2. Ist das Zielnetz über einen **benachbarten Router** zu erreichen, entscheidet der Router anhand seiner Metrik (Maß für die Güte einer Verbindung), welches der richtige Weg zum Ziel ist. Das kann z. B. der Weg mit der größten Bandbreite oder aber auch der Weg mit den geringsten Kosten sein. Weitere mögliche, zur Auswahl stehende Wege können durch statische Routing-Einträge vorgegeben sein oder sind Wege, die der Router mithilfe eines dynamischen Routing-Protokolls erlernt hat. Anhand dieser Wahl leitet er das IP-Paket zum nächsten passenden Router (Next Hop), indem er es in einem neuen Frame an dessen MAC-Adresse schickt.
3. Gibt es weder einen passenden Eintrag in der statischen noch in einer dynamischen Routing-Tabelle, ist der Weg zum Ziel unbekannt. In diesem Fall leitet der Router das IP-Paket an die MAC-Adresse des Routers, der als **Default-Router** (auch Gateway of Last Resort genannt) eingetragen ist. Dieser kümmert sich um die weitere Zustellung.
4. Findet er in der genannten Reihenfolge keinen verwertbaren Eintrag, so **verwirft** er das Paket und sendet die Nachricht „Zielnetz nicht erreichbar“ an den Absender.

Das Erstellen einer statischen Route zum Zielnetz (z. B. mit dem Befehl `route add <Zielnetz> mask <Ziel-Maske> <Next-Hop-Router>`) ist nur dann sinnvoll, wenn wenige Netze geroutet werden und damit die Anzahl der möglichen Routen überschaubar ist. Werden jedoch viele Netze geroutet und gibt es hierzu noch redundante Wege, ist dies nicht mehr praktikabel.

Unter IPv6 unterstützen Router die Netzwerk-Konfiguration. Sie verschicken dazu **Router-Advertisements** (Ankündigungen), die angeschlossene Hosts darüber informieren, in welchem Netzwerk sie sich befinden, welche Art der Autokonfiguration es gibt und wie sie passende Router finden. Die Informationen können von den Rechnern auch per Router-Solicitation („Ersuchen“) abgerufen werden. Siehe auch HERDT-Buch *Netzwerke – IPv6*.

Dynamische Routingprotokolle

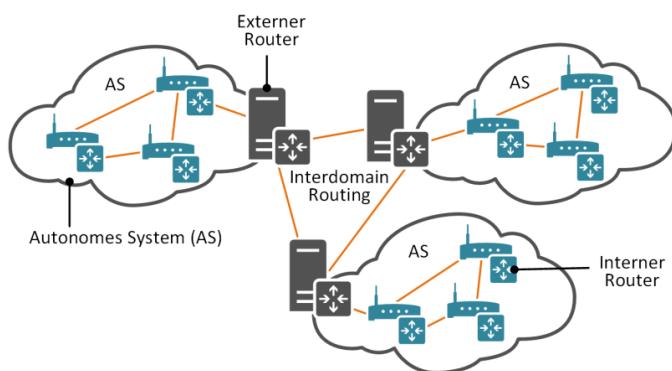
Eine Alternative zur statischen Konfiguration von Routern schaffen dynamische Routingprotokolle, mit deren Hilfe Router benachbarte Netzwerke kennen lernen. Die Entscheidung, welcher Weg in das Zielnetz gewählt wird, trifft der Router auf Basis mathematischer Verfahren. Das Ergebnis könnte die Wegewahl auf Basis der kürzesten Verbindung, der aktuellen Lastsituation oder der günstigsten Verbindungskosten sein.

Interne/externe dynamische Routingprotokolle

Interne Routingprotokolle werden ausschließlich im Intranet, also im LAN selbst bzw. innerhalb von Autonomen Systemen, eingesetzt. Typische Vertreter sind die Standardprotokolle **Routing Information Protocol (RIP)** und **Open Shortest Path First (OSPF)**. Externe Routingprotokolle finden Anwendung im WAN, also im Internet und zwischen Autonomen Systemen. Ein Beispiel hierfür ist das **Border Gateway Protocol (BGP)**, obwohl auch OSPF hierfür geeignet ist.

Autonomes System

Würde jeder Router alle verfügbaren Netze lernen, so käme er schnell an seine Grenzen. Aus diesem Grunde hat man Autonome Systeme (**AS**) eingeführt. Ein Router in einem AS erkennt nur seine Nachbarnetze.



Der Vorteil von AS besteht darin, dass die internen Router nur einen Teil der Netze kennen müssen und demzufolge ihre Routingentscheidung effizienter treffen können. **Externe Router** (auch **Border-Router** genannt) übernehmen die Vermittlung zwischen den AS. Vorrangig vernetzen sich ISP auf diese Weise (**Interdomain Routing**).

RIP

RIP war das erste dynamische Standardprotokoll. Es arbeitet nach dem Distanz-Vektor-Algorithmus, d. h., die Wegewahl wird anhand der geringsten Anzahl der Router (Hops) zwischen Quell- und Zielnetz getroffen. Dazu versucht jeder Router seine Routinginformationen im 30-Sekunden-Takt an seine Nachbarn.

Auf diese Weise ergänzen Router ihre Routingtabelle mit Pfaden zu entfernten Netzwerken. Als Weiterleitungsziel wird der benachbarte Router verwendet, der über die kürzeste Strecke (Anzahl der Hops) zum Ziel verfügt. Im Verlauf des Informationsaustauschs lernt jeder Router die vorhandenen Wege zwischen den einzelnen Datennetzen kennen. Die maximale Anzahl von Hops, die RIP unterstützt, beträgt 15. Die aktuellen Versionen sind **RIPv2** (RFC 2453) bzw. bei der Nutzung des IPv6-Protokolls **RIPng** (RFC 2080).

OSPF

Das Protokoll **Open Shortest Path First (OSPF)** ist ebenfalls ein dynamisches Routing-Protokoll und basiert auf der Link State Database. In dieser Datenbank sind alle benachbarten Router bzw. deren Link-Status enthalten, für die Aktualisierung der Datenbank der Router untereinander sind feste Regeln definiert.

Das OSPF-Protokoll berechnet die Güte eines Weges zu einem benachbarten Router anhand der Leitungskosten, d. h., je höher die verfügbare Bandbreite der Hops zwischen Quell- und Zielnetz ist, desto geringer sind die Kosten und desto günstiger ist der Weg dorthin.

Nach dem erstmaligen Austausch der kompletten Routing-Tabelle werden im Gegensatz zu RIP nur kleine Hello-Pakete miteinander ausgetauscht. Diese signalisieren, dass es keine weiteren Änderungen in den Routing-Tabellen gibt. Treten Änderungen in Routing-Tabellen auf, z. B. bei Nichterreichbarkeit eines Netzes, werden diese sofort an die benachbarten Hops weitergegeben. Alle 30 Minuten wird die komplette Tabelle mit den Nachbarn ausgetauscht.

Alle Router, die Routing-Tabellen miteinander austauschen, müssen sich in einem Autonomen System (siehe auch https://de.wikipedia.org/wiki/Autonomes_System) befinden. Zwischen den Autonomen Systemen vermittelt ein **Border-Router**.

OSPF wurde der von IETF entwickelt und ist in der Version 2 im RFC 2328 beschrieben. Die Version 3 ist für die dynamischen Routen von IPv6-Protokollen in der RFC 2740 definiert.

BGP

Das **Border Gateway Protocol (BGP)** nutzt den Path-Vektor-Algorithmus, der ähnlich dem Distanz-Vektor-Algorithmus arbeitet. Jedoch können hierbei keine Routingschleifen auftreten. Es kann sowohl innerhalb eines Autonomen Systems als **iBGP** (internal BGP) als auch zwischen AS als **eBGP** (external BGP) eingesetzt werden.

BGP wurde anfangs in der RFC 1163 beschrieben. Die aktuelle Version BGPv4 bzw. BGP-4 ist in der RFC 4760 definiert. Global gilt im Internet BGP-4 als der De-Facto-Standard.

Load Balancing

Die meisten Routing-Protokolle ermöglichen ein sogenanntes Load Balancing, was bedeutet, dass alternative Wege zur Zieladresse verwendet werden können. Load Balancing heißt, dass bei zwei gleichwertigen Wegen (gleiche Metrik) die Datenströme wechselseitig auf beide Wege verteilt werden.

13.6 Firewall

Sowohl zum Schutz des lokalen Netzes (Intranet) als auch zwischen Intranet und Internet ist heute die Filterung durch eine Firewall unabdingbar. Eine Firewall kann in Abhängigkeit von ihrem Funktionsumfang ein- und ausgehenden Datenverkehr auf den Layern 2 bis 7 des OSI-Modells anhand festgelegter Regeln filtern. Dabei sind nur drei Aktionen erlaubt.

- ✓ **Allow**, der Verkehr wird über die Firewall durchgelassen.
- ✓ **Deny**, die Firewall verwirft die ankommenden Daten, wobei der Sender keine oder die Nachricht „Time Out“ bekommt.
- ✓ **Reject**, die Daten werden von der Firewall abgewiesen und der Sender erhält eine Fehlermitteilung.

Auf Basis unterschiedlicher Anforderungskriterien gibt es verschiedene Implementierungsverfahren für eine Firewall, die auf unterschiedliche OSI-Schichten zielen. Man unterscheidet zwischen:

Paketfilter

Paketfilter stellen eine einfache Variante einer Firewall dar. Hierbei wird der Header der Layer-3-Protokolle (z. B. IP-Header, ICMP-Header) bzw. der Layer-4-Protokolle (TCP-Header, UDP-Header) überprüft und in Abhängigkeit der eingestellten Filter-Regeln eine Aktion ausgelöst. Aufgrund der geringen Komplexität ergibt sich ein guter Datendurchsatz (Performance).

Nachteilig ist jedoch, dass u. a. der Missbrauch von Protokollfunktionen (z. B. Fragmentierungs-Attacken oder Buffer Overflow) möglich ist. Zudem ist eine Verschleierung durch Verwendung erlaubter Ports für auf Port x nicht erlaubte bzw. vorgesehene Anwendungen möglich, ohne dass der Paketfilter diese unerwünschten Daten herausfiltern kann.

Die meisten Router können auch als Paketfilter konfiguriert werden.

Stateful Inspection Firewall

Die Stateful Inspection Firewall wurde erstmals vom Hersteller Checkpoint vorgestellt. Sie ist eine Weiterentwicklung des Paketfilters. Zusätzlich ist sie jedoch in der Lage, sich aktuelle Status- und Kontextinformationen zu merken bzw. diese bei der Filterung zu berücksichtigen.

Damit lässt sie (wie z. B. in den meisten DSL-Routern vorhanden) nur Antwort-Pakete auf Anfragen ins Internet in das interne Netz zurück passieren, während sie alle anderen Pakete aus dem Internet blockiert. Über Ausnahmeregeln können bestimmte Verbindungen dennoch erlaubt werden. Auf diese Weise kann z. B. eine Fragmentierungs-Attacke verhindert oder ein manipulierter Verbindungsaufbau erkannt und unterbunden werden.

Durch spezielle Filterregeln kann zudem ein Schutz vor etlichen **Denial of Service (DoS-Attacken)** erreicht werden, indem die Anzahl der Verbindungsaufnahmen pro Sekunde begrenzt wird. DoS-Attacken zielen auf die Verfügbarkeit des Systems durch Überflutung mit Anfragen.

Application Level Firewalls (ALF) /Proxy-Server

Die **Application Level Firewall** arbeitet auf Layer 7 des OSI-Modells und wird zwischen Client und Server geschaltet. Sie fungiert in Richtung Client als stellvertretender Server und gegenüber dem Server als stellvertretender Client. Für jeden Dienst wird eine eigene Applikation (Proxy) benötigt. Über generische Proxys kann man jedoch einige Dienste zusammenfassen. Der Proxy überwacht den kompletten Verkehr bis zur Applikationsebene, und die vor dem Proxy liegenden Netze sind von „außen“ nicht sichtbar. Durch die hohe Komplexität hat eine ALF eine geringere System-performance.

Weitere Firewalltypen

Die folgenden Typen beinhalten die oben beschriebenen Implementierungsverfahren:

- ✓ **Transparent Firewall** – Sonderform der Stateless oder Stateful Inspection Firewall, filtert ab Layer 2 und verhält sich im Netzwerk transparent gegenüber den Kommunikationspartnern. Diese sehen in der Firewall quasi nur einen Router ohne dahinterliegendes Netzwerk.
- ✓ **Personal Firewall/Desktop Firewall** – wird nicht im Netz, sondern auf den Endsystemen als Programm/ Dienst installiert (bzw. ist bereits in das Betriebssystem integriert) und stellt eine Mischung aus Paketfilter und Stateless oder Stateful Inspection Firewall dar. Zudem können auf dem Endsystem installierte Programme von der Firewall berücksichtigt werden.
- ✓ **Application Inspection/Next Generation Firewall** – untersucht den Datenstrom auf Applikationsebene, erkennt unterschiedliche Anwendungen und kann Sicherheitsrichtlinien auf Applikations- und Nutzerebene umsetzen.
- ✓ **Unified Threat Management (UTM)** – steht für zentrale Sicherheit für das gesamte Netzwerk. Damit wird versucht, verschiedene Schutzfunktionen unter einem Dach zu vereinen. Wichtige Bestandteile davon sind ein Intrusion Detection System, Contentfilter und Virus- sowie Spam- und Surf Protection.

Das Thema **Network Address Translation (NAT)** spielt bei Firewalls eine wichtige Rolle im Bezug darauf, wie die Firewall gegenüber anderen Netzwerkteilnehmern in Erscheinung tritt.

Zu den Themen Sicherheit und Firewall bietet das HERDT-Buch *Netzwerke – Sicherheit* weiterführende Informationen.

13.7 Gateway (Schicht 7)

Vermittlung auf allen Schichten

Gateways verbinden Netzwerke mit völlig unterschiedlichen Protokollen und Adressierungen, sie stehen als Oberbegriff für die Vermittlung und Umwandlung auf allen 7 Schichten des OSI-Modells.

Ein Gateway kann damit inkompatible Netze miteinander verbinden und im Extremfall eine ankommende Nachricht bis auf Schicht 7 entpacken, um sie dann für das andere Netz passend wieder bis auf Schicht 1 zu verpacken. Ein Gateway wandelt also real ein Protokoll in ein anderes um.

Der Begriff Gateway wird teilweise auch als Synonym für Router verwendet.

13.8 Multifunktionsgeräte

Viele Geräte enthalten mehrere Komponenten. So besteht ein DSL-Router intern nicht nur aus einem DSL-Modem und einem Router. Dieses Gerät enthält noch etliche weitere Funktionen, wie Switch, Access Point für WLAN, evtl. eine Telefonanlage mit DECT-Basis, Druckserver, USB-Anschluss, sowie Funktionen wie Media-Server, DNS-, DHCP-Server und etliches mehr.

Man spricht in diesem Zusammenhang von Multifunktionsgeräten (siehe Bild rechts). Ein derartiges Gerät kann auch als Gateway (zum Internet) angesehen werden.



DSL-Router mit Access Point und Switch mit 4 LAN-Ports

13.9 Übung

Fragen zu Netzwerkkomponenten

Übungsdatei: --

Ergebnisdatei: uebung13-E.pdf

1. Sie testen über Fast Ethernet einmal mit einem Hub und einmal mit einem Switch, wie lange die Übertragung einer sehr großen Datei dauert. Welches Gerät überträgt sie schneller?
2. Sie stecken ein Gerät, welches an einem Switch angeschlossen ist, an einen anderen Port um. Wird es ein Problem geben und wenn ja, welches?
3. Sie verbinden mehrere Switches in Ihrem Netzwerk so, dass unbeabsichtigt der erste Switch wieder mit dem letzten verbunden ist (Loop). Welches Ergebnis wird sich zeigen?
4. Die Anzahl der Ports von Ihrem Switch reicht nicht mehr. Welche Abhilfe gibt es?
5. Wie verhindert ein Switch Kollisionen?
6. In Ihrem DSL-Router sehen Sie eine Möglichkeit zur Priorisierung. Was verbirgt sich in der Regel dahinter?
7. Wodurch kann ein Rechner ein Router werden?
8. Auf welches Netzwerk (unter IPv4 und IPv6) zeigt die Default-Route und warum?
9. Erklären Sie den Unterschied zwischen statischem und dynamischem Routing sowie deren Anwendungsbereiche.
10. Was ist der besondere Vorteil von einer Stateful Inspection Firewall?

14

Erweiterung der Geschwindigkeit

14.1 Gigabit-Ethernet

Standards beibehalten

Ethernet ist inzwischen die dominierende LAN-Technologie, weil es damit gelungen ist, Standards zu schaffen. Viele Administratoren und Netzbetreiber wünschen sich das Ethernet unter Beibehaltung möglichst vieler bestehender Standards schneller zu machen. Ein Ziel bei der Entwicklung ist es, nur die Netzwerkadapter oder Switches unter Beibehaltung der Verkabelung und der Protokolle austauschen zu müssen. Ausgehend vom 1-GBit-Netzwerk als aktuellem Standard sollen sich neue Technologien problemlos und mit minimalem Aufwand für die Administratoren in bestehende Strukturen einbinden lassen.

Normierung

Der große Nachteil ist, dass es in der Praxis nicht einfach ist, auf den bestehenden Kabeln, und hier vor allem bei Kupferkabeln, diese Geschwindigkeitssteigerung bei den gegebenen Eigenschaften des Kabels umzusetzen. Deshalb wurden folgende neuen Arbeitsgruppen des IEEE ins Leben gerufen:

Standard	Bezeichnung	Kabeltyp	Längenbegrenzung
IEEE 802.3 Clause 38	1000Base-SX	Multimode-Lichtwellenleiter Laser mit 850 nm (short wavelength)	Zwischen 220 und 550 m, je nach Glasfaser und Bandbreite
IEEE 802.3 Clause 38	1000Base-LX	Multi- und Monomode-Lichtwellenleiter Laser mit 1270-1355 nm (long wavelength)	Bis zu 550 m bei Multimode, bis zu 5000 m bei Monomode
Kein IEEE Standard	1000Base-ZX	Monomode-Lichtwellenleiter Laser mit 1550 nm	Bis zu 70 km, mit dispersionskompensierter Faser bis 100 km
IEEE 802.3 Clause 39	1000Base-CX	STP-Kabel mit 150 Ohm, Kategorie 6/7	25 m
IEEE 802.3 Clause 40	1000Base-T	UTP-Kabel mit 100 Ohm, Kategorie 5	100 m

Die Normen für Gigabit-Ethernet wurden anfänglich unter der Bezeichnung 802.3z (Gigabit-Ethernet STP/ LWL) und 802.3ab (1000Base-T CAT5 UTP) geführt. Inzwischen ist die Normung umfangreich in Klauseln (Clauses) überführt worden.

Problematik

Bei der Verwendung von Glasfaserkabeln gibt es selten Probleme, benötigte Reichweiten bereitzustellen. Allerdings werden spezielle Patchkabel benötigt, und bei Multimode-Fasern ist die Länge auf 550 m beschränkt.

Der Einsatz von Kupferkabeln (STP, 150 Ohm) dagegen ist mit seiner Einschränkung auf 25 m keine Lösung, und so spielt 1000Base-CX in der Praxis auch keine Rolle. Bei 1000Base-T ist erwähnenswert, dass alle acht Adern verwendet werden und so kein cable-sharing mehr möglich ist. Darunter versteht man den parallelen Betrieb von zwei Ethernet-Steckdosen (also zwei unabhängigen Kommunikationsstrecken) über ein Kabel, wie er bei 10/100-Mbit-Netzwerkverbindungen über ein achtadriges Twisted-Pair-Kabel möglich ist (die nur je zwei Adernpaare für die Datenübertragung benötigen).

Auch das Erkennen von Kollisionen, bevor die Übertragung vom Sender abgeschlossen wurde, stellt ein Problem dar. Bei sehr kleinen Datenpaketen, z. B. 64 Byte als mögliche Untergrenze eines Ethernetframes, ist es möglich, dass eine Kollision gar nicht mehr registriert wird. Die Konsequenz wäre, dass kein neuer Sendeversuch des zerstörten Datenpakets unternommen wird. Deshalb muss die Kollision trotzdem erkannt oder gänzlich vermieden werden.

Drei mögliche Ansätze wurden diskutiert, um dieses Problem zu lösen:

- ✓ **Packet Extension:** Jedes Paket wird auf eine Mindestlänge von 512 Byte gebracht.
- ✓ **Packet Bursting:** Nur das erste Paket wird auf die Mindestlänge von 512 Byte gebracht, andere Pakete werden zusammengefasst auf die maximale Länge von 1518 Byte.
- ✓ **Full Duplex Gigabit Ethernet:** Es stehen getrennte Leitungen für Senden und Empfangen zur Verfügung. Kollisionen würden keine Rolle spielen, dafür müssen aber auch entsprechend geeignete Hardware wie beispielsweise Switches zur Verfügung stehen.

In der Praxis durchgesetzt hat sich der dritte Ansatz. Darüber hinaus werden im Umfeld von Gigabit Ethernet ausschließlich Switches eingesetzt, sodass das Problem der Kollisionen außer Kraft gesetzt wird. In der Zwischenzeit gibt es zahlreiche preiswerte Produkte, die den Gigabit-Ethernet-Standard in allen Varianten unterstützen und somit helfen, bestehende Investitionen in die Netzwerkinfrastruktur zu schützen.

Als Zwischenlösung zu 10-Gigabit-Ethernet wurde 2016 der Standard **IEEE 802.3bz**, auch **NBase-T** genannt, ratifiziert. Das Signal wird dabei mit reduzierter Nyquist-Frequenz übertragen. Damit werden auf bisherigen Kabeln nach CAT 5 (Kategorie 5 bzw. CAT 5e) bis zu 55 m Länge Übertragungsraten von **2,5 Gbit/s**, und mit Kabeln nach CAT 6 bis zu **5 Gbit/s** ermöglicht. Power over Ethernet nach IEEE 802.3at wird ebenfalls unterstützt. Informationen zur Ratifizierung des IEEE 802.3bz Standards finden Sie hier: [https://www.heise.de/newsticker/meldung/IEEE-802-3bz-als-Standard-für-2-5-und-5-GBit-LAN-ratifiziert-3339594.html](https://www.heise.de/newsticker/meldung/IEEE-802-3bz-als-Standard-fuer-2-5-und-5-GBit-LAN-ratifiziert-3339594.html)

10-Gigabit-Ethernet

Bereits im Juli 1999 begann unter dem Namen Highspeed Study Group die IEEE-802.3-Gruppe mit den Arbeiten an einem neuen Standard für 10-Gigabit-Ethernet. Unter der Bezeichnung 10GEA wurde auch dieser Standardisierungsprozess von der Gigabit-Ethernet-Allianz bis ins Jahr 2003 mit technischen Ressourcen unterstützt. Danach wurden die Forschungsergebnisse an die IEEE übergeben und die Allianz offiziell aufgelöst.

Die Rahmendaten, z. B. in Bezug auf Übertragungsmedien und Längenbeschränkungen, wurden Ende 1999 in einem ersten Vorschlag festgelegt. Ab Mitte 2000 fanden die ersten Versuche statt, und schon ein Jahr später wurde ein mehr als 500 Seiten starker Entwurf genehmigt. Der endgültige Standard wurde im Jahre 2002 unter der Bezeichnung **IEEE 802.3ae** verabschiedet.

Einer der wichtigsten Aspekte des Standards war, dass er anfänglich ausschließlich auf Glasfaser zugeschnitten war. Dafür wurden bereits für eine Vielzahl unterschiedlicher Glasfaser-Typen auch jeweils unterschiedliche physikalische Spezifikationen festgelegt. Als **New Fiber Cable** wurde ein neuer Multimode-Fasertyp aus hochreiner Gradientenfaser hinzugefügt.

10-Gigabit-Ethernet arbeitet nur im **Vollduplex-Verfahren**, was das endgültige Ende von **CSMA/CD** bedeutet. Als Steckverbindung werden in der Regel LC- oder SC-Verbindungen für die Glasfasern genutzt.

Details für Glasfaser

Die folgende Tabelle zeigt eine Übersicht über die einzelnen Festlegungen von IEEE 802.3ae:

Bezeichnung	Wellenlänge	Längenbegrenzung
10Gbase-SR	850 nm	82 m mit Multimode, 30–500 m mit Monomode *
10Gbase-LR	1310 nm	10 km mit Monomode
10Gbase-ER	1550 nm	40 km mit Monomode
10Gbase-LX4	1270 bis 1355 nm (4 Kanäle)	300 m mit Multimode
10Gbase-LW4	1275 bis 1350 nm (4 Kanäle)	10 km mit Monomode

* in Abhängigkeit von der Kategorie und damit auch der Faserdicke des Glasfaserkabels

Wenn sich am Ende der ersten drei Bezeichnungen nicht der Buchstabe R, sondern W befindet, handelt es sich um die Spezifikation für WAN, z. B. 10 GBase-EW. Hier werden leicht abweichende Datenraten zur besseren Integration in die im Weitverkehrsbereich verwendeten Strukturen definiert.

Bei der vierten (LX4) und letzten Bezeichnung (LW4) werden für die Übertragung vier Kanäle mit jeweils unterschiedlicher Wellenlänge gebildet und so sind für die weitverbreiteten Multimode-Lichtwellenleiter zumindest 300 m Distanz überbrückbar.

Details für Kupfer

Im April 2003 begann die Arbeitsgruppe IEEE 802.3ak mit den Planungen für 10-Gigabit-Ethernet auf Kupferkabelbasis und verabschiedete im Februar 2004 einen ersten Standard für sogenannte Twinax-Verkabelungen. Die Arbeitsgruppe IEEE 802.3an verabschiedete im Juni 2006 ebenfalls einen Standard für 10-Gigabit-Ethernet auf Kupferkabelbasis, allerdings für Twisted-Pair-Verkabelungen. Als Modulationsverfahren wird eine **Puls-Amplituden-Modulation in 16 Stufen (PAM16)** verwendet.

Standard	Bezeichnung	Beschreibung
IEEE 802.3ak	10GBase-CX4	Maximale Länge von 15 m über 8 Twinax-Paare
IEEE 802.3an	10GBase-T	Maximale Länge von 100 m, mindestens Kabel CAT 6A

Für **10GBase-T** sind mindestens Kabel nach CAT 6A mit RJ-45-Steckern für 100 m Kabellänge erforderlich (bis ca. 40 m reicht oft auch Kabel nach CAT 5); besser geeignet sind Kabel der Kategorie 7 mit den Steckertypen GG-45 und TERA (vgl. Kapitel 4.3).

Vom LAN zum WAN

Eines der Ziele der Entwicklung von 10-Gigabit-Ethernet ist es, die traditionell aus dem LAN kommende Ethernet-Technologie auch im Weitverkehrsbereich oder in Citynetzen einzusetzen. Es gibt bereits Umsetzungen, wie z. B. das deutsche Forschungsnetz (X-WiN) oder einige Provider, die das 10-Gigabit-Ethernet im Backbone verwenden.

100-Gigabit-Ethernet

Mitte 2010 wurde der IEEE-802.3BA-Standard freigegeben, der auch den Standard für 40-Gigabit-Ethernet integriert hat. Dieser Standard wurde sowohl auf der Basis von Kupfermedien als auch für Lichtwellenleiter spezifiziert. Die Kupfermedien werden nur im LAN, z. B. bei der Anbindung von Clustern oder SAN-Komponenten in Rechenzentren, genutzt. Im Juni 2016 wurde der Standard IEEE P802.3BQ spezifiziert.

Standard	Bezeichnung	Beschreibung
IEEE 802.3BA	40GBase-CR4	4 x Twinax-Kabel bis 10 m
IEEE 802.3BA	100GBase-CR10	10 x Twinax-Kabel bis 10 m
IEEE P802.3BQ	40GBase-T	30 m über CAT8-Kabel

Ebenfalls verabschiedet wurde die preisgünstigere Version 25GBase-T nach IEEE P802.3BQ über CAT8-Kabel. Siehe auch <https://www.lanline.de/ieee-802-3-verabschiedet-2540gbase-t/>

Die Ethernetspezifizierungen für Lichtwellenleiter finden sowohl im LAN als auch im WAN Anwendung. Damit hat man eine Alternative zur klassischen WAN-Technologie SDH.

Nachfolgend die LWL-Spezifizierung:

Bezeichnung	Wellenlänge	Längenbegrenzung
40GBase-SR4	850 nm	Multimode mit 4 Faserpaaren bis 125 m
40GBase-LR4	1310 nm	Monomode mit 4 Wellenlängen bis 10 km
40GBase-ER4	1550 nm	Monomode mit 4 Wellenlängen bis 40 km
100GBase-SR10	850 nm	Multimode mit 10 Faserpaaren bis 125 m
100GBase-LR4	1310 nm	Monomode mit 4 Wellenlängen bis 10 km
100GBase-ER4	1310 nm	Monomode mit 4 Wellenlängen bis 40 km

Ausblick

An der nächsten Stufe, Terabit-Ethernet, wird seit einigen Jahren gearbeitet, wobei man sich als Übertragungsmedium auf Lichtwellenleiter mit dem **Optical Time-Division Multiplexing (OTDM)**-Verfahren geeinigt hat.

14.2 Weitere Überlegungen

Viele Ansatzpunkte zur Steigerung der Geschwindigkeit/Bandbreite

Neben dem Ansatz, mehr Bandbreite und Kapazität durch Steigerung der Übertragungsgeschwindigkeit zu erreichen, gibt es eine ganze Reihe erwähnenswerter Punkte, die konzeptionell die Leistung eines großen lokalen Netzwerks steigern können.

Darunter fallen die bei der Strukturierung des Netzes bereits erwähnten VLANs genauso wie die folgenden drei sehr unterschiedlichen Aspekte WDM, MPLS und die Bündelung von Netzwerkadapters. Die Auswahl dieser drei Gesichtspunkte ist willkürlich und soll nur exemplarisch andeuten, in welch unterschiedliche Richtungen Überlegungen zur Verbesserung der Netzwerkleistung gehen können. Gemeinsam ist allen dreien, dass sie ursprünglich aus dem WAN-Bereich kommen.

WDM

Wavelength Division Multiplexing (WDM) ist ein Verfahren, um mehrere Datenströme auf ein Übertragungsmedium zu bringen, und dient als Technik zur Erhöhung der Kapazität von Glasfasern. Durch den simultanen Einsatz mehrerer Wellenlängen werden mehrere parallele Übertragungen möglich.

WDM existiert bereits seit Längerem in den zwei Ausprägungen DWDM und CWDM. Während Coarse WDM (CWDM) zwar kostengünstiger umzusetzen ist, kommt meist Dense WDM (DWDM) zum Einsatz, da es höhere Durchsatzraten bietet. Außerdem wurde DWDM zuerst entwickelt mit Blick auf den WAN-Bereich und CWDM erst danach mit dem Schwerpunkt LAN.

Ähnlich wie bei vielen der international arbeitenden Carrier, die WDM einsetzen, um die Übertragungsgeschwindigkeiten zwischen den Vermittlungsstellen zu erhöhen, wird WDM auch bei 10GBaseLX4 verwendet. An manchen Stellen findet sich hier die Abkürzung WWDM für Wide WDM.

MPLS

Multi-Protocol Label Switching (MPLS) setzt beim Routing als Engpass für die Datenübertragung an und versucht, diesen Vorgang zu beschleunigen. Der Originalansatz stammt von der Firma Cisco, die im Router-Bereich nach wie vor eine führende Rolle spielt. Er wurde unter dem Namen Tag Switching angeboten, konnte sich jedoch nicht nennenswert am Markt etablieren.

Die Grundidee von MPLS ist, dass Routing-Entscheidungen nicht mehr pro Paket, sondern pro Verbindung getroffen werden. Stark vereinfacht könnte es so formuliert werden, dass ein erster Router die Route bestimmt und diese Information als zusätzliches Label (engl. Etikett, Schildchen) an alle betroffenen Pakete anhängt.

Alle nachfolgenden Router müssen nur noch diese kurze Information auswerten, um die Pakete weiterzuleiten. Einer der Hauptvorteile von MPLS ist damit, dass die Router, die mit diesem System vertraut sind, Pakete nicht mehr bis auf Layer 3 auslesen müssen und somit spürbar schneller arbeiten.

MPLS kann beispielsweise als Virtualisierung bzw. Tunnel dienen, um geroutete Firmen-Netzwerkstrukturen über das Transport-Netzwerk eines Providers abzubilden.

Normierungen zu MPLS sind in den RFCs 3031, 3032 und 3036 festgehalten.

Alternativ kann man mehr Routing-Entscheidungen mit schnelleren Hardware-Bausteinen bearbeiten, was zwar zu höheren Kosten führt, aber dennoch in der heutigen Praxis eher dem Standard entspricht als MPLS. In großen Netzwerken wird MPLS häufig als zusätzliche Methode zur Beschleunigung des Datenverkehrs eingesetzt.

Port-Bündelung per LACP

Neben proprietären Herstellerlösungen (Cisco, Hewlett-Packard etc.) oder weiteren Verfahren, die das gleiche Ziel verfolgen, hat sich das Netzwerkprotokoll nach **IEEE 802.1ax** (früher **IEEE 802.3ad**) mit Namen **Link Aggregation Control Protocol (LACP)** als offizieller Standard für die Bündelung von Netzwerkadaptersn etabliert. Hardware aller renommierten Hersteller unterstützt dieses Protokoll. Weiterführende Informationen zu LACP finden Sie unter:

- ✓ <http://www.ieee802.org/3/ad/>
- ✓ https://www.thomas-krenn.com/de/wiki/Link_Aggregation_und_LACP_Grundlagen

Mit der Bündelung von Netzwerkadaptersn erhalten Sie jedoch **nicht** eine doppelte oder vierfache Übertragungsrate für eine einzelne Anwendung. Beispielsweise erhält bzw. verschickt der Server die Pakete vom Client 1 über Port 1 seines Netzwerkadapters und die vom Client 2 über dessen Port 2. Die Gesamtübertragungsrate des Servers ist damit größer, als wenn beide Clients ihre Daten nur über einen einzigen Port des Netzwerkadapters des Servers bekommen würden, unabhängig davon, ob das Netzwerk auf 1-Gbit-Technik basiert oder eine andere Infrastruktur vorhanden ist.

MPTCP (Multipath-TCP)

Besonders mobile Geräte wie Smartphones, Tablets etc. zeigen das Problem, dass sich ihre IP-Adresse immer wieder ändert, wenn sich deren Benutzer in ein anderes Netzwerk bewegt. Mit MPTCP (nach RFC 6824) erhält ein Gerät mehrere Zugänge zum Internet, die es zu einer Verbindung bündelt (per **Multi-Streaming**). Damit lassen sich Durchsatz und Zuverlässigkeit erhöhen.

Diese Technik ist allerdings (wie der Name schon sagt) nur bei Verbindungen über TCP anwendbar. In Linux und aktuellen Geräten mit IOS-System (von Apple) ist sie bereits eingebaut.

Multihoming

Multihoming bezeichnet mehrere Anschlüsse zum Internet über unterschiedliche Zugangsprovider. Dies erhöht nicht nur die Zuverlässigkeit (falls eine Verbindung ausfällt), sondern kann auch den Daten-Durchsatz verbessern, oft zusammen mit MPTCP.

Die Auswahl der Pfade erfolgt dabei meist über das Routing-Protokoll **BGP**. Dies setzt normalerweise **PI-Adressen** (Provider Independent Address) voraus. PI-Adressen sind offizielle IP-Adressen, die nicht vom Provider, sondern von übergeordneten Stellen (RIR – Regional Internet Registry) vergeben sind.

15

Netzwerküberwachung und Fehlersuche

15.1 Protokolle

Für die Verwaltung, Überwachung und Konfiguration gibt es eine Reihe von Protokollen. Sofern Sie nur wenige Komponenten managen, stehen beispielsweise Verbindungen über **Secure Shell (SSH)** oder HTTP zur Verfügung. Dies ist jedoch bei einem umfangreichen Netz ineffizient.

SNMP

Die effektive Verwaltung eines großen Netzes und das schnelle Eingrenzen von Fehlerquellen sind ohne ein Netzwerkmanagementsystem nicht mehr möglich. Für diese Zwecke ist das **Simple Network Management Protocol (SNMP)** der am weitesten verbreite Protokolltyp.

SNMP stammt aus der TCP/IP-Protokollfamilie und wurde von der IETF entwickelt. Es hat sich inzwischen als Standard für die Überwachung von Netzwerken und deren Bestandteilen etabliert. SNMP gehört zu den anwendungsorientierten Protokollen der OSI-Schicht 7.

Das Protokoll kann z. B. zur Überwachung der Netzwerkkomponenten, zur Gerätekonfiguration, für die Fehlererkennung und Alarmauslösung, zur grafischen Darstellung der Netzwerktopologie oder für die Inventarisierung der Geräte genutzt werden. Das Protokoll kann lesend (mit den Befehlen **get** und **trap**) oder schreibend (mit dem Befehl **set**) ausgeführt werden. Durch das Zuweisen zu den Gerätegruppen(Communities (deutsch: Gemeinde/Gemeinschaft)) werden die Zugriffsrechte autorisiert. Per Default ist als Community Name **public** für den Lesezugriff und **private** für den kombinierten Lese- und Schreibzugriff voreingestellt.

! Die Default-Communities sollten im Praxiseinsatz unbedingt geändert werden, zumindest aber der Name der R/W-Community zum Lesen und Schreiben.

Arbeitsweise

Das Grundkonzept der Überwachung mit SNMP baut im Wesentlichen auf drei Komponenten auf:

- ✓ Auf einer **Network Management Station (NMS)** wird ein Serverdienst (SNMP-Manager) implementiert.
- ✓ Auf den Clients, die überwacht werden sollen, werden sogenannte **SNMP-Agenten** (Windows-SNMP-Agent-Service, SNMP-Service etc.) installiert.
- ✓ Der SNMP-Manager hat Zugriff auf eine vorhandene Datenbank (**Management Information Base (MIB)**) der Clients mit standardisierten Informationen, die er auswerten kann.

Die Managementinformationen werden zwischen einem **Managed Node (Agent)** und einer Management Station (**NMS**) über ein Managementprotokoll (SNMP) ausgetauscht.

Im Wesentlichen wird unterschieden in:

- ✓ **Netzwerk-Überwachung:** Auch **Netzwerk-Monitoring** genannt. Dabei werden die Statusmeldungen und Betriebswerte, die die einzelnen Netzwerk-Komponenten liefern, zentral gespeichert und/oder in Grafiken dargestellt. Beim Über- bzw. Unterschreiten von vorher festgelegten Werten kann eine Warnung oder ein Alarm ausgelöst werden.
- ✓ **Netzwerk-Management:** Hiermit wird nicht nur ein Netzwerk überwacht, sondern es können zusätzlich von einem zentralen Rechner aus, bestimmte Einstellungen der Komponenten verändert und gesteuert werden. Dabei können neben SNMP auch weitere Protokolle zum Einsatz kommen. Ein weiterer Begriff für Netzwerk-Management ist **Operation, Administration and Maintenance (OAM)**.

Polling und Trap

Die NMS fordert periodisch den Status der überwachten Geräte an. Diese Managed Nodes sind im Allgemeinen Geräte wie z. B. Router, Managed Switches, Server oder einfache PCs. Die dort installierten SNMP-Agenten beantworten die Anfrage der NMS. Dieser Vorgang wird als **Polling** bezeichnet.



Je häufiger die NMS die überwachten Geräte abfragt und je mehr Geräte überwacht werden, desto aussagekräftiger sind die ermittelten Werte, aber desto stärker wird das Netzwerk mit Datenverkehr belastet. Es kann passieren, dass kurz nach der Antwort des Agenten eine Störung auftritt. In diesem Fall bleibt die Störung unbemerkt, bis die NMS das nächste Mal den Agenten abfragt.

In der Regel sind diese Polling-Intervalle auf Werte zwischen 30 Sekunden bis 5 Minuten eingestellt.

Ein anderer Weg, um den Datenverkehr zwischen der NMS und den Agenten zu verringern, ist die Implementierung von Traps auf den Agenten. Ein **Trap** ist eine Mitteilung, die durch ein vordefiniertes Ereignis ausgelöst wird. Tritt ein solches Trap-Ereignis ein, schickt der Agent (Client) sofort eine Meldung an den SNMP-Manager.

Operationen

Es sind mehrere Arten von Operationen festgelegt, die zwischen NMS und Agenten ausgetauscht werden können, wobei die ersten vier in der nachfolgenden Tabelle von der NMS zum Agenten gesendet werden und die letzten beiden Typen in umgekehrter Richtung. Hier die wesentlichen Namen der Operationen (Kommandos):

Meldung	Verwendung
get	Abrufen eines MIB-Datensatzes (Management Information Base), z. B. Name einer Komponente, Übertragungsrate etc.
getnext	Abrufen des nachfolgenden MIB-Datensatzes
getbulk	Abrufen eines MIB-Datensatzblocks
walk	Abrufen aller verfügbaren MIB-Datensätze
set	Setzen eines Wertes einer MIB-Variable, z. B. das Einschalten der Funktion „IP Forwarding“
response	Antwort auf eine hierfür geeignete Operation
trap	Senden einer Ereignismeldung aufgrund eines vordefinierten Wertes

Während SNMP für das Versenden der entsprechenden Get- und Set-Befehle über UDP den Port 161 verwendet, werden Trap-Meldungen über den UDP-Port 162 gesendet.

MIB

Alle Geräteinformationen werden über eine **Management Information Base (MIB)** definiert, deren erste Version in der RFC 1156 definiert und als MIB-II in der RFC 1213 erweitert wurde. Die aktuelle MIB-Struktur ist durch RFC 3418 definiert. Die MIB ist eine Datenbank, in der die zu überwachenden Parameter der Komponente als Objekte mit Attributen festgelegt werden.

Der Aufbau dieser Datenbank wird durch die **Structure of Management Information (SMI)**, einer Regelsammlung zum Beschreiben von Netzwerkobjekten, festgelegt, die anfänglich in der RFC 1155 spezifiziert und in der Zwischenzeit mehrfach ergänzt wurde. Die Darstellung der einzelnen Objekte erfolgt in einer hierarchischen Baumstruktur (MIB-Tree). Vom ursprünglichen Wurzel-Objekt des MIB-Baums abgeleitet existieren die **Standard-MIB** (MIB-II) und die sogenannten **Private-MIB**.

Erstere beinhaltet alle Variablen, die von jedem Hersteller standardgemäß genutzt werden. Das können u. a. System-, Interface-, IP-, UDP- und TCP-Variablen sein. Jeder Hersteller, der Geräte oder Komponenten anbietet, die das SNMP-Protokoll unterstützen, kann zusätzlich seine eigene Private-MIB nutzen. Sie findet Anwendung, um herstellerspezifische MIB-Variablen abzubilden.

Objekt ist die Bezeichnung für eine Ressource, die einen bestimmten Teilbereich der MIB darstellt. Objekte sind u. a. Systeminformationen, Interfaces, Routing-Tabellen usw., die die Teileigenschaften eines Gerätes (z. B. eines Routers) beschreiben. Jede dieser Ressourcen kann über eine Vielzahl von Parametern verfügen.

Ein kleines Beispiel soll dies verdeutlichen:

Eine NMS möchte von einem Agenten dessen Systemnamen erfahren. Dazu schickt sie eine *get*-Anfrage mit dem Parameter *1.3.6.1.2.1.1.5.0*. Diese Nummerierung weist innerhalb der MIB auf die Objektvariable Systemname. Der Agent antwortet darauf mit einem Response, der seinen Namen enthält.

Meist werden nicht solche sperrigen Parameter, wie im vorherigen Beispiel verwendet, sondern besser zu merkende Namen, wie in folgendem Beispiel der Gerätename (*sysName.0*) unter Linux. Wegen der einfacheren Syntax verwendet das Beispiel SNMPv2c und fragt das Gerät in der Community „public“ ab:

```
snmpget -v 2c -c public localhost sysName.0
```

RMON

Eine wichtige Erweiterung von SNMP ist **Remote Monitoring (RMON)**. RMON bietet die Möglichkeit, in Netzwerkkomponenten statistische Daten (z. B. der Netzaktivitäten) aufzuzeichnen und in einer Datenbank zu speichern. RMON-Informationen können ebenfalls per SNMP ausgelesen werden. Im NMS können sie grafisch aufbereitet werden und als Hilfen zur Netzanalyse und -optimierung dienen. Das ursprüngliche RMON erlaubt Monitoring auf Layer 1 und 2, die verbesserte Version **RMON2** das Monitoring auf allen 7 Layern des OSI Modells.

Es gibt Switches und Router mit RMON-Funktionalitäten, jedoch können auch eigenständige Geräte (sogenannte Probes) oder PCs mit einer Messsoftware verwendet werden.

SNMPv2

Dieses Protokoll baut auf der ersten Version von SNMP auf und ergänzt es vor allem um Sicherheitsmechanismen und erweiterte Formen der Ressourcenverwaltung. SNMPv2 ist abwärts-kompatibel, sodass die bisherigen MIB-Informationen weiterhin verwendet werden können.

Die Arbeiten an diesem Protokoll beanspruchten einen längeren Zeitraum, wodurch ersichtlich wird, warum dafür mehrere RFCs (RFC 1901–1907 und RFC 2578–2580) existieren. Das Ergebnis der Arbeit in diesem Zeitraum waren drei Versionen, nämlich SNMPv2p (Party-Based), SNMPv2u (User-Based) und SNMPv2c (Community-Based).

Durch den deutlich erweiterten Funktionsumfang wurde die Verwaltung und Konfiguration von SNMPv2 sehr komfortabel. Von den drei oben genannten Versionen ist heute nur noch SNMPv2c praxisrelevant.



Die Sicherheit von SNMP **vor** Version 3 ist nicht sehr hoch, da die „Community-Passwörter“ im Klartext übertragen werden und somit leicht auszuspähen sind. Das verwendete Gerät sollte deshalb durch eine Firewall geschützt sein und ausschließlich lesenden Zugriff bieten oder den Vollzugriff nur über eine verschlüsselte Verbindung gestatten. Seit SNMPv3 sind eine Benutzerauthentifizierung und der verschlüsselte Zugriff verfügbar.

SNMPv3

Die Kriterien der Weiterentwicklung des Protokolls waren folgende Punkte:

- ✓ kein neues Managementsystem zu entwickeln, sondern nur Zusatzfunktionen zu den bisherigen,
- ✓ Verschlüsselung und Authentifizierung,
- ✓ Kompatibilität zu den Versionen SNMPv1 und SNMPv2.

Die entsprechende Arbeitsgruppe wurde bereits Ende 1996 gegründet. Daher sind (wie bei SNMPv2) diverse RFCs entstanden, die sich mit dieser Version beschäftigen, siehe RFC 3410–3418.

Zusammenfassend unterscheiden sich die einzelnen SNMP-Versionen vor allem in den Sicherheitsstandards. Die folgende Tabelle gibt hierzu einen Überblick:

Version	Authentifizierung	Passwort-Verschlüsselung
SNMPv1	Communities *	Nein
SNMPv2c	Communities *	Nein
SNMPv3	Benutzername und MD5- oder SHA-Algorithmus	DES-Algorithmus

* **Communities** sind einfache Benutzernamen mit zugeordneten Berechtigungen, so hat beispielsweise der Benutzer PUBLIC nur Lesezugriff, während der Benutzer PRIVATE auch schreiben darf. Kompliziertere Benutzernamen führen nicht zu mehr Sicherheit, da wie oben schon erwähnt die Passwörter im Klartext übertragen werden.

15.2 Hinweise zur Umsetzung

Standardaktivitäten

Für den sinnvollen Einsatz von Überwachungsprogrammen in der täglichen Praxis müssen zu allererst Standardwerte (Standardaktivitäten) des Netzwerks ermittelt werden. Diese Daten können dann als Referenzwerte (baseline) dienen, um überhaupt beurteilen zu können, wann sich z. B. die Netzbelaistung kritisch verändert.

Auswerten von Protokolldateien

Die meisten Serverprodukte bieten die Möglichkeit, Vorgänge zu protokollieren. Diese Aufzeichnungen können Anmeldevorgänge an einem Server sein oder auch die Zugriffe auf eine Website. Die Bandbreite der dabei entstehenden sogenannten Log-Files reicht von einfachen Text-Dateien bis hin zu Einträgen in einer Datenbank-Tabelle, die wiederum alle gewünschten Auswertungskriterien liefert.

! Dabei ist es aber nicht sinnvoll, immer alles vom System protokollieren zu lassen. Schon die Größe der Log-Files würde dem widersprechen. (Wenn Logfiles die Festplatte füllen, bleibt das Betriebssystem stehen!) Wichtiger ist es, sich gezielt die Informationen zu verschaffen, die auch wirklich benötigt werden. Geschieht dies regelmäßig, ergibt sich daraus ein sehr aussagekräftiges Bild über die Leistungsfähigkeit des Netzwerkes.

Programme zur Netzwerküberwachung

Oft wird unterschieden in:

- ✓ **Netzwerk-Management:** Hier geht es vor allem um die Überwachung und Steuerung von Netzwerk-Komponenten. Es setzt vorwiegend auf SNMP-Agenten und einen laufenden SNMP-Dienst auf.
- ✓ **System-Management:** Hier werden nicht nur die Netzwerk-Komponenten überwacht. Es bindet auch die Rechner mit deren Komponenten (Lüfter, Netzteil, Festplatten, Temperatur etc.) ein. Dies geschieht im überwachten Netzwerk durch spezielle Software-Agenten bzw. Plugins von Monitoring-Programmen. Meist gestatten entsprechende Management-Tools erhebliche Eingriffe in die Systeme, wodurch Konfigurationen, Software-Installationen u.v.m. über das Netzwerk, von einem zentralen Rechner, ermöglicht werden.

Bei den zur Verfügung stehenden SNMP-Programmen müssen Sie grundsätzlich zwei Kriterien beachten. Einerseits existieren SNMP-Applikationen, die primär die Standard-MIBs auswerten, und andererseits spezifische Programme der Hersteller, die neben den Standard-MIBs nur die MIBs (Private-MIBs) des Herstellers berücksichtigen. Durch zusätzliche Module (Add-ons) können weitere Private-MIBs eingebunden werden, was sich jedoch in den Kosten für dieses System niederschlägt.

Grundsätzlich unterstützt jeder SNMP-Manager die Standard-MIBs. Ein Beispiel ist WhatsUpGold der Firma Ipswitch Inc., https://www.whatsupgold.com/?k_id=ipswitchhome

Daneben existiert eine Vielzahl von SNMP-Managern auf der Basis von Open Source, wie das Monitoring-Programm **Nagios** oder dessen Nachfolger **Icinga**.

Hersteller von Netzwerkkomponenten und Software bieten oft auch ihre eigenen Management-Tools an. Um nur einige zu nennen:

- ✓ CiscoWorks der Firma Cisco Systems Inc.
<https://www.cisco.com/c/en/us/products/cloud-systems-management/index.html>
- ✓ Ridgeline Network and Service Management der Firma Extreme Networks
<https://www.extremenetworks.com/product/extreme-management-center/>
- ✓ System Center von Microsoft
<https://www.microsoft.com/en-us/cloud-platform/system-center-solutions>

Diese Programme sind stark proprietär, d. h., die Einbindung von Komponenten anderer Hersteller wird kaum unterstützt. Die Einbindung von MIBs ist oft möglich, doch liegt der Mehrwert der Tools in einer grafischen Darstellung und der gezielten Auswertung herstellerspezifischer Informationen. Haben Sie beispielsweise vorrangig Cisco-Switche in Ihrem Unternehmensnetzwerk im Einsatz, sollten Sie auch die Tools von Cisco einsetzen, um wirklich alle Informationen zu erfassen. Hierbei kommen sowohl Cloud-Lösungen wie auch lokale Installation in Betracht.

Die Palette der Möglichkeiten eines SNMP-Managers ist sehr umfangreich und bedarf einer strategischen Planung, um die Möglichkeiten voll auszuschöpfen, beispielsweise:

- ✓ **Device-Management:** Überwachung, Konfiguration und Troubleshooting von Geräten,
- ✓ **Topologie-Management:** Visualisierung der Netzwerkstruktur,
- ✓ **Event-Management:** Einstellen von Schwellwerten im Netzwerk,
- ✓ **Accounting-Management:** Protokollierung und der Nachweis des Nutzerverkehrs.

Sie sollten im Vorfeld entscheiden, welche der exemplarischen Punkte Ihnen wichtig sind und anhand dieser Analyse den SNMP-Manager auswählen.

Protokollanalysatoren und Port-Mirroring

Programme wie Wireshark (<https://www.wireshark.org>, früher Ethereal) oder der Netzwerk-Monitor von Microsoft sind in der Lage, alle Frames (nicht nur die, die für einen bestimmten Netzwerkadapter bestimmt sind) **aufzuzeichnen** und zu **analysieren**. Die Inhalte der einzelnen Pakete können aufbereitet und gefiltert werden (Quelle, Ziel, Art des Pakets etc.), um die mögliche Ursache von Problemen zu erkennen.

Bei Switchen ist das Abgreifen von Daten zur Analyse schwierig, wenn diese nicht für das eigene Gerät bestimmt sind. Managebare Switches bieten daher **Port-Mirroring**. Dabei kann der Administrator festlegen, welcher zu untersuchende Port auf einem anderen Port gespiegelt wird. An diesem **Spiegelport** wird der Diagnoserechner angeschlossen.

Es können auch Statistiken über den Datenverkehr im Netz erstellt werden, um das Netzwerk gezielt zu optimieren. Diese gilt natürlich nur für den Netzwerkverkehr, in dem der Protokollanalysator angeschlossen ist. Neben fehlerhaften Netzwerkkomponenten werden auch Konfigurationsfehler, Protokollprobleme oder Engpässe im Datenverkehr aufgedeckt. Die Protokollanalyse der von solchen Programmen aufgezeichneten Daten setzt allerdings Expertenwissen in Bezug auf Netzwerkprotokolle und deren Arbeitsweise voraus.

! Viele Protokollanalyseprogramme können den Datenteil der Pakete auslesen und dadurch den Datenverkehr protokollieren. Datensicherheit gegen Spionage kann hier nur durch verschlüsselte Übertragungen erreicht werden. Außerdem sollte der Einsatz einer derartigen Software nur mit Genehmigung der Firmenleitung und des Betriebsrats erfolgen, um gegen den Vorwurf der Verletzung der Privatsphäre von Mitarbeitern abgesichert zu sein.

Außerdem muss die jeweils aktuelle Gesetzeslage in Bezug auf den Einsatz solcher Werkzeuge berücksichtigt werden. Weitere Hinweise zu dieser Problematik finden Sie unter anderem auf der Website des Bundesamtes für Sicherheit in der Informationstechnik <https://www.bsi.bund.de>, in Österreich beim Zentrum für sichere Informationstechnologie <https://www.a-sit.at/> und in der Schweiz beim Informatiksteuerungsorgan des Bundes ISB <https://www.isb.admin.ch/isp/de/home.html>.

15.3 Begleitende Maßnahmen

Unterstützende Arbeiten zur Überwachung im Netzwerk

Die bisher geschilderten Möglichkeiten beschreiben die direkte Überwachung des Netzwerkverkehrs. Es kann aber auch präventiv einiges getan werden, um mögliche Engpässe zu prognostizieren. Neben einer durchdachten Planung des Netzwerks sollen hier exemplarisch zwei Bereiche erwähnt werden, die indirekt das Thema Überwachung betreffen, nämlich Dokumentation und Sicherheit.

Dokumentation

Insgesamt gesehen ist eine sorgfältige und ausführliche Dokumentation des Netzwerkaufbaus unerlässlich. Dazu gehören Anschaffungs- und Installationsdatum, Garantiebedingungen, Aufzeichnungen zur Konfiguration, Protokolle und vieles mehr. Dies kann in Form von Textdateien oder Tabellen geschehen.

Darüber hinaus sollten aber auch Angaben über die Positionierung der Server und Clients, eine Darstellung der Verbindungen zwischen den Netzwerknoten oder die logische Zuordnung einzelner Teilnetze festgehalten werden. Dies geschieht am besten in grafischer Form mit Programmen wie Microsoft Visio, das, angelehnt an Programme zur Erstellung von Zeichnungen, eine Palette vorgefertigter und standardisierter Piktogramme (Shapes) zur Visualisierung von Vernetzungen nutzt.

Bei größeren Netzwerken lässt sich nicht mehr jedes Endgerät in einer Grafik erfassen. Stattdessen wird nur der Kern des Netzwerks (Router, Switches) abgebildet und die einzelnen Geräte in Form von Tabellen oder Datenbanken aufgelistet.

Sicherheit

Grundsätzlich sollten bestimmte Sicherheitsvorkehrungen eingehalten werden. Dazu gehört u. a., dass wichtige Netzwerkkomponenten in abschließbaren Schränken verbaut sind, zu denen nur befugte Personen einen Schlüssel haben. Auch IT-Richtlinien, die jeder Mitarbeiter nach entsprechender Unterweisung unterschreiben muss, tragen zur Sicherheit bei. Darin sollte beispielsweise festgelegt sein, dass der Betrieb eigener DHCP-Server verboten ist und dass jegliche Art von Patch-Versuchen zu unterlassen ist, um Schleifen im Netzwerk zu vermeiden.

Auch die Installation von Virensiegern (auf Windows-Rechnern), regelmäßige Updates, Backups sowie Richtlinien für komplexe Kennwörter sichern den IT-Betrieb nachhaltig.

15.4 Troubleshooting

Checkliste vorbereiten

In jedem Netzwerk können Probleme auftreten, die nur schwer einzugrenzen sind. Checklisten reduzieren den Aufwand und ermöglichen ein strukturiertes Vorgehen bei der Störungssuche. Kombiniert mit Aufzeichnungen, wie in der Vergangenheit ein Problem gelöst wurde, ist eine Basis geschaffen, auf der man weiter aufbauen kann.

Da ein Teil der Probleme die Netzwerkphysik betreffen, bieten die nächsten Abschnitte einige Informationen zu Test-, Diagnose- und Analysegeräten. Eine weitere Fehlerquelle sind Konfigurationsfehler. Dazu sind am Ende des Kapitels Hinweise zu einfachen Diagnoseprogrammen aufgelistet, die bei der Fehlersuche helfen können.

Kabeltester

Diese Gerätekategorie ist relativ preiswert und dient (je nach Ausführung) dem Testen verschiedener Kabeltypen (Netzwerk, Telefon, USB etc.). In der Regel erfolgt die Stromversorgung dieser Geräte per Batterie. Leuchtdioden zeigen Fehler in der Verdrahtung oder Störungen im Signalfluss an. Das Durchschalten der einzelnen Adern kann manuell oder automatisch in unterschiedlichen Geschwindigkeiten erfolgen.

Zum Testen eines verlegten Netzwerkkabels wird der eigentliche Tester per Patchkabel ① an einen Port am Patchfeld angeschlossen. Das abziehbare Remotemodul wird ebenfalls per Patchkabel ② an die entsprechende Dose am anderen Ende der Leitung angeschlossen.

Mithilfe dieser Geräte lassen sich relativ schnell falsch angeschlossene oder defekte Leitungsdämmen ermitteln.



Kombinierter Kabeltester für LAN- und USB-Kabel

Netzwerdiagnosegeräte

Mit einem Netzwerdiagnosegerät können die physikalischen Parameter des Mediums (u. a. Leitungslänge, Leitungsgüte, Portbelegung, Signallevel und Bitfehlerrate), die Data-Link-Parameter (wie Überprüfung des Ethernetverfahrens, Kontrolle der Frames) und Network-Parameter (Erkennen angeschlossener Geräte durch **ping**) ermittelt werden. Derartige Geräte eignen sich für das Finden von Fehlern bis Layer 4 des OSI-Modells (Daten, Sprache, Video).



Netzwerkanalysegeräte

Dieser Gerätetyp eignet sich für die Analyse innerhalb eines Netzwerkes. Dabei wird das Gerät, das über unterschiedliche Interfacetypen verfügt, in den Bitstrom des Mediums geschaltet. Über Filterfunktionen kann dediziert ein bestimmter Traffictyp (z. B. anhand der Ethernet- oder der IP-Adresse bzw. der Portnummer) ausgewählt werden. Durch eine integrierte Speicherfunktionalität können auch Langzeitanalysen realisiert werden. Ein Remotemanagement erleichtert dabei die Einstellung des Gerätes.

Einfache Diagnoseprogramme

Betriebssysteme stellen einfache, meist befehlszeilenorientierte Programme zur Verfügung, mit denen schnell und übersichtlich einige Konfigurationsfehler aufgespürt werden können. Die folgenden Beispiele beziehen sich auf Microsoft Windows und stellen nur einen Auszug aus den verfügbaren Programmen dar.

arp

Der Befehl **arp** liefert die Übersetzungstabelle zwischen IP- und physikalischen Adressen (MAC-Adressen), die vom ARP (Address Resolution Protocol) verwendet und im ARP-Cache gespeichert worden sind. So zeigt z. B. der Befehl **arp -a** eine Liste der zuletzt angesprochenen Netzwerkressourcen.

getmac

Der Befehl `getmac /v` liefert die MAC-Adressen der Netzwerkadapter des eigenen Rechners.

ipconfig

Der Befehl zeigt die Netzwerk-Konfiguration. Mit `ipconfig /all` werden alle Einstellungen ausgegeben.

netstat

Mit dem Befehl `netstat` können Sie sich Informationen beispielsweise über offene Ports (an denen ein Dienst oder Programm auf dem Rechner lauscht) oder die Routing-Tabelle des Rechners anzeigen lassen: `netstat -r`.

nslookup

Das Programm `nslookup` kann zur Überprüfung der DNS-Namensauflösung verwendet werden, z. B. per `nslookup www.herdt.com`. Es zeigt auch den DNS-Server, der die Informationen liefert.

ping

Mit dem Befehl `ping` kann die Erreichbarkeit eines Netzwerkteilnehmers überprüft werden. `ping localhost` oder `ping 127.0.0.1` (Loopback-Adresse) überprüft, ob der Netzwerkstack des eigenen Rechners in Ordnung ist. Durch die Eingabe von `ping <IP-Adresse des anderen Netzwerkteilnehmers>` können Sie die Erreichbarkeit eines anderen Netzwerkteilnehmers überprüfen. Voraussetzung ist jedoch, dass die Windows Firewall Antworten auf `ping` zulässt.

Beispiel: `ping 192.168.0.123`

`ping <Name>` prüft zudem die korrekte Namensauflösung (wichtig bei Systemen, die nicht nur Namen per DNS auflösen, wie dies oft bei Windows der Fall ist).

Beispiel: `ping www.herdt.com`

route

Der Befehl `route` bietet mehrere Optionen, über die Einträge in der IP-Routing-Tabelle des jeweiligen Hosts kontrolliert und geändert werden können. Hier einige Beispiele unter Windows:

Befehl	Bedeutung
<code>route print</code>	Anzeige der IP-Routing-Tabelle
<code>route add <Zielnetz> mask <Ziel-Maske> <Gateway></code>	Hinzufügen einer Route
<code>route delete <Zielnetz></code>	Löschen einer Route

Sind mehrere Netzwerk-Schnittstellen vorhanden, kann die Nummer der gewünschten Schnittstelle über `if` angegeben werden, z. B.

```
route add 192.168.0.0 mask 255.255.255.0 192.168.1.1 if 1
```

tracert

Der Befehl `tracert www.herdt.com` unter Windows verfolgt die Route vom ausführenden Rechner bis hin zu dem Webserver, der die Website `www.herdt.com` hostet. Die dabei passierten Stationen werden Ihnen mit Namen und IP-Adresse sowie Zeitangaben aufgelistet. Verwenden Sie alternativ den Befehl `pathping`: `pathping -q 1 www.herdt.com`.



Unter **Linux** bzw. **UNIX** heißen entsprechende Befehle ähnlich, beispielsweise `ifconfig` anstelle `ipconfig` oder `traceroute` anstelle `tracert`. Sie können einen Hilfetext ausgeben, z. B. mit `ifconfig --help`. Alternativ gibt es die sogenannten Manpages, die Sie beispielsweise so aufrufen können: `man ifconfig`.

Zusätzlich zu `nslookup` gibt es unter Linux weitere Programme zum Test der Namensauflösung, wie `host` und `dig`. Sie liefern weit mehr Informationen als das als veraltet geltende `nslookup`.

Vorgehensweise bei Netzwerkproblemen am Beispiel eines Windows-Rechners

- ▶ Prüfen Sie zuerst, ob die Verbindung physikalisch besteht (Netzwerkkabel eingerastet in der Netzwerkbuchse am Rechner bzw. in der Wand, im Zwischenboden, im Kabelkanal oder im dazwischengeschalteten Switch). Entsorgen Sie Netzwerkkabel mit abgebrochener oder loser „Nase“ (Verriegelung).
- ▶ Überprüfen Sie die Rechnerkonfiguration (`ipconfig`, `route`).
- ▶ Lassen Sie den Rechner sich selbst anpingen (`ping`).
- ▶ Pingen Sie Router (Standardgateway) bzw. Server (beispielsweise den DNS-Server) an (`ping`).
- ▶ Testen Sie die Namensauflösung (`nslookup`) und ermitteln Sie gegebenenfalls, welcher DNS-Server konfiguriert wurde (`ipconfig`).
- ▶ Geben Sie `ipconfig /release` und anschließend `ipconfig / renew` ein, um bei Problemen mit DHCP die IP-Adresse neuzubeziehen.
- ▶ Verfolgen Sie die Route zu einer bekannten Website bzw. sehen Sie nach, bis zu welchem Ziel Sie gelangen (`pathping`, `tracert`, `ping`).
- ▶ Überprüfen Sie die MAC-Adressen der beteiligten Netzwerkgeräte (Rechner, Router etc.) (`arp`, `getmac`).

Für die Ausgabe aller möglichen Optionen des jeweiligen Befehls geben Sie `<Befehl> /?` bzw. `<Befehl> /help` ein, z. B. `arp /?`.



Wissenstest: Große Netzwerke

15.5 Übung

Fragen zur Überwachung und Fehlersuche in Netzwerken

Übungsdatei: --

Ergebnisdatei: uebung15-E.pdf

1. Warum ist eine Überwachung von Netzwerken sinnvoll?
2. Welches Protokoll eignet sich dafür und warum?
3. Wie können die nötigen Informationen ermittelt werden?
4. Welches ist der Hauptvorteil der Version 3 von SNMP?
5. Warum sind bei Switchen Protokollanalysatoren schwierig anzuwenden und welche Lösung gibt es?
6. Welcher Befehl ist Standard zum Test der Erreichbarkeit eines Netzwerkteilnehmers?
7. Mit welchem Befehl können Sie testen, welcher Server die IP-Adresse von einer DNS-Namensauflösung liefert?

16

Praxis 2

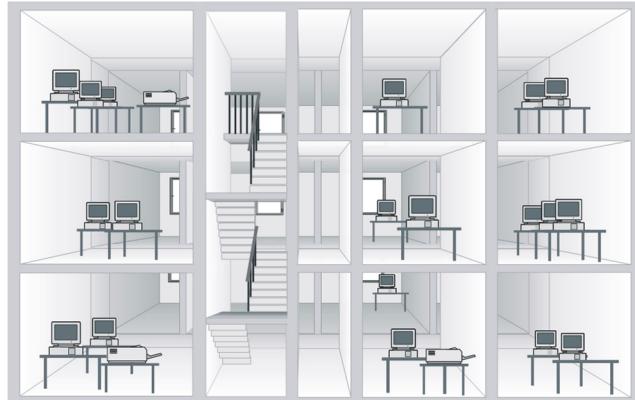
16.1 Planung des Ausbaus

Situationsbeschreibung

Das Erdgeschoss und der zweite Stock des angemieteten Gebäudes werden demnächst mit neuen Mitarbeitern besetzt.

Ein zusätzliches Gebäude auf dem gleichen Grundstück wird teilweise als Lager und für die Marketingabteilung genutzt. Außerdem ist ein großer Besprechungsraum geplant.

Zusätzlich wurde im Gebäude auf der gegenüberliegenden Straßenseite der erste Stock angemietet. Dort soll die Buchhaltungsabteilung neu eingerichtet werden.



Querschnitt eines Gebäudes

Weitere Überlegungen

Sämtliche Räume der neu hinzukommenden Gebäude verfügen über keine Verkabelung, die für den geplanten Ausbau des Netzwerks geeignet wäre. Ziel ist, dass das Netzwerk zentral vom bisherigen Büro aus verwaltet werden soll.

Außerdem soll eine strukturierte Verkabelung zum Einsatz kommen. Eine wesentliche Frage betrifft hier die Art der Verkabelung zwischen den einzelnen Gebäuden (Primärbereich) und zwischen den einzelnen Stockwerken (Sekundärbereich). Hier muss auch die Entscheidung fallen, mit welcher Technologie im Backbone gearbeitet werden soll.

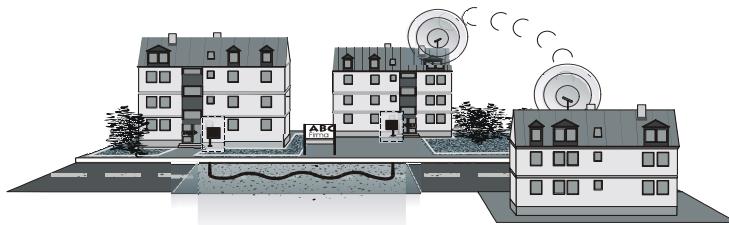
Neben der Positionierung und Anbindung der Server muss überlegt werden, wie die Segmentierung des Netzwerks vorgenommen wird. Dazu gehören auch die Auswahl und die Aufstellung der Komponenten, die die Kopplung der Teilnetze leisten sollen.

16.2 Umsetzung

Primärer Bereich

Die Musterfirma muss zunächst drei Gebäude miteinander verbinden. Die ersten zwei Objekte befinden sich auf dem Firmengelände. Hier wird die Verbindung über Glasfaserkabel hergestellt.

Um das dritte Gebäude zu integrieren, muss eine öffentliche Straße überquert werden. Eine mögliche Lösung wäre, die Genehmigung einzuholen, auch hier Erdarbeiten vorzunehmen und Glasfaserkabel zu verlegen. Falls dies nicht möglich ist, bleiben folgende Alternativen:



- ✓ Anmieten öffentlicher Leitungen,
- ✓ Aufbau einer WLAN-Funkstrecke,
- ✓ Nutzung einer optischen Richtfunkstrecke,
- ✓ Nutzung einer VPN-Verbindung über das Internet.

Mietleitungen von öffentlichen Anbietern stehen vielerorts in ausreichendem Maß zur Verfügung und ermöglichen relativ hohe Datenübertragungsraten. In Bezug auf die laufenden Kosten einer derartigen Verbindung herrscht eine große Vielfalt. Daher ist es sehr wichtig, vor den Verhandlungen mit den Anbietern den eigenen Bedarf an Übertragungskapazität sehr genau zu definieren.

Für den Aufbau einer WLAN-Funkstrecke ist die Entfernung zwischen dem Access Point und der Outdoor-Antenne wichtig, um die Signaldämpfung so gering wie möglich zu halten. Kann die externe Antenne in Nähe des Access Points angebracht werden, so können Indoor Access Points genutzt werden. Ist dies nicht möglich, muss man auf Outdoor Access Points ausweichen, die im Freien montiert werden können.

Über WLAN-Funkstrecken sind, in Abhängigkeit von der Entfernung, Datenübertragungsraten erzielbar, die Netto mit Fast-Ethernet (100 Mbit/s) vergleichbar oder größer sein können. Es kann zur Trennung von Netzwerken auch ein Access Point mit Routingfunktion eingesetzt werden. Entsprechende Komponenten werden u. a. von der Firma LANCOM Systems GmbH angeboten (<https://www.lancom-systems.de>).

Sind höhere Geschwindigkeiten (bis in den Gigabit-Bereich) erforderlich, kann dies über eine optische Richtfunkstrecke (auch als Laser-Link bezeichnet) erreicht werden. Dazu werden Laserkomponenten eingesetzt, die mitunter über ein integriertes Mikrowellen-Richtfunksystem als Backup verfügen, womit von einer Verfügbarkeit von 99,99 % ausgegangen werden kann. Die Laser-Link-Verbindungen nutzen das Ethernet-Protokoll, sind also reine Layer-2-Geräte. Ein Anbieter für derartige Lösungen ist z. B. die Communication by light – Gesellschaft für optische Kommunikationssysteme mbH (CBL, <https://www.cbl.de>).

Die Nutzung einer VPN-Verbindung ist nur dann in Betracht zu ziehen, wenn die zu verbindenden Gebäude über eine Internetverbindung mit entsprechender Bandbreite verfügen. Die Verbindung muss in beiden Richtungen die erforderliche Bandbreite aufweisen, was oft symmetrisches DSL (SDSL) mit gleichen Sende- wie Empfangsraten bedingt.

Sekundärer Bereich

Für den Bereich der Etagenverkabelung sollten, soweit vorhanden, Versorgungsschächte verwendet werden. Zwischen den Etagen werden, auf der Basis der strukturierten Verkabelung, Multimode-Lichtwellenleiter verlegt. Eventuell kann es auch aufgrund der Übertragungslängenbeschränkungen erforderlich sein, Monomode-Lichtwellenleiter (auch Singlemode) statt der Multimode-Lichtwellenleiter zu verlegen. Die Verwendung von Lichtwellenleitern dient gleichzeitig auch der Potenzialtrennung zwischen den Etagen.

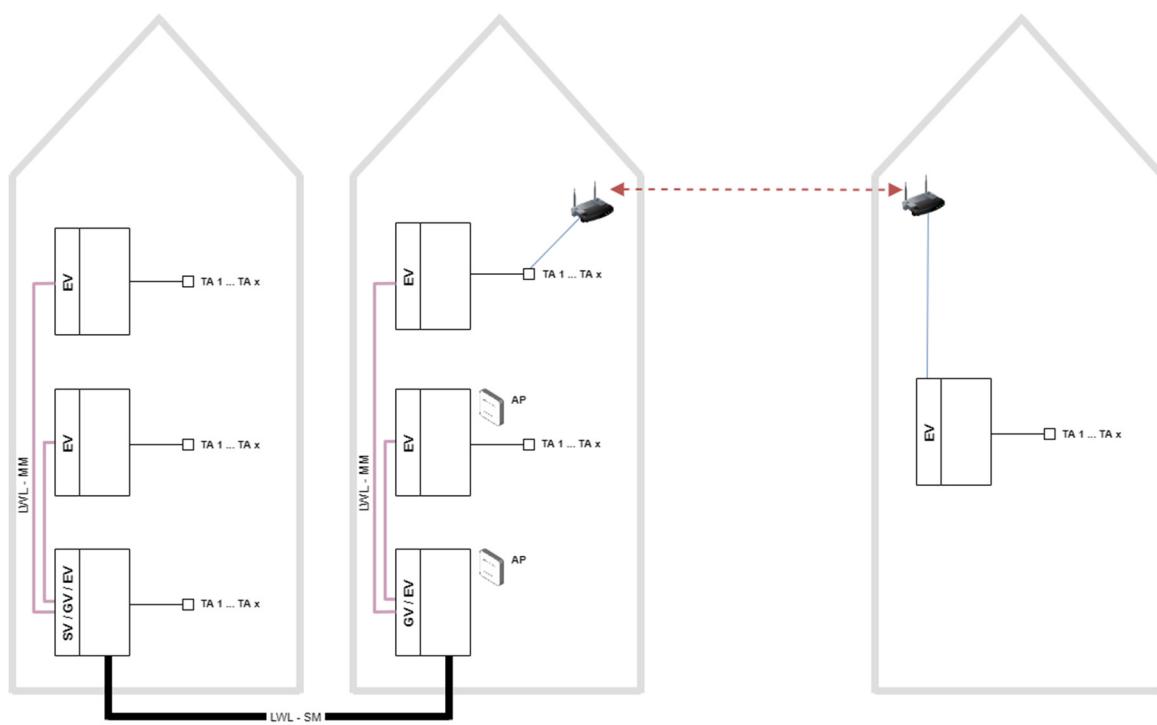
Auf jedem Stockwerk wird ein Switch installiert. Für den Fall, dass VLANs aufgebaut werden, ist geplant, Managed Switches für die Kommunikation zwischen diesen VLANs einzusetzen. Diese sollen dann aber nicht auf jeder Etage, sondern an ein oder zwei zentralen Stellen innerhalb des Gebäudes aufgestellt werden.

Tertiärer Bereich

Pro Arbeitsplatz sollten mindestens zwei Anschlussdosen vorhanden sein. Für eine strukturierte Verkabelung kommt TP-Kabel mindestens der Kategorie 6A oder 7 zum Einsatz. Dies erfordert jedoch, dass die Entfernung zwischen Etagen-Switch und angeschlossener Komponente maximal 100 m (inkl. der Patch-Leitungen) betragen darf.

Verteilerplan und Kabelstruktur

Zur Planung der bevorstehenden Installationsarbeiten wird eine Verteiler- und Kabelübersicht erstellt:



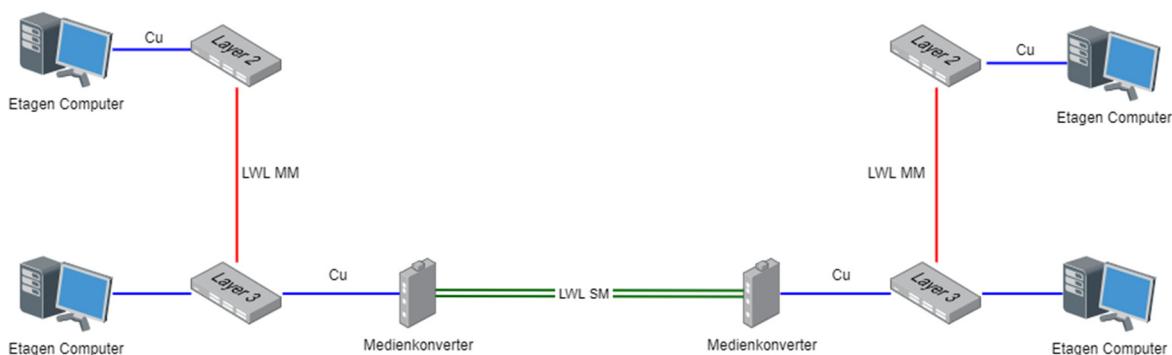
Verteiler- und Kabelstruktur

Benötigte Netzwerkgeräte für die Realisierung

Um die gewünschte Verkabelung in den einzelnen Gebäuden zu realisieren, muss Hardware beschafft werden, die über Anschlüsse für LWL verfügt. Hierzu können Switches benutzt werden, die Steckplätze für GBIC (Gigabit Interface Converter)-Module bereitstellen. Ein weiterer Weg besteht darin, mit Medienkonvertern zu arbeiten, die die Wandlung von LWL auf Kupfer und umgekehrt bewerkstelligen.

Die Fasern des Monomode-Lichtwellenleiters (auch Singlemode) werden auf beiden Seiten auf ein LWL-Panel aufgelegt. Mithilfe von LWL-Patch-Leitungen werden 2 Fasern über einen Medienkonverter zu einem Gigabit Ethernet Port gewandelt.

Für die steigenden LWL-Leitungen, die in Multimode-Technologie ausgelegt sind, werden fertig konfektionierte Kabel in den entsprechenden Längen bestellt.



Vereinfachte Darstellung der Netzwerkstruktur

Gebäude 3 wird über zwei Access Points mit Gebäude 2 verbunden. Hierbei ist darauf zu achten, dass die Geräte im Bridge Modus arbeiten, damit sich die Buchhaltung anschließend im gleichen Subnetz wie Gebäude 2 befindet. Die beiden Layer-3-Switches werden notwendig, da analog zu Gebäude 1 ein separates Subnetz im IP-Bereich 192.168.1.0 / 24 benutzt wird. Hierdurch wird der Transport der Pakete auf Basis der IP-Adressen notwendig. Da alle Server im Rechenzentrum des Gebäude 1 verbleiben, muss auf dem Layer-3-Switch im Gebäude 1 ein so genannter Relay-Agent konfiguriert werden, der DHCP-Anfragen aus dem Subnetz von Gebäude 2 empfängt und in das Subnetz mit dem DHCP-Server weiterleitet. Lager und Besprechungsraum im Gebäude 2 erhalten je einen AP für mobile Endgeräte.

Auswirkung auf die vorhandene Serverlandschaft

Bedingt durch den Einzug der neuen Mitarbeiter kann die bestehende Lizenzierung für den Server Essential 2022 nicht fortgeführt werden, da die Anzahl der Benutzer und Geräte die Grenzen übersteigen. Hier findet ein Wechsel zu Windows Server 2022 Standard statt.

Die Anbindung an das Internet wird überarbeitet und mit einem Proxyserver versehen, um unerwünschte Inhalte zu blockieren und zentral zu scannen. Da sich für die neu entstandenen Benutzergruppen unterschiedliche Anforderungen in Bezug auf Kommunikation und Office-Anwendungen ergeben haben, werden unterschiedliche Business Mietmodelle eingesetzt, um die Anforderungen abzubilden. Die bisherige Festplatte für die Datensicherung wird gegen ein leistungsfähigeres Wechselplattensystem für den Rack-Einbau ausgetauscht. Der Einsatz von IP-Telefonen wird ausgebaut.

17

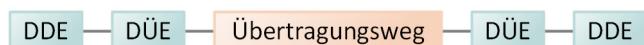
Weitverkehrsnetze

17.1 Einführung in Weitverkehrsnetze

Was ist ein Weitverkehrsnetz?

Ein Weitverkehrsnetz oder **Wide Area Network (WAN)** dient wie ein LAN zur Übertragung von Informationen vom Sender zum Empfänger. Aber damit sind die Gemeinsamkeiten zwischen WAN und LAN schon fast zu Ende. Angefangen von den Konzeptionen und Gründen der Verbindung bis hin zu den verwendeten Technologien haben sich Weitverkehrsnetze historisch ganz anders entwickelt als lokale Netze. Inzwischen haben sich jedoch auch Teile der Ethernet-Technologie im WAN-Bereich etabliert.

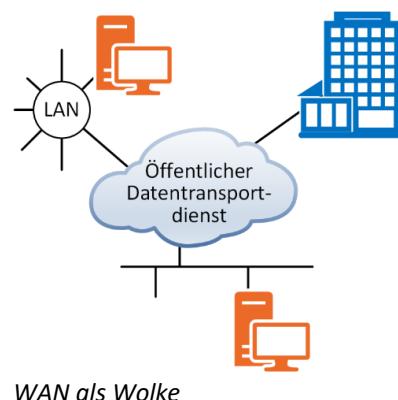
Dieses Kapitel soll dazu dienen, ein Grundverständnis für Weitverkehrsnetze zu schaffen, indem Hintergründe geklärt und Fachbegriffe eingeführt werden. Obwohl das Thema sehr vielschichtig ist, reduziert sich die Komplexität von Weitverkehrsnetzen für viele Benutzer auf folgendes Schema:



Der Benutzer ist über seine Datenendeinrichtung (DEE, z. B. DSL-Modem) mit einer Datenübertragungseinrichtung (DÜE, z. B. Telefonbuchse) verbunden.

Was sich auf dem Übertragungsweg abspielt, welche Leitungen oder Vermittlungseinrichtungen hier beteiligt sind, ist für den Benutzer normalerweise unwichtig, solange die gewünschte Übertragung funktioniert. Für viele Menschen stellt sich dieser Übertragungsweg deshalb oft als eine Blackbox oder eine Wolke dar.

Diese Wolke wiederum ist im Normalfall gekennzeichnet durch eine Vielzahl verschiedener Übertragungsmöglichkeiten und ständig wechselnder Verbindungen, d. h., es gibt keinen Standardweg für die Übertragung der Daten von einem Ort zu einem anderen.



Im Laufe der Entwicklung wurden weltweit verschiedene Netze konzipiert, die zum Teil nicht miteinander kompatible Übertragungsverfahren verwendeten. Dies wurde durch die Standardisierung relativ schnell überwunden. Damit wurde auch der wachsenden Bedeutung des Internets und dem immer weiter steigenden Bedarf an Bandbreite Rechnung getragen.

Weitverkehrsnetze existieren flächendeckend in allen Industrieländern und stehen für geschäftliche und private Kommunikation zur Verfügung. Sie haben für die Wirtschaft eine ähnlich große Bedeutung wie andere Netze aus dem Bereich einer funktionierenden Infrastruktur, wie z. B. Straßennetz, Eisenbahnnetz, Fluglinien. Im Folgenden steht die Übermittlung von (digitalen) Daten im Mittelpunkt.

Arten von Netzen

Wird der Begriff „Weitverkehrsnetz“ allgemeiner betrachtet, können unterschiedliche Typen von Netzen ausgemacht werden. Die Konzeption und Umsetzung des Netzes ist dann jeweils geprägt von der Dienstleistung, die damit angeboten wird. Beispiele dafür sind:

- ✓ Fernsprechnetz Public Switched Telephone Network (**PSTN**),
- ✓ digitale Netze für Daten (**Integrated Digital Network (IDN)**),
- ✓ Kabelfernsehnetz für Video- und Rundfunksendungen (auch für Datenverbindungen ins Internet und für Telefonie geeignet),
- ✓ Unterseekabel (heute meist mit Glasfasern realisiert) für die Verbindung von Kontinenten.

Öffentliche WLAN-Hotspots, Mobilfunk- und Satelliten-Netze sind weitere Beispiele für teilweise weltweit verfügbare Infrastrukturen.

Public Switched Telephone Network

Das weltweit offene Fernsprechnetz (PSTN) ist es sicher wert, aus der obigen Auflistung herausgenommen und extra gewürdigt zu werden. Es spielt für die elektronische Kommunikation eine sehr wichtige Rolle. In einigen Ländern ist dieses Netz noch analog, in vielen anderen dagegen (wie Deutschland) sind die Vermittlungsstellen bereits vollständig digitalisiert.

Beispiel X-WiN

Als Beispiel für ein Netz, das primär einer bestimmten Benutzergruppe zur Verfügung steht, sei das Wissenschaftsnetz **X-WiN** erwähnt. Als Fortsetzung von **B-WiN** (Breitband-Wissenschaftsnetz) und **G-WiN** (Gigabit-Wissenschaftsnetz) sowie finanziell gefördert mit Mitteln des Bundesministeriums für Bildung und Forschung dient es in erster Linie der Wissenschaft. Inzwischen sind mehr als 500 Hochschulen und Forschungseinrichtungen an dieses Netz angeschlossen.

Der Verein zur Förderung eines Deutschen Forschungsnetzes (**DFN**-Verein) spielt in diesem Zusammenhang eine wichtige Rolle und kümmert sich um die Sicherstellung der Service-Qualität und um das Internet-Routing dieses Netzes. Als deutsche Internet2-Initiative gehört das WiN seit Jahren zu den leistungsstärksten Netzen der Welt und ist mit dem europäischen Backbone GÉANT2 direkt im weltweiten Verbund der Forschungs- und Wissenschaftsnetze integriert.

Das X-WiN wurde 2006 in Betrieb genommen und nutzt modernste Glasfasertechnologie mit Anschlusskapazitäten bis zu 10 Gbit/s. Es verfügt über ein Multi-Gigabit-Kernnetz, das sich zwischen mehr als 70 Kernnetz-Standorten aufspannt. Weitere Informationen zu diesem Netz erhalten Sie unter <https://www.dfn.de>.

Beispiel IVBB

Der Informationsverbund Berlin-Bonn (**IVBB**) ist ein Kommunikationsverbund der obersten Bundesbehörden der Bundesrepublik Deutschland. Alle Bundesministerien sind hierüber einheitlich mittels VPN vernetzt. Über das IVBB werden auch die zentralen Dienste (wie E-Mail, DNS, WWW) und die einheitliche Domäne *bund.de* verwaltet. Beispielsweise ist das Bundesministerium des Innern über <https://www.bmi.bund.de> erreichbar.

Weitere Beispiele

In Österreich existiert ein vergleichbares Wissenschaftsnetz unter dem Namen **Austrian Academic Computer Network (ACOnet)** <https://www.aco.net>. Es wird von der Universität Wien in Kooperation mit Universitätsstandorten in ganz Österreich betrieben. Das Wissenschaftsnetz **SWITCHlan** der Schweiz ist erreichbar über <https://www.switch.ch/de/network>.

Gegenüberstellung LAN/WAN

Ein zentrales Merkmal im LAN ist, dass sich alle Komponenten der Vernetzung im Besitz der jeweiligen Firma befinden, während diese Komponenten im WAN normalerweise in irgendeiner Form angemietet werden müssen.

Zudem werden im WAN meist wesentlich höhere Anforderungen an Bandbreiten, Verfügbarkeit oder Latenzen gestellt.

	Lokales Netz	Weitverkehrsnetz
Konzept	Übertragung von Sprache, Daten und Video in einem begrenzten Bereich	Übertragung von Sprache, Daten und Video über weite Entfernung
Übertragungsraten	100 Mbit/s bis 10 Gbit/s	2 Mbit/s–565 Mbit/s (PDH), 50 Mbit/s–15 Gbit/s (SDH), 1 Gbit/s bis 100 Gbit/s (Glasfaser, Ethernet)
Eigentum	Im Besitz des Benutzers	Im Besitz öffentlicher oder privater Betreiber

Zu der Bedeutung der Begriffe **PDH** und **SDH** siehe E-Übertragungsschnittstellen weiter unten.

Nur für sehr wenige Unternehmen oder Organisationen ist der Aufbau eines eigenen Weitverkehrsnetzes sinnvoll und rentabel. Die entstehenden Kosten, z. B. für Kabel, Wartung oder Überwachung des Netzes, würden sich oft erst unter einem extrem langfristigen Aspekt amortisieren. Außerdem sind häufig Überkapazitäten vorhanden, so dass viele Leitungen zu günstigen Preisen gemietet werden können.

In diesem Zusammenhang sollen die Begriffe Internet, Intranet und Extranet kurz erwähnt werden, da sie den Wandel deutlich machen, dem die klassischen Begriffe LAN und WAN unterworfen sind.

Internet

Das Internet ist das größte WAN, das es gibt. Unzählige Rechner, Smartphones, Tablets usw. können weltweit über die unterschiedlichsten Wege miteinander in Verbindung treten und Informationen austauschen.

Immer mehr Bereiche der Wertschöpfungskette innerhalb der Wirtschaft verändern sich durch den Einfluss des Internets. Gleiches gilt für den kulturellen Bereich (Beispiel Arabischer Frühling). Die Ausmaße der durch das Internet ausgelösten Veränderungen in der Menschheitsgeschichte kann man ohne Übertreibung mit denen der industriellen Revolution vergleichen.

Intranet

Ein Intranet ist ein lokales Netz, das unter Verwendung der Internettechniken wie IPv4, IPv6 und weiterer Protokolle aufgebaut ist. Es werden Webserver eingesetzt, die die Mitarbeiterkommunikation auf der Basis von Browser-Technologien unterstützen. Ein Intranet nutzt die firmeneigenen Netzwerkverbindungen für den unternehmensweiten Austausch von Text-, Sprach- und Videodaten.

Extranet

Ein Extranet ist laut ISO/IEC 2382 eine Erweiterung eines firmeneigenen Intranets nach außen für legitime Zugriffe einer festgelegten externen Benutzergruppe. Dies kann auch durch eine Koppelung mit anderen Intranets erfolgen. Ein Extranet ist nicht für die Öffentlichkeit zugänglich.

Beispiele

Ein Beispiel für ein Extranet ist das **European Network Exchange (ENX)**. Es handelt sich dabei um ein Branchennetz der europäischen Automobilhersteller, Zulieferer und anderer Partner. Der Datenaustausch zwischen den einzelnen ENX-Nutzern findet über **Virtual Private Network (VPN)** mittels Netzen der Kommunikationsdienstleistern (British Telecom, Telefonica, Orange, T-Systems u. a.) statt.

Mittlerweile ist das ENX auch mit dem amerikanischen Gegenstück, dem **Automotive Network Exchange (ANX)**, verbunden. Projekte ähnlicher Art sind z. B. auch in Japan, Korea und Australien in Betrieb.

Ein weiteres Beispiel sind Zusammenschlüsse kommerzieller Provider, die häufig mit dem Kürzel **CIX (Commercial Internet Exchange)** benannt werden, so z. B. DE-CIX, einem Projekt von ursprünglich drei Internet-Service-Providern, an das inzwischen über 450 andere Internetdienstanbieter und Organisationen aus mehr als 52 Ländern angebunden sind. Die **DE-CIX** in Frankfurt verfügt über eine verteilte Switch-Infrastruktur, die es den Providern ermöglicht, kostenneutral miteinander Daten auszutauschen. Dies wird auch als Peering bezeichnet.

Typische WAN-Anwendungen sind auch die Verkehrsüberwachung oder die Zugangs- und Transportüberwachung bei Logistik-Unternehmen. Des Weiteren nutzen **Enterprise-Resource-Planning (ERP)**-Systeme bzw. Datenbanksysteme das WAN, genauso IP-Telefonie (VoIP, Voice over IP) oder Videokonferenzsysteme.

17.2 Begriffe

Dienste

Der Begriff Dienste wird im Zusammenhang mit Weitverkehrsnetzen häufig und teils sehr unterschiedlich verwendet. Der folgende Abschnitt ist eine Auflistung der verschiedenen Aspekte, die mit diesem Begriff angesprochen werden.

Gegenstand der Übertragung

Eine häufige Verwendung des Wortes Dienst betrifft den Gegenstand der Übertragung, den ein Weitverkehrsnetz anbieten soll, nämlich die Übertragung von Sprache, Video oder Daten.

Integration von Diensten

In diesem Zusammenhang fällt oft das Stichwort Dienstintegration. Dahinter verbirgt sich die Absicht, nicht für jeden einzelnen Zweck ein eigenständiges Netz aufzubauen, sondern über ein einziges Netz mehrere verschiedene Dienstleistungen anzubieten bzw. diese in einem Netz zu integrieren.

Beispiele sind Rufnummernübermittlung, Konferenzschaltung oder Rückruf, wenn die Leitung besetzt ist.

Da diese Dienste inzwischen verstärkt innerhalb von LANs genutzt werden (z. B. Multimedia und Video-Conferencing), ist auch dies ein Grund, dass Techniken aus dem WAN-Bereich in den LAN-Bereich integriert werden.

Übertragungsverfahren und Serviceleistungen

Der Begriff Dienste wird ebenso verwendet, wenn von Übertragungsverfahren die Rede ist, mit denen die Daten konkret auf die Übertragungsmedien gebracht werden. Hier geht es sowohl um die Technologie, die der entsprechende Anbieter (wie Internet Service Provider, ISP) einsetzt (z. B. DSL oder UMTS), als auch um die Leistungen, die er bietet (z. B. Netzüberwachung, Inhalte oder Leitungen). Weitere Informationen zu Providern siehe Kapitel 20.

Internetdienste

In diesem Zusammenhang bezieht sich der Begriff Dienst oder Server-Applikationen nach dem Client-Server-Modell auf Dienstleistungen (Funktionen), die z. B. über HTTP (**H**yper **T**ext **T**ransfer **P**rotocol) bzw. das sichere HTTPS für das **W**orld **W**ide **W**eb (WWW), FTP (**F**ile **T**ransfer **P**rotocol), SMTP (**S**imple **M**ail **T**ransfer **P**rotocol) oder viele weitere Protokolle erreichbar sind.

QoS

Quality of Service (Dienstgüte, Dienstqualität) bedeutet die Festlegung von Parametern für die Qualität der Übertragung. Die Regelung der Übertragung ist notwendig und ist Bestandteil des Vertrags zwischen dem Unternehmen und dem Anbieter der Datenübertragungsleistung.

Die folgende Liste zeigt eine Reihe von typischen Parametern, die jedoch nicht von allen Anbietern gleichermaßen gewährleistet werden:

- ✓ Dauer des Verbindungsaufbaus,
- ✓ Ausfallwahrscheinlichkeit,
- ✓ Durchsatzraten,
- ✓ Übertragungsverzögerung,
- ✓ Priorisierung bestimmter Protokolle, z. B. für Sprachübertragungen.

Kernnetz/Core Network

Das **Kernnetz (core network)** ist der Backbone, der aus einem breitbandigen Glasfasernetz gebildet wird und stellt eine flächendeckende Anbindung mit hoher Übertragungsgeschwindigkeit über große Entfernung zur Verfügung.

Die Struktur (Topologie) ist vermascht, sodass für den Fall einer Störung redundante Leitungen zur Verfügung stehen. Durch Glasfaser-Seekabel, Mobilfunk und Satelliten kann das Kernnetz erweitert werden.

Anschlussbereich/Last Mile

Mit **Last Mile** wird der Bereich bezeichnet, der zwischen der **Vermittlungsstelle** (Netzseitiger Vermittlungsknoten) und der hausinternen Vermittlungsstelle (**Benutzerendeinrichtung**) liegt.

Im Fall des Telefonnetzes befindet sich dieser Teil im Besitz eines Telekommunikationsanbieters. Wenn andere Firmen diesen Bereich nutzen wollen, um ihre Dienstleistung an den Kunden zu bringen, müssen sie die entsprechenden Leitungen mieten. Um diese zum Teil sehr hohen Kosten zu vermeiden, versuchen manche Anbieter, diese letzte Meile auf andere Weise zu überbrücken. Dazu stehen mehrere Möglichkeiten zur Verfügung, wie z. B. Stromnetz, Kabelfernsehnetz, Richtfunk oder Satellit.

Die Technologie, die auf dieser letzten Meile eingesetzt wird, muss nicht dieselbe sein, die danach im eigentlichen WAN zum Einsatz kommt.

Schnittstellen

In Europa und Nordamerika werden unterschiedliche Übertragungsschnittstellen und damit verbunden unterschiedliche Bandbreiten angeboten. Im Folgenden ein kurzer Überblick über gängige Standards:

E-Übertragungsschnittstellen

Die Grundbitrate beträgt 64 Kbit/s mit der Bezeichnung E-0. Diese Bezeichnungen werden in Europa verwendet und sind unter ITU G.7xx genormt.

E-1, auch bekannt als CEPT1, bündelt 32 Kanäle zu je 64 Kbit/s. Es stehen 30 Nutzkanäle für Sprache und Daten, 1 Kanal für die Signalisierung und 1 Kanal für Service und Wartung zur Verfügung. Die weiteren Kürzel ergeben sich in Bezug auf die Bandbreite als jeweils 4faches des vorherigen Kürzels:

- ✓ E-1: 2,048 Mbit/s
- ✓ E-2: 8,448 Mbit/s
- ✓ E-3: 34,368 Mbit/s
- ✓ E-4: 139,264 Mbit/s
- ✓ E-5: 564,992 Mbit/s

Diese Übertragungsraten werden von der **Plesiochrone digitale Hierarchie (PDH)**-Technik auf der Schicht 1 des OSI-Referenzmodells zum Multiplexen digitaler Bitströme angewendet. **PDH** wird vornehmlich zwischen Access- und Kernbereich genutzt, d. h. zur Bündelung von unterschiedlichen Datenraten für die Übergabe an die Technologien, z. B. **Synchrone Digitale Hierarchie (SDH)** des Kernbereichs. Weiterführende Informationen finden Sie hier:

- ✓ https://de.wikipedia.org/wiki/Plesiochrone_Digitale_Hierarchie
- ✓ https://de.wikipedia.org/wiki/Synchrone_Digitale_Hierarchie

Schmalband und Breitband

Häufig wird im Rahmen von WAN-Technologien zwischen Breitband und Schmalband unterschieden. Für die Grenzen zwischen beiden Übertragungsraten existieren keine einheitlichen Definitionen, jedoch ist oft Folgendes damit gemeint:

- ✓ Schmalband: eine Verbindung mit Datendurchsatzraten bis zu 2 Mbit/s
- ✓ Breitband: eine Verbindung mit Datendurchsatzraten ab 2 Mbit/s

17.3 Verbindungsarten

Festverbindung

Verbindungsarten geben an, wie die Leitungen zwischen Sender und Empfänger konkret geschaltet werden. Grundlegend erfolgt eine Trennung in Fest- und Wählverbindungen. Aktuell schrumpft deren Bedeutung angesichts von DSL und VPNs.

Eine Festverbindung (Standleitung, Standverbindung oder Mietleitung) ist eine fest geschaltete Verbindung zwischen zwei Standorten einer Firma. Sie steht permanent zur Verfügung. Dem Kunden wird ein exklusives Nutzungsrecht eingeräumt. Es ist kein Einwählvorgang notwendig, um die Verbindung verwenden zu können.

Vorteile	Nachteile
<ul style="list-style-type: none"> ✓ Keine Wartezeit für den Verbindungsaufbau ✓ Jederzeit exklusiver Zugriff 	<ul style="list-style-type: none"> ✓ Teuer bei geringer Auslastung ✓ Kein Ersatzweg bei Ausfall der Leitung

Datendirektverbindung

Neben den oben genannten Bezeichnungen wird eine Festverbindung häufig auch als Daten-direktverbindung (DDV) bezeichnet. Datendirektverbindungen können als VPNs (siehe Abschnitt **VPN**) geschaltet werden und sind für den permanenten Online-Betrieb gut geeignet.

Wählverbindung

Ähnlich wie beim Telefon wird bei Bedarf eine Verbindung aufgebaut. Der Kunde zahlt dementsprechend nur, wenn er die Leistung in Anspruch nimmt.

Vorteil	Nachteile
<ul style="list-style-type: none"> ✓ Größere Sicherheit gegen Totalausfall, da eine Neuanwahl über alternative Wege möglich ist 	<ul style="list-style-type: none"> ✓ Störungsanfälliger und dadurch geringere Übertragungssicherheit ✓ Es kann passieren, dass kein freier Anschluss vorhanden und die gewünschte Verbindung somit besetzt ist.

Semipermanente Verbindungen

Eine Sonderstellung nehmen semipermanente Verbindungen ein. Ursprünglich waren damit ISDN-Verbindungen mit einer garantierten Aufbauzeit von unter 0,8 Sekunden gemeint. Dafür gibt es keine Anbieter mehr. Dagegen sind heute vor allem DSL-Verbindungen quasi semipermanente Verbindungen, die im privaten Bereich eine tägliche Zwangstrennung erfahren, sich sonst aber nach dem Verbindungsaufbau wie eine Festverbindung verhalten.

Virtuelle Verbindung

Eine virtuelle Verbindung oder **Virtual Circuit(VC)** wird bei der Paketvermittlung eingesetzt. Zwischen Sender und Empfänger stehen dabei keine exklusiven, festen Leitungen zur Verfügung, sondern logische Kanäle innerhalb des Transportnetzes.

Der Weg, den die Datenpakete über die verschiedenen Knoten in diesem Transportnetz nehmen, wird am Anfang einer Verbindung ausgewählt. Danach nehmen alle Pakete, die zu dieser Verbindung gehören, diesen Weg. Die weiteren Pakete einer Sendung erhalten dementsprechend auch keine Zieladresse mehr, sondern nur noch eine Kennung, zu welcher virtuellen Verbindung sie gehören.

In der Praxis werden zwei Arten von virtuellen Verbindungen unterschieden, nämlich PVC und SVC.

PVC

Einen **Permanent Virtual Circuit (PVC)** kann man sich als Quasi-Standleitung vorstellen (wie eine Telefonverbindung). Auf diese Art kann die Datenübertragung schneller erfolgen, da der gesamte Weg der Übertragung von Beginn an bekannt ist. Das Zerlegen und erneute Zusammensetzen von Paketen (z. B. um Adressinformationen auszulesen oder um Paketgrößen für verschiedene Teilstrecken anzupassen) entfällt.

SVC

Der **Switched Virtual Circuit (SVC)** ist ebenfalls eine logische Verbindung zwischen zwei Endgeräten. Im Unterschied zu PVC gibt es eine Verbindungsauftauphase am Anfang der Datenübertragung und am Ende, eine Verbindungsabbauphase. Der Vorteil gegenüber einer permanenten virtuellen Verbindung ist, dass eine SVC nur bei Bedarf Übertragungskapazität in Anspruch nimmt und dafür berechnet wird. Sie kommen bei den Protokollen **X.25** und **Asynchronous Transfer Mode (ATM)** zum Einsatz.

Corporate Network (CN)

Wenn ein Unternehmen beschließt, mehrere Standorte (LANs) miteinander zu koppeln, wird häufig zwischen Corporate Network und Virtual Private Network unterschieden.

Corporate Network (CN) ist die Zusammenfassung bisher getrennter Netzwerke eines Unternehmens zu einem gemeinsamen Netzwerk. Manchmal wird auch die Abkürzung **CTN** für **Corporate Telecommunication Network** verwendet. **CNs** sind private Netze, die für spezielle Anforderungen von Unternehmen konzipiert sind. Es besteht eine exklusive physikalische oder logische Verbindung zwischen den Standorten des Unternehmens. Diese exklusiven Verbindungen werden durch einen Carrier oder Provider mit dedizierten Mietleitungen hergestellt.

Das Management des CNs kann durch das Unternehmen selbst oder als Serviceleistung durch den Carrier oder Provider vorgenommen werden. Die physikalische Ausdehnung kann regional, national oder international sein.

Falls sich ein Anbieter von CNs nur um die Vermittlung von Informationen kümmert und nicht um die Netzinfrastruktur, wird meist auf das vorhandene Angebot der Telecoms zurückgegriffen.

Da die Firma die Verbindungen nicht mit anderen teilen muss, können Übertragungsmerkmale, wie z. B. eine bestimmte Bandbreite, garantiert werden. Dies ist eine wichtige Voraussetzung bei der Integration verschiedener Dienste wie Sprache, Daten und vor allem Video-Übertragungen.

Das Strategic Review Committee 5 stellt in einer Erklärung fest, dass ein CN aus einer Anzahl von Einrichtungen besteht, die dem Kunden gehören oder von ihm gemietet sind. Diese Einrichtungen befinden sich an geografisch verschiedenen Orten und werden miteinander verbunden. Dadurch kann eine bestimmte Gruppe von Anwendern auf einheitliche Netzwerkdienste zugreifen.

Seit 1.1.1993 gibt es ein Genehmigungskonzept für CNs von der Bundesregierung, aber in Deutschland unterlagen Corporate Networks für Sprachkommunikation bis 1998 noch der Genehmigungspflicht des Bundesministeriums für Post und Telekommunikation.

Virtual Private Network (VPN)

Ein Virtual Private Network ist ebenfalls in der Lage, einer Firma einen Zusammenschluss mehrerer Standorte (einzelne LANs) über das Internet zur Verfügung zu stellen. Die Kommunikation der einzelnen Standorte läuft dabei über Tunneling-Protokolle wie z. B. **Layer 2 Tunneling Protocol (L2TP)**, **Internet Protocol Security (IPsec)**, **OpenVPN** etc. (siehe Kapitel 18.6) verschlüsselt ab.

Das ebenfalls lange eingesetzte **Point to Point Tunneling Protocol (PPTP)** ist sehr unsicher und sollte nicht mehr benutzt werden. Durch VPNs können übermittelte Daten vor Unbefugten geschützt werden, und so kann das unsichere Medium Internet für den Transport solcher privater Daten verwendet werden.

Logische Verbindung

Durch einen Carrier oder Provider wird eine exklusive logische Verbindung (LAN-LAN-Kopplung) hergestellt. Aus der Sicht des Unternehmens besteht damit ein (virtuelles) privates Netzwerk. Die physikalischen Übertragungswege hingegen können mehrfach belegt sein und stehen der Firma damit nicht exklusiv zur Verfügung. Aus diesem Grund kann auch keine garantierte Bandbreite bzw. garantierte Datendurchsatzrate festgelegt werden. Der Carrier oder Provider managt die für das VPN genutzte Infrastruktur.

Remote Access Service (RAS)

RAS bezeichnet die Möglichkeit, über Telefon-, Mietleitungen oder das Internet auf ein Firmennetz zuzugreifen. Ein gutes Beispiel hierfür sind Heimarbeitsplätze oder Vertriebs- und Service-Mitarbeiter, die von außerhalb Zugriff auf das Firmennetz benötigen. Bei entsprechender Konfiguration kann ein Benutzer remote genauso arbeiten, als ob sich sein Computer im Firmennetz befinden würde. Nur die Datenübertragung erfolgt normalerweise langsamer.

RAS arbeitet auf OSI-Schicht 2 meist über das Protokoll PPP und diversen Authentifizierungsprotokollen beim Verbindungsauflauf (vgl. Kapitel 18). In den darüberliegenden Schichten können Protokolle wie **TCP/IP** oder **TCP/IPv6** benutzt werden. Durch die Unterstützung der Tunneling-Protokolle kann für einzelne Clients über RAS auch eine **VPN-Verbindung** konfiguriert werden. Bei Microsoft Windows gehört RAS (früher als **DFÜ-Netzwerk** bezeichnet) zum festen Bestandteil der Netzwerkfunktionalität.

17.4 Vermittlungsprinzip

In Bezug auf die Vermittlung werden im WAN zwei Grundprinzipien unterschieden, nämlich Paketvermittlung und Leitungsvermittlung.

Paketvermittlung

Bei der Paketvermittlung besteht keine dedizierte physikalische Verbindung zwischen Sender und Empfänger. Die Daten werden zwischen Sender und Empfänger an verschiedenen Stationen zwischengespeichert (z. B. Router). Eine Garantie über den Datendurchsatz kann nicht gegeben werden. Wenn ein Zwischenspeicher keine Kapazität mehr zur Verfügung hat, können Pakete verloren gehen.

Zur Verdeutlichung dieser Art der Vermittlung kann als Beispiel der Paketversand per Post dienen: Wie bei der Post werden Datenpakete unterschiedlicher Größe verschickt. Die Daten werden dem Vermittlungsnetz übergeben, das sie über unterschiedliche Stationen ans Sendeziel bringt.

Leitungsvermittlung

Bei der Leitungsvermittlung besteht eine physikalische oder virtuelle Verbindung zwischen Sender und Empfänger. Zur Datenübertragung wird eine feste Verbindung aufgebaut, die entsprechende Kapazitäten und eine bestimmte Qualität hat. Während der Verbindung existieren dementsprechend definierte Rahmenbedingungen. Nach Ende der Datenübertragung wird die Verbindung wieder abgebaut.

Als Beispiel kann hier ein Telefongespräch erwähnt werden. Dieses Beispiel zeigt auch das Problem, das hier auftauchen kann, nämlich der Verbindungsaufbau. Ein Teilnehmer kann belegt sein.

Vergleich von Paketvermittlung und Leitungsvermittlung

Kennzeichen	Paketvermittlung	Leitungsvermittlung
Verbindungsaufbau	Nein	Ja
Dedizierte Leitung	Nein	Ja
Gleiche Route für alle Pakete	Nein	Ja
Verfügbare Bandbreite	Dynamisch	Fest, garantiert
Zwischenspeicherung	Ja	Nein
Abrechnung	Datenmenge	Zeiteinheit

17.5 Netzneutralität

Bisher wurden die über das Internet verschickten Daten im Wesentlichen **gleich behandelt** (mit Ausnahme der Priorisierung zeitkritischer Dienste). Dieses Vorgehen wird mit Netzneutralität bezeichnet. Die klassischen Dienste wie World Wide Web (WWW), Telefonie über das Internet (VoIP), Mailversand etc. haben heute jedoch immer weniger Anteil am Datenaufkommen im Internet.

Netzbetreiber müssen riesige Datenmengen (hauptsächlich von Videoportalen) transportieren, ohne zusätzliche Einnahmen zu erhalten. Daher möchten sie an der Übertragung bestimmter Inhalte mit einer garantierten Service-Qualität mitverdienen. Sie führen auch aus, dass bisher im Internet die Übertragung von Daten mit einer bestimmten Qualität nicht geregelt ist. Verschärfte Regulierung und Diskriminierung bestimmter Dienste könnten die Folge sein.

Für Gleichbehandlung treten andererseits viele Online-Firmen (Content-Provider) wie Google, Facebook, Youtube, ein. Sie argumentieren, dass gerade durch ihre Angebote das Internet erst attraktiv wird.

Hierzu hat die amerikanische Telekommunikations-Aufsichtsbehörde **Federal Communications Commission (FCC)** im Mai 2014 einen Entwurf zur Diskussion gestellt. Kritiker befürchten, dass damit ein Zwei-Klassen-Internet entstehen könnte, in dem im Extremfall bestimmte Dienste nicht mehr möglich wären, währenddessen Dienste mit populären Inhalten das Netz überschwemmen. Denkbar wäre auch eine Finanzierung durch zeitweise eingebblendete Zwangswerbung.

Die Diskussion über diese Themen dauert noch an bzw. flammt je nach persönlichem Standpunkt immer wieder auf. Auch sorgen gerichtliche Entscheidungen für neuerliche Diskussionen, daher ist eine abschließende Betrachtung im Rahmen dieses Buches nicht möglich.

Hinweise zur Netzneutralität finden Sie z. B. hier:

- ✓ <https://www.zdnet.de/88193370/netzneutralitaet-fcc-erlaubt-priorisierung-von-internet-traffic/>
- ✓ <https://www.zeit.de/digital/internet/2017-12/netzneutralitaet-streamon-bundesnetzagentur-verbraucher-interesse>
- ✓ <https://de.wikipedia.org/wiki/Netzneutralit%C3%A4t>
- ✓ <https://netzpolitik.org/tag/netzneutralitaet/>

17.6 Privatsphäre im Internet

Internet und Nutzerdaten

Wer sich mit dem Internet verbindet, bleibt nicht anonym. Sobald eine Verbindung mit einem anderen Rechner (Server) erfolgt, ist diesem die vom Provider vergebene offizielle IP-Adresse bekannt, mit der sogar Rückschlüsse auf den ungefähren Aufenthaltsort des Benutzers möglich sind. Solange der Provider diese IP-Adresse speichert, kann daraus der angemeldete Nutzernname ermittelt werden. Auch die **Metadaten** (wie die Verbindungsdaten, Betreffzeilen etc.) werden in aller Regel unverschlüsselt übertragen. Im Gegensatz zu den Daten, werden diese selbst beim Versand von verschlüsselten Mails (per PGP bzw. SMIME) oder beim Verbindungsaufbau einer sicheren Verbindung per HTTPS nicht besonders geschützt.

Vor allem die Firma Google hat in letzter Zeit mit etlichen Beispielen gezeigt, wie sie intensiv Daten von Benutzern sammelt. Hinzu kommt, dass viele Benutzer von Facebook, Google+ und anderen sozialen Plattformen sehr freigiebig ihre persönlichen Daten veröffentlichen. Dabei ist nicht sicher, wie diese Firmen mit den ihnen anvertrauten Daten umgehen, ob sie z. B. vollständig oder teilweise verkauft werden und wann Geheimdienste mitlesen.

Grundsätzlich können Sie heute davon ausgehen, dass so gut wie alle übertragenen Daten und andere Tätigkeiten in Weitverkehrsnetzen abgehört werden, selbst Telefonate, Mails, SMS-Nachrichten, Faxe etc. Schutz vor dem Abhören bietet nur eine gute **Verschlüsselung**.

Anonymisierungs-Netzwerke

Anonymisierungs-Netzwerke, wie z. B. **the onion router(Tor)**, bieten Schutz durch eine Kaskade von zufällig verbundenen Rechnern aus einem Pool registrierter Rechner. Für den eigentlichen Ziel-Server, mit dem sich der Benutzer verbindet, bleibt dabei die IP-Adresse des Anwenders anonym. Innerhalb dieser Netze (vom Eintritt in das Netz bis zum Aufruf der Daten im Internet) werden die Daten in der Regel **verschlüsselt** übertragen. Problematisch daran ist die relativ geringe Übertragungsrate. Außerdem ist unklar, wer die Ein- bzw. Austritts-Rechner betreibt und damit Daten im Klartext mitlesen könnte.

Möglicherweise werden erst durch die Benutzung dieser Netzwerke Geheimdienste (z. B. die amerikanische NSA) auf Sie aufmerksam, wie dies Mitte 2014 einem deutschen Betreiber eines Tor-Servers erging. Anonymisierungs-Netzwerke bieten einen Schutz für Andersdenkende in vielen totalitären Staaten, jedoch werden sie oft auch durch Kriminelle genutzt, die ihre Geschäfte damit verschleiern (Stichwort „Darknet“).

Nutzerprofile

Viele Content-Provider versuchen intensiv, die Nutzer ihrer Dienste jederzeit wiederzuerkennen, um Nutzerprofile zu erstellen, die sie dann u. a. für das Anbieten gezielter Werbung verwenden. Machbar ist dies beispielsweise mit **Cookies**, Supercookies (**LSO** = Local Shared Objects, auch Flash-Cookies), **Tracking**, **Browser-Fingerprints**, **Clock-Skew-Fingerprinting** oder **Apps** (installierbaren Applikationen). Diese Methoden wirken sogar durch Anonymisierungs-Netzwerke hindurch, da der Anwender eindeutig identifiziert werden kann, wenn sich ein eindeutiger Cookie auf seinem System befindet. Einige dieser Aktionen können in den Einstellungen des Browsers abgeschaltet werden, jedoch ist die Verwendung von **Cookies** häufig nötig. Viele Webseiten (z. B. Shoppingportale) würden ohne Cookies nicht funktionieren. Ein Browser kann aber so eingerichtet werden, dass er Cookies beim Beenden automatisch löscht.

Herkömmliche Cookies hinterlassen Spuren auf dem eigenen Rechner, andere Methoden sind vom Anwender jedoch nicht erkennbar. In der Datenschutz-Gesetzgebung werden viele Technologien noch nicht berücksichtigt, sodass oft nicht klar geregelt ist, wie weit ein Internetanbieter gehen darf.

Identitätsdiebstahl

Dabei handelt es sich um die Übernahme von Anmeldeinformationen durch Kriminelle. Sie können sich damit bei Online-Portalen, Mail-Versendern, sozialen Netzwerken, Versandhändlern, Banken usw. unter anderem Namen anmelden und den eigentlichen Inhaber des Kontos erheblich schädigen. Falls Sie betroffen sind, sollten Sie auf jeden Fall erst Strafanzeige erstatten und danach alle beteiligten Stellen informieren.

Abhilfe kann nur die Verwendung sicherer Passwörter bieten. Laut BSI sollten sie mindestens 12 Zeichen lang sein und Zahlen und Sonderzeichen enthalten, jedoch keine Begriffe aus Wörterbüchern.

Für jedes Konto sollte das Passwort anders lauten. Sonst kann ein einmal erbeutetes Passwort der Schlüssel zu weiteren Konten sein. Wer prüfen will, ob seine eigenen Anmeldedaten bereits von Kriminellen erbeutet wurden, kann dies auf folgenden Internetseiten checken:

- ✓ <https://sec.hpi.uni-potsdam.de/leak-checker> (Identy Leak Checker vom Hasso Plattner Institut)
- ✓ <https://Haveibeenpwned.com> (Seite von Troy Hunt)

Weitere Hinweise zur Sicherheit in Netzwerken finden Sie im HERDT-Buch *Netzwerke – Sicherheit*.

Privacy Extentions bei IPv6

Unter IPv6 kann jeder Rechner eine eigene offizielle IP-Adresse haben. **NAT** ist dann zwar nicht mehr erforderlich, aber dennoch nutzbar, um die interne Netzwerk-Topologie geheim zu halten.

Mit einer IPv6-Adresse kann der eigene Rechner jederzeit wiedererkannt werden. Besonders bei der Vielzahl der Geräte beim Internet der Dinge (IoT, vgl. Kapitel 4.7) kann dies ein Problem darstellen. Um ein Wiedererkennen zu verhindern, gibt es die **Privacy Extentions** nach RFC 4941, mit denen zufällige Änderungen in die Host-ID (Interface Identifier) der **IPv6-Adresse** einfließen (der davor stehende Präfix bleibt gleich).

Windows aktiviert diese auf Desktop-Versionen seit Windows XP automatisch. Unter Linux sind sie ebenfalls aktivierbar (falls nicht bereits automatisch geschehen, wie bei Ubuntu seit Version 12.04).

Perfect Forward Secrecy

Mit **Perfect Forward Secrecy** (PFS) ist eine verschlüsselte Verbindung langfristig erheblich besser geschützt, solange das Zertifikat nicht entschlüsselt oder öffentlich ist. Der geheime Sitzungsschlüssel, über den die eigentliche Verschlüsselung erfolgt, wird dabei nicht mit übertragen. Die Kommunikationspartner einigen sich auf einen Schlüssel, der über das **Diffie-Hellmann** Verfahren ausgetauscht wird.

So kann eine aufgezeichnete Verbindung **nicht** nachträglich entschlüsselt werden. Auch nicht über ein eventuelles Bekanntwerden des geheimen Schlüssels, wie dies zum Beispiel Anfang 2014 durch den Heartbleed-Exploit möglich war.

18

Übertragung in Weitverkehrsnetzen

18.1 Übertragungsverfahren

Arten der Informationsübertragung

In Weitverkehrsnetzen bzw. bei der Verbindung mit dem Internet über Provider erfolgt auf **OSI-Layer 1** eine Übertragung von Daten hauptsächlich per Modulation, per Multiplex oder einer Mischung aus beidem. Diese werden auch in Funktechniken (WLAN, Mobilfunk) eingesetzt.

Auf **OSI-Layer 2** ist in der Regel das **Point-to-Point Protocol (PPP)** und bei DSL-Verbindungen dessen Ableger **Point-to-Point Protocol over Ethernet (PPPoE)** (vgl. Kapitel 18.5) das Trägerprotokoll für alle weiteren Protokolle zum Internet (IP, TCP, UDP usw.).

Modulation

Bei der Übertragung per Modulation wird eine **Trägerfrequenz** mit festgelegter Bandbreite durch verschiedene Modulationsarten mit dem Nutzsignal verändert (**moduliert**), dann übertragen und am Ziel das Nutzsignal extrahiert (**demoduliert**). Bei den nicht mehr gebräuchlichen klassischen Modems (als Abkürzung für **MOdulator – DEModulator**) spricht man ebenfalls von Modulation; hier wurde ursprünglich für eine logische „1“ ein anderer Ton als für eine logische „0“ über das Telefonnetz (Sprachband (300 Hz–3,4 kHz) gesendet.

Multiplex

Per **Multiplex** werden **mehrere** Trägerfrequenzen durch entsprechende Verfahren so verbunden, dass sie über das gleiche Medium (Kupferkabel, Funkstrecke, Lichtleiter) zusammen verschickt werden können. Es gibt hier hauptsächlich Zeitmultiplex (mit zeitlicher verteilter Übertragung) und Frequenzmultiplex (mit Modulation auf eine oder mehrere Trägerfrequenzen).

Ferner gibt es Mischformen beider Techniken. Beispiele hierfür sind DSL und ISDN. Bei DSL erfolgt zunächst mit **Discrete Multi Tone (DMT)** die **Modulation** der Trägerfrequenzen (Multi-Carrier) und bei ISDN mit **Pulse Coded Modulation (PCM)**, bevor sie per **Multiplex** gebündelt verschickt werden.

Das Telefonnetz als Basis

Das klassische Telefonnetz mit seinen flächendeckend verlegten 2-Draht-Leitungen ist seit mehreren Jahrzehnten die kostengünstige Basis, um Weitverkehrsverbindungen zur Datenübertragung aufzubauen. Sie werden sowohl von analogen Modems wie von ISDN- und DSL-Geräten für die Übertragung der Informationen benutzt.

Verbindungen über **Funk** (UMTS, LTE, Satellit etc.) und das **Kabelfernsehnetz** holen in der Bedeutung auf (vgl. Kapitel 19).

18.2 Analoge Übertragung

Analoge Übertragung mit Modems

Modems arbeiten mit unterschiedlichen Modulationsverfahren, d. h. verschiedene Zuordnungen von Datenbits zu Tonsignalen. Diese wurden von der früheren CCITT (heute **ITU**) in verschiedenen V-Normen standardisiert. Die Tabelle zeigt einige Definitionen aus dieser Gruppe.

Die in der Tabelle angegebenen Bitraten sind nominelle Raten, die nur bei optimalen Bedingungen erreichbar sind.

Norm	Beschreibung und maximale Bitrate
V.34	28800 Bit/s
V.34+	33600 Bit/s
V.90	56 Kbit/s Downstream, 33,6 Kbit/s Upstream, eine spezielle Gegenstelle ist nötig
V.92	56 Kbit/s Downstream, 48 Kbit/s Upstream

Analoge Datenübertragungen spielen heute, mit Ausnahme vom Versand von Fax-Mitteilungen, keine Rolle mehr.

ISDN

Hinter der Abkürzung ISDN (**Integrated Services Digital Network**) steht das Ziel eines dienst-integrierenden Netzes für Sprache und Daten auf digitaler Basis. Seit 1993 steht es in Deutschland flächendeckend zur Verfügung.

Grundsätzlich werden zwei verschiedene Anschlüsse unterschieden:

- ✓ **Basic Rate Interface (BRI):** ein Basis-Anschluss mit **zwei** sogenannten B-Kanälen à 64 Kbit/s und einem D-Kanal mit 16 Kbit/s
- ✓ **Primary Rate Interface (PRI):** Primärmultiplex-Anschluss mit **30** B-Kanälen à 64 Kbit/s und 2 Steuerkanälen

ISDN arbeitet sowohl bei PRI als auch bei BRI mit B- und D-Kanälen. Deren Arbeitsweise unterscheidet sich bei beiden Anschlussarten nicht. Nur die Anzahl bzw. Kapazität der zur Verfügung stehenden Kanäle ist unterschiedlich.

Ein **B-Kanal** ist ein bittransparenter Kommunikationskanal mit einer Übertragungsgeschwindigkeit von 64 Kbit/s. Er stellt den eigentlichen Datenkanal dar. Mehrere Kanäle können zusammengefasst werden, um höhere Datenübertragungsraten zu erreichen. Es wird dann von Kanalbündelung gesprochen.

Der **D-Kanal** hat eine Übertragungsgeschwindigkeit von 16 Kbit/s (BRI) bzw. 64 Kbit/s (PRI) und dient zur Übertragung von Steuerinformationen für die B-Kanäle. Der Verbindungsaufl- und -abbau sowie die Steuerung der Kommunikation in den Nutzkanälen finden im D-Kanal statt, auch die Übermittlung der Telefonnummer des Anrufers.

! Da die deutsche Telekom ISDN nicht mehr unterstützt, gilt es als veraltet. Neuanschlüsse werden bereits seit einigen Jahren nicht mehr angeboten. Sprachübertragungen werden nur noch auf Basis von **VoIP** (Voice over IP) angeboten. Auch viele der analogen Telefonanschlüsse werden auf VoIP umgestellt, was der Kunde allerdings nicht bemerkt, da die Umsetzung in den Vermittlungsstellen erfolgt. Eine weitere Praxis ist es, analoge Anschlüsse, die über DSL verfügen, zu kündigen, um sie durch VoIP zu ersetzen.

18.3 DSL

Hintergrund

DSL steht für **Digital Subscriber Line**. xDSL ist der Oberbegriff für etliche DSL-Varianten, die durch einen jeweils anderen Anfangsbuchstaben differenziert werden. Allgemein versucht die DSL-Technologie, auf vorhandenen ungeschirmten, verdrillten Kupferkabeln (bestehende Telefon- oder UTP-Kabel) höhere Durchsatzraten umzusetzen. Die Deutsche Telekom AG z. B. bietet ADSL unter dem Kürzel T-DSL an.

Die verschiedenen Varianten unterscheiden sich durch anwendungsspezifische Merkmale. Allen gemein ist die Ansiedlung auf der Schicht 1 des OSI-Modells. Die wichtigsten Parameter für die zu erreichenden Übertragungsraten sind der jeweilige Leitungsdurchmesser und die Entfernung zum Endteilnehmer.

ADSL

Asymmetric Digital Subscriber Line (ITU G.992.1) unterstützt Breitband-Datenverkehr in Hochgeschwindigkeit auf dem normalen Kupferkabel-Telefonnetz. Die Bezeichnung „asymmetrisch“ besagt, dass bei dieser Technologie mit unterschiedlichen Übertragungsraten für den Upstream (Senderichtung) und Downstream (Empfangsrichtung) gearbeitet wird, im Gegensatz zu SDSL (siehe weiter unten). Für ADSL lassen sich folgende Basiswerte nennen:

- ✓ die maximale Senderate liegt bei 1,0 Mbit/s,
- ✓ die maximale Empfangsrate liegt bei 10 Mbit/s.

Mit **ADSL2+** (nach ITU G.992.5) wurden die Werte für Upstream auf 3,5 Mbit/s und für Downstream auf 25 Mbit/s erweitert. Die maximale Leitungslänge zur Vermittlungsstelle beträgt 6 km bei einer Geschwindigkeit unter 1,5 Mbit/s und 4 km bei einer höheren Geschwindigkeit.

Beschreibung

ADSL wurde Anfang der 90er-Jahre von Bellcore entwickelt und vom ANSI als Standard T1.413 übernommen. Es eignet sich vor allem für schnelle Internetanbindungen von Privatpersonen und kleinere Firmen. Zur Verbindungsaufnahme ist entweder ein DSL-Modem oder ein Kombigerät (DSL-Router) nötig, in dem DSL-Modem, Router, Switch, WLAN-Access-Point und etliches mehr gemeinsam verbaut sind. Prominentester Vertreter dürften die Geräte mit Namen FRITZ!Box der Berliner Firma AVM sein.

Über das **Discrete Multi Tone (DMT)**-Modulationsverfahren, das viele schmale Hochfrequenz-Bänder („Bins“) mit je 4,3125 kHz Bandbreite verwendet, wird bei DSL die Übertragung verteilt. Die Anzahl der Bänder kann von 256 DMT-Trägern bei ADSL bis zu 4096 bei VDSL2 und mehr betragen. Gestörte Bänder (z. B. durch Rundfunksender) bleiben so lange abgeschaltet, bis die Störung vorüber ist.

Auf der Telefonleitung befinden sich die Frequenzbereiche von analogem Telefon (0,3 bis 3,4 kHz) bzw. von ISDN (bis zu 120 kHz) unter den Frequenzbereichen von DSL (138 kHz bis in den MHz-Bereich). Die Trennung erfolgt beim Kunden über einen **Splitter**. Bei Komplettanschlüssen (der Provider bietet kombiniert Daten-Übertragung und Telefonie an) entfällt der Splitter, da dabei auch die Telefonate per VoIP über die DSL-Verbindung übertragen werden. Verfahren wie SDSL verwenden ebenfalls den kompletten Frequenzbereich (ohne Splitter).

DSL-Light

Besonders in ländlichen Gebieten ist ADSL immer noch nicht flächendeckend verfügbar. Da dort die Leitungen zur nächsten Vermittlungsstelle oft sehr lang sind, ist die Mindest-Übertragungsrate von 768 Kbit/s meist nicht erreichbar. In diesen Regionen wird mitunter eine Sparversion mit 384 Kbit/s mit Namen „DSL-Light“ bzw. „DSL 384“ (nach ITU G.992.2) angeboten.

VDSL

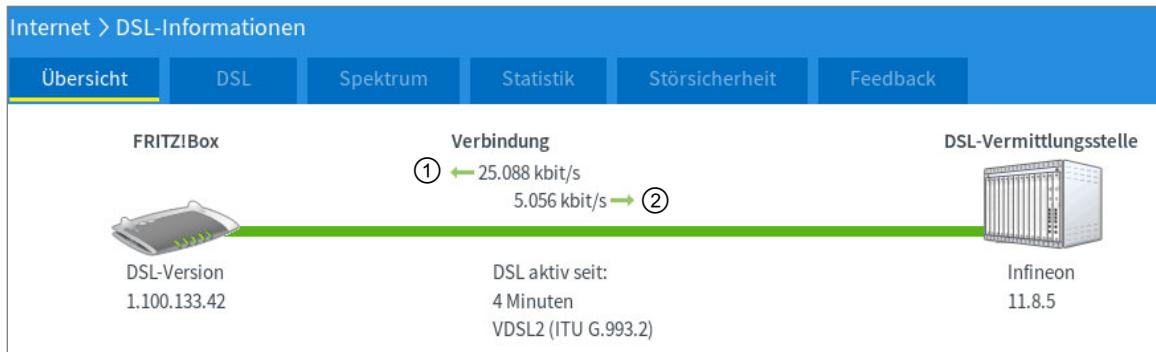
Very High Bitrate Digital Subscriber Line beruht auf denselben technischen Überlegungen wie ADSL und ist die schnellste DSL-Variante für den privaten Gebrauch bzw. Einsatz in kleineren Unternehmen. Es können mit **VDSL1** (nach ITU G.993.1) Datenraten im Downstream bis 52 Mbit/s und im Upstream bis 11 Mbit/s realisiert werden.

Allerdings sind diese Angaben stark von der Entfernung zur Vermittlungsstelle abhängig. So halbiert sich bereits bei etwa 1000 m Entfernung die maximale Übertragungsbandbreite, in ca. 2000 m Entfernung sind nur noch Werte erreichbar, die denen von ADSL entsprechen. VDSL1 konnte sich jedoch kaum durchsetzen.

Der Nachfolgestandard **VDSL2** (nach ITU G.993.2, früher VHDSL) bietet bis zu 100 Mbit/s im Downstream und ist ebenfalls stark abhängig von den Eigenschaften der Leitung.

Alle hier genannten Varianten von DSL basieren auf der gleichen **DMT**-Technik (siehe oben) und sind zu ADSL abwärtskompatibel. Welche letzten Endes zum Einsatz kommt, hängt zum einen von der Leitung ab (Länge, Querschnitt, Entfernung zur nächsten Vermittlungsstelle) und davon, ob dort ein **DSL-Access-Multiplexer (DSLAM)** bzw. eine DSL-Vermittlungsstelle verfügbar ist.

Weiter hängt es von den vertraglichen Möglichkeiten ab, welcher Typ von Anschluss dem Kunden in seinem Bereich zur Verfügung steht (Übertragungsrate der Provider, Anzahl öffentlicher IP-Adressen aus welchen Adressbereich, vereinbare Leistungen und Garantien (z. B. Verfügbarkeit)).



Down- ① und Upload-Raten ② an einem VDSL2-Anschluss (Konfigurationsausschnitt eines DSL-Routers)

Die erforderliche Hardware (z. B. ein DSL-Router) wird meist vom Provider ohne weitere Kosten zur Verfügung gestellt. Besonders bei professionellen Verbindungen per SDSL, G.SHDSL oder SHDSL sind genaue Festlegungen wichtig.

VDSL2-Vectoring

Das Verfahren **VDSL2-Vectoring** (nach ITU G.993.5, G.vector) kann die wechselseitigen Störungen eliminieren, die in parallel verlegten Leitungsbündeln auftreten. Damit kann die Reichweite auf verlegten alten Telefonleitungen gesteigert werden. Bis zu 600 Metern Distanz sind es bis zu 100 Mbit/s im Downstream und bis 40 Mbit/s im Upstream. Das theoretische Maximum liegt aktuell bei 200 Mbit/s. Allerdings müssen dabei alle Signale eines Kabelverzweigers zeitlich koordiniert werden, was nur dann möglich ist, wenn alle Anschlüsse dem gleichen Anbieter gehören.

HDSL

Für **High Data Rate Digital Subscriber Line** wurden in Europa Datenraten von 2,048 Mbit/s (E1-Leitung) und in den USA von 1,544 Mbit/s (T1-Leitung) spezifiziert. Die europäische Norm erfordert drei, die amerikanische nur zwei vorhandene Adernpaare. Es können Entfernung bis 5 km überbrückt werden. Der Nachfolger ist **SDSL**.

HDSL2

HDSL2 wurde Anfang 1998 als Normenvorschlag dem **ANSI** vorgelegt. Der Kern des Vorschlags betrifft die Leistung einer T1-Leitung über nur ein Adernpaar. Es ist in den Standard G.SHDSL übergegangen.

SDSL

Symmetric Digital Subscriber Line(SDSL) ist wie **HDSL** ein Vollduplexverfahren mit symmetrischen Übertragungsgeschwindigkeiten von bis zu 2,048 Mbit/s. Symmetrisch bedeutet, dass die freigeschaltete Übertragungsrate in beiden Richtungen gleich groß ist. Die maximale Reichweite liegt bei 3,5 km. SDSL ist auch unter dem Namen Single-Pair High-Speed Digital Subscriber Line bekannt, wobei die Abkürzung SHDSL zu Verwechslungen führen kann.

Eine gleichzeitige Verwendung von Telefonen ist an einem SDSL-Anschluss nicht möglich bzw. nur per VoIP. Heute erhält man in der Regel einen G.SHDSL-Anschluss, wenn SDSL gewünscht wird.

Vom Europäischen Institut für Telekommunikationsnormen ETSI wurde es über die Norm TS101524 und von der ITU über die Norm G.991.2 unter dem Namen SHDSL definiert.

G.SHDSL

Global Standard for Single-Pair High-Speed Digital Subscriber Line (G.SHDSL) fasst die Standards SDSL und HDSL2 zusammen (nach ITU-Standard G.991.2). Dabei ist die Übertragungsrate in beide Richtungen gleich groß, es handelt sich also um eine symmetrische Verbindung. Über eine Doppelader erreicht es bis zu 2 Mbit/s, mit zwei Doppeladern bis zu 4 Mbit/s. Mit der Erweiterung **SHDSL.bis** sind 5,696 Mbit/s möglich, die zusätzlich über bis zu 4 Kupferdoppeladern gebündelt werden können.

SHDSL

Symmetrical High-Density Digital Subscriber Line bzw. auch Symmetrical High Bitrate Digital Subscriber Line ist ebenfalls eine symmetrische Verbindung. Es wird darunter eine DSL-Standleitung verstanden, die bis zu 8 Mbit/s in beiden Richtungen bereitstellen kann. Es handelt sich ebenfalls um ein SDSL-Verfahren und wird oft auch mit **SHDSL.bis** bzw. **G.SHDSL** gleichgesetzt.

18.4 SDH/SONET

Hintergrund

SDH/SONET wurde für Weitverkehrssysteme entwickelt und 1988 weltweit als Standard definiert. Es werden zwei Varianten unterschieden, nämlich die europäische ETSI-SDH und die nordamerikanische ANSI-SONET. Beide sind auf der Schicht 1 des OSI-Modells angesiedelt und unterscheiden sich nur geringfügig.

SDH

Synchronous Digital Hierarchy (SDH) löste die veraltete Übertragungsstruktur PDH (**Plesiochronous Digital Hierarchy**) aus den 70er-Jahren ab. Im Vergleich mit PDH sind z. B. alle SDH-Netze und -Systeme kompatibel, es sind mehr Funktionen genormt und es lassen sich logische Verbindungen zwischen Teilnehmern aufbauen. SDH kann von ATM als physikalisches Transportmedium genutzt werden.

SDH beschreibt dabei im Wesentlichen nur die Struktur von Übertragungsrahmen auf Multiplexsystemen in der Bitübertragungsschicht. In der Empfehlung ITU G.707 werden 155,52 Mbit/s als Grundbitrate definiert. Die Bitraten der nächsten Stufen sind jeweils ein Vielfaches davon.

SONET

Synchronous Optical Network wurde von den Bell-Laboratories als Übertragungsverfahren für Weitverkehrsnetze entwickelt und ist die amerikanische Variante von SDH. SONET verwendet auf der ersten Hierarchiestufe eine Bitrate von 51,84 Mbit/s.

Die folgende Tabelle stellt einige der gebräuchlichsten Geschwindigkeiten mit deren Kürzeln vor, wobei die Abkürzung STM für **Synchronous Transfer Mode** steht, STS für **Synchronous Transport Signal** und OC für **Optical Carrier**.

SDH (Europa)	SONET (Amerika)		Übertragungsrate
	STS-1	OC-1	51,840 Mbit/s
STM-1	STS-3	OC-3	155,520 Mbit/s
STM-4	STS-12	OC-12	622,080 Mbit/s
STM-8	STS-24	OC-24	1.244,160 Mbit/s
STM-16	STS-48	OC-48	2.488,370 Mbit/s
STM-64	STS-192	OC-192	9.953,280 Mbit/s
STM-128	STS-384	OC-384	19.906,560 Mbit/s
STM-256	STS-768	OC-768	39.813,120 Mbit/s
STM-512	STS-1536	OC-1536	79.626,240 Mbit/s
STM-1024	STS-3072	OC-3072	159.252,480 Mbit/s

Zukunftsträchtig

Obwohl SDH und Sonet eigentlich als Zeitmultiplexsysteme konzipiert wurden, sind sie offen für **Wavelength Division Multiplexing (WDM)**, was von vielen Carriern zunehmend als Verfahren eingesetzt wird, um die vorhandenen Kapazitäten der Glasfaserleitungen zu vervielfachen.

18.5 Protokolle der Sicherungsschicht

Vorbemerkungen

In den folgenden Abschnitten werden etliche Protokolle aufgelistet, die grundlegend auf Schicht 2 des OSI-Modells angesiedelt sind und den Verkehr über Weitverkehrsnetze betreffen. Die Normung der Protokolle geschieht in erster Linie über das Internet Architecture Board (**IAB**) bzw. deren Teilgruppe IETF und wird in Form von **RFCs (Request for Comments)** veröffentlicht.

Verschlüsselung

Die Verschlüsselung von Daten steht in einem engen Zusammenhang mit diesen Protokollen, denn sobald Informationen über Weitverkehrsnetze übertragen werden, haben die beteiligten Kommunikationspartner keine vollständige Kontrolle mehr über den Datenfluss. Besonders bei wichtigen Daten auf Notebooks, USB-Sticks und Smartphones sollte auf eine sichere Verschlüsselung (vor allem mit **Advanced Encryption Standard (AES)**-Verfahren) geachtet werden, da beim Verlust dieser Geräte ein wesentlich größerer Schaden entstehen kann, als der Wert der Hardware selbst darstellt. Auch bei Daten, die im Internet abgelegt sind (z. B. in Cloud-Speichern), ist eine Verschlüsselung sehr wichtig, wenn es sich um sensible Informationen handelt.

Vor allem bei der Speicherung im Internet (Cloud-Speichern, wie bei Amazons S3, Dropbox u. a.), sollte eine Verschlüsselung der Daten selbstverständlich sein, deren Schlüssel nicht in fremden Händen liegt. Von dem Angebot des Anbieters, eine eigene Verschlüsselung anzubieten, sollte Abstand genommen werden. Hier ist nicht sicher, ob der Anbieter oder andere Organisationen die Daten im Klartext ebenfalls lesen.

Zur Verschlüsselung von Daten gibt es mehrere Verfahren, wobei grundlegend zwischen symmetrischen und asymmetrischen Kryptografieverfahren unterschieden wird.

Symmetrische Verschlüsselungsverfahren

Zu dieser Gruppe gehören z. B. **Data Encryption Standard (DES)**, **Triple DES (3DES)**, **International Data Encryption Algorithm (IDEA)**, **Ron's Cipher 4 und 5 (RC4, RC5)**, **Advanced Encryption Standard (AES)** und **Blowfish**. Hier besitzen beide an der Kommunikation beteiligten Partner den **gleichen** Schlüssel zur Ver- und Entschlüsselung. Übliche Schlüssellängen sind 128 Bit bis 256 Bit. Der Nachteil dieser Verfahren ist das logistische Problem des Schlüsselaustausches.

Symmetrische Verschlüsselungsverfahren mit genügend langen Schlüsseln werden auch in Zukunft von einer neuen Art von Rechner, dem Quantencomputer, nicht zu knacken sein. Asymmetrische Verfahren dagegen schon.

Asymmetrische Verschlüsselungsverfahren

Bei diesem Verfahren wird ein Schlüsselpaar zum Ver- und Entschlüsseln benutzt. Über komplexe Algorithmen werden zwei Schlüssel erzeugt, wobei der eine Schlüssel der Verschlüsselung und der andere der Entschlüsselung dient. Der Schlüssel zur Verschlüsselung kann offen weitergereicht werden, da aus diesem der Entschlüsselungsschlüssel nicht berechnet werden kann.

Diesen Schlüssel bezeichnet man als öffentlichen Schlüssel, **Public-Key**. Der andere bleibt geheim beim Besitzer des Schlüsselpaares (der **Private-Key**). Daher spricht man auch von Public-Key-Verfahren. Übliche Schlüssellängen sind 1024 Bit bis 4096 Bit.

Aufwendig ist die Verwaltung der Schlüssel, da jeder, der z. B. eine verschlüsselte E-Mail-Nachricht senden möchte, zunächst den öffentlichen Schlüssel des Empfängers benötigt. Diese sind über Trustcentren, öffentliche Schlüsselserver, als Download auf der Webseite des Empfängers oder im Zweifelsfall beim Empfänger selbst erhältlich.

Zur Gruppe der asymmetrischen Verschlüsselungsverfahren zählen:

- ✓ **RSA** (Rivest Shamir Adleman): Dies ist ein nach seinen Erfindern benannter asymmetrischer Verschlüsselungsalgorithmus. Die Schlüssellänge sollte mindestens 1024 Bit betragen.
- ✓ **Diffie-Hellmann**: Die „DH-Gruppe“ legt quasi die Länge der verwendeten Primzahl fest. Gruppe 1 benutzt 768 Bit (dies bietet mitunter keine ausreichende Sicherheit mehr), für Gruppe 2 sind dies 1024 Bit, für Gruppe 5 1536 Bit, bei höheren Ansprüchen mit Gruppe 7 3072 Bit usw. Dieses Verfahren wird heute fast nur noch zum sicheren Schlüsselaustausch verwendet.

Anwendung finden asymmetrische Verschlüsselungsverfahren beispielsweise in folgenden Protokollen bzw. Standards:

- ✓ OpenPGP und S/MIME (Verschlüsselung von E-Mails),
- ✓ HTTPS (gesicherte Verbindung zu einem Webserver, beispielsweise für das Onlinebanking),
- ✓ SSH (geschützte Terminalverbindung, z. B. zu einem Linux- oder UNIX-Server).

Hybride Verfahren

Da die asymmetrische Verschlüsselung langsamer ist als die symmetrische, werden beide Verfahren meist miteinander gemischt. Am Anfang jeder Übertragungssitzung wird über ein Public-Key-Verfahren ein „Session-Key“ generiert, mit dem danach für den Rest der Übertragung über ein symmetrisches Verfahren ohne Geschwindigkeitsverlust weitergearbeitet wird.

Die genannten Verfahren bieten eine **Transportverschlüsselung** bzw. **Punkt-zu-Punkt-Verschlüsselung**, was bedeutet, dass die Daten nur während deren Transport verschlüsselt sind und am Ziel im Klartext vorliegen.

Im Gegensatz dazu bietet eine **Inhaltsverschlüsselung** bzw. **Ende-zu-Ende-Verschlüsselung** besseren Schutz, da dabei die Daten bereits vor der Übertragung auf dem eigenen Rechner verschlüsselt werden und auch auf dem Zielsystem verschlüsselt abgelegt bleiben. Bei einer Auslagerung (Outsourcing) von Rechenleistung ist dies jedoch nicht machbar, da verschlüsselte Daten bisher nicht verarbeitet werden können. **Homomorphe Verschlüsselung** stellt einen Ansatz dar, in naher Zukunft auch mit verschlüsselten Daten in Rechenzentren zu arbeiten.

Verifizierung und Signierung

Zur Verifizierung des Inhalts von Dateien, Programmen, E-Mails, DVDs etc. werden oft **Message Digest Algorithm 5 (MD5)** oder **Secure Hash Algorithm (SHA)** Prüfsummen verwendet. Es sind kryptografische Hash-Funktionen, die einen kurzen Hashwert erzeugen (typisch 32–128 Zeichen), der nur für diesen Inhalt der Datei (Programm, E-Mail, DVD etc.) zum Zeitpunkt der Erzeugung des Hashwertes gilt. Jede noch so kleine Änderung an der Datei (Programm, E-Mail, DVD etc.) zu einem späteren Zeitpunkt ergibt einen anderen Hashwert.

Um zu prüfen, ob der Inhalt exakt dem Original entspricht, braucht man nur einen MD5- bzw. SHA-Hashwert zu erzeugen (z. B. mit den Programmen `md5sum`, `sha1sum` etc.) und mit dem abgespeicherten oder mitgelieferten Prüfsummenwert zu vergleichen. Da MD5 und SHA sich in letzter Zeit als nicht sicher herausgestellt haben, sollte eines der SHA2-Verfahren (SHA-224, SHA-256, SHA-384, SHA-512) den Vorzug erhalten. Mit einer Verschlüsselung hat dies aber nichts zu tun.

Kurze Hashwerte (Fingerabdruck bzw. Fingerprint) werden beispielsweise benutzt, um Schlüssel (Keys, die z. B. für die Verschlüsselung von E-Mails benutzt werden) eindeutig zu identifizieren und damit einem bestimmten Benutzer zuzuordnen.

Zertifikate

Ein **Zertifikat** nach dem Standard X.509 enthält den öffentlichen Schlüssel für den Aufbau einer verschlüsselten Verbindung sowie weitere Attribute, wie Angaben zum Antragsteller, zum Aussteller, den Zeitraum der Gültigkeit etc. Es ist auf den **Namen** des Servers ausgestellt. Um die Sicherheit von einem Zertifikat zu erhöhen, kann es auf eine Smartcard (Karte mit integriertem Prozessor) ausgelagert werden.

Auch bei verschlüsselten Verbindungen über das Protokoll HTTPS erfolgt in der Regel eine Verschlüsselung über erworbene Zertifikate, die nur so sicher sind wie die Institute, die sie ausstellen. Ein kostenloses Zertifikat der Initiative „Let's Encrypt“ können Sie beispielsweise von folgender Adresse erhalten: <https://letsencrypt.org/>.

Autorisierung

Damit der Anwender sicher sein kann, an den richtigen Server zu gelangen und nicht einem **Man-in-the-Middle-Angriff** aufzusitzen (bei dem ein Angreifer vorgibt, er sei der gewünschte Server, um an die Passwörter des Benutzers zu kommen), ist ein wesentlicher Zweck eines Zertifikates auch die **Autorisierung**. Damit weist sich der Server als berechtigt aus, den verwendeten Namen zu führen, was Täuschungen unberechtigter Angreifer erheblich erschwert.

Protokolle

Nach diesem Exkurs zur Verschlüsselung von Daten erfolgt die eigentliche Auflistung der relevanten Protokolle. Weitere Informationen zur Verschlüsselung finden Sie im HERDT-Buch *Netzwerke – Sicherheit*.

HDLC

High Level Data Link Control definiert einen Satz von Protokollen (Standards), der die Mittel bestimmt, mit denen ungleiche Geräte über Datennetze miteinander kommunizieren können. HDLC ist unter anderem in der X.25-Empfehlung ITU-T, in ISO 6256 und ISO/IEC 13239:2002 sowie in DIN 66222 Teil 2 beschrieben.

Zum Definitionsumfang gehören auch folgende **Link Access Procedure (Lap)**-Varianten:

- ✓ LAPM: eine Verbindungsprozedur für analoge Modems,
- ✓ LAPB: eine Verbindungsprozedur für Packet-Switching-Netze nach ITU-T X.25,
- ✓ LAPD: das Übermittlungsprotokoll für den ISDN-D-Kanal,
- ✓ LAPE, LAPF und MTP Level 2.

Neben verschiedenen Sicherungsdiensten übernimmt HDLC den Auf- und Abbau von Verbindungen. Unter anderem wird bei folgenden Verfahren und deren Varianten HDLC angewendet: X.25, GSM, ISDN, PPP etc. Heute ist es fast nur noch für PPP relevant.

PPP

Der Name **Point-to-Point Protocol** steht nicht für ein einzelnes Protokoll, sondern für eine Protokollgruppe und kann als eine Variante von HDLC betrachtet werden. **PPP** dient auf OSI Layer 2 zum Transport von Netzwerkprotokollen, die oberhalb von Schicht 2 liegen (z. B. IP, IPv6), über eine **Punkt-zu-Punkt-Verbindung**. Dabei unterstützt PPP eine Fehlererkennung sowie die Aushandlung von Verbindungsparametern und Authentifizierung über das **Link Control Protocol (LCP)**.

Die eigentliche Authentifikation (nach RFC 1661) erfolgt über die Authentifizierungsprotokolle **Password Authentication Protocol (PAP)** oder **Challenge Handshake Authentication Protocol (CHAP)**. Der Hauptunterschied zwischen beiden ist, dass bei CHAP die Benutzernamen und Passwörter chiffriert übermittelt werden und bei PAP unverschlüsselt und damit ausspähbar.

Folgende wichtige Merkmale lassen sich auflisten:

- ✓ Verkapselung von Paketen höherer Protokollsichten
- ✓ LCP (Link Control Protocol) ist ein Verbindungssteuerungs-Protokoll zum Anschalten und Testen von Leitungen, Aushandeln von Optionen, Beenden von Verbindungen und Überprüfen der Authentifizierung.
- ✓ Definitionen für eine Familie von NCPs (Network Control Protocols). Optionen können auf der Vermittlungsschicht ausgehandelt werden.

Das folgende Beispiel soll die Vorgehensweise verdeutlichen:

- ✓ PC wählt einen Service-Provider an.
- ✓ LCP-Frames (im PPP-Rahmen) handeln PPP-Parameter aus.
- ✓ NCP-Frames kommunizieren mit der Vermittlungs-Schicht (z. B. Vergabe einer IP-Adresse).
- ✓ Übertragung des Internetverkehrs.
- ✓ Bei Sitzungsende wird über NCP-Frames die Verbindung zur Vermittlungsschicht abgebaut und LCP beendet das Protokoll auf der Sicherungsschicht.

Spezifikationen zum Point-to-Point Protocol sind unter anderem festgelegt in den RFCs 1661, 1662, 1663, 1570, 1994, 1996, 2153 und 2637.

PPPoE

Eine wichtige Anwendung von PPP ist das Protokoll **PPPoE** (PPP over Ethernet). Es ermöglicht bei DSL die Verbindung zwischen dem eigenen **DSL-Modem** und dem **Zugangs-Router** (bzw. dem DSL Access Concentrator) des Providers. Zu diesem Zweck wird über die Ethernetverbindung eine virtuelle PPP Einwahl durchgeführt.

PPTP

Das **Point-to-Point Tunneling Protocol** ist eine Erweiterung von PPP für den Remote-Zugriff auf private Netze über das Internet. Es wurde ursprünglich von Microsoft und Ascend entwickelt. Durch die Integration in Windows und die Implementierung in anderen Betriebssystemen, wie z. B. Linux, ist es sehr weit verbreitet. In RFC 2637 vom Juli 1999 finden sich Erläuterungen zu PPTP.

PPTP tunnelt PPP-Datagramme (chiffrierte Datagramme werden in PPP-Rahmen verpackt). Es ermöglicht somit das Einrichten von gesicherten Verbindungen über das Internet und kann letztendlich zum Aufbau von VPNs herangezogen werden.

Die Authentifizierung erfolgt über die Protokolle **PAP** oder Varianten von **CHAP**. Auf Betriebssystemen von Microsoft ist MSCHAPv2 (eine Variante von CHAP) seit Windows 2000 Standard. Der PPP-Rahmen wird mit dem Protokoll **GRE** (**G**eneral **R**outing **E**ncapsulation, Protokoll Nr. 47) hinter einem IP-Header gekapselt. Eine eventuell vorhandene Firewall muss daher so konfiguriert sein, dass sie nicht nur den TCP-Port 1723, sondern auch das Protokoll Nr. 47 durchlässt.



PPTP bietet im Gegensatz zum im Folgenden beschriebenen L2TP keine Datenintegrität. Eine gegenseitige Authentifizierung der Computer fehlt, sodass sich ein Angreifer als jemand anderes ausgeben kann. In der Fachwelt gilt es als sehr **unsicher** und sollte deshalb nicht mehr benutzt werden!

Seit Windows Vista SP1 und Windows Server 2008 arbeitet Microsoft mit dem neuen Protokoll **Secure Socket Tunneling Protocol (SSTP)**, welches das PPTP abgelöst hat und nun SSL-3 als Verschlüsselungsprotokoll verwendet. Obwohl SSTP verschiedene Standards nutzt, ist es nicht durch die IETF standardisiert. SSTP Client Anwendungen sind auch für BSD, Mac und Linux erhältlich.

L2TP

Das Layer 2 Tunneling Protocol wurde von der IETF entwickelt und im RFC 2661 erläutert. Es vereint die Vorteile von PPTP und Layer 2 Forwarding (**L2F**), unterstützt aber selbst keine Verschlüsselung. Daher wird es oft zusammen mit **IPsec** benutzt. Der RFC 3193 (Securing L2TP using IPsec) beschreibt diese Zusammenarbeit.

L2TP hat sich für den Aufbau von VPNs am Markt etabliert. Es ist ein Tunnelprotokoll auf OSI-Layer 2. Für die Authentifizierung dienen die bekannten Verfahren CHAP (Challenge Handshake Authentication Protocol) und PAP (Password Authentication Protocol). Eine eventuell vorhandene Firewall muss die UDP-Ports 500 und 4500 sowie das Protokoll **Encapsulated Security Payload (ESP)** mit Protokoll-Nummer 50 durchlassen.

IPsec

Das IP Security Protocol war ursprünglich für IPv6 geplant, aber inzwischen ist es durch die RFCs 2401 bis 2412 auch für IPv4 komplett genormt. Im Unterschied zu den bisher genannten Protokollen arbeitet es auf OSI-Schicht 3 und bietet die Verschlüsselung von Daten nach beliebigen Verfahren (DES, 3DES usw.).

Arten der Verbindung

- ✓ **Transport-Modus** für die direkte Verbindung von zwei Rechnern mit L2TP. Der Original-Header bleibt erhalten, nur die Daten werden verschlüsselt. Ein zusätzlicher IPsec-Header wird integriert.
- ✓ **Tunnel-Modus** zur transparenten Verbindung von kompletten Netzwerken. Die Pakete werden inklusive des IP-Headers verschlüsselt und um neue IP-Header für die Übertragung erweitert.

IPsec ist kein einzelnes Protokoll, sondern eine Protokoll-Sammlung. Die Verschlüsselung erfolgt immer symmetrisch, die Schlüssel selbst werden bei Verbindungsauftnahme ausgetauscht.

Wichtige Protokolle von IPsec sind:

- ✓ **Encapsulated Security Payload Protocol** (ESP; Protokoll-Nr. 50)
Es erstellt einen zusätzlichen ESP-Header und verschlüsselt die Daten des kompletten Pakets (ohne den IP-Header). Zur Verschlüsselung können mehrere Verfahren benutzt werden, wie AES, DES, 3DES, Twofish etc. ESP kann zusätzlich für Authentifizierung der Benutzer sorgen. Es ist sowohl im Transport-Modus als auch im Tunnel-Modus einsetzbar.
- ✓ **Authentication Header Protocol** (AH; Protokoll-Nr. 51)
Es kümmert sich um die Integrität der Daten und die Authentifizierung der Benutzer. Es signiert nur die Pakete. AH hat selbst keine Verschlüsselungsfunktionen. Es ist nur im Transportmodus einsetzbar.
- ✓ **Internet Key Exchange** (IKE)
Es ist für das Management der Schlüssel zuständig, wie der gegenseitigen Aushandlung und dem Austausch der IPsec-Schlüssel und den Schlüsseloptionen (z. B. wird AH oder ESP benutzt?, welcher Schlüssel-Algorithmus mit welcher Schlüssel-Länge?, welche Lebensdauer hat der Schlüssel?). Die Verschlüsselungs-Optionen werden für jede Verbindung extra als **Security Association (SA)**, auch als Sicherheitszuordnung benannt, in einer **Security Association Database(SAD)** abgelegt.
Das grundlegende Gerüst für IKE wird durch das **Internet Security Association Key Management Protocol (ISAKMP)** bereitgestellt.
Die Komplexität von IKE Version 1 reduziert der Nachfolger IKEv2. IKE bzw. IKEv2 benutzen jeweils den UDP-Port 500.

Eine eventuell vorhandene Firewall muss so konfiguriert sein, dass sie die oben erwähnten Ports und Protokolle passieren lässt, was die Komplexität weiter erhöht. Auch verhindert NAT den Einsatz von AH.

Fritz!Boxen können aktuell nur **IKEv1** verwenden! Hinweise zur Einrichtung einer VPN Verbindung finden Sie unter:

https://avm.de/service/fritzbox/fritzbox-7590/wissensdatenbank/publication/show/3331_FRITZ-Box-mit-einem-Firmen-VPN-verbinden/

IPsec ist als sehr sicher, aber auch als sehr komplex anzusehen. Daher entstanden in letzter Zeit mehrere andere Lösungen, die ebenfalls auf hohe Sicherheit setzen, aber einfacher zu implementieren sind.

OpenVPN

Eine der bekanntesten VPN-Lösungen bietet das plattformübergreifende **OpenVPN**, welches auf OpenSSL aufsetzt. Ein VPN über das Internet zwischen selbst genutzten Geräten ist damit relativ einfach einzurichten. Für die heute gängigen Betriebssysteme ist es kostenlos verfügbar von <https://openvpn.net/index.php/download/community-downloads.html>.

OpenVPN kann ähnlich wie IPsec sowohl einzelne Rechner als auch komplett Netzwerke sicher über ein unsicheres Netzwerk (wie das Internet) über eine verschlüsselte Übertragung verbinden.

Für Firewalls ist es dagegen sehr viel einfacher zu handhaben, da nur **ein** einzelner Port (meist UDP 1194) zu öffnen ist.

**Ergänzende Lerninhalte:** *Weitere Übertragungsprotokolle.pdf*

In diesem BuchPlus-Dokument finden Sie Informationen zu früher verwendeten Protokollen.

18.6 Übung

Fragen zur Datenübertragung in WANs

Übungsdatei: --**Ergebnisdatei:** uebung18-E.pdf

1. Über welche Übertragungs-Verfahren werden auf OSI Layer 1 hauptsächlich die Daten übertragen?
2. Ist ADSL zum Anschluss einer Firma geeignet, die im Internet z. B. einen Webshop führt? Begründung?
3. Welche Vorteile bietet eine asymmetrische Verschlüsselung?
4. Beschreiben Sie den Unterschied zwischen einem Anonymisierungs-Netzwerk und einem VPN?
5. Welches Protokoll sollte für ein VPN nicht mehr benutzt werden, da es unsicher ist?
6. Nennen Sie einige Verfahren, die sich für den Aufbau eines sicheren VPN eignen.
7. Welche Probleme können beim Einsatz einer VPN auftreten?

19

Zugangsmöglichkeiten

19.1 Telefonnetz

Analoges Modem und ISDN-Anschluss

Ein **Modem** (Modulator/Demodulator) ist ein Gerät, das digitale Daten in analoge (Ton-)Signale moduliert und in umgekehrter Richtung, Tonsignale in digitale Daten demoduliert. Es wurde in der Anfangszeit des World Wide Web (WWW) für die Datenfernübertragung (DFÜ) über das konventionelle, analoge Telefonnetz verwendet. Heute wird diese Technik (mit Ausnahme von FAX-Übertragungen) nicht mehr genutzt.

Wenn ein ISDN-Anschluss vorhanden ist, kann auch ein ISDN-Adapter eingesetzt werden. Auch diese Art des Internetzugangs wurde inzwischen fast vollständig von DSL-, UMTS- und LTE-Internet-Zugängen verdrängt. Laut ursprünglicher Planung der Telekom sollte die Umstellung von ISDN (vgl. Kapitel 18) auf ALL-IP bis Ende 2018 abgeschlossen sein. Tatsächlich zogen sich die Umstellungsarbeiten noch weit bis ins Jahr 2019 hinein. Andere Anbieter wie Vodafone gewähren ihren Geschäftskunden einen Weiterbetrieb bis 2022. Fakt aber ist, dass ISDN zukünftig keine Rolle mehr spielen wird.

Internetanschluss per DSL

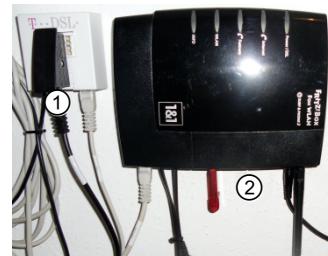
Eine DSL-Verbindung kann über jeden Telefonanschluss betrieben werden, wenn dieser vom Anschlussinhaber entsprechend eingerichtet ist. Separate DSL-Modems werden nicht mehr angeboten. Sie sind in einem sogenannten DSL-Router integriert. Telefonate und Faxe überträgt bei einem Komplettanschluss nur noch der Internetzugang per Voice over IP. Aktuelle DSL-Router (siehe unten) stellen die nötige Hard- und Software zur Verfügung. Bei herkömmlichen Anschlüssen (keinen Komplettanschlüssen) werden noch Telefonate (bzw. Faxe) und DSL-Verbindungen durch einen Splitter in unterschiedliche Frequenzbänder aufgeteilt und über den Telefonanschluss gemeinsam übertragen (vgl. Kapitel 18).

DSL-Router

Router dienen dazu, unterschiedliche Netzwerke zu verbinden oder auch zu trennen. Heute kommen fast ausschließlich nur noch **DSL**-Router für die Verbindung des Netzwerks mit dem Internet zum Einsatz.

An dem DSL-Router können viele Geräte (per NAT, vgl. Kapitel 11) oder auch nur ein einziger Rechner angeschlossen sein.

In solchen Geräten ist ein Router in Kombination mit anderer Hardware wie DSL-Modem, Switch, WLAN-Access-Point, Telefonanlage für Internet- und Festnetztelefonie usw. im gleichen Gehäuse eingebaut. Einer der bekanntesten Vertreter für derartige Kombi- bzw. Multi-funktionsgeräte ist im deutschsprachigen Raum die FRITZ!Box der Berliner Firma AVM. Aber auch von anderen Firmen wie Zyxel, Linksys (Cisco), Belkin, DrayTek gibt es vergleichbare Geräte.



DSL-Splitter ① und DSL-Router ② (Fritz!Box)

Ein solches Kombigerät bietet meist mehrere Dienste an, wie DNS-Weiterleitung, DHCP-Server, Stateful Inspection-Firewall oder NAT. Damit ist die Anbindung aller Rechner und Geräte in einem Netzwerk an das Internet einfach und vor allem sicher über eine solche zentrale Komponente machbar. Alle internen IP-Adressen werden auf die öffentliche IP-Adresse abgebildet, die der Provider liefert. Der Leistungsbedarf ist dabei gering (ca. 5–10 W). Die Konfiguration solcher Kombigeräte ist heutzutage über den integrierten Webserver mit jedem Web-Browser möglich. Aus Sicherheitsgründen sollte dies jedoch nur im lokalen Netz erfolgen.

In der Regel werden derartige Kombigeräte (DSL-Router) bei gleichzeitigem Abschluss eines entsprechenden Provider-Vertrags kostenlos zur Verfügung gestellt. Von den ursprünglich drei Tarifarten (zeit- oder volumenabhängige Abrechnung und Flatrate) bieten die meisten Provider inzwischen nur noch die **Flatrate** (in der Regel keine Begrenzung von Dauer und Daten-Volumen) für eine monatliche Pauschale an.

Router im professionellen Bereich bieten oft auch die Option, den darüber abgewickelten Datenverkehr zu überwachen bzw. zu protokollieren (per SNMP auf einem Network Management System, vgl. Kapitel 15).

Ebenfalls anzutreffen sind **UMTS-Router** und **LTE-Router**, auch kombiniert mit einem DSL-Router, die einem Rechnernetz den Zugang zum Internet über ein Mobilfunknetz gestatten. Die möglichen Übertragungsraten sind dabei abhängig vom verwendeten Mobilfunkstandard (vgl. Kapitel 19.2).

Mobilfunk-Modem (auch Surf-Stick)

Die Palette reicht von Geräten, die über die USB-Schnittstelle eines Computers angeschlossen werden, bis zu UMTS- und LTE-Routern, die Anschluss auch über Ethernet und WLAN bieten. In etlichen Geräten, wie Handys, Notebooks, Tablets etc., ist ein Mobilfunk-Modem fest eingebaut.

UMTS- bzw. LTE-Datenkarten bieten ebenfalls eine Vernetzung über Mobilfunk. Sie kommen als USB-Stick (Web-Stick oder Surf-Stick), als PCMCIA-Karte oder Express-Card in den Handel. Mit eingelegter SIM-Karte ermöglichen sie, über das eingebaute Mobilfunk-Modem, eine direkte Verbindung ins Internet. Ist keine Verbindung per UMTS bzw. LTE möglich, verwenden sie stattdessen EDGE und im schlimmsten Fall nur GSM (siehe folgende Seiten).



Surf-Stick

Auch können DSL-Router mit zusätzlicher UMTS- bzw. LTE-Anbindung eine Fallback-Lösung anbieten, wenn die DSL-Leitung gestört ist. Nicht alle Router beherrschen aber automatisches Fallback bzw. Fallforward, also den automatischen Übergang zurück auf die DSL-Leitung, wenn diese wieder benutzbar ist.

Privatkunden erhalten meist nur einen Zugang zum Internet über das Providernetzwerk, das per Adressumsetzung (NAT/PAT) die Internetverbindung bereitstellt. Einige Funktionen (wie Port-Weiterleitungen, Fernkonfiguration etc.) sind dann nicht möglich. Auch ist die Latenzzeit höher (mindestens 80 ms im Gegensatz zu typischen 20–30 ms bei DSL).

Internettelefonie per VoIP (Voice over IP)

Geeignete Hardware ermöglicht auch das Telefonieren über das Internet. Dabei wird die Sprache digitalisiert, in IP-Pakete verpackt und mit der vorhandenen Internettechnik zum Ziel gebracht.

Als Hardware kann ein Computer mit Mikrofon und Soundausgabe dienen. Über oft proprietäre Protokolle von Dienstleistern, z. B. Skype, ist dann ein Telefonat mit einem Empfänger möglich. Die IP-Adresse des Empfängers kennt der Server des Betreibers nach dessen Anmeldung (ähnlich einem Telefonbuch). Beide Beteiligten, die auf diese Art miteinander telefonieren, müssen allerdings das gleiche Protokoll benutzen und bei Verwendung eines DSL-Routers die nötigen Ports darauf freigeben. Neben Skype gibt es noch viele andere Anwendungen für das Telefonieren per **Session Initiation Protocol (SIP)**. Softwareanwendungen wären zum Beispiel Phoner, SJphone u. a. Als Provider für die SIP-Telefonie kommt der Provider des DSL-Anschlusses oder einer der freien Provider wie sipgate in Frage. (siehe auch Folgeabschnitte)

Komfortabler ist der Gebrauch von Internettelefonie über spezielle, mit dem Netzwerk verbundene **Internettelefone** oder über eine Internettelefonanlage, die bereits viele DSL-Router mitbringen (wie z. B. viele FRITZ!Boxen). Diese Geräte bieten zusätzliche Buchsen, über die analoge Telefone (und auch ISDN-Anlagen) einfach anschließbar sind. Der Provider leitet die IP-Pakete, die das Telefonat beinhalten, über ein eigenes Gateway an Festnetz- oder Handy-Anschlüsse weiter. Damit sind Telefonate wie bisher von Telefon zu Telefon möglich, ohne dass ein Computer involviert ist. Es sind lediglich eine oder mehrere vorhandene Telefonnummern beim Provider freizuschalten und in der Internettelefonanlage zu konfigurieren.

Eine spezielle Internettelefonnummer ist die **SIP-Adresse**. Standardisiert ist der Verbindungs-aufbau bei der Internettelefonie über **SIP** nach RFC 3261. Dabei erhält der Teilnehmer eine SIP-Adresse im **Uniform-Resource-Identifier-Format (URI-Format)**, die einer E-Mail-Adresse ähnelt. Ein Beispiel wäre `sip:1234567@example.de`.

- ✓ Ein großes Problem bei VoIP ist die Latenzzeit. Deshalb priorisieren die Provider die Weiterleitung über das **DSCP-Flag (Differentiated Service Code Point, bzw. ToS - Type of Service)** aus dem Header der entsprechenden IP-Pakete. Ein anderes Verfahren mit der Bezeichnung **Traffic Shaping** steht auf vielen Switches und DSL-Routern bereit, die VoIP bieten.
- ✓ Ein weiteres Problem bei VoIP ist die **Verfügbarkeit** der Internetverbindung allgemein. Ist diese gestört, ist weder ein Telefonat nach außen möglich, noch ist man selbst über diese Leitung erreichbar. Internetverbindungen sind immer noch weniger zuverlässig, als die Telefonleitungen selbst. Oft kommt es zu weiteren Problemen mit Faxgeräten, wenn diese nicht mit T.38 (Empfehlung für Fax over IP) umgehen können. Das kann sich beispielsweise darin äußern, dass jede Seite einer Faxsendung einzeln verschickt werden muss.

Aktuell gibt es Firmen (Telekom, sipgate, Nfon, Placetel uvm.), die virtuelle Telefonanlagen als Cloud-Dienst anbieten. Sie ermöglichen Leistungsmerkmale wie in klassischen Telefonanlagen (Makeln, Weiterleiten, Gruppenruf etc.) auf Basis der IP-Telefonie.

19.2 Mobilfunknetz

Unterschiedliche Techniken

Mobilfunknetze sind inzwischen flächendeckend verfügbar und werden sowohl für Sprache als auch für Datenübertragung genutzt.

Generell gilt dabei, dass eine Basisstation viele Empfänger versorgen kann, die sich die Übertragungsrate untereinander teilen müssen. Eine Funkverbindung bildet immer ein **Shared Media**, ähnlich wie Vernetzungen mit einem Hub. Die verfügbare Datenübertragungsrate kann daher stark schwanken, je nachdem, wie viele Benutzer sich dasselbe Medium teilen müssen.

GSM

Der **Global Standard for Mobile Communication (GSM)** ermöglicht Datenaustausch üblicherweise per Handy, Navigationsgerät oder Smartphone.

GSM-Geräte benutzen den Frequenzbereich um 900 MHz (D-Netze, Deutschland), um 1800 MHz (E-Netze, Deutschland) oder um 1900 MHz (Amerika) mit einem Kanalabstand von 200 KHz. Pro Kanal kann mit einer Geschwindigkeit von **9,6 Kbit/s** gearbeitet werden, die einer Modem-Verbindung aus der Computersteinzeit entspricht. Wegen der geringen Reichweite von nur wenigen Kilometern sind viele Basisstationen notwendig.

Es können auch ISDN-Gegenstellen angerufen werden, soweit diese auf das V.110-Protokoll mit 9,6 Kbit/s eingestellt sind. Der Short Message Service erlaubt das Versenden von Nachrichten bis zu einer Länge von 160 Zeichen.

HSCSD

Das **High-Speed-Circuit-Switched-Data**-Verfahren bietet höhere Datenübertragungsraten, indem es mehrere GSM-Kanäle à 9,6 Kbit/s bündelt. Theoretisch könnten dies bis zu 8 Kanäle sein, die dann eine Geschwindigkeit von 76,8 Kbit/s hätten. In der Praxis sind es meist nur 4 Kanäle mit einer Geschwindigkeit von **38,4 Kbit/s**.

Eine weitere Steigerung ist möglich, indem durch spezielle Verfahren die Kapazität eines Kanals auf 14,4 Kbit/s erhöht wird, was bei einer erneuten Bündelung von 4 Kanälen 57,6 Kbit/s erlaubt.

In Deutschland bietet das System in Vertragstarifen nur noch Vodafone an, und es verliert an Bedeutung.

GPRS

General Packet Radio Service ist eine Erweiterung von GSM, die, unter Verzicht z. B. auf Fehlerkorrekturen und Ähnliches, theoretisch bis zu **171,2 Kbit/s** übertragen kann. In der Praxis wird die Kapazität eines einzelnen Kanals in vier Bandbreiten (GSM-Zeitschlitzten) angeboten, nämlich 9,05 Kbit/s, 13,4 Kbit/s, 15,6 Kbit/s und 21,4 Kbit/s. Häufigster Einsatz ist die Bündelung von 4 Zeitschlitzten à 13,4 Kbit/s, sodass eine Geschwindigkeit von **53,6 Kbit/s** Standard ist.

GPRS unterstützt TCP/IP mit dynamischer Adressvergabe und das Datenprotokoll **Wireless Application Protocol (WAP)**. Somit ist es für die mobile Einwahl bei Internet-Service-Providern geeignet.

EDGE

Enhanced Data Rates for GSM Evolution (auch als Evolved GSM bezeichnet) ist ein Verfahren, das bis zu 473 Kbit/s auf der Basis von GSM-Netzen möglich macht. Zur Erzielung dieser Bandbreite vergrößert ein Modulationsverfahren die Datenübertragungsrate eines einzelnen GSM-Kanals von 9,6 Kbit/s auf bis zu 59,2 Kbit/s. Bis zu acht Kanäle können gleichzeitig genutzt werden.

Für diese Technik sind, wie bei HSCSD und GPRS, spezielle Endgeräte notwendig. Auch die Infrastruktur der Netzbetreiber muss angepasst werden.

UMTS

Universal Mobile Telecommunications System wird auch als 3G-Funknetz bezeichnet (Funknetz der dritten Generation) und bietet Geschwindigkeiten von 384 Kbit/s bis zu **42,2 Mbit/s** mit dessen Übertragungsverfahren **High Speed Downlink Packet Access (HSDPA)**. Diese Geschwindigkeitssteigerung ist mit den bisher erwähnten Technologien nicht vergleichbar und nur dadurch erreichbar, dass UMTS andere Übertragungsarten, andere Modulationen und andere Frequenzen verwendet als GSM. In diesem Zusammenhang müssen die Netzbetreiber einerseits ihre gesamte Infrastruktur anpassen, andererseits die für den Betrieb notwendigen Lizenzen erwerben.

Die Lizenzvergabe für die Nutzung der entsprechenden Frequenzen erfolgt durch Regulierungsbehörden einzelner Staaten und wurde nicht so kostengünstig abgewickelt wie damals die Vergabe der ersten Lizenzen für den Mobilfunk.

! UMTS bzw. 3G ist mittlerweile überholt und wurde von den Providern im Laufe des Jahres 2021 abgeschaltet. Die freigewordenen Frequenzen werden für den Ausbau von 4G und 5G verwendet.

LTE

Long Term Evolution ist der Mobilfunkstandard der vierten Generation (4G). Er ist in Europa aktuell zumeist auf den Frequenz-Bändern 800 MHz, 1,8 GHz und 2,6 GHz im Einsatz. Frequenz-Lizenzen hierfür wurden 2010 in Deutschland für insgesamt 4,4 Milliarden Euro versteigert, in Österreich 2013 im 800 MHz-Band für 2 Milliarden Euro. Da in anderen Ländern oft andere Frequenzen (wie in Amerika) üblich sind, können aus diesen Ländern importierte Geräte mit LTE hierzulande nicht betrieben werden.

Cat-3-Geräte (nach Kategorie 3) erreichen brutto 100 MBit/s (Downstream) und 50 Mbit/s zum Sender (Upstream). Seit August 2013 sind mit LTE-Kategorie 4 (**LTE Cat-4**) im 2,6 GHz-Band brutto bis zu 150,8 MBit/s Down und 51 MBit/s Up möglich, mit **LTE Cat-5** bis zu 300 MBit/s Down mit 75 MBit/s Up.

Mit dem **3GPP Release 10** (LTE-Advanced) sind es bei **LTE Cat-6** bis zu 300 MBit/s Down mit 50 MBit/s Up, mit **Cat-7** 300 MBit/s Down und 100 MBit/s Up und zukünftig mit **Cat-8** bis zu 3000 MBit/s Down und 1500 MBit/s Up (siehe hierzu auch: <http://www.lte-anbieter.info/technik/kategorien-und-3gpp-release.php>). Weitere Informationen zu den LTE Cat-Klassen finden Sie hier: <https://www.4g.de/news/was-ist-eigentlich-lte-cat-11050/>.

Die verfügbare Übertragungsrate wird allerdings unter allen angeschlossenen Benutzern aufgeteilt. Durch die garantierte Bandbreite, eine geringe Latenzzeit (ca. 10 ms), **QoS** usw. ist es für die Protokolle des Internets bestens geeignet, vor allem in ländlichen Gegenden, in denen DSL noch nicht vorhanden ist.

Die LTE-Erweiterung **LAA-LTE** (License-Assisted Access) soll das LTE-Netz zukünftig entlasten. Um den Anforderungen der Nutzer gerecht zu werden, wird dabei das lizenfreie 5 GHz-Band von WLAN mit verwendet. Eine Beeinträchtigung von WLAN im 5 GHz-Band wird befürchtet, wenn in Zukunft immer mehr WLAN-Geräte das 5 GHz-Band belegen.

Ob sich LAA-LTE durchsetzt, wird sich zeigen. Ein Probelauf der Telekom fand bereits statt. Siehe <https://www.telekom.com/medien/konzern/299774>.

5G

5G nennt sich die neueste Generation im Mobilfunk. Telekom-Kunden können dieses Netz seit 2019 nutzen, allerdings ist es im heutigen Ausbau meist nur in Ballungsräumen verfügbar. Wegen seiner kurzen Reaktionszeiten (Latenz) ist 5G auch für Echtzeitanwendungen, z. B. in der Automobiltechnik, geeignet. Es wird im Endausbau eine Geschwindigkeit von bis zu 10 Gbit/s erreichen.

WiMAX

Worldwide Interoperability for Microwave Access nach IEEE 802.16 soll vor allem in ländlichen Gegenden die Versorgung mit Netzen hoher Datenübertragungsrate verbessern. Bei WiMAX wurde ebenfalls großer Wert auf eine geringe Latenzzeit und **QoS** gelegt.

WiMAX kann bis zu 50 Kilometer überbrücken. Da sich die Datenübertragungsrate mit zunehmender Entfernung verschlechtert, bleiben in der Praxis wenige Kilometer. Auf kurze Entferungen sind bis zu 60 Mbit/s möglich. In Deutschland und Europa hat es kaum Bedeutung, dafür in anderen Ländern, wie USA, Japan, Russland und Teilen von Afrika.

Praktische Umsetzung

Der Aufbau der Netze sowie die Entwicklung von Endgeräten sind immer noch im Gange. Allerdings zwingen die hohen Investitionskosten viele Netzbetreiber zu Kooperationen, denen oft langwierige Verhandlungen vorausgehen, oder zur Aufgabe.

Auf den Websites der verschiedenen Netzanbieter kann man sich über den aktuellen Ausbaustatus informieren (z. B. Vodafone: <https://www.vodafone.de/hilfe/netzabdeckung.html>).

Die Anzahl verkaufter Endgeräte (Tablets und Smartphones) ist in den letzten Jahren sprunghaft angestiegen. Derzeit dominieren bei Smartphones Geräte verschiedener Hersteller mit dem Betriebssystem Android und Geräte von Apple mit dem Betriebssystem iOS den Markt.

19.3 Weitere Netze

Nutzung vorhandener Infrastrukturen

Neben dem Telefonnetz und den Mobilfunknetzen gibt es noch weitere, zum Teil bereits flächendeckend vorhandene Infrastrukturen. Es ist daher durchaus naheliegend, Datenübertragung auch auf diesen Wegen durchzuführen.

Satellitennetz

Hier erfolgt der Datenverkehr über **Satellit**. Für den Empfang am Boden stehen Parabolantennen und Receiver zur Verfügung. Die Nutzer-Authentifizierung wird über eine Chipkarte realisiert. Der Zugriff geschieht über ein Terminalprogramm. Nachdem es anfänglich nur die Möglichkeit des Downloads gab, können inzwischen Daten in beide Richtungen transportiert werden.

Dem Vorteil der Ortsungebundenheit stehen eine geringe Zuverlässigkeit und die Übertragungssicherheit gegenüber. Auch sind die Latenzen hoch.

Kabelfernsehnetz

Über ein spezielles Kabelmodem wird Datenverkehr über das Kabelfernsehnetz realisiert. Da dieses Netz als Übertragungsmedium bereits Koaxialkabel verwendet, ist es grundsätzlich für breitbandigen Datenverkehr und damit originär für Ton- und Videoübertragung geeignet. Das größte Hindernis auf der technischen Seite ist, dass dieses Netz ursprünglich als reines Verteilnetz (Simplexbetrieb) geplant war. Die Umrüstung der Verteilerknoten auf Duplexbetrieb durch Einbau von einem Rückkanal ist bereits abgeschlossen.

Der Standard **Data Over Cable Service Interface Specification (DOCSIS)** bildete die Grundlage für das Angebot von weiteren Diensten wie Internet und Telefonie im Kabelfernsehnetz. Aktuell ist die Version 3.1 von DOCSIS im Einsatz – mit Datenraten bis zu 10 Gbit/s im Downstream und 1 Gbit/s im Upstream (oft vom Provider reduziert).

Per **DS-Lite** (nicht zu verwechseln mit DSL-Light) erhalten die Kunden von Kabelfernsehanbietern über ein Kabelmodem Zugang zum Internet. Es handelt sich um die IPv6-Technik Dual-Stack Lite (DS-Lite, nach RFC 6333).

Die Anwender bekommen dabei nur private **IPv4-Adressen**, die beim Provider intern per Carrier-Grade-NAT (vergleichbar zu NAT bei IPv4) in **IPv6-Pakete** gekapselt werden. Benötigen Protokolle eine Portweiterleitung, sind sie damit nicht oder nur eingeschränkt benutzbar, wie z. B. Online-Spiele oder VPN-Anwendungen. Die zulässige Größe der **MTU** (Maximum Transmission Unit) ist dabei für IPv4-Pakete verringert, sodass sie fragmentiert übertragen werden, wenn sie größer als **1460 Byte** sind. Hiermit angebotene Dienste können vom Internet her nur über IPv6 erreicht werden.

Die 2013 durch Vodafone übernommene Firma Kabel-Deutschland bietet seit Mitte 2005 Internetzugang über das Kabelfernsehnetz an. Ein Verfügbarkeitscheck auf der Webseite <https://www.vodafone.de/festnetz/> informiert potenzielle Kunden nach Adresseingabe über mögliche Geschwindigkeiten und Leistungen.

Stromnetz

Bei dieser Variante, die auch als **Powerline Communication (PLC)** oder **Trägerfrequenzanlage (TFA)** bezeichnet wird, spielt im Weitverkehrsbereich heute keine Rolle, da die Energieversorgungs-Unternehmen wegen erheblicher Probleme die Nutzung eingestellt haben.

Im häuslichen Bereich spielt sich der Datenverkehr auf normalen Stromleitungen im Wechselstromnetz ab. Zur Verfügung stehen Niederspannungsleitungen mit 230V oder 400V im LAN. Als Schnittstellen können Ethernet und USB (Universal Serial Bus) verwendet werden. Die Übertragung basiert auf dem HomePlug-Standard nach IEEE 1901 Access. Übertragungsraten von 1000 Mbit/s und mehr sind erreichbar, die mit größer werdendem Abstand stark sinken.

Die Hauptvorteile bestehen darin, dass vorhandene Stromkabel genutzt werden können, da das Stromnetz flächendeckend verfügbar ist. Manche Steckernetzteile können die Übertragung beeinträchtigen und damit den Datendurchsatz herabsetzen.

Produkte für Privathaushalte finden Sie im Handel meist unter dem Begriff **PowerLAN**, z. B. von Devolo, Allnet, AVM, Belkin oder Netgear. Sie sind oft auch für die Anbindung von WLAN-Repeatern bzw. Access-Points geeignet. Die Übertragung funktioniert meist gut auf gleich verbundenen Phasenleitungen, schlecht über den Sicherungskasten hinweg in andere Phasenleitungen. Ein weiterer Kritikpunkt ist die Abstrahlung über die ungeschirmten Versorgungsleitungen.

20

WAN-Anbieter

20.1 Übersicht WAN-Zugänge

Überlegungen zu möglichen Verbindungsarten von LAN und WAN

Da nur in den seltensten Fällen eine Firma eigene Weitverkehrsverbindungen betreibt, werden solche Verbindungen üblicherweise angemietet. Da die verfügbaren Variationsmöglichkeiten enorm sind, ist es umso wichtiger, dass eine Firma im Vorfeld der Verhandlungen mit einem Anbieter den eigenen Bedarf so genau wie möglich kennt. Zur Bestimmung des Bedarfs sollte man sich einen Überblick über die grundlegenden Arten einer Kopplung verschaffen:

- ✓ **LAN-zu-LAN**
Die lokalen Netze verschiedener Standorte sollen miteinander verbunden werden.
- ✓ **LAN-zu-Internet**
Das eigene LAN soll mit dem Internet verbunden oder aus dem LAN soll Zugang zum Internet möglich sein. Hier muss unterschieden werden, ob nur auf das Internet zugegriffen oder ob auch eine eigene Internetpräsenz (Website) innerhalb des Unternehmens nach außen angeboten werden soll (alternativ könnte Webspace oder ein eigener virtueller oder physikalischer Webserver bei einem Provider angemietet werden).
- ✓ **Endgerät-zu-LAN**
Durch einen Außendienstmitarbeiter oder von einem Heimarbeitsplatz aus soll eine Verbindung zum Firmennetz aufgebaut werden. Als Endgeräte kommen auch Messgeräte oder Produktionsmaschinen in Frage.

Entscheidungskriterien bei der Wahl der geeigneten WAN-Anbindung

Auch die folgenden Fragen sollten vorab so genau wie möglich beantwortet werden, um aus der Vielzahl der Angebote das passende Produkt auszuwählen:

- ✓ Welche Kapazitäten und Geschwindigkeiten werden benötigt?
- ✓ Welche Bandbreite (Menge der gleichzeitig zu übertragenden Daten) wird benötigt?
- ✓ Liegt der Schwerpunkt auf hohen Download-Raten (asymmetrische Anbindung) oder sollen die Übertragungsraten in beiden Richtungen gleich hoch sein (symmetrische Anbindung)?
- ✓ Welche Geräte, Schnittstellen bzw. Benutzer-Endeinrichtungen werden benötigt?
- ✓ Wird nationale oder internationale Verfügbarkeit benötigt?

- ✓ Können oder dürfen Applikationen bzw. Dienstleistungen zu hierzu spezialisierten Anbietern ausgelagert werden? Besondere Bedeutung bekommt dies, nachdem im Jahre 2015 durch den Europäischen Gerichtshof das **Safe-Harbor**-Abkommen mit den USA für ungültig erklärt wurde.
- ✓ Welche Sicherheitsanforderungen bestehen?
- ✓ Sind längere Unterbrechungen bei Leitungsausfall akzeptabel bzw. welcher Verfügbarkeitsgrad ist notwendig?
- ✓ Ist eine Wiederholung der Übertragung bei einer Störung zumutbar?
- ✓ Welche Kosten (fixe Anschlusskosten und variable Verkehrskosten) entstehen bzw. wie hoch ist das zur Verfügung stehende Budget?
- ✓ Besteht Kompatibilität mit dem vorhandenen LAN?
- ✓ Welche Art der Kommunikationsanforderung (Daten, Sprache, Bild) soll umgesetzt werden?

Carrier/Provider

Obwohl im Zusammenhang mit den verfügbaren Netzen oft von öffentlichen Netzen gesprochen wird, ist klar, dass es auch hier, genauso wie z. B. im Straßenverkehr, Organisationen geben muss, die diese Netze aufbauen, verwalten, pflegen und zur Nutzung anbieten. Ein **Provider** ist generell ein Anbieter einer Dienstleistung, der speziellere Begriff **Carrier** bezeichnet einen Anbieter von Leitungskapazitäten.

Internetdienstanbieter (Internet Service Provider, ISP) gliedern sich grundsätzlich in:

- ✓ **Zugangs-Provider** gewähren Privatpersonen und Firmen Zugang zum Internet gegen eine monatliche Zahlung, inklusive Speicherplatz für eigene Daten und Homepage, Mailadressen etc. Sie mieten selbst Anschlüsse und Leitungen zum Internet von Netz-Providern.
- ✓ **Content-Provider** bieten Inhalt über verschiedene Dienste an, wie Suchmaschinen, Videoportale, Zeitungen, Webshops, soziale Netzwerke etc.
- ✓ **Cloud-Service-Provider (CSP)** bieten Komponenten für das Cloud-Computing. Dazu gehört vor allem die Bereitstellung von Datenspeichern und Rechenleistung über das Internet (vgl. Kapitel 20.2, „Outsourcing/Cloud-Computing“).
- ✓ **Netz-Provider** bzw. **Carrier** oder Netzbetreiber sind Firmen, die im Besitz von Leitungskapazitäten sind und diese an andere Firmen national bzw. international vermieten. Über diese Leitungen erfolgt der größte Teil vom Datentransfer im Internet, ein kleinerer Teil über interne Verbindungen.

Viele Unternehmen bieten mehrere der genannten Dienstleistungen aus einer Hand, z. B. die Deutsche Telekom AG.

Ein Großteil der Leitungen in Deutschland gehört der Deutschen Telekom AG, die freie Kapazitäten an Zugangs-Provider wie beispielsweise die 1&1 Internet AG vermietet. Eine Firma wie 1&1 mit seinen Millionen Kunden ist selbst Kunde bei der Deutschen Telekom AG, bekommt als Großkunde allerdings andere Konditionen als Einzelkunden der Deutschen Telekom AG. Einen Teil ihres Gewinns erwirtschaften die Provider also über ihre Einkaufsspanne bei Leitungskapazitäten.

Telecom

Die Bezeichnung Telecom wird häufig für jeweils national tätige Telekommunikationsgesellschaften verwendet, unabhängig von ihrem tatsächlichen Namen. Der Begriff findet sich in Firmenbezeichnungen wieder, die aus mehreren Wörtern bestehen, und weist damit auf einen Teil des angebotenen Dienstleistungsspektrums des Unternehmens hin (beispielsweise 1&1 Telecom GmbH).

Anbieter in allen Größenordnungen

Die Palette der Anbieter reicht von regionalen über nationale bis hin zu international tätigen Unternehmen. Zwangsläufig differiert das angebotene Leistungsspektrum dabei zum Teil erheblich, aber gerade für kleinere Firmen kann es sich lohnen, regionale Angebote einzuholen. Es gibt inzwischen etliche Internetseiten, die Tarifübersichten anbieten und so die Suche nach dem passenden Angebot erleichtern. Eine davon ist z. B. <https://www.teltarif.de/> (für Österreich: <https://www.providerliste.at/>)

Die nachfolgende Aufzählung enthält beispielhaft einige Namen und Web-Adressen von Firmen, die am deutschen Markt als Carrier und/oder als Provider tätig sind:

- ✓ Telekom Deutschland GmbH,
<https://www.telekom.de/start>
- ✓ Vodafone D2 GmbH,
<https://www.vodafone.de/>
- ✓ 1&1 Internet AG,
<https://www.1und1.de/>
- ✓ Telefónica Germany GmbH & Co. OHG,
<https://www.o2online.de/>
- ✓ 1&1 Versatel,
<https://www.1und1.net/business>
- ✓ Colt Technology Services Group Limited,
<https://www.colt.net/de>

Im Bereich der international tätigen Unternehmen gibt es etliche Zusammenschlüsse, die durch Kooperationen nationaler Anbieter entstanden sind. Für ein weltweit operierendes Unternehmen bedeutet das beispielsweise, nur einen Ansprechpartner vor Ort in der Firmenzentrale zu haben, der sich um sämtliche Belange kümmert.

Gesetzeshintergrund

Seit der vollständigen Liberalisierung des Telekommunikationsmarktes ab 01.01.1998 hat die Deutsche Telekom AG Konkurrenz durch weitere Carrier und Provider bekommen. Durch die bis heute stattgefundene Marktbereinigung bzw. durch technische Weiterentwicklungen (beispielsweise hat das Telefonieren und Faxen über die DSL-Leitung bzw. das Telefonieren über das Handynetz vielerorts Analog- und ISDN-Telefonie verdrängt) sind von den mehreren Hundert Providern nur noch wenige übrig geblieben. Lange Vorwahltabellen für Telefongespräche sind inzwischen Geschichte.

Anbieter im regionalen und nationalen Bereich sind oft Energieversorgungsunternehmen oder Unternehmen, die sich auf die Bereitstellung von MANs (Metropolitan Area Network) spezialisiert haben. Im internationalen Bereich finden sich als Anbieter häufig Joint Ventures der großen nationalen Telecoms und zunehmend auch private Konzerne mit potenteren Kapitalgebern.

Ähnliches gilt auch in Österreich, der Schweiz und vielen weiteren europäischen Ländern, wo der Telekommunikationsmarkt ebenfalls seit dem 1. Januar 1998 vollständig liberalisiert ist.

Unterschiedliche Verbindungsarten

Viele Anbieter gliedern ihre Angebote grundlegend in zwei verschiedene Verbindungsarten, nämlich in Fest- und Wählverbindungen. Bei der Deutschen Telekom AG geschieht dies zum Beispiel über die beiden Begriffe **Leased Link** und **Switched Link**.

Leased Link oder Standleitungen

Hier handelt es sich um feste Punkt-zu-Punkt-Verbindungen. Die Leitung steht exklusiv nur für den Datenverkehr des Kunden zur Verfügung. Die Kosten sind abhängig von der angemieteten Bandbreite und der Entfernung zwischen den Endpunkten. Leased Link teilt die Deutsche Telekom ein in:

- ✓ **Daten-Direkt-Verbindung (DDV)**: besonders sichere Standleitungen, die vor Übertragungsfehlern und Datenverlust schützen, für höchste Übertragungsqualität ausgelegt.
- ✓ **Standard-Fest-Verbindung (SFV)**: Standard-Standleitung für Sprache und Daten (wird seit 30. September 2009 nicht mehr angeboten).

Die Angebote reichen bis zu digitalen Hochgeschwindigkeitsübertragungen, die für die Kopplung von Rechenzentren bzw. für die performante Verbindung der Standorte einer Firma benötigt werden sowie für den Anschluss von SAN-Speicherlösungen.

Switched Link oder Wählverbindung

Hier handelt es sich **nicht** um feste (permanente), sondern um vermittelte Verbindungen. Switched Link ist dabei ein Überbegriff, der die unten aufgeführten Angebote umfasst. Vermittelte Netze sind vor allem für den Datenaustausch mit wechselnden Kommunikationspartnern geeignet.

Bei Wählverbindungen, die das Internet nutzen (wie z. B. mit DSL), können andere die Übertragung belauschen und vertrauliche Informationen missbrauchen. Um hier eine Abschottung der übertragenen Daten zu erreichen, gibt es die Technik **VPN (Virtual Private Network)**.

Mittlerweile ist die Unterscheidung in Leased Link und Switched Link im Grunde hinfällig. Heute erfolgt die Verbindung letzten Endes über Multiplexsysteme, die bei Bedarf von einem zentralen Netzmanagementsystem eingerichtet werden.

MPLS

Über das Vermittlungsverfahren **Multi Protocol Label Switching (MPLS)**, das oft bei großen Carriern zum Einsatz kommt, kann ebenfalls ein Netz, für die Benutzer, wie eine Art Standleitung erscheinen. Allerdings erfolgt die Übertragung unverschlüsselt, sodass es ein VPN nicht ersetzen kann.

20.2 WAN-Standardangebote

Die Palette der konkreten einzelnen Angebote der verschiedenen Unternehmen ist unterschiedlich groß. Sie reicht von DSL-Paketen bis zu Outsourcing-Lösungen. Besonders wichtig für den professionellen Einsatz sind weniger die Kosten, sondern vor allem die Verfügbarkeit und die Zuverlässigkeit. So kann der Ausfall der Webpräsenz eine Firma ruinieren, selbst wenn dies nur wenige Tage umfasst.

Die IT-Landschaft hat sich in den letzten Jahren erheblich verändert. Waren vor noch nicht allzu langer Zeit, Leitungen mit 2 Mbit/s nur für große Firmen erschwinglich, sind heute selbst im privaten Bereich 50 Mbit/s und mehr Standard (vgl. dazu auch die Breitbandstrategie der Bundesregierung unter <https://initiatived21.de/arbeitsgruppen/deutsche-breitbandinitiative/>).

So genügt meist das Standard-Paket eines Providers, um sich optimal zu vernetzen. Bei höheren Anforderungen an Zuverlässigkeit und Netzbereitschaft sind deren Business-Lösungen vorzuziehen. Verbindungen zu Privat- oder Firmen-Netzen sollten immer per VPN-Lösung geschützt sein.

ADSL

Für Ein-Mann-Betriebe, Freiberufler, kleinere Unternehmen wie Rechtsanwaltskanzleien usw. kann ein ADSL-Anschluss durchaus genügen. Er bietet hohe Übertragungsraten bei niedrigen Kosten. Die wichtigsten Nachteile dabei sind, dass es einmal pro Tag eine Zwangstrennung gibt (in der Regel in den Nachtstunden) und die Upload-Rate wesentlich geringer ist, als die Download-Rate.

Aufgrund der Zwangstrennung verfügt der Kunde über **keine** statische, öffentliche IP-Adresse, da mit jeder neuen Einwahl eine andere öffentliche IP-Adresse zugewiesen werden kann. Die wesentlich geringere Upload-Rate macht sich z. B. beim Versenden von vielen E-Mail-Nachrichten bzw. E-Mails mit größeren Datei-Anhängen bemerkbar und schließt quasi den Betrieb eines eigenen Inhouse-Webservers für Zugriffe aus dem Internet aus.

Möchten Sie trotzdem einen eigenen Webserver über eine ADSL-Leitung betreiben, können Sie wie folgt vorgehen: Über eine Anmeldung Ihrer Website bei einem **DynDNS-Server** (Dynamisches DNS, z. B. <http://www.dyndns.com.de/>), können Interessenten aus dem Internet auf die jeweils aktuelle IP-Adresse Ihrer Website zugreifen. Sie müssen nur Ihren DSL-Router entsprechend konfigurieren. Firmen sollten jedoch vorrangig auf Lösungen setzen, die **SDSL** als Basis verwenden.

ADSL2+ (**Asymmetric Digital Subscribe Line 2**) und **VDSL** (**Very High Speed Digital Subscribe Line**) bzw. VDSL2 stellen Weiterentwicklungen von ADSL dar, mit denen wesentlich höhere Übertragungsgeschwindigkeiten erreicht werden.

SDSL

Firmen können mit **SDSL** (Symmetric Digital Subscribe Line) bei vielen Providern eine Anbindung erhalten, die die oben genannten Nachteile nicht hat. Bei SDSL gibt es keinen Unterschied zwischen Download- und Upload-Geschwindigkeit. So beträgt bereits bei einer 2-Mbit-Leitung die Upload-Rate ebenfalls 2 Mbit/s und ist damit beispielsweise rund **doppelt** so hoch wie bei einer ADSL-Leitung mit 16 Mbit/s.

Hier erfolgt auch keine Zwangstrennung nach 24 Stunden und der Kunde bekommt oft noch einige öffentliche IP-Adressen mit dazu, über die seine Server vom Internet her erreichbar sind. Der Preis ist dafür entsprechend höher.

Mobilfunk

Vor allem in Gebieten, in denen kein DSL bzw. nur DSL mit einer geringen Übertragungsrate angeboten wird, kann der Einsatz eines Mobilfunk-Modems eine gute Alternative darstellen, wenn die erzielbare Bandbreite trotz weiterer Nutzer akzeptabel ist. Bei einer Versorgung mit UMTS sind dies aktuell bis zu 42,2 Mbit/s, bei LTE bis zu 300 Mbit/s (zukünftig mit Kategorie 8 noch mehr). Zudem kann Mobilfunk eine eventuelle Unterbrechung einer DSL-Leitung überbrücken (Fallback) oder auch über Load-Balancing deren Leistung erhöhen.

Das Angebot reicht von einem einfachen Web- bzw. Surf-Stick bis zu den Business-Lösungen der Mobilfunk-Provider, die UMTS- und LTE-Router u. Ä. beinhalten (vgl. Kapitel 19.2).

Hosting

Viele Anforderungen an Vernetzung und Datenverarbeitung sind für kleinere Firmen zu teuer, wenn sie sich selbst darum kümmern müssen. Dazu gehören das Mieten von leistungsfähigen Verbindungen zum Internet, die Konfiguration und Administration von Servern, ein regelmäßiges Backup, die Gewährleistung von Updates, der Austausch defekter oder veralteter Hardware, die Sicherstellung der ständigen Verfügbarkeit und vieles mehr.

Ein Provider ist hervorragend mit dem Internet verbunden (meist über Leitungen mit mehreren Gbit/s) und hat auch das nötige Wissen, um die IT-Technik optimal einzurichten. Diese Leistungen kann er seinen Kunden anbieten. So kann sich der Kunde auf seine Webpräsenz und seine eigentliche Arbeit konzentrieren, ohne sich um die Technik kümmern zu müssen. Er benötigt dann nur noch eine normale Verbindung zum Internet, um die eigenen Daten zu pflegen.

Folgende Unterscheidungen sind möglich:

✓ **Web-Hosting**

Der Provider stellt meist ohne Aufpreis etwas Platz für die eigene Homepage auf einem seiner Webserver zur Verfügung. Weitere Leistungen, wie mehr Speicherplatz für Website-Inhalte, Zugriff über einen eigenen Domain-Namen, Ausführung eigener Scripts, Anbindung an eine Datenbank etc., sind Gegenstand weiterer Vertragsvereinbarungen.

✓ **Server-Hosting**

Die Host-Provider stellen dabei entweder einen kompletten Rechner (einen dedizierten bzw. **Root-Server** mit eigener Hardware) oder einen **virtuellen Server** (der sich die Hardware eines Rechners mit vielen anderen virtuellen Servern teilt) mit unterschiedlicher Performance und unterschiedlichem Ausbau zur Verfügung.

Der Kunde kann diesen dann nach eigenen Wünschen einrichten, meist über ein vorinstalliertes Windows- oder Linux-Betriebssystem. Viele Provider bieten auch spezielle Programme oder Webinterfaces zur einfachen Konfiguration des Servers an. Leistungen wie eine schnelle Anbindung an das Internet, Service und Backup sind oft inbegriffen.

Eine Aufstellung einiger nationaler Host-Provider:

- ✓ 1&1 Internet AG, <https://www.1und1.de/>
- ✓ Strato AG, <https://www.strato.de/>
- ✓ Deutsche Telekom AG, <https://www.telekom.de/start>
- ✓ Host Europe GmbH, <https://www.server4you.de/>
- ✓ Host Europe GmbH, <https://www.hosteurope.de/>

✓ **Domain-Hosting**

Es beinhaltet die Registrierung der Kunden-Domains und die Bereitstellung der erforderlichen DNS-Server. Die meisten Provider bieten diesen Service gegen geringe Kosten an.

✓ **E-Mail-Hosting**

Der Provider stellt einen Mailserver für den Versand und Empfang von E-Mails zur Verfügung. Meist sind Virenscanner und Spamfilter mit eingerichtet. Die Palette reicht vom kostenlosen Freemailer über Premium-Angebote bis zu Firmenlösungen.

Über die IP-Adressen, die private Anwender erhalten (z. B. bei ADSL-Verbindungen), ist wegen der Spam-Problematik meist kein direktes Versenden von E-Mails möglich. Diese IP-Adressen sind oft in einer sogenannten **Realtime Blackhole List (RBL)** eingetragen, die u. a. viele Provider für das Blockieren verdächtiger E-Mails verwenden.

Outsourcing/Cloud-Computing

Nicht jede Firma kann es sich leisten, immer die neuesten Versionen von speziellen Programmen zu kaufen und eine Hochverfügbarkeits-Lösung für die eigene Datenverarbeitung aufzubauen. Beim Outsourcing lagert eine Firma ihre Datenverarbeitung in ein hierfür spezialisiertes Unternehmen aus, das die benötigten Programme und das weitere IT-Umfeld dazu bietet.

Cloud-Computing ähnelt Outsourcing. Es teilen sich dabei mehrere Kunden die verwendete Infrastruktur. Cloud-Computing besagt, dass Rechenleistung und Datenspeicherung auf anderen Rechnern über eine schnelle und sichere Leitung erbracht werden. Auf welchen Rechnern die Verarbeitung der gewünschten Programme genau stattfindet, ist dabei für den Kunden unerheblich. Ein Teilbereich des Cloud-Computings ist **Software as a Service (SaaS)**. Daneben gibt es weitere Bereiche wie **Infrastructure as a Service (IaaS)** oder **Platform as a Service (PaaS)**, auf die an dieser Stelle nicht weiter eingegangen werden soll. Beispiele für das Cloud-Computing sind Office 365 von Microsoft oder die Google Apps.

Outsourcing kann sehr problematisch sein. Zumindest ist dabei großes Vertrauen in den Betreiber erforderlich, da dieser sensible Daten erhält, mit denen er sorgfältig umgehen muss. Beispielsweise haben US-Behörden im Rahmen des „USA PATRIOT Act“ im Verdachtsfall Zugriff auf Daten in der Cloud, wenn die entsprechenden Server in den USA stehen. Eine andere Lösung bei größeren Firmen kann die Zusammenlegung der Datenverarbeitung an einem Standort sein (**Shared Services**).



Bei der Datenübermittlung ist auch die Frage wichtig, ob davon Betroffene für ihre personenbezogenen Daten eine Einwilligung abgeben müssen.

Eine Verschlüsselung hilft nur beim Transport und beim Lagern der Daten. Sie ist wirkungslos, wenn auf Cloud-Servern Daten verarbeitet werden, da dabei die Hardware (und damit auch der Betreiber) Zugriff auf die Daten im Klartext haben muss. Die **homomorphe Verschlüsselung** soll in Zukunft Abhilfe schaffen.

Weitere Angebote

Techniken, die heute als Standard gelten, können morgen schon veraltet sein (siehe X.25, Datex-P, Frame-Relay und ATM für kleine Netzwerke). Dafür geht der Trend dahin, die Vernetzung auch für WANs immer öfter auf Internettechnik aufzubauen und diese durch VPN oder Verschlüsselung zu schützen. Über die Standardangebote hinaus gibt es je nach Unternehmen eine unterschiedlich große Palette weiterer Angebote. Darunter fallen auch branchenspezifische Lösungen. Da es sich hier um einen sich sehr schnell entwickelnden Markt handelt, ist es sinnvoll, sich so aktuell wie möglich über die entsprechenden Angebote zu informieren.

Daneben gibt es noch etliche Protokolle und Verfahren, die zwar älter und teilweise schon veraltet sind, aber in vielen Installationen immer noch Verwendung finden. Für neue Vernetzungen sollten sie aber nicht mehr benutzt werden.



Ergänzende Lerninhalte: Weitere Übertragungsprotokolle.pdf

Wissenstest: Weitverkehrsnetze

21

Praxis 3

21.1 Vorüberlegungen

Abwägen unterschiedlicher Aspekte

Die Musterfirma mit Sitz in Hamburg expandiert weiter und übernimmt einen ehemaligen Mitbewerber mit je einer Zweigstelle in München und Salzburg. Dort existieren bereits LANs, die nun mit der Zentrale gekoppelt werden sollen.

Außerdem gibt es mittlerweile etliche Außendienstmitarbeiter, deren Aktionsradius es nicht mehr zulässt, dass sie jeden Abend nochmals in die Firma kommen, um ihre Daten mit denen im Firmennetz abzugleichen. Auch diese Mitarbeiter brauchen Zugriff auf das LAN.

Bei der Vielzahl an möglichen Anforderungen der Firma müssen für jede Art von gewünschter Verbindung Vorüberlegungen berücksichtigt und miteinander abgeglichen werden:

- ✓ **Wirtschaftlichkeit**
Wie hoch sind die Aufwendungen für die Einrichtung der Verbindungen (Hardware, Installation)? Wie hoch sind die Kosten für den laufenden Betrieb?
- ✓ **Performance**
Welche Übertragungsraten werden benötigt?
- ✓ **Verfügbarkeit**
Wie wichtig ist es, dass eine Verbindung permanent vorhanden ist? Wie hoch ist die Zuverlässigkeit vom Zugangs-Provider bzw. von einem bestimmten Übertragungsverfahren? Gibt es redundante Leitungswege, wenn die Verbindung ausfällt?
- ✓ **Sicherheitserwägungen bezüglich Datenschutz und Datensicherheit**
Wie sensibel sind die Daten, mit denen gearbeitet wird? Hier geht es zum einen darum, dass Daten während der Übertragung nicht abgehört oder verändert werden können. Zum anderen muss sichergestellt werden, dass (von außen) keine unbefugten Zugriffe auf das Firmennetz möglich sind.
- ✓ **Web-Präsenz**
Soll die Firma auch im Internet vertreten sein?

Spätestens an dieser Stelle stößt ein einführendes Werk zum Thema Netzwerkgrundlagen an seine Grenzen. Für konkrete Entscheidungen und Umsetzungen in diesem Rahmen werden weiterführende spezifische Kenntnisse nötig, so z. B. zu den Themen Router, Proxy oder Firewall. Es geht nun immer mehr um den Einsatz von Datenübertragungseinrichtungen, die entweder von darauf spezialisierten Firmen angeboten werden oder für die das notwendige Wissen in produkt-spezifischen Schulungen erst erworben werden muss.

21.2 Umsetzung

Art, Performance und Verfügbarkeit der Verbindungen

Die folgenden Bemerkungen beschränken sich darauf, mögliche Lösungen zu skizzieren. In Bezug auf die Wirtschaftlichkeit ist abzuschätzen, welche Verbindungen eingesetzt werden. Dies ist letztendlich vom Datenaufkommen abhängig.

- ✓ Da in der Zentrale in Hamburg und der Zweigstelle in München häufig in Schichten gearbeitet wird und sich nachts die Server abgleichen, werden die Standorte über eine Festverbindung gekoppelt.
- ✓ München und Salzburg sowie Hamburg und Salzburg werden über sogenannte DSL-Router (Router mit DSL-Zugang) verbunden. Diese werden als Backup-Verbindung für den Fall, dass die Festverbindung ausfällt, auch zwischen Hamburg und München eingerichtet.
- ✓ Die DSL-Router an sämtlichen Standorten werden so konfiguriert, dass sich die Außendienstmitarbeiter mithilfe einer VPN-Verbindungssoftware, ins Firmennetz einwählen können.

Abgesehen von der Aufstellung der Router vor Ort und der Konfiguration der Notebooks, Tablets etc. der Außendienstmitarbeiter sind keine hardwarespezifischen Arbeiten notwendig. In Bezug auf die benötigten Leitungen müssen Verträge mit Anbietern abgeschlossen werden.

Sicherheitserwägungen

Die Datenübertragung soll dort, wo es notwendig ist, verschlüsselt erfolgen. Kann beispielsweise der Datenaustausch nicht über eine Standleitung, sondern nur per DSL über das öffentlich zugängliche Internet realisiert werden (dies betrifft die Außendienstmitarbeiter in ihrem Home-office), müssen VPN-Verbindungen eingerichtet und entsprechend konfiguriert werden.

An der Grenze der einzelnen LANs zum Weitverkehrsnetz wird jeweils eine Firewall konfiguriert.

Web-Präsenz

Die Firma beschließt, die Veröffentlichung und Verwaltung der Firmen-Website nicht selbst durchzuführen, sondern schließt dazu einen Vertrag mit einem ISP (**I**nternet **S**ervice **P**rovider) ab.

Weitere Fragen

Beim Zusammenschluss von Netzwerken ergeben sich häufig Probleme, die die verwaltungstechnisch-organisatorische Seite der (ehemalig einzelnen) LANs betreffen. Dies betrifft Fragen wie z. B. die Benutzerverwaltung (Directory Services), den Speicherort für Daten, die Vergabe von Berechtigungen oder IP-Adressen (eventuell wurden mehrfach verwendbare private IP-Adressen in den vormals getrennten Netzwerken eingesetzt). Kann sich ein Benutzer aus Hamburg im Münchner LAN anmelden? Was darf er dort und von wem bzw. von wo aus wird das Netz administriert? Fragen dieser Art werden sicher den größeren Teil der anstehenden Arbeiten ausmachen.

Schulversion

1		802.11g	40	Backup	78	
		802.11h	41	Bandbreite	33, 181, 183, 184	
	1000Base-LX	65	802.11i	41	Baum-Topologie	23
	1000Base-SX	65	802.11n	40	Benutzerendeinrichtung	180
	1000Base-T	63, 65	802.11s	41	Benutzerverwaltung	12, 68
	1000Base-ZX	65	802.11w	41	Betriebssystem	10, 66
	100Base-FX	63, 65	802.11z	40	BGP, Border Gateway Protocol	147, 148
	100Base-T	62	802.1as	59	Bindung	48
	100Base-T4	65	802.1x	36	Bit	25
	100Base-TX	62, 65	802.3BQ	155	Bitübertragungs-Schicht	103
	100GBase	63	802.3bz	41, 153	B-Kanal	191
	100GBase-LR4	65			Bladeserver	67
	100GBase-SR10	65			BLE, Bluetooth Low Energy	43
	100-Gigabit-Ethernet	155			Blowfish	196
	10Base-F	62	Access Point	37, 91	Bluetooth	43
	10Base-T	62	Adaptive Switching	141	Bluetooth Low Energy	44
	10GBase-LR	65	Ader, Kabel	26	BMC, Baseboard Management Controller	53
	10GBase-SR	65	ADSL	191, 215	BNC-Kabel	27
	10GBase-T	63, 65, 155	ADSL2+	191	Border-Router	147, 148
	10-Gigabit-Ethernet	154	AES	41	Breitband	181
2		AH	116	BRI	190	
	2,4-GHz-Band	38	AMT, Active Management Technology	53	Bridge	137
	25GBase-T	155	Anonymisierungs-Netzwerke	186	Broadcast	55
3		ANSI	104, 192, 193	Broadcast-Adresse	113, 114	
	3DES	196	Anwendungs-Protokolle	108, 121	Browser-Fingerprints	187
	3G	207	Anwendungs-Schicht	104	BSD	71
4		APIPA	118	Bus-System	49	
	4G	208	App	12	Bus-Topologie	20
	40-Gigabit-Ethernet	155	Appliance Server	77	B-WiN	176
	4in6	144	Application Layer	104	Byte	25
5		Application Level Firewall	150			
	5G	208	Application-Server	11	C	
	5-GHz-Band	38	Apps	187		
		arp	167	Cable-sharing	153	
		ARP, Address Resolution Protocol	118, 167	Campus Backbone	128	
6		ARPANet	109	Carrier	184, 212	
	60-GHz-Band	38	ASCII	104	Carrier Sense Multiple Access with Collision Avoidance	58
	6in4	144	ASIC	144	CCITT	97
8		ASN.1	104	CCMP	36, 41	
		ATM	24, 183, 194	Cell-Backplane-Switch	141	
		Authentication Header	116	Ceph	80	
		Authentifikation	199	CHAP	199	
		Authentifizierung	97	CIDR, Classless Inter-Domain Routing	113, 115, 117	
		Autokonfiguration	119	CIDR-Schreibweise	115	
		Automatic Private IP Addressing	118	CIX	178	
				Cladding	30	
				Clause	153	
				Client-Server	10, 66	
	80/20-Regel	126		Clock-Skew-Fingerprinting	187	
	802.11a	39		Cloud	24	
	802.11ac	40		Cloud-Computing	217	
	802.11ac Wave 2	40, 41		Cloud-Service-Provider	212	
	802.11ad	40		Cloud-Speicher	196	
	802.11ah	40, 44				
	802.11ax	40				
	802.11ay	40				
	802.11b	40				
	802.11e	41				

Cluster	69, 76	DMT, Discrete Multi Tone	189, 192	Festverbindung	181, 182					
Cluster Shared Volumes	80	DNS, Domain Name Service	118	FHSS, Frequency Hopping						
Cluster-Dateisystem	80	DNS-Server	12	Spread Spectrum	37, 43					
CN, Corporate Network	183	Docker-Container	73	Fibre Channel	81					
Collapsed Backbone	129	DOCSIS	209	Fibre to the desk	34					
Content-Provider	212	Domain-Hosting	217	File-Server	11, 68					
Cookies	187	Domänencontroller	68	Firewall	69, 149					
Core	30	DOS, Disk Operating System	67	Firewire	52					
Core Network	180	Dotted-Decimal-Format	111	Flatrate	204					
Core Services	68	Downstream	192	Flow Control (Flusskontrolle)	140					
CRC	103, 106	Drahtlose Übertragung	35	Flusskontrolle	140					
Cross-Bar-Switch	141	DSCP, Differentiated Service		Fragment-Free-Modus	141					
Cross-Over-Patchkabel	50	Code Point	140	Fragmentierung	106					
CSMA/CA	58	DSL	191, 203	Frame	54, 103, 106					
CSMA/CD	55, 154	DSLAM	192	FSF	72					
Cut-Through	141	DS-Lite	209	FTP	110					
		DSL-Light	192	Funktionsverbund	16					
		DSL-Router	204, 220	Funkzelle	37					
D										
Dämpfung	26	DSSS, Direct Sequence Spread Spectrum	38	G						
Darstellungs-/Präsentations-Schicht	104	DÜE	175	G.SHDSL	194					
Data Link Layer	103	Dynamisches Routing	146	GAN	14					
Datagramme	106	E								
Datenbank	69	EBCDIC	104	GARP	131					
Datenbankmanagementsystem	12	ECC-Speicher	53, 75	Gateway	108, 150					
Datenbank-Server	12	EIA/TIA	29	GÉANT2	176					
Datenpakete	54	E-Mail-Hosting	217	getmac	168					
Datensicherung	11, 16, 89	Embedded-System	67	GG-45	155					
Datenübertragungsrate	103	EN 50173	127	Giga-IR	45					
Datenverbund	15	Ende-zu-Ende-Verschlüsselung	197	Glasfaser	25					
DDV	214	ENX	178	Glasfaserkabel	30					
DDV, Datendirektverbindung	182	Erpressungs-Trojaner	78	GlusterFS	80					
DECT	87	Error-Free-Cut-Through	141	GNU	72					
DEE	175	Ethernet	59, 105, 152	Gradientenindexfasern	33					
Default-Route	114, 116	Ethernet, Entwicklung von	61	Gradientenindexprofil	33					
Default-Router	145, 146	Ethernet-Adresse	118	Gradientenprofil	33					
Demoduliert, Trägerfrequenz	189	Ethernet-Frame	123	GSM	206, 207					
DES	196	Ethernet-II	107	GUI, Graphical User Interface	67					
Dezibel	26	Ethernet-Rahmen	106	GVRP	131					
DFN-Verein	176	Exchange Server	71	G-WiN	176					
DFS, Dynamic Frequency Selection	40, 41	Extranet	178	H						
DFÜ	184	F								
DHCP, Dynamic Host Configuration Protocol	119	Faser, Kabel	26	Halogenfreie Kabel	27					
DHCP-Server	12, 119	Fast-Forward-Modus	141	HDLC	198, 199					
Dienst	179, 183	FC, Fibre Channel	81	HDSL	193					
Dienstgüte	179	FC-AL, Fibre Channel Arbitrated Loop	81	HDSL2	193					
Dienstintegration	179	FCC	185	Header	101, 103					
Diffie-Hellmann	188, 197	FCoE	81	High-Availability	76					
Diffusionsnetz	20	FCS, Frame Check Sequence	103, 106	Hochverfügbarkeit	75					
dig	169	FC-SW, Fibre Channel Switch	81	Homomorphe Verschlüsselung	197, 218					
Directory Services	68	Fernsprechnetz	176	Hop	145					
Dispersion	32	Fernwartung	53	host	169					
Distributed Backbone	130	Schulversion								
DMT	192									8

Host-ID	112	ISDN, Basis-Anschluss	190	Linux	72
Hosting	216	ISDN, Primärmultiplex-Anschluss	190	Linux-Distributionen	72
Hot Plugging	75	ISM-Band	38	LLC	105
Hot Swapping	75	ISP, Internet Service Provider	115, 220	Load Balancing	17, 148
HSCSD	206	ITU	97	Loop	138
HSDPA	207	IVBB	177	Loopback-Adresse	114
HTTP	104, 110			LoRa	45
HTTPS	110, 198			LPWAN	45
Hub	63, 136			LSA-Technik	30
		K		LSF, Low Smoke and Fume	27
		Kabel, Ader	26	LSO, Local Shared Objects	187
		Kabel, Anforderungen	27	LTE	208
IaaS	217	Kabel, Faser	26	LTE-Router	204
IANA	98, 111	Kabel, Glasfaser-	30		
ICANN	98	Kabel, Litze	29	M	
Icinga	164	Kabel, Mantel	26	MAC	105
ICMP, Internet Control Message Protocol	118	Kabel, Massivleiter	29	MAC-Adresse	47, 105, 106, 111, 112, 118, 137, 168
ICMPv6	118	Kabelfernsehnetz	209	Mail-Server	12
IDEA	196	Kabeltester	167	Mainframe	8, 66
Identitätsdiebstahl	187	Kaskadierung	139	MAN	13
IDN, Integrated Digital Network	176	Kernel-Module	48	Managed Node	160
IEEE	96, 152	Kernnetz	180	Managed Switches	139
IEEE 1394	52	Koaxialkabel	27	Man-in-the-Middle-Angriff	198
IEEE 1588	59	Kollision	56, 153	Mantel, Kabel	26
IEEE 1901 Access	210	Kommunikation	15	Maschennetz	23
IEEE 802.1ax	157	Kommunikationssteuerungs-/Sitzungs-Schicht	104	Masquerading	120
IEEE 802.3ad	157	Konvergenz	17	MC2UC, Multicast-to-Unicast	42
IETF	98, 109	Kupfer	25	MD5	197
ifconfig	169			Medienkonverter	136
IGMP-Snooping	42			Meshing	138
Industrie-LAN	134	L		Mesh-WLAN	42
Infrarot	45	L2TP	144, 183, 200	Metadaten	186
Inhaltsverschlüsselung	197	LAA-LTE	41, 208	MIB, Management Information Base	160, 161
Integration von Diensten	125	LACP, Link Aggregation Control Protocol	142, 157	Mietleitung	181
Interdomain Routing	147	LACP, Netzwerkadapter, Bündelung	157	MIMO, Multiple Input Multiple Output	40
Internet	114, 178, 183, 211	LAN	13, 211	Mobilfunk	216
Internet Protocol Security	116	Laser	46	Mobilfunk-Modem	204
Internettelefon	205	Last Mile	180	Mobilfunknetz	206
Internettelefonie	205	Lastverbund	17	Mobilität	17
Intranet	178	Layer 1	189	Modem	190, 203
Investitionsschutz	91	Layer 2	189	Modulation	189
IoT, Internet of Things	44	Layer-3-Switch	140, 142, 143	Moduliert	189
IP	110	Layer-3-Switching	142	Monitoring	160
IP Forwarding	143, 161	Layer-3-VLAN	133	Monomode	31
ipconfig	168	Layer-4-Switching	143	MPLS	157, 214
IPMI, Intelligent Platform Management Interface	53	Layer-7-Switching	143	MPTCP, Multipath-TCP	158
IP-Netze, private	117	LDAP, Lightweight Directory Access Protocol	68, 74	MRP	131
IPnG	115	Learning Bridge	138	MTU	106, 210
IPsec	116, 144, 183, 200	Leased Link	214	Multicast	55
IPv4-Adresse	111	Leitungsvermittlung	185	Multicast-to-Unicast	42
IPv6	115	Lichtwellenleiter	30	Multifunktionsgeräte	151
IPv6, Adressaufbau	116	Link Extender	136	Multihoming	158
ISAKMP	201	Link-Klassen	127	Multilayer-Switch	142
iSCSI	82				
ISDN	190				

Multimode	32	OFDMA	40	Protokoll	10, 108, 150, 195
Multiplex	189	OpenVPN	144, 183, 201	Protokollanalysatoren	165
Multiportrepeater	136	Orngefs	80	Protokollanalyseprogramm	165
Multiprotokoll	144	OS, Operating System	67	Protokoll-Stack	108
Multi-Streaming	158	OSI-Referenz-Modell	99	Provider	184, 212
Multi-User-MIMO	40	OSPF	147, 148	Proxy, Cache	119
MVRP	131	Outsourcing	217	Proxy-Server	12, 119, 150
				PSTN	176
N					
Nagios	164	PaaS	217	Public Switched Telephone Network, PSTN	176
Namensauflösung	104	Pakete	153, 182	Pull-Prinzip	78
NAS	14, 80	Paketfilter	149	Punkt-zu-Punkt-Verbindung	199
NAT	117	Paketvermittlung	54, 184, 185	Punkt-zu-Punkt-Verschlüsselung	197
NAT/PAT	120	PAP	199, 200	PVC	182
NAT-Traversal	120	Passwort, sicheres	187	PXE	47
NBase-T	41, 153	PAT	117		
NDIS	48	Patchkabel	30	Q	
NDP, Neighbor Discovery Protocol	118	Patch-Panel	30	QAM, Quadratur-Amplituden-Modulation	39
netstat	168	pathping	169	QoS, Quality of Service	41, 116, 140, 179, 208
Network Layer	103, 105	Payload	144		
Netzneutralität	185	PCI	49	R	
Netz-Provider	212	PCIe, PCI-Express	49	RADIUS	36, 142
Netzwerk	8	PCM, Pulse Coded Modulation	189	Rahmen	106
Netzwerk-Adresse	112, 113	PCMCIA	48	RAID	78
Netzwerkanalysegeräte	167	PDH	181	RAS	184
Netzwerkdiagnosegeräte	167	Peer-to-Peer	9	RBL, Realtime Blackhole List	217
Netzwerke, serverbasiert	139	Personal Computer	9	Rechenzentrum	8, 10
Netzwerk-ID	112	PFC, Priority Flow Control	140	Redundanz	16, 75
Netzwerkkarte	47, 108	PFS, Perfect Forward Secrecy	188	Regulierung	185
Netzwerkkomponenten, Zuordnung OSI-Schichten	135	Physical Layer	103	Repeater	20, 136
Netzwerk-Management	160, 164	Physische Adresse	112	Request For Comment	98
Netzwerk-Protokolle	121	Piconet	43	RFC	109, 195
Netzwerkschnittstelle	47	ping	168	RFC-Dokumente	98
Netzwerk-Überwachung	160	PoE	50	RFID, Radio Frequency Identification	43
Netzwerküberwachung, Programme	164	Port	136	RFID-Tag	43
New Fiber Cable	154	Port-Mirroring	142, 165	Ring-Topologie	22
Next Hop	145	Portnummer	111	RIP	147
NFC, Near Field Communication	43	Power Delivery	51	RJ-45	29
NIC, Network Interface Card	47	PowerLAN	14, 210	RMON, Remote Monitoring	162
NMS, Network Management Station	160	Powerline Communication	210	Root-Server	73
Norm	95	PPP	189, 199	route	168
Normierung	152	PPP, Point-to-Point Protocol	199	Router	109, 143
nslookup	168	PPPoE	189, 199	Router-Advertisements	146
Nutzerprofile	187	PPTP	184, 199	Router-Solicitation	146
		Präambel	106	Routing	103, 109, 145, 157
O					
OAM	160	Privacy Extentions bei IPv6	188	RPC	110
ODI	48	Private IP-Netze	117	RSA	197
OFDM	38	Private-MIB	161		
OFDM, Orthogonal Frequency Division Multiplex	38	Privatsphäre, Internet	186	S	
		Proprietär	8	SA, Security Association	201
				SaaS	217

Safe-Harbor	212	SNMP-Trap	160	Telefonnetz	190
SAN, Storage Area Network	14, 59, 80	SNMPv2	162	TERA	155
SAP, Service Access Point	101	SNMPv3	163	Teredo	144
SAS, Serial Attached SCSI	75	Socket	111	Terminals	8
Satellit	209	SoL, Serial over LAN	53	Terminal-Server	11
Schicht 3	144	SONET	195	Tertiärer Bereich	173
Schichten-Modell	98	Spanning Tree	97, 138	Tertiärverkabelung	128
Schleifenunterdrückung	138	Spiegelport	165	Thin Clients	9
Schmalband	181	Splitter	192	Thin-Server	77
Schnittstelle	101, 180	Spread-Spectrum	37	Thunderbolt	52
SDH	181, 194	SQL Server	71	TKIP	36, 41
SDH/SONET	194	Squid, Proxy	120	Topologie	19, 144
SDSL	193, 215, 216	SRN, Short Range Networks	44	Topologie, Baum-	23
Segment	129, 137	SSH	159	Topologie, Bus-	20
Segmentierung	104	SSID, Service Set Identifier	35	Topologie, logische	19
Sekundärer Bereich	173	SSTP, Secure Socket Tunneling Protocol	200	Topologie, Maschennetz	23
Sekundärverkabelung	128	Stacking	132, 139, 142	Topologie, physikalische	19
Sequenznummer	104	Standard-MIB	161	Topologie, Ring-	22
Server	74, 87	Standleitung	181, 214	Topologie, Stern-	21
Serveraufgaben	11	Start Frame Delimiter	106	Tor, Anonymisierungs-	
Serverbasierte Netzwerke	139	Stateful Inspection Firewall	149	Netzwerk	186, 202
Serverbasiertes Netzwerk	12	statisches Routing	146	ToS, Type of Service	140
Server-Farm	76	Stecker	33	TPC	41
Server-Hosting	216	Steckkarten	48	TPC, Transmit Power Control	40
Session Initiation Protocol	205	Stern-Topologie	21	TPM	53
SFD	106	Storage	78	traceroute	168, 169
SFV	214	Store-and-Forward	141	tracert	169
SHA	197	Störempfindlichkeit	27	Tracking	187
Shared Media	20, 55, 136, 206	STP, Shielded Twisted-Pair	28, 138, 143	Traffic Shaping	140, 151, 206
Shared Services	217	Stromnetz	210	Trägerfrequenz	189
SHDSL	194	Strukturierte Verkabelung	127	Trailer	103
SHDSL.bis	194	Stufenindexprofil	33	Transmission Control Protocol	104
Short Message Service	206	Subnetting	114	transparenter Proxy	119
Sicheres Passwort	187	Subnetz	114	Transport Layer	104, 115
Sicherheit	10, 17, 34	Subnetze	114	Transport-Schicht	104
Sicherungs-/ Datenverbindungs-Schicht	103	Subnetzmaske	112, 113	Transportverschlüsselung	197
SI-Einheiten	25	Supernetting	115	Treiber	105
Signaldämpfung	26	SVC	182, 183	Tunneling	144, 183
Signierung	197	Switch	21, 63, 90, 139	Tunneling-Protokolle	144
Silent Data Corruption	80	Switched Link	214	Twisted-Pair	28
Singlemode	31	Synchronisation	104	Typ C Stecker für USB	51
SIP	205	Synchronous Digital Hierarchy	194	Typ-C-Authentication	51
SIP-Adresse	205	Synchronous Optical Network	195	Typ-Feld	106
Smart Home	44	System V	71	U	
Smartcard	198	System-Management	164	Übersprechdämpfung	26
Smart-Switch	140			Übertragung, drahtlose	25, 35
SMI, Structure of Management Information	161	T		Übertragungsgeschwindigkeit	25, 46
SMS	206	Tagging	131	Übertragungsmodus	103
SMTP	104, 110, 159	TCO	13	Übertragungsprotokolle	108
SNMP	142	TCP	104, 110	Übertragungsverfahren	189
SNMP-Agent	160	TCP/IP	109, 184	UDP	110
SNMP-Manager	160	TCP/IPv6	184	UMTS	207
SNMP-Polling	160	Telecom	183, 213	UMTS-Router	204
		Telefonanlage, virtuelle	206	Unicast	55
				UNIX	71

Uplinkport	132, 142	VLAN, protokollbasiertes	133	WLAN	14, 26, 58, 59, 91
Upstream	192	VLAN, Virtual Local Area Network	130	WLAN-Adapter	42
URI, Uniform Resource Identifier	205	VLAN-ID	131	WLAN-Repeater	42
URL, Unified Resource Locator	118	VLAN-Tag	107	WLAN-Router	42
USB	51	V-Normen	190	Wolke	24
USB-OTG	51	VoIP, Voice over IP	87, 191, 205	WPA2	41
USV	16, 76, 87	Vollduplex	154	WPA3	36
UTP, Unshielded Twisted-Pair	28	VPN	15, 183, 200	WPAN, Wireless Personal Area Network	44

V

VC	182
VDSL	192
VDSL2	192
VDSL2-Vectoring	193
Verfügbarkeitsverbund	16
Verifizierung	197
Verkabelung, strukturierte	127
Vermittlungs-/Netzwerk-Schicht	103
Vermittlungsstelle	180
Verteilerschrank	30
Verzeichnisdienst	74
Virtualisierung	73
Virtuelle Verbindung	182
VLAN	14, 20, 97
VLAN, anwendungsbasiertes	133
VLAN, dynamisches	132
VLAN, IEEE 802.1Q	131
VLAN, MAC-Adressenbasierte	133
VLAN, portbasiertes	132

W

Wählverbindung	182
WAN,	14, 175, 211
WAP	207
WaveLAN	14
WDM	156, 195
Web-Hosting	216
Web-Server	12
WECA	35
Wellenwiderstand	20
WEP, Wired Equivalent Privacy	36
WHEA	53
whois	117
Widgets	67
Wi-Fi Alliance	35
WiFiDirect	42
WiMAX	208
Wireless USB	51
Wireshark	165

X

X Window System	73
X.25	183, 198
X.509	198
X-WiN	176
Zellen	103
Zero-Day-Exploits	72
Zertifikat	198
ZigBee	44
Zugangs-Provider	212
Zugriffsverfahren	54
Zuverlässigkeit	74
Z-Wave	44

Z

Impressum

Matchcode: NW_2022

Autor: Karsten Bratvogel

Produziert im HERDT-Digitaldruck

1. Ausgabe, Dezember 2021

HERDT-Verlag für Bildungsmedien GmbH
Am Kuemmerling 19
55294 Bodenheim
Internet: www.herdt.com
E-Mail: info@herdt.com

© HERDT-Verlag für Bildungsmedien GmbH, Bodenheim

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Verlags reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Dieses Buch wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Wenn nicht explizit an anderer Stelle des Werkes aufgeführt, liegen die Copyrights an allen Screenshots beim HERDT-Verlag. Sollte es trotz intensiver Recherche nicht gelungen sein, alle weiteren Rechteinhaber der verwendeten Quellen und Abbildungen zu finden, bitten wir um kurze Nachricht an die Redaktion.

Die in diesem Buch und in den abgebildeten bzw. zum Download angebotenen Dateien genannten Personen und Organisationen, Adress- und Telekommunikationsangaben, Bankverbindungen etc. sind frei erfunden. Eventuelle Übereinstimmungen oder Ähnlichkeiten sind unbeabsichtigt und rein zufällig.

Die Bildungsmedien des HERDT-Verlags enthalten Verweise auf Webseiten Dritter. Diese Webseiten unterliegen der Haftung der jeweiligen Betreiber, wir haben keinerlei Einfluss auf die Gestaltung und die Inhalte dieser Webseiten. Bei der Bucherstellung haben wir die fremden Inhalte daraufhin überprüft, ob etwaige Rechtsverstöße bestehen. Zu diesem Zeitpunkt waren keine Rechtsverstöße ersichtlich. Wir werden bei Kenntnis von Rechtsverstößen jedoch umgehend die entsprechenden Internetadressen aus dem Buch entfernen.

Die in den Bildungsmedien des HERDT-Verlags vorhandenen Internetadressen, Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen waren zum Zeitpunkt der Erstellung der jeweiligen Produkte aktuell und gültig. Sollten Sie die Webseiten nicht mehr unter den angegebenen Adressen finden, sind diese eventuell inzwischen komplett aus dem Internet genommen worden oder unter einer neuen Adresse zu finden. Sollten im vorliegenden Produkt vorhandene Screenshots, Bezeichnungen bzw. Beschreibungen und Funktionen nicht mehr der beschriebenen Software entsprechen, hat der Hersteller der jeweiligen Software nach Drucklegung Änderungen vorgenommen oder vorhandene Funktionen geändert oder entfernt.