Inhaltsverzeichnis

Grundlagen der Netzwerktechnik

Grundlagen Netzwerktechnik 10
Grundbegriffe Netzwerktechnik 15
Organisationen in der Netzwerktechnik 22
LAN - Local Area Network 24
WAN - Wide Area Network 25
Internet 26
Schichtenmodelle 28
DoD-Schichtenmodell 31
ISO/OSI-7-Schichtenmodell 32
Netzwerk-Topologie 37
Strukturierte Verkabelung 42
Netzwerk-Kabel 46
Twisted-Pair-Kabel (UTP / FTP / STP) 46
Koaxialkabel 57
Lichtwellenleiter (LWL / Glasfaser) 59
Netzwerkkarte / Netzwerkadapter (NIC) 63
Hub 64
Switch 65
Router 66
Layer-3-Switch 67
Gateway 69

Übertragungstechnik

IEEE 802 72
IEEE 802.3 / Ethernet-Grundlagen 73
CSMA/CD und Kollisionen (Ethernet) 75
MAC-Adresse 80
Fast-Ethernet / IEEE 802.3u 83
Gigabit-Ethernet / 1000Base-T / IEEE 802.3z / IEEE 802.3ab 85
IEEE 802.3bz / NBase-T (2,5GE und 5GE) 86
10-Gigabit-Ethernet / 10GE / IEEE 802.3ae / IEEE 802.3an 87
40- und 100-Gigabit-Ethernet / IEEE 802.3ba 88
Power-over-Ethernet (PoE) 90
IEEE 802.11 / WLAN-Grundlagen 93

WLAN-Frequenzen und -Kanäle 97
CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance 104
WLAN-Topologie 108
IEEE 802.11b / WLAN mit 11 MBit 111
IEEE 802.11g / WLAN mit 54 MBit 111
IEEE 802.11a / IEEE 802.11h / IEEE 802.11j 112
IEEE 802.11n / WLAN mit 150 MBit/s 113
IEEE 802.11ac / Gigabit-WLAN 117
IEEE 802.11ad - Wireless Gigabit (WiGig) 122
IEEE 802.11ax / High Efficiency WLAN 122
WLAN-Sicherheit 123
WPA - WiFi Protected Access 125
WPA2 - WiFi Protected Access 2 / IEEE 802.11i 126
WPS - WiFi Protected Setup 127
HomePlug-Powerline 130

TCP/IP

TCP/IP 136
IPv4 - Internet Protocol Version 4 140
IPv4-Adressen 141
IPv4-Konfiguration 149
IP-Routing 153
DHCP - Dynamic Host Configuration Protocol 156
NAT - Network Address Translation 159
ARP - Address Resolution Protocol 165
ICMP - Internet Control Message Protocol 166
IPv6 - Internet Protocol Version 6 167
IPv6-Adressen 172
Schreibweise/Notation von IPv6-Adressen 176
IPv6-Autokonfiguration 179
Übergangsverfahren (Transition Strategy) 184
Dual Stack 187
TCP - Transmission Control Protocol 189
TCP- und UDP-Ports 191
UDP - User Datagram Protocol 195
RTP - Realtime Transport Protocol 196
NetBIOS - Network Basic Input/Output System 196
Zeroconf / Bonjour / Avahi 198

Anwendungen und Dienste

WWW - World Wide Web 204
E-Mail 206
Namensauflösung 210
DNS - Domain Name System 214
URL - Uniform Resource Locator 223
HTTP - Hypertext Transfer Protocol 225
HTTP Version 2.0 228
WebDAV - Web-based Distributed Authoring and Versioning 229
FTP - File Transfer Protocol 230
NTP - Network Time Protocol 232
Verzeichnisdienste (X.500) 233
LDAP - Lightweight Directory Access Protocol 237
VoIP - Voice over IP 238
SIP - Session Initiation Protocol 245
QoS - Quality of Service 247

Netzwerk-Sicherheit

Grundlagen der Netzwerk-Sicherheit 254
Kryptografie / Kryptographie 257
Verschlüsselung / Chiffrierung 263
Kryptografische Protokolle / Verschlüsselungsverfahren 266
Hybride Verschlüsselungsverfahren 270
SSH - Secure Shell 271
SSL - Secure Socket Layer 273
TLS - Transport Layer Security 282
Sichere E-Mail 282
Firewall 284
DMZ - Demilitarisierte Zone 288
VPN - Virtual Private Network 290
IPsec - Security Architecture for IP 294
SSL-VPN 303
OpenVPN 306
Authentifizierung im Netzwerk 308
IEEE 802.1x / RADIUS 310

Stichwortverzeichnis

Grundlagen der Netzwerktechnik

Grundlagen

Schichtenmodelle

Netzwerk-Kabel

Netzwerk-Komponenten

Grundlagen Netzwerktechnik

Als es die ersten Computer gab, waren diese sehr teuer. Peripherie-Geräte und Speicher waren fast unbezahlbar. Zudem war es erforderlich zwischen mehreren Computern Daten auszutauschen. Aus diesen Gründen wurden Computer miteinander verbunden bzw. vernetzt.

Daraus ergaben sich einige Vorteile gegenüber unvernetzten Computern:

- zentrale Steuerung von Programmen und Daten
- Nutzung gemeinsamer Datenbeständen
- erhöhter Datenschutz und Datensicherheit
- größere Leistungsfähigkeit
- gemeinsame Nutzung der Ressourcen

Die erste Möglichkeit, Peripherie-Geräte gemeinsam zu nutzen, waren manuelle Umschaltboxen. So konnte man von mehreren Computern aus einen Drucker nutzen. An welchem Computer der Drucker angeschlossen war, wurde über die Umschaltbox bestimmt. Leider haben Umschaltboxen den Nachteil, dass Computer und Peripherie beieinander stehen müssen, weil die Kabellänge begrenzt ist.

Was ist ein Netzwerk?

Ein Netzwerk ist die physikalische und logische Verbindung von Computersystemen. Ein einfaches Netzwerk besteht aus zwei Computersystemen. Sie sind über ein Kabel miteinander verbunden und somit in der Lage ihre Ressourcen gemeinsam zu nutzen. Wie zum Beispiel Rechenleistung, Speicher, Programme, Daten, Drucker und andere Peripherie-Geräte. Ein netzwerkfähiges Betriebssystem stellt den Benutzern auf der Anwendungsebene diese Ressourcen zur Verfügung.

Netzwerk-Dimensionen

Jedes Netzwerk basiert auf Übertragungstechniken, Protokollen und Systemen, die eine Kommunikation zwischen den Netzwerk-Teilnehmern ermöglichen. Bestimmte Netzwerktechniken unterliegen dabei Beschränkungen, die insbesondere deren Reichweite und Ausdehnung

begrenzt. Hierbei haben sich verschiedene Netzwerk-Dimensionen durchgesetzt für die es unterschiedliche Netzwerktechniken gibt.

- PAN - Personal Area Netzwerk: personenbezogenes Netz, z. B. Bluetooth
- LAN - Local Area Network: lokales Netz, z. B. Ethernet
- MAN - Metropolitan Area Network: regionales Netz
- WAN - Wide Area Network: öffentliches Netz, z. B. ISDN
- GAN - Global Area Network: globales Netz, z. B. das Internet

In der Regel findet ein Austausch zwischen den Netzen statt. Das heißt, dass Netzwerk-Teilnehmer eines LANs auch ein Teilnehmer eines WANs oder eines GANs ist.
Eine 100%ig klare Abgrenzung zwischen diesen Dimensionen ist nicht immer möglich, weshalb man meist nur eine grobe Einteilung vornimmt. So unterscheidet man in der Regel zwischen LAN und WAN, wobei es auch Techniken und Protokolle gibt, die sowohl im LAN, als auch im WAN zum Einsatz kommen.

Protokolle in der Netzwerktechnik

In der Netzwerktechnik bestimmen Protokoll den Ablauf der Kommunikation zwischen den Systemen. Netzwerk-Protokolle sind eine Sammlung von Regeln, die den Ablauf einer Kommunikation zwischen zwei oder mehr Systemen festlegen. Ein Netzwerk-Protokoll definiert, wie die Kommunikation aufgebaut wird, wie und über was sich die Systeme austauschen und wie die Kommunikation wieder beendet wird. Während einer Kommunikation werden also nicht nur Informationen oder Daten ausgetauscht, sondern zusätzlich Protokoll-Informationen, die beim Empfänger verarbeitet werden.
Typischerweise ist nicht nur ein Netzwerk-Protokoll für die Kommunikation verantwortlich, sondern mehrere, die ganz bestimmte Teilaufgaben innerhalb der Kommunikation übernehmen. Die Einteilung erfolgt anhand eines Schichtenmodells. Ein Protokoll ist in der Regel einer bestimmten Schicht zugeordnet.

Schichtenmodelle

Weil ein Netzwerk möglichst universell sein soll, also von mehreren Teilnehmern und mehreren Anwendungen gleichzeitig genutzt werden soll, ist die Netzwerk-Kommunikation in Schichten aufgeteilt. Jede Schicht hat ihre Aufgabe und löst dabei ein bestimmtes Teilproblem einer Kommunikation. Sender und Empfänger müssen dabei mit dem gleichen Schichtenmodelle arbeiten.
Es gibt verschiedene Schichtenmodelle, die sich in der Anzahl der Schichten und somit der Verdichtung der Aufgaben unterscheiden.

Datenübertragung im Netzwerk

Die Kommunikation kann grundsätzlich auf zwei Arten erfolgen. Entweder verbindungsorientiert oder verbindungslos.
Bei der verbindungsorientierten Datenübertragung wird vor dem Austausch der Daten erst eine logische Verbindung hergestellt. Während der Übertragung bleibt die Verbindung zwischen den Kommunikationspartnern aufrechterhalten. Die logische Verbindung bleibt so lange bestehen, bis sie durch einen Verbindungsabbau beendet wird.
Bei der verbindungslosen Kommunikation wird keine logische Verbindung und damit auch keine dauerhafte Verbindung aufgebaut. Die Daten werden in kleine Einheiten geteilt. Die Übertragung jeder Einheit wird auf den meisten Protokoll-Schichten als abgeschlossener Vorgang behandelt. Je nach Technik werden die einzelnen Übertragungseinheiten allgemein als Paket oder Datenpaket bezeichnet. Protokolle bzw. die OSI-Schichten haben meist eigene Begriffe, die meist für das gleiche stehen.

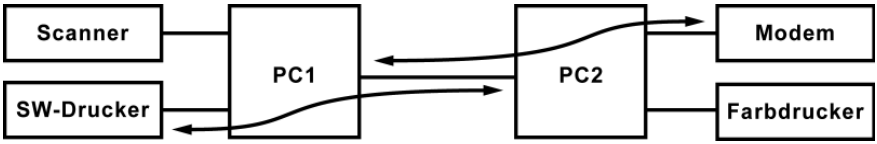
Netzwerk-Adressen

Innerhalb eines Netzwerks werden spezielle Netzwerk-Adressen verwendet, um Sender und Empfänger eines Datenpakets oder einer Nachricht zu adressieren. Dabei unterscheiden sich Netzwerk-Adressen anhand ihrer Funktion, Anwendungen und Protokoll-Schicht. Das bedeutet, dass eine Kommunikation auf jeder OSI-Schicht mit eigenen Adressen arbeitet.

Protokoll	Adresse
Anwendung	URL, Domain, E-Mail-Adresse, …
Transport	Port
Vermittlung	IPv4-Adresse, IPv6-Adresse
Netzzugang	MAC-Adresse

Internet-Adressen ist ein Überbegriff für Netzwerk-Adressen, die im Internet verwendet werden.

Peer-to-Peer-Architektur

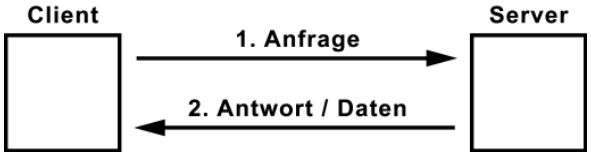


In einem Peer-to-Peer-Netzwerk ist jeder angeschlossene Computer zu den anderen gleichberechtigt. Jeder Computer stellt den anderen Computern seine Ressourcen zur Verfügung. Ein Peer-to-Peer-Netzwerk eignet sich für bis zu 10 Stationen. Bei mehr Stationen wird es schnell unübersichtlich. Diese Art von Netzwerk ist relativ schnell und kostengünstig aufgebaut. Die Teilnehmer sollten möglichst dicht beieinander stehen.
Einen Netzwerk-Verwalter gibt es nicht. Jeder Netzwerk-Teilnehmer ist für seinen Computer selber verantwortlich. Deshalb muss jeder Netzwerk-Teilnehmer selber bestimmen, welche Ressourcen er freigeben will. Auch die Datensicherung muss von jedem Netzwerk-Teilnehmer selber vorgenommen werden.

Client-Server-Architektur

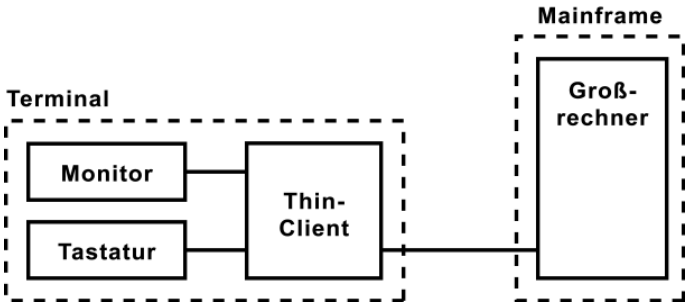
In einem serverbasierten Netzwerk werden die Daten auf einem zentralen Computer gespeichert und verwaltet. Man spricht von einem dedizierten Server, auf dem keine Anwendungsprogramme ausgeführt werden, sondern nur eine Server-Software und Dienste ausgeführt werden.
Diese Architektur unterscheidet zwischen der Anwender- bzw.

Benutzerseite und der Anbieter- bzw. Dienstleisterseite. Der Anwender betreibt auf seinem Computer Anwendungsprogramme (Client), die die Ressourcen des Servers auf der Anbieterseite zugreifen. Hier werden die Ressourcen zentral verwaltet, aufgeteilt und zur Verfügung gestellt.



Für den Zugriff auf den Server (Anfrage/Antwort) ist ein Protokoll verantwortlich, dass sich eine geregelte Abfolge der Kommunikation zwischen Client und Server kümmert.
Die Client-Server-Architektur ist die Basis für viele Internet-Protokolle, wie HTTP für das World Wide Web oder SMTP/POP3 für E-Mail. Der Client stellt eine Anfrage. Der Server wertet die Anfrage aus und liefert eine Antwort bzw. die Daten zurück.

Mainframe-Architektur



Die Mainframe-Architektur sieht wie die Client-Server-Architektur eine Aufteilung des Netzwerks in Terminals und den Großrechner vor, der auch als Mainframe bezeichnet wird. Der Mainframe ist ein sehr leistungsfähiger Computer. Dort sind meist speziell entwickelte Applikationen installiert, die über die Terminals bedient werden. Über serielle Leitungen sind die Terminals mit dem Mainframe verbunden. Wobei das Terminals nur aus einem Bildschirm und einer Tastatur besteht.

Bei der Mainframe-Architektur bilden Terminal und Mainframe eine Einheit. Das Terminal dient als Eingabe-Ausgabe-Schnittstelle zwischen Benutzer und Mainframe. Benutzereingaben werden vom Mainframe verarbeitet und vom Terminal dargestellt.

Die Mainframe-Architektur stammt aus einer Zeit, als es finanziell und aus Platzgründen noch nicht möglich war, jedem Mitarbeiter einen eigenen vollwertigen Computer zur Verfügung zu stellen. Stattdessen beschränkte man sich auf ein einfaches Terminal. Die zentrale Steuerung, Datenhaltung, Anwendungen, sowie die kostengünstige Erweiterung zusätzlicher Terminals, gelten als die Vorteile dieser Architektur. Allerdings führt der Ausfall des Mainframes zum Ausfall der Terminals. Der Betrieb steht dann komplett.

Moderne Formen des Terminals sind mit Arbeitsspeicher, Prozessor und Schnittstellen ausgestattet. Hier laufen ein Großteil der Anwendungen im Terminal. Diese müssen mangels lokalem Massenspeicher vom Mainframe in den Arbeitsspeicher geladen werden. Statt dem Mainframe ist ein Terminalserver für die Auslieferung der Programme zuständig.

Grundbegriffe Netzwerktechnik

Die Reihenfolge der folgenden Grundbegriffe hat didaktische Gründe, weshalb hier auf eine alphabetische Sortierung verzichtet wurde.

Node

Ein Node ist ein Gerät, das über ein oder mehrere Schnittstellen (Interfaces) an ein oder mehrere Netzwerke angeschlossen ist. Dieses Netzwerk bezeichnet man manchmal auch als Link (Verbindung). Zu diesem Netzwerk gehören alle Nodes, die an dem selben Link angeschlossen sind.
Ein Netzwerk und die daran angeschlossenen Nodes bilden eine Site, wenn sie einer gemeinsamen und zusammenhängenden Verwaltung unterstellt sind.
Ein Node kann ganz allgemein ein Host, ein Router oder ein Gateway sein.

Host

Ein Host ist ein Node ohne Router-Eigenschaft, die damit eine Endstelle in einem Netzwerk darstellt. Typischerweise wird ein Client oder Server als Host bezeichnet.

Knoten

Allgemein formuliert ist ein Netzknoten ein Verzweigungspunkt in einem Kommunikationsnetzwerk. Knoten sind im Telefonnetz die Vermittlungsstellen oder auch Telefonanlagen. In einem IP-Netzwerk sind Router und in einem Ethernet-Netzwerk sind Switche die Netzknoten. Zugangspunkte zu einem Netzwerk werden häufig auch als Knoten bezeichnet.

Client

Der Client ist als Teil der Client-Server-Architektur in größere Zahl in allen Netzwerken zu finden. Ein Client ist ein Endgerät oder auch nur eine Software-Komponente, die von einer zentralen Stelle Dienste oder Daten anfordert oder über einen zentralen Zugang am Netzwerk teilnimmt. Typische Hardware-Clients sind PCs, Smartphones, Tablets und Notebooks. Auf diesen laufen dann mehrere Software-Clients für unterschiedliche Dienste. WWW, E-Mail, Messaging, usw.

Server

Ein Server ist ein Computer, der Rechenleistung, Speicher, Daten und Dienste in einem Netzwerk bereitstellt und Zugriffsrechte verwaltet. Auf dem Server laufen mehrere Dienste und Anwendungen, die von anderen Netzwerk-Teilnehmern mit einem Software-Client über das Netzwerk anfordern werden.

Router

Ein Router ist ein Node, der Pakete weiterleitet, die nicht an ihn selbst gerichtet sind. In einem dezentralen Netzwerk ist der Übertragungsweg der Datenpakete nicht fest vorgegeben. Genau genommen weiß niemand in einem dezentralen Netzwerk über alle Verbindungen Bescheid. Deshalb

entscheiden sogenannte Router bei jedem Datenpaket aufs Neue, welchen Weg das Datenpaket geht.

Routing

Die Art und Weise, wie Datenpakete in einem dezentralen Netzwerk oder IP-Netzwerk verarbeitet werden, bezeichnet man als Routing. Man könnte das als Wegfindung bezeichnen. Dabei wird der Weg zum Ziel anhand mehrerer Kriterien (metric) ermittelt. Je mehr Kriterien berücksichtigt werden müssen, desto genauer und gezielter ist der Weg zum Ziel. Aber desto (zeit-)aufwendiger ist die Bestimmung oder Berechnung des Wegs. In der Regel ist das maßgebliche Kriterium die Zieladresse und damit der kürzeste bzw. schnellste Weg zum Ziel. In gewisser Weise suchen sich die Datenpakete ihren Weg zum Empfänger selber. Beim Routing geht darum den optimalen Weg vom Sender zum Empfänger zu finden.
Das maßgebliche Hilfsmittel beim Routing ist die Routing-Tabelle, die in jedem Router mögliche Wege festlegen.

Gateway

Ein Gateway ist eine Hardware oder Software oder eine Kombination daraus, die eine Schnittstelle zwischen zwei inkompatiblen Netzwerken darstellt. Das Gateway kümmert sich darum, dass die Form und Adressierung der Daten in das jeweilige andere Format oder Protokoll des anderen Netzes konvertiert werden.

Bridge

In den Anfangszeiten von Ethernet stand der Begriff "Bridge" (Brücke) für ein Gerät zur Kopplung zweier Ethernet-Segmente. Die Bridge war eine wichtige Komponente, um große lokale Netzwerke zu betreiben. Die Segmentierung begrenzt die Größen der Kollisions-Domänen und das Risiko einer Schleifenbildung.
Heute hat der Name Bridge eine zweite Bedeutung. Eine Bridge verbindet zwei Teilnetze, die auf der Schicht 1 und 2 des OSI-Schichtenmodells arbeiten. Für die Stationen im Netzwerk ist die Bridge transparent, sie können sie nicht sehen.

Switching

In einem geswitchten Netzwerk bestimmt ein konstanter Pfad mit einer definierten Bandbreite, welchen Weg die Datenpakete gehen. Wenn ein Datenpaket abgeschickt wird, steht der Weg durch das Netzwerk praktisch schon fest. Switching eignet sich für Anwendungen, die eine definierte Bandbreite benötigen.

Protokoll

In der Netzwerktechnik ist ein Protokoll der Ablauf einer Kommunikation zwischen zwei Systemen. In der Netzwerktechnik sind die Protokolle meist einer bestimmten Schicht des OSI-Schichtenmodells zugeordnet.

Domäne

Ein Domäne bezeichnet in der Netzwerktechnik ein logisches Subnetz, einen Namensbereich oder ein Objekt, das an der Spitze eines Verwaltungsbereichs steht.
Im Zusammenhang mit Verzeichnisdienste und großen lokalen Netzwerken spricht man öfter von einer Domäne.

Ressourcen

In der Netzwerktechnik spricht man häufig von Ressourcen. In der Hauptsache meint man damit Speicher, auf dem man Daten ablegen kann. Dazu zählen aber auch Drucker, Server und andere Netzwerkgeräte, die einen Dienst bereitstellen, der zentral in einem Netzwerk zur Verfügung steht.

Datenpaket / Paket

In der Netzwerktechnik werden einzelne Übertragungseinheiten als Paket oder Datenpaket bezeichnet. Datenpakte werden neben den Daten mit eine Sender- und Empfänger-Adresse ausgestattet. Fehlerkorrektur und Verschlüsselung sind zusätzliche Merkmale.

Frame

Ein Frame ist ein logischer Rahmen, in dem sich ein Bit-Strom befinden. Frames werden von einer Netzwerkkarte oder einem Netzwerk-Interface über ein Übertragungsmedium gesendet und empfangen. Das Frame ist jeweils mit Daten und einem Protokoll-Header und einem Ethernet-Header versehen. Darin sind Start- und Endsequenzen, Kontrollzeichen, Adressen und Prüfsummen enthalten. Frames werden auch Pakete bzw. Datenpakete genannt. In Zusammenhang mit Ethernet ist die Bezeichnung Frame für ein Datenpaket korrekt.

Datagramm

Ein Datagramm ist eine in sich geschlossene Einheit. Ein IP-Paket, das an den Netzwerk-Adapter (NIC, Network Interface Card) übergeben wird, wird als Datagramm bezeichnet.

Datenstrom / Datastream / Stream

Datastream oder Stream ist ein Datenstrom aus logisch zusammenhängenden Datenpaketen, die über ein Netzwerk übertragen werden. Die logische Verbindung der Datenpakete ist üblicherweise die Empfänger-Adresse. Auf IP-Ebene wäre das die IP-Adresse. Auf TCP- oder UDP-Ebene wäre das die Portnummer.
Die Datenpakete können aber auch auf der Anwendungsebene eine logische Verbindung zueinander haben.

Port

In der Netzwerktechnik kann ein Port eine Steckverbindung an einem Switch, Router, etc. oder eine logische Assoziation sein. Zum Beispiel der Zugang zum Netzwerk für einen WLAN-Client an einem WLAN-Access-Point.
Der Port bei den Protokollen TCP und UDP ist eine Art Adresse, die die Zuordnung zwischen einem Protokoll und einer Anwendung oder zwischen einem Datenstrom und einer Anwendung definiert.
Ein Port, egal ob logisch oder physisch, wird häufig durch eine Nummer oder Adresse gekennzeichnet.

Unidirektionale Kommunikation

Unidirektional bedeutet "in eine Richtung". Bei der unidirektionalen Kommunikation oder Übertragung steht nur ein Kanal zur Verfügung, der nur in eine Richtung genutzt werden kann. Einen Rückkanal gibt es nicht.

Bidirektionale Kommunikation

Bidirektional bedeutet "in beide Richtungen". Bei der bidirektionalen Kommunikation oder Übertragung können Signale, Daten oder Informationen in beide Richtungen fließen. Es gibt zwischen Sender und Empfänger zwei Kanäle. Einen Hin- und einen Rückkanal. Manchmal spricht man auch von Upstream und Downstream bzw. Uplink und Downlink.
Bei der bidirektionalen Übertragung unterscheidet man zwischen Halbduplex, bei der nur jeweils ein Kommunikationspartner senden und empfangen darf, und Vollduplex, bei der beide Kommunikationspartner gleichzeitig senden und empfangen dürfen.

Anycast / Anycasting

Bei Anycast geht die Nachricht an einen Empfänger aus einer Gruppe von Empfängern. An wen aus der Gruppe ist hierbei egal. Hinter Anycast steckt das Verständnis, dass es eine Adresse mehrfach gibt bzw. geben kann (Anycast-Adresse). Das bedeutet dann aber, dass kein wechselseitiger Dialog möglich ist, weil nicht sicher ist, ob man immer mit der selben Maschine verbunden ist.

Anycast wird bspw. für Root-Nameserver benutzt. Hier gibt es nicht nur einen Root-Server, sondern in der Regel ganz viele davon, die auf der ganzen Welt verteilt sind. Aber alle haben die selbe Adresse. Ein Router kennt die Route zu einem von diesen Root-Servern und reicht das Anycast-Paket an diesen weiter.

Unicast / Unicasting

Bei Unicast sind zwei Stationen miteinander verbunden. Sie können direkt oder über ein Netzwerk miteinander kommunizieren. Die Verbindung kann sowohl unidirektional als auch bidirektional sein.

Beim Unicasting steigt die notwendige Bandbreite bei jedem zusätzlichen Host im Netzwerk an. Dabei kann die Netzlast soweit steigen, dass die Informationen bei keinem Host mehr in ausreichender Geschwindigkeit ankommt. So kommt es beim Audio- und Video-Streaming zu Aussetzern beim Abspielen.

Broadcast / Broadcasting

Der Broadcast ist ein Datenpaket, dass an einem Punkt ins Netzwerk eingespeist und von dort an alle Hosts übertragen wird. Dabei empfängt jeder Host die Daten, ob er will oder nicht. Es handelt sich dabei um das klassische Gießkannenprinzip bei der Verteilung von Informationen, wie es zum Beispiel beim Rundfunk (UKW/DAB) oder Fernsehen (Satellit, Kabel, Funk) gemacht wird.

Multicast / Multicasting

Bei Multicast gibt es einen Sender, der zu einer definierten Gruppe von Empfängern Signale, Daten und Informationen überträgt. Hier spielt es keine Rolle, wie viele Empfänger die Daten empfangen. Die Bandbreite wird nur für einen Teilnehmer verbraucht. Die letzte Verteilstelle (Router) ist dann für die Verteilung an die einzelnen Empfänger verantwortlich. Die Daten werden beim letzten Router dupliziert.

Tunneling

Tunneling bezeichnet ein Verfahren, wenn ein Protokoll-Frame mit allen seinen Eigenschaften als Nutzdaten innerhalb eines anderen Protokolls eingebettet ist.

Topologie

Die Struktur des Netzwerks wird als Topologie bezeichnet. Bus, Ring und Stern sind typische Netzwerk-Topologien. Die Verbindungen innerhalb der Topologie erfolgt über Funk, Kupfer- oder Glasfaserkabel.

Backbone

Backbone ist eine Bezeichnung für die Hauptübertragungsstrecke in einem Netzwerk. Der Backbone verbindet in der Regel mehrere Netzknoten. Die Netzknoten sind die Zugangspunkte zum Backbone. Man spricht in dem Zusammenhang auch vom Kernnetz oder Core Network. Bei größeren Vernetzungen mit mehreren Netzwerkstrukturen bildet ein Backbone die Infrastruktur im Hintergrund. Zum Beispiel um lokale
Netze und Hochleistungssysteme miteinander zu verbinden. Ein Backbone wird dabei redundant ausgelegt.

Organisationen in der Netzwerktechnik

An der Entwicklung der zukünftigen Netzwerktechnik sind verschiedene nationale und internationale Organisationen beteiligt. Sie nehmen Normungen vor und entscheiden so über den Einsatz neuer Entwicklungen.
Es folgt ein Auszug der wichtigsten internationalen Organisationen, die im Bereich der Netzwerktechnik besondere Relevanz besitzen.

IANA - Internet Assigned Numbers Authority

Die IANA verwaltet wichtige Datenbanken. Dazu gehören die zentralen Adress-Pools für IPv4 und IPv6 und die zentrale Root-Zone des DNS.

ICANN - Internet Corporation for Assigned Names and Numbers

Bei der ICANN handelt es sich um eine private Stiftung mit Sitz in Marina del Rey in Kalifornien (USA). Die ICANN verantwortet eine Reihe technischer und organisatorischer Vorgaben, die den reibungslosen Betrieb des Internets gewährleisten. Die ICANN hat ihre Aufgaben von der IANA (Internet Assigned Numbers Authority) und anderen Organisationen übertragen bekommen.
Zur reibungslosen internationalen Kommunikation und dem Austausch von Daten bedarf es weltweit einmaliger Namen, Adressen und Nummern. Die ICANN koordiniert unter anderem die Vergabe bestimmter Namen und Adressen. Hierzu zählen Domain-Namen, der Betrieb der DNS-Root-Nameserver, die Vergabe von IP-Adressen,

Protokoll-Parametern und Port-Adressen der Protokoll-Familie (TCP/IP). Während alle Regierungen der Welt in einem Regierungsbeirat vertreten sind, unterliegt die ICANN der US-amerikanischen Rechtsprechung.

IETF - Internet Engineering Task Force

Die IETF ist eine internationale Vereinigung von Organisationen, Herstellern, Netzbetreibern, Wissenschaftlern und Anwendern, die für die Standardisierung im Internet zuständig ist. Die IETF verantwortet unter anderem die RFCs.

ISO - International Organization for Standardization

Die ISO ist die Internationale Organisation für Normung und erarbeitet international gültige Normen in allen Bereichen. Ausnahmen bilden die Bereich der Elektrik und der Elektronik, für den die Internationale elektrotechnische Kommission (IEC) zuständig ist, und der Bereich der Telekommunikation, für den die Internationale Fernmeldeunion (ITU) zuständig ist.
Bei ISO-Normen handelt es sich um so genannte Best-Practice-Empfehlungen. Die Einhaltung der ISO-Normen ist freiwillig, kann aber von Kooperationspartner, Kunden und technischen Einrichtungen gefordert und festgeschrieben sein.

IEEE - Institute of Electrical and Electronics Engineers

Das IEEE ist eine internationale Organisation von Fachleuten und Experten aus der Elektrotechnik und dem Ingenieurwesen, ähnlich dem deutschen VDE (Verband der Elektrotechnik Elektronik Informationstechnik e. V.).
Das IEEE umfasst über 360.000 Mitglieder in über 176 Ländern und ist damit die weltweit führende Organisation für die Standardisierung im Bereich Elektronik und Informationstechnik. Das Spektrum der Aktivitäten ist extrem breit und unübersichtlich.
Das IEEE kennt man vor allem durch Standardisierungen im Bereich Local Area Network (LAN) und Schnittstellen. Die bekanntesten Standards sind 1394 für FireWire, 1284 für die Centronics-Druckerschnittstelle und 802 für die Netzwerkschnittstelle Ethernet, die auch heute noch weiterentwickelt wird.

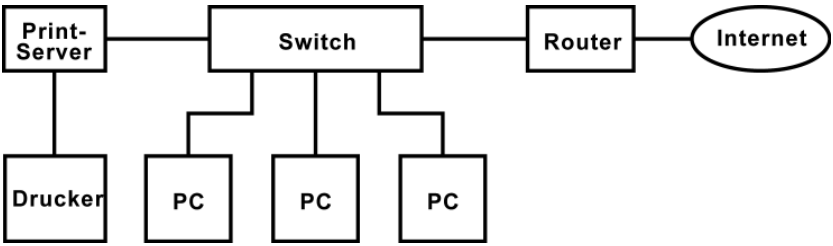
LAN - Local Area Network

Netzwerke unterscheidet man häufig in ihrer räumlichen Ausdehnung. LAN (Local Area Network) bezeichnet in der Regel ein lokales Netzwerk, das mehrere Computer und Peripheriegeräte innerhalb eines Gebäudes umfasst. Allerdings kann ein LAN auch größere Ausmaße annehmen. So wird ein Netzwerk häufig auch dann als LAN bezeichnet, wenn es privat und nichtöffentlich betrieben wird. Dabei muss dieses Netzwerk nicht lokal beschränkt sein. Ein LAN ist auch nicht auf wenige Stationen beschränkt. Die Anzahl der Stationen kann auch mehrere hundert oder tausend betragen. Wenn es sich dabei zum Beispiel um das LAN eines großen Unternehmens handelt.

LAN: Einfaches lokales Netzwerk

Ein einfaches Netzwerk besteht aus mindestens zwei Computersystemen, die über eine Direktverbindung (Crossoverkabel) oder einem Kopplungselement (Hub oder Switch) verbunden sind. Bei mehr als zwei Computersystemen ist zwingend einzentrales Kopplungselement notwendig. Das Kopplungselement sorgt für eine physikalische und logische Verbindung zwischen den Computersystemen

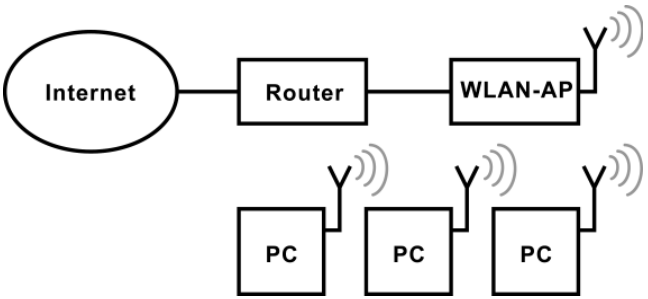
LAN: Lokales Netzwerk mit Internet-Zugang und Print-Server



Ein lokales Netzwerk mit Internet-Zugang besteht in der Regel aus einem Switch und einem Router. Der Switch dient auch hier als Kopplungselement. Der Internet-Zugang erfolgt über einen Router der auch am Switch angeschlossen ist. Über den Router bekommen alle Stationen im Netzwerk gleichzeitig Zugriff auf das Internet. In kleinen LANs befinden sich Switch und Router in einem Gerät.

Ein zusätzlicher Print-Server ermöglicht die Anbindung eines Druckers, auf dem alle Stationen drucken und sich somit einen Drucker teilen können. Der Print-Server kann ein eigenständiges Gerät sein, oder im Drucker oder einem Komplett-Gerät aus Router, Switch und Print-Server integriert sein. Im Privat-Bereich und kleinen Büros sind solche Geräte üblich.

Wireless LAN: Lokales Funknetzwerk



Anstatt kabelbasierende Verbindungen kann auch der freie Raum per Funk als Übertragungsstrecke genutzt werden. Ein einfaches Wireless LAN ist ein lokales Netzwerk mit einem WLAN-Access-Point (WLAN-AP) als Basisstation und den Computersystemen, in denen WLAN-Adapter (Netzwerkkarten mit Antenne) eingebaut sind.
Anstatt einer Kabelverbindung zwischen Computer und Switch wird ein oder mehrere WLAN-Access-Points aufgestellt, in deren Reichweite sich alle Computer befinden und über die der gesamte Netzwerkverkehr abgewickelt wird. Router und WLAN-Acess-Point gibt es auch als Komplett-Geräte, die man als WLAN-Router bezeichnet. Sie werden im Privat-Bereich und kleinen Büros eingesetzt.

WAN - Wide Area Network

Das WAN ist ein Netzwerk, das einen großen geografischen Bereich abdeckt. Es handelt sich dabei weniger um große LANs, sondern eher um Netze, die von Providern und Telekommunikationsanbietern unterhalten und betrieben werden.

Während in kleinen lokalen Netzen die Auslastung eher eine geringe Rolle spielt, sind Netzbetreiber daran interessiert, dass ihre Leitungen immer ausgelastet sind. Denn ungenutzte Leitungen und Übertragungsstrecken kosten Geld und bringen nichts ein. Zudem liegen die Anforderungen an Abrechnungsmodellen, parallele Nutzbarkeit und Netz-Management, z. B. bei einem Ausfall sehr hoch. Im WAN-Bereich haben sich deshalb ganz andere Techniken entwickelt, als im LAN. Vornehmlich Übertragungstechniken zum Verbinden von LANs. Auf diese Weise ist dann auch das Internet entstanden.

Klassische WAN-Netze bestehen aus leitungsvermittelten Verbindungen, Punkt-zu-Punkt-Verbindungen, paketorientierte Verbindungen und virtuellen privaten Netzen.

MAN - Metropolitan Area Networks

Eine Sonderform des Wide Area Network (WAN) ist das Metropolitan Area Network (MAN). Es besteht aus Netzwerken, die große Städte und Regionen miteinander verbindet. Meist fallen darunter Firmennetzwerke, die über öffentliche Wählleitungen oder angemietete Standleitungen von Netzbetreibern verbunden sind.

Internet

Das Internet ist eine großes, weltweites Netzwerk, das aus vielen kleinen, mittleren und großen Netzen zusammengeschaltet ist. Die Netze verbinden Computer, die Dienste, Anwendungen und Informationen bereitstellen, um weltweit uneingeschränkt Informationen auszutauschen. Das Internet ist also ein Informations- und Kommunikationsnetzwerk über das Informationen und Daten übermittelt und ausgetauscht werden. Dazu nutzen die verschiedenen Anwendungen unterschiedliche Protokolle. Die Verbindungen werden mittels TCP/IP hergestellt und erfolgen auf unterschiedlichen Übertragungssystemen.

Die wichtigsten Internet-Anwendungen sind E-Mail, das World Wide Web (WWW) und Cloud Computing. Obwohl mit der Bezeichnung Internet häufig das World Wide Web (WWW) gemeint ist, gibt es noch viel mehr Dienste und Anwendungen, die allerdings eher unpopulär sind oder im Hintergrund arbeiten.

- WWW - World Wide Web
- E-Mail
- IM - Instant Messaging
- Usenet / Newsgroups
- Internet-Telefonie
- P2P - Peer-to-Peer
- Cloud Computing

Das Internet unterliegt keiner bestimmten Struktur. Es gibt auch keine Zentrale. Stattdessen sind alle Netze und Computer irgendwie miteinander verbunden. Das dezentrale und paketorientierte Internet Protocol (IP) ist für die Vermittlung und Adressierung der Datenpakete zuständig. Das Transmission Control Protocol (TCP) kümmert sich um die Aufteilung und Zuordnung der Informationen und Daten in kleine handliche Datenpakete, die über IP an den Empfänger verschickt werden. Zusammen sind TCP und IP die Protokollfamilie TCP/IP.
Die wesentliche Funktion von TCP/IP ist dafür Sorgen zu tragen, dass Datenpakete innerhalb eines dezentralen Netzwerks beim Empfänger ankommen. TCP/IP findet Stationen über Netze hinweg, auch wenn deren Standort nicht bekannt ist.
Der Erfolg des Internets ist zum großen Teil auch TCP/IP zu verdanken.

Internet-Adressen

Die Internet-Adresse ist ein Überbegriff für die verschiedenen Adressen, mit denen man im Internet Dienste, Anwendungen, Computer und Personen adressiert und dadurch erreichbar macht. Die Bezeichnung Internet-Adresse ist ungenau. Für unterschiedliche Anwendungen gibt es unterschiedliche Adressen. Die bekanntesten Internet-Adressen sind Domain-Namen und E-Mail-Adressen.

Geschichtliches

Zur Zeit des Kalten Krieges, in den 60er und 70er Jahren entwickelten in den USA militärische Institutionen und Universitäten das ARPANET. Dahinter stand die Advanced Research Projects Agency des Verteidigungsministeriums der USA (Department of Defense). Ziel war es die anfällige zentralistische Netzwerkarchitektur durch ein dezentrales System mit vielen unabhängigen Querverbindungen zu ersetzen. Dadurch

sollte nach einem Atomschlag ein Totalausfall des nationalen Netzwerks verhindert werden. Dank der Protokolle TCP und IP konnten an das ARPANET immer mehr Netzwerke angeschlossen werden.
1984 wurde das Projekt in einen militärischen Bereich und einen wissenschaftlichen Bereich aufgeteilt. Gleichzeitig wurde die TCP/IP-Protokollfamilie eingeführt. Der wissenschaftliche Bereich wurde das Internet genannt, das erst nur die amerikanischen Hochschulen und Forschungseinrichtungen miteinander verband. Schnell wurde das Internet weltweit ausgebaut und auch Privatpersonen und Firmen konnten sich an das Internet anschließen.

Internet-Anschluss

Der Internet-Anschluss ist ein physikalischer und logischer Zugang zum Internet. Auf der Hardwareseite wird eine physikalische Verbindung hergestellt. Softwareseitig sorgt eine Software oder ein Netzwerk-Protokoll dafür, dass eine logische Verbindung ins Internet möglich ist.

Schichtenmodelle

Jede Technik oder jeder Vorgang, der zur Datenübertragung genutzt wird, lässt sich in 3 Teile gliedern:

- Übertragungsweg
- Protokoll
- Anwendung

Der Übertragungsweg ist das Medium, welches zur Datenübertragung genutzt wird. Z. B. Kabel oder Funk. Die Anwendung stellt die Daten bereit und nimmt sie auch wieder entgegen. Das Protokoll regelt den Zugriff auf den Übertragungsweg und die Kommunikation zwischen zwei oder mehr Teilnehmern. Das Protokoll hat zusätzlich die Aufgabe die Anwendung vom Übertragungsweg unabhängig zu machen. Das Protokoll vermittelt sozusagen zwischen Übertragungsweg und Anwendung. In der Praxis sorgt das Protokoll dafür, dass eine Anwendung jeden beliebigen Übertragungsweg nutzen kann.

Proprietäre Systeme

Kommen Übertragungsweg, Protokoll und Anwendung von einem einzigen Hersteller, hat man in der Regel keine Möglichkeit Details dieses proprietären Systems in Erfahrung zu bringen. Alles ist ein abgeschlossenes System, dass wenig flexibel und schon gar nicht transparent ist. Der Anwender ist in jedem Fall an den Hersteller gebunden. Insbesondere dann, wenn das System Probleme macht, erweitert werden oder ersetzt werden soll.

Offene Systeme

In offenen Systemen sind Übertragungsweg, Protokoll und Anwendung genormt, spezifiziert und offengelegt. D. h., jeder kann sich einen Teil heraussuchen und dazu eine Implementierung entwickeln, die sich dann auf dem Markt als Produkt behaupten muss und im Optimalfall austauschbar ist. Dabei besteht vom Grundsatz her die Möglichkeit, dass Produkte unterschiedlicher Hersteller zusammenarbeiten und untereinander getauscht werden können.

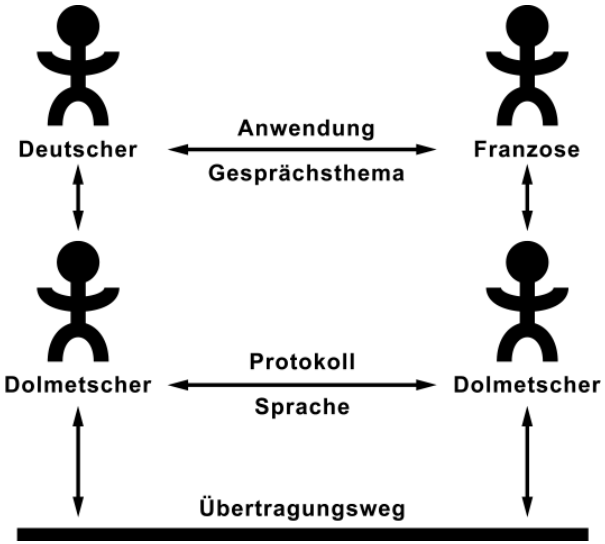
Schichtenmodell

In der hochspezialisierten Computer- und Netzwerkwelt haben sich schnell Schichtenmodelle etabliert, in denen komplexe Vorgänge in einzelnen Schritten aufgegliedert werden. Jeder Schritt oder auch jede Aufgabe wird als Schicht dargestellt, die übereinander gestapelt sind. Jede Schicht sorgt dafür, dass an den Schnittpunkten zur anderen Schicht Schnittstellen zur Kommunikation zwischen den Schichten enthalten sind. Im Gegensatz zu hochintegrierten Systemen, sind Schichtenmodelle nicht für hohe Geschwindigkeit oder Leistung ausgelegt. Es geht mehr um eine hohe Flexibilität, damit Implementierungen der Schichten leichter angepasst und ausgetauscht werden können.

Beispiel für ein Schichtenmodell

Zur Beschreibung eines Schichtenmodells dient häufig der klassische Anwendungsfall zwischen zwei Personen, die zwei unterschiedliche Sprachen sprechen. Beide Personen sind wegen der unterschiedlichen

Sprache nicht in der Lage direkt miteinander zu kommunizieren. Beide bedienen sich deshalb eines oder zwei Dolmetscher.



Die Anwendung ist also das Gespräch, in diesem Beispiel, zwischen einem Deutschen und einem Franzosen. Beide verstehen sich nicht und nutzen deshalb die Dienste eines Dolmetschers. Wäre der Dolmetscher auf beiden Seiten ein und die selbe Person, so läge hier ein proprietäres System vor. Denn der Dolmetscher wäre auch gleichzeitig der Übertragungsweg. Im vorliegenden offenen Schichtenmodell sind es zwei Dolmetscher, die das Protokoll bilden und sich miteinander einigen, in welcher Sprache sie kommunizieren wollen. Als Übertragungsweg dient meist eine technisch Einrichtung, z. B. Telefon, Fax oder E-Mail. Alternativ treffen sich alle vier Personen an einer Stelle und kommunizieren direkt miteinander.

Nachteile von Schichtenmodellen

In einem paketvermittelnden Netzwerk wird beim Durchlaufen der Schichten bei jeder Schicht ein Informations-Datensatz dem Datenpaket vorangestellt. In dem sogenannten Header befinden sich Informationen, die für die Bearbeitung in der selben Schicht beim Empfänger wichtig sind. Jeder Header vergrößert dabei das ursprüngliche Datenpaket um ein

paar Byte. Die zu übertragenden Daten sind auf alle Fälle größer als die eigentlichen Daten.

DoD-Schichtenmodell

Das DoD-Schichtenmodell ist das Schichtenmodell auf dem das Internet basiert. Da das Internet eine Entwicklung des amerikanischen Verteidigungsministeriums ist, wurde die Bezeichnung des Schichtenmodells von der englischen Bezeichnung Department-of-Defense (DoD) abgeleitet.
Insgesamt sind 4 Schichten im DoD-Schichtenmodell definiert, die sich mit dem OSI-Schichtenmodell (ISO-Standard) vergleichen lassen. Man kann sagen, dass das DoD-Schichtenmodell eine vereinfachte Variante des OSI-Schichtenmodells ist.

<table>
<tr><th>DoD-Schichtenmodell</th><th>OSI-Schichtenmodell</th></tr>
<tr><td rowspan="6">Anwendungsschicht
Application Layer

Transportschicht
Transport Layer

Internetschicht
Internet Layer

Netzzugangsschicht
Network Access Layer</td><td>Anwendungsschicht</td></tr>
<tr><td>Darstellungsschicht</td></tr>
<tr><td>Kommunikationsschicht</td></tr>
<tr><td>Transportschicht</td></tr>
<tr><td>Vermittlungsschicht</td></tr>
<tr><td>Sicherungsschicht</td></tr>
<tr><td></td><td>Bitübertragungsschicht</td></tr>
</table>

Anwendungsschicht - Application Layer

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

Transportschicht - Transport Layer

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

Internetschicht - Internet Layer

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

Netzzugangsschicht - Network Access Layer

Diese Schicht ist die unterste Schicht des DoD-Schichtenmodells und stellt das Zugriffsprotokoll dar. In lokalen Netzwerken ist das Ethernet, in Telefonnetzen z. B. ISDN.

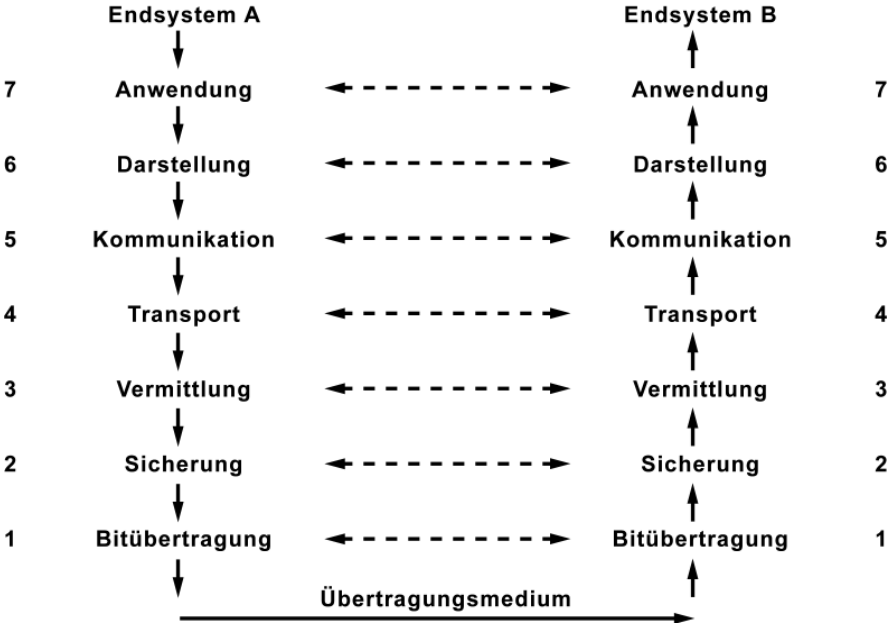
ISO/OSI-7-Schichtenmodell

Das OSI-7-Schichtenmodell ist ein Referenzmodell für herstellerunabhängige Kommunikationssysteme bzw. eine Design-Grundlage für Kommunikationsprotokolle und Computernetze.
Das OSI-Schichtenmodell oder auch OSI-Referenzmodell basiert auf dem DoD-Schichtenmodell, auf dem das Internet basiert. Im Vergleich zum DoD-Schichtenmodell ist das OSI-Schichtenmodell feiner und detaillierter gegliedert.

OSI bedeutet Open System Interconnection (Offenes System für Kommunikationsverbindungen) und wurde von der ISO (International Organization for Standardization), das ist die Internationale Organisation für Normung, als Grundlage für die Bildung von offenen Kommunikationsstandards entworfen.
Bei allen ISO-Standards handelt es sich um Handlungsempfehlungen. Die Einhaltung einer ISO-Norm ist freiwillig. In der Regel wird die

Einhaltung der ISO-Standards von verschiedenen Seiten, zum Beispiel Kooperationspartnern, Herstellern und Kunden, gefordert.

Das 7-Schichten-Modell



Das OSI-Schichtenmodell besteht aus 7 Schichten. Jede Schicht hat innerhalb der Kommunikation zwischen zwei Systemen eine bestimmte Aufgabe. Für jede Schicht werden Funktionen und Protokolle definiert, die bestimmte Aufgaben bei der Kommunikation zwischen zwei Systemen erfüllen müssen.
Bei der Kommunikation zwischen zwei Systemen durchläuft die Kommunikation oder der Datenfluss alle 7 Schichten des OSI-Schichtenmodells zweimal. Einmal beim Sender und einmal bei Empfänger. Je nach dem, wie viele Zwischenstationen die Kommunikationsstrecke aufweist, durchläuft die Kommunikation auch mehrmals das Schichtenmodell.

Protokolle im OSI-Schichtenmodell

Protokolle sind eine Sammlung von Regeln zur Kommunikation auf einer bestimmten Schicht des OSI-Schichtenmodells. Die Protokolle einer Schicht sind zu den Protokollen der über- und untergeordneten Schichten weitestgehend transparent, so dass die Verhaltensweise eines Protokolls sich wie bei einer direkten Kommunikation mit dem Gegenstück auf der Gegenseite darstellt.
Die Übergänge zwischen den Schichten sind Schnittstellen, die von den Protokollen verstanden werden müssen. Weil manche Protokolle für ganz bestimmte Anwendungen entwickelt wurden, kommt es auch vor, dass sich Protokolle über mehrere Schichten erstrecken und mehrere Aufgaben abdecken. Dabei kommt es vor, dass in manchen Verbindungen einzelne Aufgaben in mehreren Schichten und somit mehrfach ausgeführt werden.

Einteilung des OSI-Schichtenmodells

- Das OSI-Schichtenmodell besteht aus 7 Schichten.
- Jeder Schicht ist eine bestimmte Aufgabe zugeordnet.
- Einzelne Schichten können angepasst, zusammengefasst oder ausgetauscht werden.
- Die Schichten 1..4 sind transportorientierte Schichten.
- Die Schichten 5..7 sind anwendungsorientierte Schichten.
- Das Übertragungsmedium ist nicht festgelegt.

Bitübertragungsschicht	
	Maßnahmen und Verfahren zur Übertragung von Bitfolgen
Schicht 1 Physical	Die Bitübertragungsschicht definiert die elektrische, mechanische und funktionale Schnittstelle zum Übertragungsmedium. Die Protokolle dieser Schicht unterscheiden sich nur nach dem eingesetzten Übertragungsmedium und -verfahren. Das Übertragungsmedium ist jedoch kein Bestandteil der Schicht 1.

Sicherungsschicht	
Schicht 2 Data Link	Logische Verbindungen mit Datenpaketen und elementare Fehlererkennungsmechanismen
	Die Sicherungsschicht sorgt für eine zuverlässige und funktionierende Verbindung zwischen Endgerät und Übertragungsmedium. Zur Vermeidung von Übertragungsfehlern und Datenverlust enthält diese Schicht Funktionen zur Fehlererkennung, Fehlerbehebung und Datenflusskontrolle. Auf dieser Schicht findet auch die physikalische Adressierung von Datenpaketen statt.
Vermittlungsschicht	
Schicht 3 Network	Routing und Datenflusskontrolle
	Die Vermittlungsschicht steuert die zeitliche und logische getrennte Kommunikation zwischen den Endgeräten, unabhängig vom Übertragungsmedium und der Topologie. Auf dieser Schicht erfolgt erstmals die logische Adressierung der Endgeräte. Die Adressierung ist eng mit dem Routing (Wegfindung vom Sender zum Empfänger) verbunden.
Transportschicht	
Schicht 4 Transport	Logische Ende-zu-Ende-Verbindungen
	Die Transportschicht ist das Bindeglied zwischen den transportorientierten und anwendungsorientierten Schichten. Hier werden die Datenpakete einer Anwendung zugeordnet.

Kommunikationsschicht	
	Prozeß-zu-Prozeß-Verbindungen
Schicht 5 Session	Die Kommunikationsschicht organisiert die Verbindungen zwischen den Endsystemen. Dazu sind Steuerungs- und Kontrollmechanismen für die Verbindung und dem Datenaustausch implementiert.
Darstellungsschicht	
	Ausgabe von Daten in Standardformate
Schicht 6 Presentation	Die Darstellungsschicht wandelt die Daten in verschiedene Codecs und Formate. Hier werden die Daten zu oder von der Anwendungsschicht in ein geeignetes Format umgewandelt.
Anwendungsschicht	
	Dienste, Anwendungen und Netzmanagement
Schicht 7 Application	Die Anwendungsschicht stellt Funktionen für die Anwendungen zur Verfügung. Diese Schicht stellt die Verbindung zu den unteren Schichten her. Auf dieser Ebene findet auch die Dateneingabe und -ausgabe statt.

Kurzbeschreibung des OSI-Schichtenmodells

7. Schicht / Anwendung: Funktionen für Anwendungen, sowie die Dateneingabe und -ausgabe.
6. Schicht / Darstellung: Umwandlung der systemabhängigen Daten in ein unabhängiges Format.
5. Schicht / Kommunikation: Steuerung der Verbindungen und des Datenaustauschs.
4. Schicht / Transport: Zuordnung der Datenpakete zu einer Anwendung.
3. Schicht / Vermittlung: Routing der Datenpakete zum nächsten Knoten.
2. Schicht / Sicherung: Segmentierung der Pakete in Frames und Hinzufügen von Prüfsummen.
1. Schicht / Bitübertragung: Umwandlung der Bits in ein zum Medium passendes Signal und physikalische Übertragung.

Hinweis: Die Endgeräte der Endsysteme und das Übertragungsmedium sind aus dem OSI-Schichtenmodell ausgeklammert. Trotzdem kann es sein, dass die Endgeräte in der Anwendungsschicht und das Übertragungsmedium in der Bitübertragungsschicht vorgegeben sind.

Das OSI-Schichtenmodell in der Praxis

Das OSI-Schichtenmodell wird sehr häufig als Referenz herangezogen, wenn es darum geht, Abläufe einer Kommunikation oder Nachrichtenübermittlung darzustellen. Doch eigentlich ist das DoD-Schichtenmodell (TCP/IP) viel näher an der Realität.
Das Problem des OSI-Schichtenmodells ist die Standardisierungsorganisation ISO, die einfach zu schwerfällig war, um in kürzester Zeit einen Rahmen für die Aufgaben von Protokollen und Übertragungssystemen in der Netzwerktechnik auf die Beine zu stellen. TCP/IP dagegen war frei verfügbar, funktionierte und verbreitete sich mit weiteren Protokollen rasend schnell. Der ISO blieb nichts anderes übrig, als TCP/IP im OSI-Schichtenmodell zu berücksichtigen.
Neben TCP/IP haben sich noch weitere Netzwerkprotokolle entwickelt. Die wurden jedoch irgendwann von TCP/IP abgelöst. Fast alle Netzwerke arbeiten heute auf der Basis von TCP/IP.

Netzwerk-Topologie

Ein Netzwerk kann man grob in eine physikalische und logische Anordnung von Geräten und Teilnetzwerken gliedern. Ein logisch gegliedertes Netzwerk definiert, wo sich welches Gerät in einem Netzwerk befindet. Die physikalische Gliederung bricht das Netzwerk auf einzelne Ports und Kabelverbindungen herunter.

Unter einer Netzwerk-Topologie versteht man die physikalische Anordnung von Netzwerk-Stationen, die über ein Übertragungsmedium miteinander verbunden sind. Die Netzwerk-Topologie bestimmt die einzusetzende Hardware, sowie die Zugriffsmethoden auf das Übertragungsmedium.

Die im folgenden beschriebenen Topologien beziehen sich auf paketvermittelnde Netzwerke.

Bus / Chain / Bus-Topologie

Die Bus-Topologie, manchmal auch Ketten-Topologie genannt, besteht aus mehreren Stationen, die hintereinander geschaltet sind. Die Stationen sind über eine gemeinsame Leitung miteinander verbunden. Alle Stationen, die an dem Bus angeschlossen sind, haben Zugriff auf das Übertragungsmedium und die Daten, die darüber übertragen werden. Um Störungen auf der Leitung zu verhindern und die physikalischen Bedingungen zu verbessern, werden die beiden Kabelenden mit einem Abschlusswiderstand versehen.

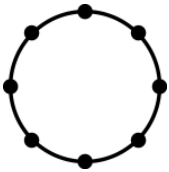
Eine zentrale Netzwerkkomponente, die die Abläufe auf dem Bus regelt, gibt es nicht. Dafür ist ein Zugriffsverfahren für die Abläufe auf dem Bus verantwortlich, an dessen Regeln sich alle Stationen halten. Die Intelligenz sitzt in den Stationen und wird in der Regel durch ein komplexes Protokoll vorgegeben. Der Kabel-Bus selber ist nur ein passives Übertragungsmedium.
Den Daten wird die Adresse des Empfängers, des Senders und eine Fehlerbehandlung angehängt. Die Stationen, die nicht als Empfänger adressiert sind, ignorieren die Daten. Die Station, die adressiert ist, liest die Daten und schickt eine Bestätigung an den Sender.
Senden zwei Stationen gleichzeitig, dann überlagern sich die Signale. Es entsteht ein elektrisches Störsignal auf dem Bus. Die Übertragung wird unterbrochen. Nach einer gewissen Zeit, versuchen die Stationen wieder Daten zu senden. Der Vorgang wird so oft wiederholt, bis eine Station es schafft die Daten erfolgreich zu verschicken.

Soll der Bus erweitert werden oder Stationen hinzugefügt oder entfernt werden, dann fällt der Bus für die Zeit der Arbeiten aus.

Ring / Ring-Topologie

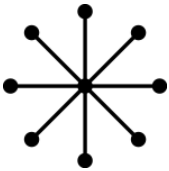
Die Ring-Topologie ist eine geschlossene Kabelstrecke in der die Netzwerk-Stationen mit einem durchgehenden Kabelring miteinander verbunden sind. Das bedeutet, dass an jeder Station ein Kabel ankommt und ein Kabel abgeht.

In der Ring-Topologie muss sich typischerweise keine aktive Netzwerk-Komponente befinden. Die Steuerung und der Zugriff auf das Übertragungsmedium regelt ein Protokoll, an das sich alle Stationen halten.



Allerdings macht ein Ring-Manager Sinn. Denn wenn an einer Stelle der Ring unterbrochen ist, dann kann er in einen Bus-Betrieb umschalten. Das bedeutet, dass die Ring-Topologie redundant ist, was in Produktionsumgebungen wichtig ist, die auf hohe Verfügbarkeit angewiesen sind.

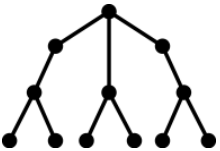
Star / Stern-Topologie



In der Stern-Topologie befindet sich eine zentrale Station, die eine Verbindung zu allen anderen Stationen unterhält. Jede Station ist über eine eigene Leitung mit der zentralen Station verbunden. Es handelt sich im Regelfall um einen Hub oder einen Switch. Der Hub oder Switch übernimmt die Verteilfunktion für die Datenpakete. Dazu werden die Datenpakete entgegen genommen und an das Ziel weitergeleitet.
Die Datenbelastung der zentralen Station ist sehr hoch, da alle Daten und Verbindungen darüber laufen. Das Netzwerk funktioniert nur so lange, bis die Zentralstation ausfällt. Die anderen Netzwerkstationen können jederzeit hinzugefügt oder entfernt werden. Sie haben keinen Einfluss auf den Betrieb des Netzwerks.
Ein Netzwerk mit Stern-Bus-Struktur ist ein Kombination aus Stern- und Bus-Topologie.

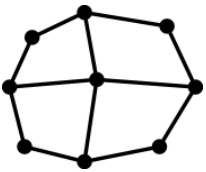
Über eine Sternstruktur sind die Stationen mit einem Hub verbunden. Mehrere Hubs sind über eine Busleitung miteinander verbunden.

Tree / Baum-Topologie



Die Baum-Topologie ist eine erweiterte Stern-Topologie. Größere Netze haben diese Struktur. Vor allem dann, wenn mehrere Topologien miteinander kombiniert werden. Meist bildet ein übergeordnetes Netzwerk-Element, entweder ein Koppel-Element oder eine anderen Topologie, die Wurzel. Von dort bildet sich ein Stamm mit vielen Verästelungen und Verzweigungen.

Mesh / Maschen-Topologie



Die Maschen-Topologie bzw. vermaschte Topologie ist ein dezentrales Netzwerk, das keinen verbindlichen Strukturen unterliegen muss und in dem alle Netzwerkknoten irgendwie miteinander verbunden sind.
Die Maschen-Topologie ist meist ein Wildwuchs mehrerer Topologien, die einem Chaos an verschiedenen Systemen und Übertragungsstrecken und damit von der Struktur her einem dezentralen Netzwerke entsprechen. Das Internet stellt ein solches Netzwerk dar, in dem aktive Netzwerk-Komponenten das Routing der Datenpakete übernehmen. Das erhöht die Reichweite insbesondere am Rand liegender Knoten und ermöglicht blockierte oder ausfallende Verbindungen zu umgehen.

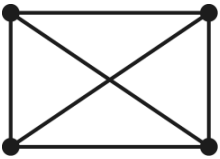
In einem Mesh-Netzwerk gibt es beim Ausfall einer Verbindung im Regelfall immer eine alternative Strecke, um den Datenverkehr unterbrechungsfrei fortzuführen. Vermaschte Netze sind in der Regel selbstheilend. Geht eine Verbindung verloren, dann wird sofort eine andere genutzt. Das Netzwerk bleibt betriebsfähig.

Fabric / Geflecht-Topologie (Gewebe)

Ein hierarchischer Aufbau und Segmentierung waren lange Zeit das Kriterium beim Strukturieren eines Netzwerks. Wegen dem vorwiegenden Client-Server-Datenstrom war hier die Stern- oder Baum-Topologie mit ihrem zentralistischen Ansatz die bevorzugte Verkabelungs- und Vernetzungsarchitektur. Heute hat der Datenverkehr durch dynamische Inhalte zwischen den Servern und dem Zusammenspiel von Web-, Applikations- und Datenbank-Servern stark zugenommen. Das heißt, die logischen Verbindungen finden nicht mehr nur zwischen Clients und Servern statt, sondern auch zwischen einzelnen Servern. Dabei treten Datenströme auf, die sehr unterschiedliche Charakteristiken aufweisen. Und deshalb müssen zukünftige Netzwerk-Topologien und Netzarchitekturen flexibel sein und über mehr Intelligenz verfügen.

Das Konzept der Fabric soll alle wichtigen Anforderungen an das Netzwerk im Rechenzentrum erfüllen:

- hohe Geschwindigkeit
- Ausfallsicherheit
- Flexibilität
- einfaches Management



Eine Fabric weist eine Sternstruktur auf, die allerdings keinen zentralen Knoten hat, sondern die verteilenden Komponenten redundant zu einer strukturiert vermaschten Topologie miteinander verbindet. Die Fabric bildet die Grundlage zu hochverfügbaren verteilten Systemen. Häufig

dient dieses Modell als perfektes Netzwerk in dem jede Netzwerk-Station mit allen anderen Stationen mit der vollen Bandbreite verbunden ist.

Die Fabric ist eine Netzwerk-Topologie, deren Begriff und technische Ansätze aus der Fibre-Channel-Welt stammen und in Speichernetzen schon sehr lange zum Einsatz kommt. Sie dienen als Vorbild für Ethernet im Rechenzentrum. Hier ist die Fabric eine verteilt angelegte Architektur, die zum Beispiel mehrere physische Switche zu einem großen logischen Switch zusammenfasst.

Für eine Gebäudevernetzung bedeutet das, dass weitere Core-, Etagen- und Access-Switche zum Einsatz kommen müssen, die über zusätzliche Leitungen miteinander verbunden sind.

Strukturierte Verkabelung

Eine strukturierte Verkabelung oder universelle Gebäudeverkabelung (UGV) ist ein einheitlicher Aufbauplan für eine zukunftsorientierte und anwendungsunabhängige Netzwerkinfrastruktur, auf der unterschiedliche Dienste (Sprache oder Daten) übertragen werden. Damit sollen teure Fehlinstallationen und Erweiterungen vermieden und die Installation neuer Netzwerkkomponenten erleichtert werden.
Unstrukturierte Verkabelungen sind meist an den Bedarf oder eine bestimmte Anwendung gebunden. Soll auf eine neue Technik oder Technik-Generation umgestellt werden, führt das zu einer Kostenexplosion mit ungeahnten Ausmaßen.

Eine strukturierte Verkabelung basiert auf einer allgemein gültigen Verkabelungsstruktur, die auch die Anforderungen mehrerer Jahre berücksichtigt, Reserven enthält und unabhängig von der Anwendung genutzt werden kann. So ist es üblich, die selbe Verkabelung für das lokale Netzwerk und die Telefonie zu benutzen.

- standardisierte Komponenten, wie Leitungen und Steckverbindungen
- hierarchische Netzwerk-Topologie (Stern, Baum, ...)
- Empfehlungen für Verlegung und Installation
- standardisierte Mess-, Prüf- und Dokumentationsverfahren

Ziele einer strukturierten Verkabelung

- Unterstützung aller heutigen und zukünftigen Kommunikationssysteme
- Kapazitätsreserve hinsichtlich der Grenzfrequenz
- das Netz muss sich gegenüber dem Übertragungsprotokoll und den Endgeräten neutral verhalten
- flexible Erweiterbarkeit
- Ausfallsicherheit durch sternförmige Verkabelung
- Datenschutz und Datensicherheit müssen realisierbar sein
- Einhaltung existierender Standards

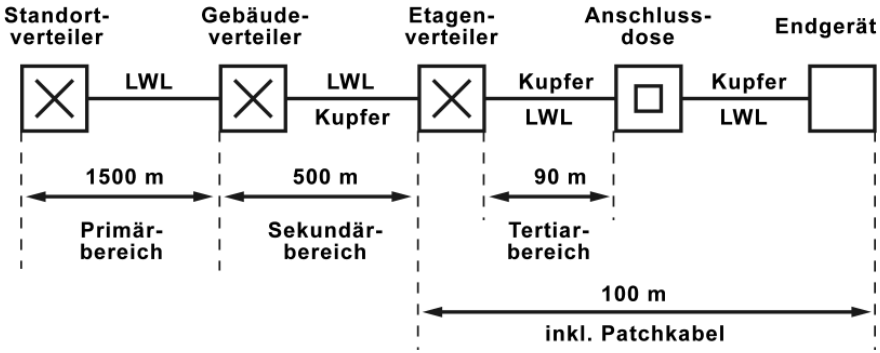
Normen für die strukturierte Verkabelung

Geltungsbereich	Norm	Beschreibung
Europa	EN 50173-1 (2003)	Verkabelungsnorm Informationssysteme - anwendungsneutrale Verkabelungssysteme
Nordamerika	TIA/EIA 568 B.1 (2001) / B.2 1 (2001)	Telekommunikations-Verkabelungsnorm für Gebäudeverkabelungen
Weltweit	ISO/IEC 11801 (2002)	Verkabelungsnorm für anwendungsneutrale Gebäudeverkabelungen

TIA/EIA 568 B.1 (2001) / B.2 1 (2001)

TIA/EIA haben ihren Ursprung in der Spezifikation ungeschirmter Kupfer-Anschluss-Komponenten. TIA/EIA ist keine weltweit gültige Norm, sondern eine Industriespezifikation, die für den nordamerikanischen Markt gültig ist. Es sind darin jedoch auch die Anforderungen von EN (Europa-Norm) oder ISO/IEC (weltweit) bei den Übertragungseigenschaften der Leitungen und Steckverbindungen enthalten.

ISO/IEC 11801 (2002) und EN 50173-1 (2003)



In der Europa-Norm (EN) und dem weltweit gültigen ISO-Standard erfolgt die Strukturierung in Form von Hierarchieebenen. Diese Ebenen werden von Gruppen gebildet, die topologisch oder administrativ zusammengehören.

Die Verkabelungsbereiche sind in Geländeverkabelung (Primärverkabelung), Gebäudeverkabelung (Sekundärverkabelung) und Etagenverkabelung (Tertiärverkabelung) gegliedert. Die Verkabelungsstandards sind für eine geografische Ausdehnung von 3000 m, einer Fläche von 1 Mio. qm und für 50 bis 50.000 Anwender optimiert. In jedem Verkabelungsbereich sind maximal zulässige Kabellängen festgelegt und bei der Installation einzuhalten. Viele Übertragungstechniken beziehen sich auf die definierten Kabellängen und Qualitätsanforderungen.

Hinweis: Bei allen ISO-Standards handelt es sich um Handlungsempfehlungen. Die Einhaltung einer ISO-Norm ist freiwillig. In der Regel wird die Einhaltung der ISO-Standards von verschiedenen Seiten, zum Beispiel Kooperationspartnern, Herstellern und Kunden, gefordert.

Primärverkabelung - Geländeverkabelung

Der Primärbereich wird als Campusverkabelung oder Geländeverkabelung bezeichnet. Er sieht die Verkabelung von einzelnen Gebäuden untereinander vor. Der Primärbereich umfasst meist große Entfernungen,

hohe Datenübertragungsraten, sowie eine geringe Anzahl von Stationen. Für die Verkabelung wird in den meisten Fällen Glasfaserkabel (50 µm) mit einer maximalen Länge von 1.500 m verwendet. In der Regel sind es Glasfaserkabel mit Multimodefasern oder bei größeren Entfernungen auch Glasfaserkabel mit Singlemodefasern. Für kleinere Entfernungen werden auch schon mal Kupferkabel verwendet.
Grundsätzlich gilt, den Primärbereich großzügig zu planen. Das bedeutet, das Übertragungsmedium muss bezüglich Bandbreite und Übertragungsgeschwindigkeit nach oben hin offen sein. Das selbe gilt auch für das eingesetzte Übertragungssystem. Als Faustregel gilt 50 Prozent Reserve zum derzeitigen Bedarf der Investition.

Sekundärverkabelung - Gebäudeverkabelung

Der Sekundärbereich wird als Gebäudeverkabelung oder Steigbereichverkabelung bezeichnet. Er sieht die Verkabelung von einzelnen Etagen und Stockwerken untereinander innerhalb eines Gebäudes vor. Dazu sind vorzugsweise Glasfaserkabel (50 µm), aber auch Kupferkabel mit einer maximalen Länge von 500 m vorgesehen.

Tertiärverkabelung - Etagenverkabelung

Der Tertiärbereich wird als Etagenverkabelung bezeichnet. Er sieht die Verkabelung von Etagen- oder Stockwerksverteilern zu den Anschlussdose vor. Während sich im Stockwerksverteiler ein Netzwerkschrank mit Patchfeld befindet, mündet das Kabel am Arbeitsplatz des Anwenders in einer Anschlussdose in der Wand, in einem Kabelkanal oder in einem Bodentank mit Auslass.
Für diese relativ kurze Strecke sind Twisted-Pair-Kabel vorgesehen, deren Länge auf 90 m, zzgl. 2 mal 5 m Anschlusskabel, begrenzt ist. Alternativ kommen auch Glasfaserkabel (62,5 µm) zum Einsatz.

Elemente der strukturierten Verkabelung

- Patchfeld (Patchpanel)
- Patchkabel
- Anschlussdosen
- Netzwerkkabel
- Verteilerschränke, Switch, Hubs, Router

Netzwerk-Kabel

Mit Netzwerkkabel werden die Stationen bzw. Teilnehmer eines Netzwerks physikalisch miteinander verbunden. Es gibt verschiedene Netzwerkkabel. Sie unterscheiden sich im Material und im Aufbau. Während es Kupferkabel entweder als Twisted-Pair-Kabel oder Koaxialkabel gibt, bestehen Lichtwellenleiter aus dem Grundstoff Glas oder Kunststoff.

- Koaxialkabel
- Twisted-Pair-Kabel
- Lichtwellenleiter (LWL Glasfaser)

Twisted-Pair-Kabel (UTP / FTP / STP)

"Twisted Pair" ist die englische Bezeichnung für ein Kupferkabel mit gekreuzten, verdrillten bzw. verseilten Adernpaaren. Es hat Ähnlichkeit mit dem in Deutschland verwendeten Telefonkabel, das man als Installationskabel J-Y(ST)Y bezeichnet.
Kabel mit verseilten Adernpaaren werden schon sehr lange bei der Signal- und Datenübertragung eingesetzt. Typischerweise in der Telefon- und Netzwerktechnik.

Vorteile von Twisted-Pair-Kabel

Die paarweise Verseilung und ein elektrisch leitender Schirm vermindert störende Einflüsse von äußeren magnetischen Wechselfeldern, wie sie durch andere stromführende Kabel hervorgerufen werden. Ebenso wird das Übersprechen zwischen benachbarten Adernpaaren innerhalb des Kabels reduziert.
Der elektrisch leitende Schirm, besteht aus einer Aluminiumfolie oder einem Drahtgeflecht, der um die Adernpaare gewickelt ist. Ein Drahtgeflecht dient als Abschirmung gegen niederfrequente Felder. Der Bedeckungsgrad des Geflechts sollte über 30% liegen. Eine Kombination aus Geflecht- und Folienschirm hat sich als sehr effektiv erwiesen, um innere und äußere elektromagnetische Einflüsse zu verringern. Allerdings wird dadurch auch das Kabel insgesamt dicker und starrer.
Um statische Aufladungen durch die Reibung zwischen Metallfolie,

Drahtgeflecht und den Adernpaaren zu vermeiden, befindet sich dazwischen eine antistatische Kunststofffolie, die aber keine abschirmende Funktion oder Wirkung hat.

Standards bei Twisted-Pair-Kabeln

Twisted-Pair-Kabel und die dazugehörigen Steckverbindungen sind genormt. Um ihre Leistungsfähigkeit zu beschreiben sind sie in unterschiedliche Klassen und Kategorien eingeteilt. Jede Klasse oder Kategorie deckt verschiedene Anforderungsprofile mit bestimmten Qualitätsvorgaben ab. Daraus ergeben sich verschiedene Einsatzszenarien.

- EIA/TIA 568 (USA)
- ISO/IEC 11801 (international)
- EN 50173 (Europa)

EIA/TIA 568A und EIA/TIA 568B

EIA/TIA sind zwei US-Standardisierungsorganisationen Electronic Industries Alliance (EIA) und Telecommunications Industry Association (TIA), die zum Beispiel für die oft zitierten Adernbelegung der RJ45-Stecker und Kabel-Kategorien für Twisted-Pair-Kabel verantwortlich sind. Dazu reichen im US-Standard EIA/TIA 568 die Kategorien für Twisted-Pair-Kabel von 1 bis 6. Die Kategorien 1 und 2 sind nur informell definiert. Solche Kabel hat es praktisch nie gegeben. Meist entsprechen Kabel im Bereich der Telefonie dieser Kategorie. Also das, was in Deutschland als Sternvierer-Installationskabel bezeichnet wird. Kabel der Kategorie 3 und 4 wurden häufig in den USA verlegte. Für sie gibt es heute keinen Anwendungsfall mehr. Ihre Qualität entspricht nicht mehr den Anforderungen heutiger Übertragungstechniken. Man findet sie höchstens noch in sehr alten Netzwerk-Installationen.
Die Standardisierung durch die EIA/TIA endete mit der Kategorie 6A.

ISO/IEC 11801

Ab der Kategorie 5 hat die ISO die Standardisierung der Twisted-Pair-Kabel und Steckverbindungen übernommen. Deshalb gibt es parallel zu den Kategorien der EIA/TIA 568 auch noch die Kategorien der ISO/IEC 11801.

EN 50173

Zusätzlich zu den Standards EIA/TIA 568 und ISO/IEC 11801 gibt es die europäische Norm EN 50172, in der Twisted-Pair-Kabel in Klassen eingeteilt sind.

Vergleichstabelle

EIA/TIA 568	ISO/IEC 11801	EN 50173	max. Frequenz	Anwendung
Cat. 1	-	-	0,4 kHz	Telefon und Modem
-	-	Class A	100 kHz	Telefon und Modem
Cat. 2	-	Class B	4 MHz	Terminals, ISDN
Cat. 3	-	Class C	16 MHz	10Base-T, ISDN
Cat. 4	-	-	20 MHz	16 MBit Token Ring
IBM Typ 1/9			20 MHz	4 und 16 MBit Token Ring
Cat. 5	Cat. 5	Class D	100 MHz	100Base-TX, SONET, SOH
Cat. 5e	Cat. 5e	Class D	100 MHz	1GBase-T
Cat. 6	Cat. 6	Class E	250 MHz	1GBase-T, 155-MBit-ATM, 622-MBit-ATM
Cat. 6A	Cat. 6_A	Class EA	500 MHz	10GBase-T
-	Cat. 7	Class F	600 MHz	10GBase-T (bis 100 Meter)
-	Cat. 7_A	Class FA	1.000 MHz	10GBase-T
-	Cat. 8	Class G	1.600 - 2.000MHz	40GBase-T und 100GBase-T

Die Übertragungsfrequenz (max. Frequenz) und die Kabellänge stehen in einem Verhältnis zueinander. Ist die Übertragungsfrequenz zu hoch, dann reduziert sich die nutzbare Kabellänge. Das bedeutet, bei einer höheren Frequenz kann nur eine geringere Entfernung überbrückt werden. Danach ist das Signal unbrauchbar und eine Übertragung nicht mehr möglich.

Hinweis: Bei allen ISO-Standards handelt es sich um Handlungsempfehlungen. Die Einhaltung einer ISO-Norm ist freiwillig. Allerdings wird die Einhaltung von verschiedenen Kooperationspartnern, Herstellern und Kunden gefordert.

Schreibweise: Category (Cat./CAT) oder Kategorie (Kat./KAT)

Die Schreibweisen für die Kabel-"Kategorie" weichen gelegentlich voneinander ab. Das liegt daran, dass manchmal die englische und manchmal die deutsche Schreib- und Sprechweise verwendet wird. Erschwerend kommt hinzu, dass Begriffe wie CAT5, CAT6, CAT6A und CAT7 nicht geschützt sind und deshalb in Produktbezeichnungen unterschiedlich verwenden werden. Das führt leider zu unterschiedlichen Bezeichnungen in der Fachwelt, die aber das gleiche ausdrücken.

Die "Kategorie" wird aus dem US-amerikanischen Standard EIA/TIA 568 abgeleitet. Dort wird die englische Schreibweise "Category" verwendet und mit "Cat." abgekürzt. Die Schreibweisen "CAT" dürfte auch vorkommen.
Im deutschsprachigem Raum spricht man eher von "Kategorie", als "Kat." abgekürzt. Die Schreibweisen "KAT" dürfte auch vorkommen.
Fachleute sprechen in der Regel von KAT- oder CAT-Kabel. Wenn das Kabel genauer bezeichnet werden soll, dann auch von CAT5-, CAT6- oder CAT7-Kabel.

Twisted-Pair-Kabel der Category 3 / Kategorie 3 (Class C)

CAT3 war in den USA lange Zeit der Standardkabeltyp bei allen Telefon-Verkabelungen. Die Kabel sind ISDN-tauglich. Aus diesem Grund werden die in Deutschland bekannten Installationskabel mit der Bezeichnung J-Y(ST)Y hin und wieder als CAT3-Kabel bezeichnet, was aber falsch ist. Diese Kabel haben mit CAT3-Kabel nichts zu tun. Sie so zu bezeichnen ist irreführend.

Twisted-Pair-Kabel der Category 5 / Kategorie 5 (Class D)

CAT5-Kabel sind wahrscheinlich die am häufigsten verlegten Netzwerkkabel und somit in den meisten älteren strukturierten Netzwerk-Verkabelungen anzutreffen. In der Regel werden sie für die parallele Nutzung von Netzwerk und Telefonie eingesetzt. CAT5-Kabel sind für Ethernet, Fast-, Gigabit-Ethernet und in Ausnahmefällen auch für 10-Gigabit-Ethernet geeignet. Telefon-Installationen profitieren von strukturierter Leitungsverlegung und fehlerfreien Kabelverbindungen.
Für Gigabit-Ethernet musste die Spezifikationen überarbeiten werden. Die Kabel wurden mit Cat5e (e = enhanced) bezeichnet. CAT5e ist genauer spezifiziert und kommt vor allem in Europa zum Einsatz. Umsichtig verlegte CAT5-Leitungen profitieren davon, dass sie nach der Messung meistens die Anforderungen für CAT5e erfüllen.
Seit der Normung im Jahr 2003 gilt für CAT5e nur noch die Bezeichnung CAT5. Die davor verlegten CAT5-Kabel unterstützen Gigabit-Ethernet nicht immer.

Twisted-Pair-Kabel der Category 6 / Kategorie 6 (Class E)

CAT6-Kabel sind in den neueren strukturierten Netzwerk-Verkabelungen anzutreffen. In der Regel werden sie für die parallele Nutzung von Netzwerk und Telefonie eingesetzt.
Für die Verlegung von CAT6-Kabel gibt es meistens keinen wirklichen Grund. Im Bereich Ethernet mit 1 GBit/s reicht CAT5 (CAT5e) vollkommen aus. Eine bessere Qualität als CAT6 ist eigentlich nicht notwendig. Deshalb dauerte es lange, bis CAT6-Kabel für strukturierte Verkabelungen eingesetzt wurden. Irgendwann wurden häufiger CAT6-Kabel als CAT5-Kabel verlegt. Sie waren besser lieferbar. Außerdem bemerkte so mancher Elektroinstallateur, dass man mit einem "reingeklatschten" CAT6-Kabel bessere Messwerte erreichen kann, als bei einem umsichtig verlegten CAT5-Kabel. Vor allem, wenn das eine oder andere Kabel länger wurde, als es eigentlich sein durfte. Nacharbeiten und Diskussionen mit dem Kunden konnten vermieden werden.
Im Vergleich zu CAT5-Kabel enthält CAT6-Kabel dickere Adern und mehr Folien- und Geflecht-Schirmung. Vor allem beim Abisolieren und Auflegen an Dosen und Patchfeldern entsteht wegen der Schirmung ein größerer Aufwand, der für geübte Installateure vernachlässigbar ist.
Eine Erweiterung von CAT6 ist CAT6A bzw. $CAT6_A$.

Twisted-Pair-Kabel der Category/Kategorie CAT6A / $CAT6_A$ (Class EA)

Mit 10-Gigabit-Ethernet (10GBASE-T) wurden Twisted-Pair-Kabel mit dem Standard CAT6A (A = augmented) spezifiziert, der für Frequenzen bis zu 500 MHz ausgelegt ist. CAT6A-Kabel enthielten anfangs Trennstege, um die Adernpaare räumlich voneinander zu trennen. Auf diese Weise soll das Übersprechen reduziert werden. Allerdings gehen damit ein größerer Kabeldurchmesser und ein größerer Biegeradius einher, wodurch sich die Kabel schwerer verlegen lassen.
Bei 10GBASE-T erreicht man mit diesen Kabeln eine maximale Entfernung von 55 Metern. Zusätzlich benötigt man Patchpanels, die den Abstand zwischen den einzelnen Anschlüssen erhöhen, geschirmte RJ45-Stecker, Spezialwerkzeug für die Konfektionierung, geschlossene Kabeltrassen und die Trennung unterschiedlicher Kabelarten, um gegenseitige Beeinflussungen zu vermeiden.

Twisted-Pair-Kabel der Category 7 / Kategorie 7 (Class F)

Spätestens bei 10-Gigabit-Ethernet sind Kabel der Kategorie 7 notwendig (oder $CAT6_A$). Da diese Technik als zukunftsweisend gilt und die Kabel nicht sehr viel teurer sind als CAT6-Kabel, werden viele Neuinstallationen mit CAT7-Kabel ausgerüstet.
Die Kategorie 7_A ist sogar bis 1000 MHz spezifiziert und wurde für Anwendungen ausgearbeitet, die über 10 GBit/s hinausgehen.
Im Unterschied zu den Kabeln der Kategorie 5 und 6 sind alle vier Adernpaare eines CAT7-Kabels einzeln geschirmt. Das bedeutet, es kommen generell Folien- und Geflecht-geschirmte Kabel zum Einsatz. Ungeschirmte UTP-Kabel sind in der Kategorie 7 möglich, aber in der Praxis eher selten anzutreffen. Es werden hauptsächlich S/FTP-Kabel verwendet.
Hinzu kommen neue Steckverbinder. Der Grund, die Abstände zwischen den RJ45-Steckern ist zu gering. Eine Verkabelung mit RJ45-Patchkabeln und -dosen und CAT7-Kabel ist also keine "echte" CAT7-Verkabelung, sondern höchstens $CAT6_A$.

In der Vergangenheit haben viele Elektroinstallateure die nötige Sorgfalt beim Verlegen von CAT6- und CAT7-Kabel vermissen lassen. Darauf angesprochen wurde meist nur milde gelächelt und abgewunken.

Natürlich, auf einem schlecht behandelten CAT7-Kabel ist Fast-Ethernet mit 100 MBit/s auch kein Problem. Doch wer lässt CAT7-Kabel verlegen, um es nur für Fast-Ethernet zu nutzen? Was ist, wenn jemand 10GBase-T auf CAT7 nutzen will? Abwegig ist das nicht. Zwar werden mit 10GBase-T kaum Arbeitsplatzrechner ans Netzwerk angebunden. Doch lässt sich mit 10GBase-T eine schnelle Netzwerk-Infrastruktur aufbauen, die ohne teure Glasfaserkabel auskommt.
Der Elektroinstallateur muss dringend davon Abstand nehmen CAT6- und CAT7-Kabel mal geschwind "reinzuklatschen". Das zeugt von geringer Kenntnis und ist Pfusch.

Der Unterschied zwischen CAT7- und CAT7A-Kabel ist der einsetzbare Frequenzbereich von 600 bzw. 1.000 MHz.

Wichtiger Hinweis: Leider werden für qualitativ hochwertige Netzwerkverkabelungen mit CAT7-Leitung oftmals CAT6-Netzwerkdosen und -Patchpanels verbaut, was die gesamte Verkabelung auf CAT6 degradiert.
Alle CAT7-Patchkabel, -Patchfelder und Anschlussdosen mit RJ45-Steckverbindern entsprechen nicht der CAT7-Spezifikation. Das bedeutet, eine Netzwerkinstallation mit CAT7-Kabel und RJ45-Steckverbindungen ist höchstens eine $CAT6_A$-Netzwerkinstallation.
Um Netzwerkkomponenten gemäß CAT7 herzustellen, wurden eigens neue Steckverbindungen konzipiert, die im Wesentlichen den Abstand zwischen den Adernpaaren vergrößern.

Twisted-Pair-Kabel der Category 8 / Kategorie 8

Eigentlich müsste mit der Kategorie 7 Schluss sein. Der nächste Schritt wäre Glasfaserkabel auch im Tertiärbereich (letzte hundert Meter zum Arbeitsplatz). Doch Kupferkabel haben gegenüber Lichtwellenleitern (LWL) signifikante Vorteile. So fallen die Gesamtkosten einer Verkabelung geringer aus, die Handhabung ist wesentlich leichter und zudem gesellt sich die PoE-Fähigkeit (Power over Ethernet) von Twisted-Pair-Kabeln hinzu.

Klar ist, dass eine Reichweite von 100 Meter nicht mehr in jedem Fall erreicht werden kann. Deshalb begnügt man sich mit 40 bis 50 Meter bei 2.000 MHz Bandbreite um damit 40 GBit/s zu erreichen. Weil sich ohne

RJ45 niemand eine Netzwerkverkabelung vorstellen kann, soll auch das mit dieser Steckverbindung möglich sein.

Zukünftig wird zwischen verschiedenen Kategorien unterschieden:

- Cat. 8 (ANSI/TIA) aufbauend auf Cat. 6A (F/UTP) mit RJ45-Steckverbinder
- Cat. 8.1 (ISO/IEC) aufbauend auf Cat. 7A (S/FTP) mit RJ45-Steckverbinder
- Cat. 8.2 (ISO/IEC) aufbauend auf Cat. 7A (S/FTP) mit Tera-, GG45- oder ARJ45-Steckverbinder

Steckverbinder für Twisted-Pair-Kabel

Der übliche Steckverbinder (Stecker-Buchse-Kombination) für Twisted-Pair-Kabel ist RJ45, der auch als Western-Stecker bezeichnet wird. Wie Kabel unterliegen auch Steckverbindungen physikalischen Gesetzmäßigkeiten, die die Übertragungsleistung begrenzt. Nur mit viel Konstruktionsarbeit an der Leiterplatte kann der RJ45-Steckverbinder über 500 MHz erreichen.
Für CAT7 sollte deshalb eine neue Steckverbindung für Patchkabel, Netzwerkdosen und Komponenten entwickelt werden. Während der Normierungsphase (ISO/IEC 11802 und EN 50173) für einen RJ45-Nachfolger wurden verschiedene Steckertypen zur Wahl gestellt. Die Entscheidung fiel auf zwei unterschiedliche Steckersysteme, die als einzige zugelassene Anschlusskomponenten für CAT7 aufwärts definiert sind.

GG45 von Nexans: Aufgrund seiner Abwärtskompatibilität zu RJ45 ist die Anschlusskomponente bei Büroverkabelungen zu bevorzugen. Zwischen GG45 und RJ45 reicht ein einfacher Adapter.
TERA von Siemon: Für multimediale Applikationen zu bevorzugen.

Eine GG45-Buchse nimmt neben dem GG45-Stecker auch einen normalen RJ45-Stecker aufnimmt.
ARJ45 ist ein weiterer, von Stewart Connector entwickelter Steckverbinder, der interoperabel zu GG45 ist.
Da sämtliche Endgeräte über RJ45-Anschlüsse verfügen, haben sich die

beiden neuen Steckverbinder-Typen beim Verbraucher nicht wirklich durchgesetzt.

Bezeichnungssystem für Twisted-Pair-Kabel nach ISO/IEC-11801 (2002) E

Neben der Einteilung in Klassen und Kategorien bezieht man sich bei der Bezeichnung von Twisted-Pair-Kabel auf deren Zusammensetzung aus Mantel, Schirm und Adernpaaren. Hier gibt es deutliche Unterschiede, die sich direkt in der Qualität der Kabel und deren Einsatzzweck bemerkbar macht.
Grundsätzlich unterschiedet man zwischen geschirmte und ungeschirmte Kabel. Im Gegensatz zu den geschirmten Kabel (STP und FTP) weisen die ungeschirmten Kabel (UTP) eine deutlich schlechtere Übertragungsqualität auf, die sich bei hohen Übertragungsraten und langen Leitungslängen negativ bemerkbar macht.
Da die alten Bezeichnungen nicht einheitlich, dafür widersprüchlich waren und oft Verwirrung gestiftet haben, wurde mit der Norm ISO/IEC-11801 (2002) E ein neues Bezeichnungssystem der Form XX/YZZ eingeführt.

XX steht für die Gesamtschirmung

- U = ohne Schirm (ungeschirmt)
- F = Folienschirm (beschichtete Kunststofffolie)
- S = Geflechtschirm (Drahtgeflecht)
- SF = Geflecht- und Folienschirm

Y steht für die Aderpaarschirmung

- U = ohne Schirm (ungeschirmt)
- F = Folienschirm (beschichtete Kunststofffolie)
- S = Geflechtschirm (Drahtgeflecht)

ZZ steht für die Verseilungsart

- TP = Twisted Pair (in der Regel)
- QP = Quad Pair

Übersicht: Bezeichnung für Twisted-Pair-Kabel

Twisted-Pair-Kabel (TP)		U/UTP	S/UTP	U/FTP	S/FTP	F/FTP	SF/FTP
Gesamtschirm	Drahtgeflecht (S)		X		X		X
	Folie (F)					X	X
Adernpaarschirm	Drahtgeflecht (S)						
	Folie (F)			X	X	X	X

U/UTP - Unscreened/Unshielded Twisted-Pair-Kabel

Das U/UTP-Kabel besteht aus einem Kunststoffmantel, in dem sich die ungeschirmten, paarweise verseilten Adernpaare befinden. Wegen des fehlenden Schirms haben U/UTP-Kabel einen geringen Außendurchmesser, sind leicht zu verarbeiten, zu verlegen und preisgünstig herzustellen.
U/UTP-Kabel sind weltweit die meistverwendeten Kabel für lokale Netzwerke mit Ethernet. Sie werden in Europa, speziell in Deutschland, seltener verwendet.

S/UTP - Screened/Unshielded Twisted-Pair-Kabel

Das S/UTP-Kabel besteht aus einem Kunststoffmantel und einem Gesamtschirm, in dem sich die paarweise verseilten Adernpaare befinden. Die Schirmung darf aus Kupfergeflecht oder Aluminiumfolie (Folie, die mit Aluminium kaschiert ist) oder aus beidem bestehen. Die Qualität dieser Kabel ist wesentlich höher als bei ungeschirmten UTP-Kabeln. Besteht der Gesamtschirm nur aus einer Folie, wird so ein Kabel auch als F/UTP-Kabel bezeichnet. Besteht der Gesamtschirm aus Folie und

Drahtgeflecht wird so ein Kabel auch als SF/UTP-Kabel bezeichnet. In der Regel spricht man trotzdem nur von S/UTP-Kabel.

U/FTP - Unscreened/Foiled Twisted-Pair-Kabel

U/FTP-Kabel bestehen aus einem Kunststoffmantel und paarweise verseilten Adernpaaren, die mit einem metallischen Folienschirm umgeben sind. Bei der Schirmung unterscheidet man zwischen PiMF (Paar in Metallfolie) und ViMF (Vierer in Metallfolie). Beim PiMF-Kabel ist jeweils ein Adernpaar von einer Metallfolie umgeben, beim ViMF-Kabel sind jeweils zwei Paare mit Metallfolie umgeben.
Durch die umfangreichere Schirmung haben U/FTP-Kabel einen größeren Außendurchmesser und einen größeren Biegeradius als U/UTP- S/UTP-Kabel. Die Verarbeitung und Verlegung dieser Kabel ist entsprechend aufwendiger.

S/FTP - Screened/Foiled Twisted-Pair-Kabel

S/FTP-Kabel bestehen aus einem Kunststoffmantel und paarweise verseilten Adernpaaren. Die einzelnen Adernpaare sind mit einer metallischen Folien umgeben. Zusätzlich ist das Adernpaar-Bündel mit einem Gesamtschirm aus einem Drahtgeflecht umgeben.

F/FTP - Foiled/Foiled Twisted-Pair-Kabel

F/FTP-Kabel bestehen aus einem Kunststoffmantel und paarweise verseilten Adernpaaren. Die einzelnen Adernpaare sind mit einer metallischen Folien umgeben. Zusätzlich ist das Adernpaar-Bündel mit einem Gesamtschirm aus einer metallischen Folie umgeben.

SF/FTP - Screened Foiled/Foiled Twisted-Pair-Kabel

SF/FTP-Kabel bestehen aus einem Kunststoffmantel und paarweise verseilten Adernpaaren. Die einzelnen Adernpaare sind mit einer metallischen Folien umgeben. Zusätzlich ist das Adernpaar-Bündel mit einem Gesamtschirm aus Drahtgeflecht und einer metallischen Folie umgeben.

Geschirmt oder ungeschirmte Twisted-Pair-Verkabelung?

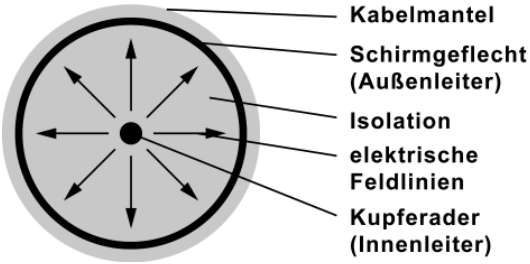
Allgemein geht man davon aus, dass geschirmte Twisted-Pair-Kabel besser gegen äußere Einflüsse geschützt sind. Das mag in den meisten Fällen auch als korrekt angenommen werden. Allerdings spricht vieles für den Einsatz ungeschirmter Twisted-Pair-Kabel. So setzen geschirmte Twisted-Pair-Kabel voraus, dass sich der Installateur auch um den Potentialausgleich kümmert, um die Ströme, die sich im Kabelschirm ergeben, abzuleiten. Dazu ist eine entsprechende Ausbildung notwendig. In Deutschland, in weiten Teilen auch in Europa, mag das zum allgemeinen Wissensstand der Elektroinstallateure zählen. Weltweit sieht es hier ganz anders aus. Hier werden Twisted-Pair-Kabel von Nicht-Fachleuten verlegt und angeschlossen und somit der Schirm abgeschnitten. Wird der Schirm nicht geerdet, dann kann er wie eine Antenne wirken und somit Störungen verursachen oder verschlimmern. Deshalb wird in solchen Fällen ganz auf die Schirmung im Kabel verzichtet. Diesem Fall wird also UTP-Kabel und nicht FTP-Kabel verwendet.

Generell spricht nichts dagegen ungeschirmte Twisted-Pair-Kabel einzusetzen. Man muss bei der Installation und Verlegung nur darauf achten, deutlich größere Abstände zu anderen stromführenden Leitungen und Komponenten einzuhalten. Zum Beispiel im Kabelkanal, Zwischenboden oder in der Decke.
Um Fremdeinflüsse von außen auf ungeschirmte Kabel zu begrenzen, werden in den Leitungen zusätzlich künstliche Asymmetrien eingebaut. Dabei steigt der Außendurchmesser deutlich, was die Vorteile gegenüber mehrfach geschirmter Kabel (z. B. SF/FTP) zunichte macht.

Koaxialkabel

Koaxialkabel oder Koaxialleitungen wurde in der Netzwerktechnik lange Zeit für Bus- oder Ring-Verkabelungen eingesetzt. Technisch und organisatorisch haben sich jedoch strukturierte Stern-Verkabelungen auf Basis von Twisted-Pair-Kabel durchgesetzt. Netzwerke mit Koaxialkabel gibt es heute praktisch nicht mehr.

Aufbau eines Koaxialkabels



In einem Koaxialkabel befindet sich eine Kupferader im Innern. Das ist der Innenleiter. Darum befindet sich ein Schirmgeflecht als Außenleiter. Durch eine Isolation werden beide voneinander getrennt und damit dem Kabel zusätzliche mechanische Stabilität verliehen.
Das elektrische Feld, das sich beim Anlegen einer Spannung aufbaut, entsteht nur zwischen Außen- und Innenleiter. Außerhalb des Kabels tritt kein magnetisches Feld auf.

Betrachtung des Koaxialkabels

Das Koaxialkabel ist ein unsymmetrisches Kabel. Bei der Übertragung von digitalen Signalen über ein Koaxialkabel (BNC) wird ein Potentialunterschied zwischen Innenleiter (Kern) und dem, als Bezugserde dienenden, Außenleiter erzeugt. Der Außenleiter wirkt als Antenne. Von ihm gehen elektromagnetische Wellen aus. Zusätzlich beeinflussen Störungen von außen den Signalfluss im Innenleiter.
Damit die elektrische Feldverteilung wirksam wird, muss der Außenleiter (Abschirmung, Abschirmmantel) an Erde gelegt werden. Hierdurch sind beide Leiter gegenüber der Erde spannungsmäßig ungleich. Deshalb sind Koaxialkabel unsymmetrische Leitungen (Paralleldrahtleitungen sind erdsymmetrisch).

Koaxialkabel charakterisiert eine Impedanz von 50 Ohm, um die Leistungsübertragung in einem System zu optimieren. Für eine minimale Dämpfung werden Systeme mit 75 Ohm verwendet.

Steckverbinder für Koaxialkabel

Die speziellen N-Steckverbinder sind robust und eignen sich für hohe Leistungen und bis über 18 GHz. SMA-Steckverbinder sind kleiner und für niedrigere Leistungen ausgelegt.
Um Fehlanpassung zu vermeiden, müssen Steckverbinder mit dem richtigen Drehmoment angeschlossen werden. Hersteller empfehlen etwa 9,5 Nm.
Kabel mit BNC-Steckverbindern eignen sich allerdings nur bis etwa 500 MHz.

Vorteil der Koaxialkabel gegenüber Twisted-Pair-Kabel

- Es können keine Störspannungen durch Influenz in das Kabel gelangen.
- Die im Kabel fließenden Ströme erzeugen keine magnetischen Störfelder.

Anwendungen von Koaxialkabel

- Netzwerkkabel (selten)
- Antennenkabel
- Übertragung von TV und Radio (Rundfunk/Broadcast)

Lichtwellenleiter (LWL / Glasfaser)

Lichtwellenleiter, kurz LWL genannt, übertragen Daten in Form von Licht bzw. Lichtsignalen über weite Strecken. Während elektrische Signale in Kupferleitungen als Elektronen von einem zum anderen Ende wandern, übernehmen in Lichtwellenleitern (LWL) die Photonen (Lichtteilchen) diese Aufgabe.

Durch Lichtwellenleiter können optische Signale ohne Verstärker große Entfernungen überbrücken. Trotz weiter Strecken ist eine hohe Bandbreite möglich. Die Bandbreite eines einzelnen Lichtwellenleiters beträgt rund 60 THz. Das macht Lichtwellenleiter zum Übertragungsmedium der Gegenwart und Zukunft. Da reicht ein Kupferkabel oder Funksystem nicht heran.

Glasfaser und Lichtwellenleiter

Die Glasfaser ist ein Lichtwellenleiter (LWL), dessen Fasern aus dem Grundstoff Glas bestehen. Er wird häufig mit dem Begriff Lichtwellenleiter verwechselt. Lichtwellenleiter ist der Oberbegriff für alle Licht-leitenden Leitungen, worunter auch die Glasfaser fällt. Lichtwellenleiter gibt es als Glas-, Quarz- oder Kunststofffaser.
Oft bezeichnet man einen Lichtwellenleiter auch dann als Glasfaser, wenn der Grundstoff kein Glas ist.

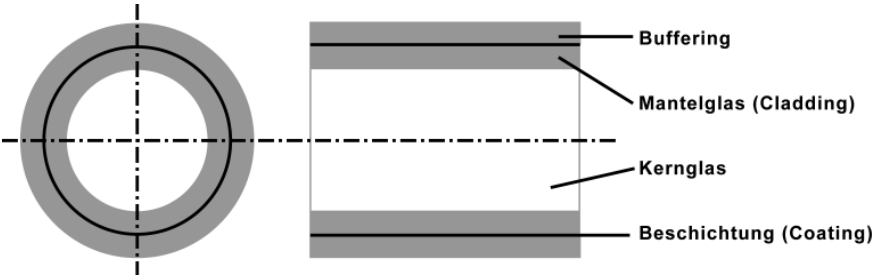
Prinzip eines Übertragungssystems auf Basis eines Lichtwellenleiters

Abhängig von der Datenform, findet zuerst eine Analog-Digital-Wandlung statt. In der Regel liegen die Daten als elektrische Signale vor, die dann noch durch eine Treiberstufe verstärkt werden. Vor der Übertragung müssen die elektrischen Signale in optische Signale umgewandelt werden. Dazu dienen spezielle Leuchtdioden (LEDs) oder Laserdioden als Lichterzeuger. Das Licht wird direkt in den Lichtwellenleiter eingespeist. Am anderen Ende des Lichtwellenleiters werden die Lichtimpulse wieder in elektrische Signale umgewandelt. Ein Fotoelement, zum Beispiel ein Fototransistor, erzeugt aus dem Licht elektrische Impulse. Dann findet noch eine Digital-Analog-Wandlung statt, wenn die Daten in analoger Form und verstärkt an den Empfänger übergeben werden müssen.

Telekommunikationsnetze mit Lichtwellenleiter

Um in Telekommunikationsnetzen hohe Geschwindigkeiten zu erreichen, setzt man in der Regel auf optische Verbindungen zwischen den Knoten. In den Schaltzentralen und Vermittlungsstellen werden die übertragenen Lichtsignale meistens in elektrische Signale umgewandelt, ausgewertet und weiterverarbeitet. Zur weiteren Übertragung werden sie dann wieder in Lichtsignale umgewandelt. An dieser Stelle werden die Nachteile optischer Übertragungssysteme sichtbar. Zur Verarbeitung müssen optische Signale erst in elektrische Signale umgewandelt werden.

Aufbau eines Lichtwellenleiters



Lichtwellenleiter (LWL) aus Kunststoff haben einen Durchmesser von etwa 0,1 mm. Sie sind äußerst flexibel aber auch empfindlich.
Der Faserkern (Kernglas) ist der zentrale Bereich eines Lichtwellenleiters, der zur Wellenführung des Lichts dient. Der Kern besteht aus einem Material mit einem höheren Brechungsindex als der darrüberliegende Mantel. An den Wänden im Innern des Lichtwellenleiters findet eine Reflexion statt, so dass der Lichtstrahl nahezu verlustfrei um jede Ecke geleitet wird. Das Mantelglas ist das optisch transparente Material eines Lichtwellenleiters an dem die Reflexion stattfindet. Das Mantelglas oder auch Cladding genannt ist ein dielektrisches Material mit einem niedrigeren Brechungsindex als der Kern. Das dielektrische Material ist nichtmetallisch und nichtleitend. Es enthält also keine metallischen Anteile.
Das Coating ist die Kunststoffbeschichtung, die als mechanischen Schutz auf der Oberfläche des Mantelglases aufgebracht ist.
Buffering nennt man das Schutzmaterial, das auf dem Coating aufextrudiert ist. Es schützt das Kabel vor Umwelteinflüssen. Buffering gibt es auch als Röhrchen, dass die Faser vor Stress im Kabel isoliert, wenn das Kabel bewegt wird.

Vorteile der Lichtwellenleiter gegenüber Kupferkabel

- Lichtwellenleiter können beliebig mit anderen Versorgungsleitungen parallel verlegt werden. Es wirken keine elektromagnetischen Störeinflüsse.
- Wegen der optischen Übertragung existieren keine Störstrahlungen oder Masseprobleme.

- Entfernungsbedingte Verluste durch Induktivitäten, Kapazitäten und Widerständen treten nicht auf.
- Nahezu Frequenz-unabhängige Leitungsdämpfung der Signale.
- Übertragungsraten sind durch mehrere Trägerwellen mit unterschiedlichen Wellenlängen (Farbspektrum) fast unbegrenzt erweiterbar.

Allerdings sind Lichtwellenleiter teurer als Kupferleitungen. Die Kosten für Material und der Aufwand bei der Montage sind höher. Dafür haben Lichtwellenleiter eine erheblich geringere Dämpfung und eignen sich somit für weite Strecken.

Brechungsindex

Der Brechungsindex ist der Faktor, um den die Lichtgeschwindigkeit in optischen Medien kleiner ist, als im Vakuum.

Moden

Moden sind die verschiedenen Wege, dem die Photonen des Lichts entlang der Faser folgen können. Multimode-Fasern können viele Moden unterstützen.

Spleiß

Der Spleiß ist die dauerhafte Verbindung zwischen zwei Glasfasern. Um eine Verbindung zwischen zwei Lichtwellenleitern herzustellen, müssen die beiden Enden verschmelzt (Schmelzspleiß) oder verklebt (Klebespleiß) werden.

Einfügedämpfung

Das Einfügen eines optischen Bauelements erzeugt eine Dämpfung des Signals. Das nennt man Einfügedämpfung.

Dispersion

Dispersion beschreibt den Effekt, dass der eingespeiste Impuls über den Ausbreitungsweg zeitlich ausgeweitet wird. Der Impuls wird breiter. Dadurch kann es zu Überlappungen mit den vorangegangenen und nachfolgenden Impulsen kommen. Bei hohen Geschwindigkeiten kann es zu Übertragungsfehlern kommen.
Um den Impuls so weit wie möglich impulsartig zu bekommen, werden keine normalen LEDs für die Lichtimpulserzeugung verwendet, sondern Laserdioden, die einen Impuls mit spektraler Breite von wenigen Nanometer erzeugen können.

Netzwerkkarte / Netzwerkadapter (NIC)

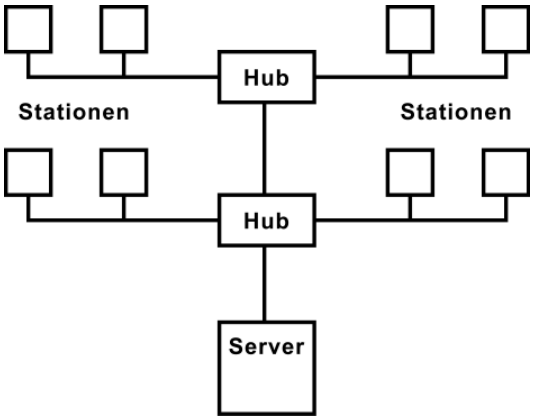
Eine Netzwerkkarte wird auch als Netzwerkadapter bezeichnet. Die englische Bezeichnung ist Network Interface Card (NIC).
Eine Netzwerkkarte ermöglicht es, auf ein Netzwerk zuzugreifen und arbeitet auf der Bitübertragungsschicht (Schicht 1) des OSI-Schichtenmodells. Jede Netzwerkkarte hat eine Hardware-Adresse (Format: XX-XX-XX-XX-XX-XX), die es auf der Welt nur einmal gibt. Anhand dieser Adresse lässt sich eine Station auf der Bitübertragungsschicht adressieren.

Bauformen von Netzwerkkarten

Netzwerkkarten gibt es in verschiedenen Bauformen. Die klassische Netzwerkkarte für den ISA-, PCI- oder PCIe-Bus ist eine Steckkarte für den Einbau in das Computergehäuse. Eine andere Variante des Netzwerkadapters bzw. -controllers ist onboard auf dem Motherboard untergebracht. Der Anschluss wird als RJ45-Buchse von der Platine herausgeführt. Es gibt auch Netzwerkkarten, die in einer Box eingebaut sind und über den USB am Computer angeschlossen werden. Allerdings sind sie eher unüblich, da jedes noch so billige Motherboard einen Onboard-LAN-Adapter hat.

Hub

Ein Hub ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Hub als Verteiler für die Datenpakete. Hubs arbeiten auf der Bitübertragungsschicht (Schicht 1) des OSI-Schichtenmodells und sind damit auf die reine Verteilfunktion beschränkt. Ein Hub nimmt ein Datenpaket entgegen und sendet es an alle anderen Ports weiter. Das bedeutet, er broadcastet. Dadurch sind nicht nur alle Ports belegt, sondern auch alle Hosts. Sie bekommen alle Datenpakete zugeschickt, auch wenn sie nicht die Empfänger sind. Für die Hosts bedeutet das auch, dass sie nur dann senden können, wenn der Hub gerade keine Datenpakete sendet. Sonst kommt es zu Kollisionen.



Wenn die Anzahl der Anschlüsse an einem Hub für die Anzahl der Hosts nicht ausreicht, dann benötigt man noch einen zweiten Hub. Zwei Hubs werden über einen Uplink-Port eines der beiden Hubs oder mit einem Crossover-Kabel (Sende- und Empfangsleitungen sind gekreuzt) verbunden. Es gibt auch spezielle "stackable" Hubs, die sich herstellerspezifisch mit Buskabeln kaskadieren lassen. Durch die Verbindung mehrerer Hubs lässt sich die Anzahl der möglichen Hosts im Netzwerk erhöhen. Allerdings ist die Anzahl der anschließbaren Hosts begrenzt. Hier gilt die Repeater-Regel.

Alle Hosts, die an einem Hub angeschlossen sind, teilen sich die gesamte Bandbreite, die durch den Hub zur Verfügung steht (z. B. 10 MBit/s oder

100 MBit/s). Die Verbindung vom Host zum Hub verfügt nur kurzzeitig über diese Bandbreite.
Das Versenden der Datenpakete an alle Hosts ist nicht besonders effektiv. Es hat aber den Vorteil, dass ein Hub einfach und kostengünstig herzustellen ist.
Wegen der prinzipiellen Nachteile von Hubs, verwendet man eher Switches, die die Aufgabe der Verteilfunktion wesentlich besser erfüllen, da sie direkte Verbindungen zwischen den Ports schalten können.

Switch

Ein Switch ist ein Kopplungselement, das mehrere Hosts in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Switch als Verteiler für die Datenpakete. Die Funktion ist ähnlich einem Hub, mit dem Unterschied, das ein Switch direkte Verbindungen zwischen den angeschlossenen Geräten schalten kann, sofern ihm die Ports der Datenpaket-Empfänger bekannt sind. Wenn nicht, dann broadcastet der Switch die Datenpakete an alle Ports. Wenn die Antwortpakete von den Empfängern zurück kommen, dann merkt sich der Switch die MAC-Adressen der Datenpakete und den dazugehörigen Port und sendet die Datenpakete dann nur noch dorthin.
Während ein Hub die Bandbreite des Netzwerks limitiert, steht der Verbindung zwischen zwei Hosts, die volle Bandbreite der Ende-zu-Ende-Netzwerk-Verbindung zur Verfügung.

Ein Switch arbeitet auf der Sicherungsschicht (Schicht 2) des OSI-Modells und arbeitet ähnlich wie eine Bridge. Daher haben sich bei den Herstellern auch solche Begriffe durchgesetzt, wie z. B. Bridging Switch oder Switching Bridge. Die verwendet man heute allerdings nicht mehr.

Switches unterscheidet man hinsichtlich ihrer Leistungsfähigkeit mit folgenden Eigenschaften:

- Anzahl der speicherbaren MAC-Adressen für die Quell- und Zielports
- Verfahren, wann ein empfangenes Datenpaket weitervermittelt wird (Switching-Verfahren)
- Latenz (Verzögerungszeit) der vermittelten Datenpakete

Ein Switch ist im Prinzip nichts anderes als ein intelligenter Hub, der sich merkt, über welchen Port welcher Host erreichbar ist. Auf diese Weise erzeugt jeder Switch-Port eine eigene Collision Domain (Kollisionsdomäne).
Teure Switche können zusätzlich auf der Schicht 3, der Vermittlungsschicht, des OSI-Schichtenmodells arbeiten (Layer-3-Switch oder Schicht-3-Switch). Sie sind in der Lage, die Datenpakete anhand der IP-Adresse an die Ziel-Ports weiterzuleiten. Im Gegensatz zu normalen Switche lassen sich auch ohne Router logische Abgrenzungen erreichen.

MAC-Adressen-Verwaltung / MAC-Tabelle

Switche haben den Vorteil, im Gegensatz zu Hubs, dass sie Datenpakete nur an den Port weiterleiten, an dem der Host mit der Ziel-Adresse angeschlossen ist. Als Zuordnung dient die MAC-Adresse, also die Hardware-Adresse einer Netzwerkkarte. Diese Adresse speichert der Switch in einer internen Tabelle. Empfängt ein Switch ein Datenpaket, so sucht er in seinem Speicher unter der Zieladresse (MAC) nach dem Port und schickt dann das Datenpaket nur an diesen Port. Die Zuteilung der MAC-Adressen lernt ein Switch mit der Zeit kennen. Die Anzahl der Adressen, die ein Switch aufnehmen kann, hängt von seinem internen Speicher ab.
Ein Qualitätsmerkmal eines Switch ist, wie viele Adresse er insgesamt und pro Port speichern kann. An einem Switch, der nur eine Handvoll Computer verbindet, spielt es keine Rolle wie viele Adressen er verwalten kann. Wenn der Switch aber in einem großen Netzwerk steht und an seinen Ports noch andere Switches und Hubs angeschlossen sind, dann muss er evt. mehrere tausend MAC-Adressen speichern und den Ports zuordnen können. Je größer ein Netzwerk ist, desto wichtiger ist es darauf zu achten, dass die Switche genügend Kapazität bei der Verwaltung von MAC-Adressen haben.

Router

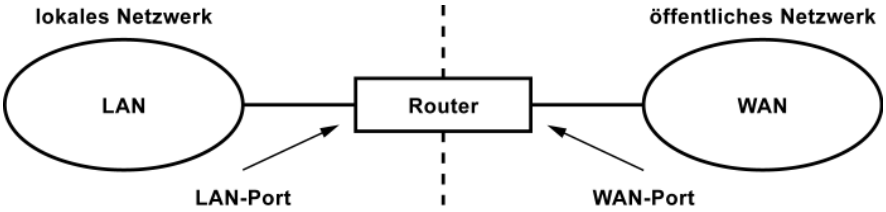
Ein Router verbindet mehrere Netzwerke mit unterschiedlichen Protokollen und Architekturen. Ein Router befindet sich häufig an den Außengrenzen eines Netzwerks, um es mit dem Internet oder einem anderen, größeren Netzwerk zu verbinden.
Über die Routing-Tabelle entscheidet ein Router, welchen Weg ein

Datenpaket nimmt. Es handelt sich dabei um ein dynamisches Verfahren, das Ausfälle und Engpässe ohne den Eingriff eines Administrators berücksichtigen kann.
Ein Router hat mindestens zwei Netzwerkanschlüssen. Er arbeitet auf der Vermittlungsschicht (Schicht 3) des OSI-Schichtenmodells.

Die Aufgabe eines Routers ist ein komplexer Vorgang, der sich in 4 Schritte einteilen lässt:

- Ermittlung der verfügbaren Routen
- Auswahl der geeignetsten Route unter Berücksichtigung verschiedener Kriterien
- Herstellen einer physikalischen Verbindung zu anderen Netzwerken
- Anpassen der Datenpakete an die Übertragungstechnik (Fragmentierung)

Router-Anschlüsse: LAN und WAN



Ein Router hat in der Regel zwei Anschlüsse. Einen für die LAN-Seite und einen für die WAN-Seite. Häufig sind die Ports mit der Bezeichnung LAN und WAN gekennzeichnet. Manchmal gibt es Port-Beschriftungen, bei denen nicht immer eindeutig ist, um was es sich handelt.
Mit LAN ist immer das lokale Netzwerk mit privaten IP-Adressen gemeint, während die WAN-Seite das öffentliche Netzwerk kennzeichnet.

Layer-3-Switch

Ein Layer-3-Switch ist eine Kombination aus Router und Switch. Er beherrscht nicht nur Switching, sondern auch Routing. Da Router und Switche sehr ähnlich funktionieren - sie empfangen, speichern und leiten

Datenpakete weiter - ist es nur logisch beide Geräte miteinander zu kombinieren, um daraus ein Multifunktionsgerät zu machen.

In der Regel arbeitet ein Switch auf der Schicht 2 des OSI-Schichtenmodells. Ein Router arbeitet auf der Schicht 3 des OSI-Schichtenmodells. In der Praxis sieht das so aus, dass die Entscheidung zur Weiterleitung von Datenpaketen anhand der MAC-Adressen oder der IP-Adressen erfolgen kann. Ein Layer-3-Switch kann einzelnen Ports verschiedenen Subnetzen zuordnen und innerhalb dieser Subnetze als Switch arbeiten. Außerdem beherrscht er auch das Routing zwischen diesen Subnetzen.
Vereinfacht kann man sagen, dass ein Layer-3-Switch ein Router mit Switching-Funktion oder umgekehrt ein Switch mit Routing-Funktion ist. Von der Funktionsweise ist es so, dass Daten ins Internet geroutet werden und Daten im lokalen Netzwerk geswitcht.

Router mit Switching-Funktion

Im Kern ist solch ein Gerät ein Router, dessen Routing-Funktionen durch den Einsatz spezifischer Hardware (ASICs) beschleunigt werden.

Switch mit Routing-Funktion

Im Kern ist solch ein Gerät ein Switch, der um die Funktionen eines Routers erweitert wurde.
Wegen der höheren Geschwindigkeit und aus finanziellen Gründen, werden Layer-3-Switche gegenüber reinen Routern bevorzugt. Zumindest in großen Netzen. Layer-3-Switche lassen sich als Router, Switch oder als Mischform betreiben. Im Vergleich zu Routern haben Layer-3-Switche eine geringere Verzögerungszeit und einen höheren Datendurchsatz. Funktionell ist es so, dass das erste Datenpaket einer Verbindung wie bei einem Router behandelt wird. Das heißt auch, dass auf Broadcasts verzichtet wird. Alle weiteren Datenpakete werden geswitcht, da die Route bereits bekannt ist. Das bringt einen Geschwindigkeitsvorteil.

Vorteile Layer-3-Switch (gegenüber Router)

- geringere Gerätekosten
- geringere Verzögerungszeit

- höherer Durchsatz
- einfachere Administration
- hohe Flexibilität
- mehr Ports

Nachteile Layer-3-Switch (gegenüber Router)

Ein Layer-3-Switch hat weniger Features. Aber auf IP-Ebene lassen sich durch Routing-Funktionen deutlich mehr Möglichkeiten zur Steuerung von Netzwerkverkehr realisieren.

Gateway

Ein Gateway ist ein aktiver Netzknoten, der zwei Netze miteinander verbinden kann, die physikalisch zueinander inkompatibel sind und/oder eine unterschiedliche Adressierung verwenden. Gateways koppeln die unterschiedlichsten Protokolle und Übertragungsverfahren miteinander. Dabei können Sie auf allen Schichten des OSI-Schichtenmodells arbeiten.

Grundsätzlich geht man von zwei verschiedene Ansätzen aus. Einmal von Medien-konvertierenden Gateways, die bei gleichen Übertragungsverfahren zwischen zwei verschiedenen Protokollen der OSI-Schichten 1 und 2 verbinden. Dann gibt es noch die Protokoll-konvertierenden Gateways, die unterschiedliche Protokolle auf den OSI-Schichten 3 und 4 miteinander verbinden.
Und dann gibt es noch Anwendungs-konvertierende Gateways, wobei es hier eher darum geht, Dateiformate zu konvertieren.
Gateways haben die Aufgabe eine logische Verbindung herzustellen und einen Datenstrom zwischen Quelle und Ziel zu übermitteln. Beim Übergang zwischen zwei Netzen berücksichtigt das Gateway die spezifischen Bedingungen beider Übertragungssysteme und den Übertragungsmedien

- Protokolle
- Adressierung
- Übertragungsgeschwindigkeit
- physikalische Bedingungen
- Datenformate

Übertragungstechnik

IEEE 802

Ethernet-Standards

WLAN-Grundlagen

Powerline

IEEE 802

802 ist die Nummer für eine Projektgruppe des IEEE (Institute of Electrical and Electronics Engineers), welches standardisierte Protokolle- und Übertragungstechniken für Local und Metropolitan Area Networks (LAN und MAN) umfasst. Der Name der Projektgruppe 802 ist aus dem Startdatum Februar 1980 abgeleitet. Vom IEEE werden Standards entworfen, Techniken und Themen vorgeschlagen und in Arbeitsgruppen diskutiert.

IEEE 802 ist ursprünglich für LAN-Techniken, wie Ethernet (802.3), Token Bus (802.4) und Token Ring (802.5) verantwortlich. Weitere Projektteile sind Wireless LAN (802.11), Bluetooth (802.15.1) und WiMAX (802.16). Die Zahl hinter dem ersten Punkt kennzeichnet den Standard. Einzelne Standards innerhalb einer Gruppe werden mit einem angehängten Buchstaben oder weiteren Ziffern oder Jahreszahlen gekennzeichnet.

Das Projekt 802 dominiert die Standardisierung von lokalen Netzen, in denen hauptsächlich Ethernet zum Einsatz kommt. Ohne Ethernet und seine vielen Erweiterungen geht es praktisch nicht mehr. Andere Netzwerkstandards spielen nur in Randbereichen eine Rolle.
Neben der Standardisierung neuer Übertragungstechniken hat das IEEE 802 die Aufgabe bestehende Techniken weiter zu entwickeln und für neue Anwendungen zu optimieren. Einige Standards bauen deshalb aufeinander auf oder hängen voneinander ab.

<table>
<tr><td rowspan="2">2</td><td rowspan="3">802.1
Internet-
Working</td><td colspan="5">802.2
Logical Link Control</td></tr>
<tr><td colspan="5">802.1
Media Access Control</td></tr>
<tr><td>1</td><td>802.3
Ethernet</td><td>802.4
Token-
Bus</td><td>802.5
Token-
Ring</td><td>802.11
Wireless
LAN</td><td>802.12
AnyLAN</td></tr>
</table>

Die Standards der 802-Familie umfassen die physikalische Übertragungsschicht (Physical Layer) bzw. Bitübertragungsschicht (OSI-

Schicht 1) und die Verbindungsschicht (Data Link Layer) bzw. die Sicherungsschicht (OSI-Schicht 2). Die Sicherungsschicht (Schicht 2) wird noch einmal in einen Logical-Link-Control (LLC) und einen Medium-Access-Control-Layer (MAC) unterteilt. Das LLC ist für die Übertragung und den Zugriff auf die logische Schnittstelle zuständig. Die MAC-Schicht umfasst die Steuerung des Zugriffs auf das Übertragungsmedium und ist somit für den fehlerfreien Transport der Daten verantwortlich.

IEEE 802.3 / Ethernet-Grundlagen

Ethernet ist eine Familie von Netzwerktechniken, die vorwiegend in lokalen Netzwerken (LAN), aber auch zum Verbinden großer Netzwerke zum Einsatz kommt (WAN).
Für Ethernet gibt es eine Vielzahl an Standards, für die das Institute of Electrical and Electronics Engineers (IEEE) verantwortlich ist. Seit der Einrichtung einer Arbeitsgruppe für den Standard eines lokalen Netzwerks ist der Name "Ethernet" das Synonym für alle unter der Arbeitsgruppe 802.3 vorgeschlagenen und standardisierten Spezifikationen.

Geschichtlicher Hintergrund

Ursprünglich wurde Ethernet in den siebziger Jahren im PARC (Palo Alto Research Center), im Forschungslabor der Firma Xerox entwickelt. In Zusammenarbeit mit den Firmen DEC und Intel wurde Ethernet später zu einem offenen Standard. Dieser Standard bildete dann die Grundlage für den offiziellen 802.3-Standard des IEEE (Institute of Electrical and Electronics Engineers).
Einer der Vorläufer von Ethernet war ein Funknetz mit dem Namen ALOHA, das die Hawaii-Inseln miteinander verbunden hat. Hier war das Übertragungsmedium die Luft. Genauso wie ALOHA wurde Ethernet für die gemeinsame Nutzung eines Übertragungsmediums durch viele Stationen entwickelt. Während es für ALOHA die Luft war, wurde für Ethernet als Übertragungsmedium ein Koaxialkabel gewählt, das die Rechner in einer Bus-Topologie miteinander verbunden hat.
Angefangen hat es in den 1980er Jahren beim 10-MBit-Ethernet über Koaxialkabel. Es folgten verschiedene Weiterentwicklungen für Twisted-Pair-Kabel und Glasfaserkabel mit höheren Übertragungsraten.
Alle Ethernet-Varianten haben eines gemeinsam: Sie basieren auf

denselben Prinzipien, die ursprünglich in den Standards 802.1, 802.2 und 802.3 festgelegt wurden. Ethernet ist unter 802.3 standardisiert und baut auf 802.1 und 802.2 auf.

Irgendwann in den 1990er Jahren hat sich Ethernet gegenüber Token Ring (auf Basis von Koaxialkabel) und FDDI (auf Basis von Glasfaserkabel) durchgesetzt. Insbesondere der einfache und kostengünstige Aufbau eines Ethernet-Netzwerks sorgte für die rasche Verbreitung auf der ganzen Welt. Von Token Ring, FDDI oder gar ATM und SDH spricht man heute fast nicht mehr. Im Prinzip werden heute fast alle Vernetzungen im LAN und WAN mit Ethernet-Technik realisiert.

Übertragungsmedium und Netzwerk-Topologie

Das ursprüngliche Ethernet basiert auf einem Koaxialkabel als Übertragungsmedium. Dabei wurde mit einem Kabel hintereinander mehreren anderen Stationen zu einer Kette verbunden. Die Netzwerk-Topologie hat man dann als Bus bezeichnet.
Stetige Verbesserungen haben dann zu einem Anstieg der Netzwerkleistung geführt. Der entscheidende Durchbruch von Ethernet im LAN kam durch den Umstieg von Shared- auf Switched-Media (von Bus zu Stern-Topologie) in Verbindung mit einer strukturierten Verkabelung. Gleichzeitig hat die konsequente Rückwärtskompatibilität dazu geführt, dass Investitionen bis zu einem gewissen Grad zukunftsfähig blieben. Im Prinzip lassen sich auch heute noch die alten Komponenten für 10 und 100 MBit/s mit Komponenten für 1 GBit/s kombinieren. Im Zweifelsfall bedarf es nur eines Medienkonverters.

Übertragungstechnik

Ethernet transportiert Daten paketweise ohne festes Zugriffsraster. Damit unterscheidet sich Ethernet von anderen paketorientierten Systemen, wie zum Beispiel ATM oder SDH/Sonet, die mit einem festen Zeitraster jedem Teilnehmer eine Mindestbandbreite garantieren können. Deshalb bereitet Ethernet Probleme bei allen Arten von zeitkritischen Anwendungen. Bei Ethernet gibt es keine Garantie, dass die Daten innerhalb einer bestimmten Zeit den Empfänger erreichen. Das bedeutet, der Erfolg einer Übertragung ist nicht sicher. Er unterliegt nur einer gewissen Wahrscheinlichkeit. So verwerfen Ethernet-Komponenten

Datenpakete, wenn nicht genug Bandbreite zur Verfügung steht. Wegen der unzuverlässigen Übertragungstechnik ist Ethernet auf die Intelligenz höherer Protokolle und Anwendungen angewiesen. Das ist auch ein Grund, warum in bestimmten Bereichen heute noch andere Vernetzungstechniken bevorzugt werden. Im Vergleich dazu ist Ethernet eine einfach zu implementierende Vernetzungstechnik, die sich über die Jahrzehnte hinweg in lokalen Netzwerken bewährt und durchgesetzt hat.

CSMA/CD und Kollisionen

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ist ein Zugriffsverfahren von Ethernet, bei dem mehrere Netzwerk-Teilnehmer auf das Übertragungsmedium zugreifen zu können. Dabei spielt die Behandlung von Kollisionen bei der Signalübertragung ein große Rolle.

CSMA/CD - Carrier Sense Multiple Access with Collision Detection

- Carrier Sense (Träger-Zustandserkennung): Jede Station prüft, ob das Übertragungsmedium frei ist.
- Multiple Access (Mehrfachzugriff): Mehrere Stationen teilen sich das Übertragungsmedium.
- Collision Detection (Kollisionserkennung): Wenn mehrere Stationen gleichzeitig senden, erkennen sie die Kollision.

Ablauf von CSMA/CD

Das ursprüngliche Ethernet entspricht einer Bus-Topologie an der mehrere Stationen angeschlossen sind (Multiple Access). Festgelegt ist, dass alle Stationen die Signale auf dem Bus lesen, aber nicht gleichzeitig senden dürfen. Welche der angeschlossenen Stationen senden darf, wird durch das CSMA/CD-Verfahren bestimmt, das nach dem Prinzip "Listen-before-Talk" arbeitet.

Alle Stationen hören permanent das Übertragungsmedium ab (Carrier Sense). Sie können zwischen einem freien und einem besetzten Übertragungsmedium unterscheiden. Bei einem freien Übertragungsmedium darf gesendet werden. Will eine Station senden,

prüft sie, ob der Bus frei ist. Ist er frei, so beginnt die Station zu senden. Das bedeutet, sie legt das Datensignal auf den Bus.

Während der Signalübertragung überprüft die Station, ob das gesendete Signal mit dem Signal auf dem Bus identisch ist. Entspricht das gesendete Signal nicht dem abgehörten Signal, dann hat eine andere Station gleichzeitig gesendet. Die beiden Signale überlagern sich. Diesen Zustand auf dem Übertragungsmedium bezeichnet man als Kollision. Durch permanentes Prüfen des Zustands auf der Leitung kann diese Kollision erkannt werden (Collision Detection).

Wurde eine Kollision erkannt, dann wird die Übertragung abgebrochen. Der Sender, der das Störsignal zuerst entdeckt, sendet ein spezielles Signal, damit alle anderen Stationen wissen, dass das Netzwerk blockiert ist. Nach einer zufälligen Wartezeit wird wieder geprüft, ob der Bus frei ist. Ist das der Fall, wird von neuem gesendet. Der Vorgang wird so oft wiederholt, bis die Daten ohne Kollision übertragen wurden.

Konnte die Übertragung ohne Kollisionserkennung beendet werden, dann gilt die Übertragung als erfolgreich. Kamen die Daten aus irgendwelchen Gründen beim Empfänger nicht an, dann müssen diese Daten durch Protokolle, wie z. B. TCP, neu angefordert werden. Tritt dies häufiger auf, werden mehr Datenpakete gesendet. Das drückt auf die effektive Übertragungsgeschwindigkeit des Netzwerks.

Kollisionen

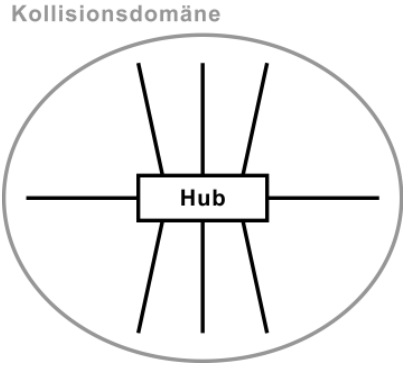
Grundsätzlich sind Kollisionen nicht als Störungen anzusehen. Kollisionen gehören im Listen-before-Talk-Betrieb zum normalen Betriebsablauf. Allerdings werden Kollisionen zu einem Problem, wenn sie Überhand nehmen. Die Anzahl der Kollisionen steigt, je mehr Stationen auf das Übertragungsmedium Zugriff haben wollen.

Durch lange Leitungen, sehr viele Stationen und Repeater (Signalaufbereiter und -verstärker) entstehen je nach Ort der Einspeisung unterschiedliche Signallaufzeiten. Sie führen dazu, dass eine Station ein freies Übertragungsmedium feststellt und ihr Signal sendet, obwohl das Signal einer anderen Station bereits unterwegs ist. Es kommt zur Kollision, also der Überlagerung von zwei Signalen.

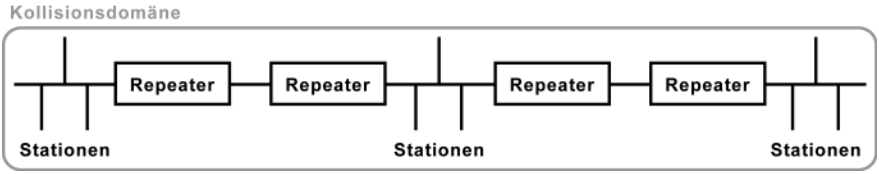
Durch CSMA/CD ergeben sich Grenzwerte für die maximale Signallaufzeit und die Rahmengröße (Datenpaket bzw. Frame). Beides darf nicht überschritten werden. Solange die Bandbreite von Ethernet nicht mehr als 30% ausgereizt wird, machen sich Kollisionen kaum bemerkbar. Mit steigender Belastung des Netzwerks nehmen aber auch die Kollisionen zu. Hier hilft nur, die Anzahl der Stationen zu reduzieren oder das gesamte Netzwerk in Teilnetz aufzuteilen.

Wegen der Kollisionen ist es nicht möglich, die theoretische Übertragungskapazität voll auszuschöpfen. In der Praxis liegt die Nominalleistung im günstigsten Fall bei etwa 70%. Unter ungünstigeren Bedingungen sind es unter 30%. Deutlich darunter bricht das Netzwerk praktisch zusammen. Die Ursache ist einfach: Je mehr Rechner in einem Netzwerk aktiv sind, desto mehr Kollisionen treten auf. Und so sinkt der erzielbare Datendurchsatz ständig ab.

Kollisionsdomäne



Die Kollisionsdomäne (collision domain) umfasst ein Netzwerk oder auch nur ein Teilnetzwerk aus Leitungen, Stationen und Kopplungselementen der Schicht 1 (OSI-Referenzmodell). In der Kollisionsdomäne müssen die Kollisionen innerhalb einer bestimmten Zeit jede Station erreichen. Das ist die Bedingung, damit das CSMA/CD-Verfahren funktionieren kann. Ist die Kollisionsdomäne zu groß, dann besteht die Gefahr, dass sendende Stationen Kollision nicht bemerken können. Aus diesem Grund ist die maximale Anzahl der Station in einer Kollisionsdomäne auf 1.023 Stationen begrenzt. Außerdem gilt, dass sich maximal zwei Repeater-Paare zwischen zwei beliebigen Stationen befinden dürfen.

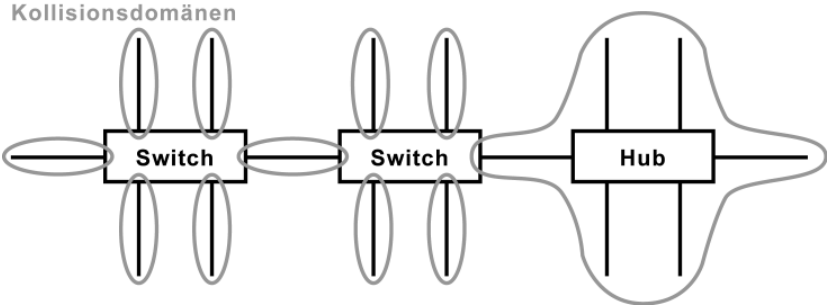


Um die Bedingungen für eine einwandfrei funktionierende Kollisionsdomäne einhalten zu können, wurde die 5-4-3-Repeater-Regel definiert: Es dürfen nicht mehr als fünf (5) Kabelsegmente verbunden sein. Dafür werden maximal vier (4) Repeater eingesetzt. An nur drei (3) Segmenten dürfen Endstationen angeschlossen sein.

Hinweis: Die Repeater-Regel gilt für 10Base2 und 10Base5 (Koaxialkabel-Netzwerk). In Twisted-Pair-Netzwerken muss man die Repeater-Regel nur beim Einsatz von Hubs beachten. Durch den konsequenten Einsatz von Switches und Routern geht man den Problemen durch das CSMA/CD-Verfahren aus dem Weg.

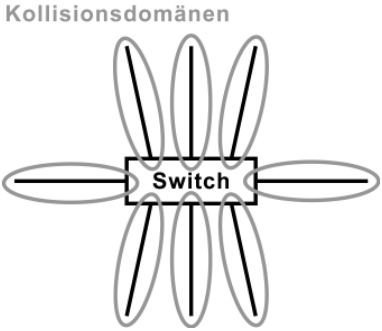
Wie kann man Kollisionen verhindern?

Grundsätzlich: Je weniger Stationen sich in einer Kollisionsdomäne befinden, desto weniger Kollisionen können auftreten.



Um Kollisionen zu vermeiden und einen höheren Datendurchsatz zu erreichen, wird ein Netz auf der Schicht 2 in mehrere Teilnetze aufgeteilt. Bei der Zusammenstellung der Teilnetze ist es sinnvoll die Stationen in einem Teilnetz zusammenzuschließen, die viel miteinander kommunizieren.

Wenn man ein logisches Netz mit Switche oder Bridges aufteilt, entstehen mehrere Kollisionsdomänen. Innerhalb einer Kollisionsdomäne befindet sich dann eine einzelne Station, ein weiterer Switch oder ein Router in ein anderes Netz. Die Einrichtung von Kollisionsdomänen reduziert den Datenverlust durch Kollisionen. Das wiederum reduziert den Netzwerkverkehr, der durch wiederholte Übertragungen verursacht wird.



Wenn man generell nur mit Switche arbeitet, wird der Begriff Kollisionsdomäne nicht mehr verwendet. In einem Switch bildet jeder Port und der mit einem Kabel verbundenen Station eine eigene Kollisionsdomäne. Es handelt sich dabei um eine Punkt-zu-Punkt-Verbindung. Der Switch sorgt dafür, dass nur die Datenpakete an den Port weiterleiten werden, über den die Ziel-MAC-Adresse des Pakets erreichbar ist.

Halbduplex und Vollduplex

Halbduplex-Ethernet basiert auf dem CSMA/CD-Verfahren. Es handelt sich dabei um das ursprüngliche Ethernet bis 10 MBit/s. Vollduplex-Ethernet ist eine Weiterentwicklung, die als Fast Ethernet bezeichnet wird und auf CSMA/CD verzichtet. Auch alle weiteren Ethernet-Entwicklungen arbeiten im Vollduplex-Betrieb. Die Stationen kommunizieren über Punkt-zu-Punkt-Verbindungen direkt miteinander. Weil Fast Ethernet in der Regel im Vollduplex-Modus arbeitet und damit auf CSMA/CD verzichtet, ist eine zusätzliche Flusskontrolle erforderlich. Dafür gibt es einen eigenen Standard: IEEE 802.3x (Flow Control).

MAC-Adresse

Der Standard IEEE 802.1 definiert Media Access Control (MAC). Hier wird unter anderem die physikalische Adresse für Netzwerk-Schnittstellen festgelegt. Und das unabhängig von der Übertragungstechnik. Die sogenannte MAC-Adressen gelten zum Beispiel für Ethernet (IEEE 802.3), Bluetooth (IEEE 802.15) und WLAN (IEEE 802.11).

Jeder Host in einem Ethernet-basierten Netzwerk hat eine eigene 48-Bit lange Adresse. Diese Adresse soll den Host weltweit eindeutig identifizieren. Diese Adresse wird als MAC-Adresse, Hardware-Adresse, Ethernet-Adresse oder physikalische Adresse bezeichnet. Die unterschiedlichen Bezeichnungen kommen daher, weil die MAC-Adresse den physikalischen Anschluss bzw. den Netzzugriffspunkt eines Hosts adressiert. Der physikalische Anschluss ist die Hardware. Zum Beispiel eine Netzwerkkarte oder Netzwerkadapter. Die Bezeichnung Ethernet-Adresse kommt daher, weil MAC-Adressen üblicherweise für Ethernet-Netzwerkkarten, aber auch WLAN- und Bluetooth-Adapter vergeben werden. Jede Netzwerkkarte besitzt eine eigene, individuelle MAC-Adresse. Sie wird einmalig hardwareseitig vom Hersteller konfiguriert und lässt sich im Regelfall nicht verändern.

In jedem Ethernet-Frame (Datenpaket) befinden sich die MAC-Adressen von Sender (Quelle) und Empfänger (Ziel). Beim Empfang eines Frames vergleicht die Empfangseinheit der empfangenden Station die MAC-Zieladresse mit der eigenen MAC-Adresse. Erst wenn die Adressen übereinstimmen, reicht die Empfangseinheit den Inhalt des Frames an die höherliegende Schicht weiter. Wenn keine Übereinstimmung vorliegt, dann wird das Frame verworfen.

Aufbau einer MAC-Adresse

Alle bekannten Zugriffsverfahren mit einer MAC-Schicht (IEEE 802.1), zum Beispiel WLAN, Bluetooth, Ethernet, Token Bus, Token Ring oder FDDI verwenden das gleiche MAC-Adressformat mit 48 Bit langen MAC-Adressen.

Bezeichnung	I/G	U/L	OUI	OUA
Bit	1.	2.	3. - 24.	25. - 48.
Bedeutung	Hersteller-Kennung			Geräte-Kennung

Die ersten beiden Bit der MAC-Adresse kennzeichnen die Art der Adresse. Das erste Bit hat eine besondere Bedeutung. Ist es gesetzt, dann handelt es sich um eine Gruppe von Rechnern (Multicast). Eine Adresse, bestehend aus lauter Einsen ist eine Broadcast-Adresse. Damit werden alle Rechner angesprochen.

- I/G = 0: Individual-Adresse (Unicast Address), Adresse für einen Netzwerkadapter
- I/G = 1: Gruppen-Adresse (Multicast Address), Ziel-Adresse für eine Gruppe von Stationen
- U/L = 0: universelle, weltweit eindeutige und unveränderbare Adresse
- U/L = 1: lokal veränderbare Adresse

Vom 3. bis zum 24. Bit wird der Hersteller der Netzwerkkarte gekennzeichnet. Man bezeichnet diese Bitfolge als Organizationally Unique Identifier (OUI). Da bei universellen Individual-Adressen die ersten beiden Bit auf "0" stehen, werden sie häufig in den OUI mit einbezogen.
IEEE vergibt die Adressbereiche der ersten 24 Bit an anfragende Organisationen. Zum Beispiel Hersteller von Hardware.
Die hinteren 24 Bit, also vom 25. bis zum 48. Bit, bezeichnet man als Organizationally Unique Address (OUA). Die darf der Hersteller an seine produzierten Geräten vergeben. Er muss nur dafür sorgen, dass er jede MAC-Adresse nur einmal vergibt.
Aktuell geht man davon aus, dass die 48-Bit-Adressen bis ins Jahr 2100 reichen.

Darstellung einer MAC-Adresse

Die 48 Bit der MAC-Adresse lässt sich als Bitfolge oder in kanonischer Form darstellen. Weil die Darstellung als Bitfolge zu lang ist, teilt man die 48 in 6 Oktette (jeweils 8 Bit) auf. Jedes Oktett wird dann als eine

zweistellige hexadezimale Zahl dargestellt. Wichtig ist, vor der Umformung der dualen in die hexadezimale Darstellung wird das Oktett umgedreht (gespiegelt).
Bei der hexadezimalen Darstellung werden die hexadezimalen Zeichenpaare durch Bindestriche getrennt. Üblich ist auch die Darstellung mit Doppelpunkten. Das kann zu Verwechslungen mit IPv6-Adressen führen.

Beispiel für eine Umformung:

00110101 -> 10101100 = [1010][1100] = AC (hex)

	Bitfolge	Kanonische Form
Beispiel 1	00110101 01111011 00010010 00000000 00000000 00000001	AC-DE-48-00-00-80
Beispiel 2	01001000 00101100 01101010 00011110 01011001 00111101	12-34-56-78-9A-BC

MAC-Multicast- und MAC-Broadcast-Adressen

Gelegentlich kommt es vor, dass ein Ethernet-Frame an mehrere Stationen (Multicast) oder alle Stationen (Broadcast) eines Netzwerks gesendet werden soll. Für diesen Zweck gibt es eine entsprechende Multicast- und Broadcast-Adressen. Sie existieren nur als Ziel-Adressen. Für spezielle Anwendungen gibt es standardisierte Multicast-Adressen. Für Broadcasts (Ethernet-Frames an alle Stationen) gibt es aber nur eine einzige Adresse. Sie lautet:

	Bitmuster	Kanonische Form
Broadcast-Adresse	11111111 11111111 11111111 11111111 11111111 11111111	FF-FF-FF-FF-FF-FF

Broadcasts können ein Netz sehr stark belasten, da in diesem Fall das ganze Netz für einen Augenblick mit einem einzigen Datenpaket belegt ist. Bei einem Broadcast-Sturm kann ein Netz sogar ganz zum Erliegen

kommen. Nach Möglichkeit vermeidet man Broadcasts über Netzgrenzen hinweg.

Fast-Ethernet / IEEE 802.3u

Fast-Ethernet gehört zu einer Familie von Netzwerktechniken, die vorwiegend in lokalen Netzwerken zum Einsatz kommen. Ethernet ist aber auch für die Verbindung großer Netzwerke geeignet. Fast-Ethernet ist sowohl für Glasfaserkabel und Twisted-Pair-Kabel entwickelt und spezifiziert. Die verschiedenen Fast-Ethernet-Varianten erlauben die Übertragung von Daten mit 100 MBit/s in beide Richtungen (Vollduplex).

In der Regel haben alle Computer, egal ob PC oder Notebook eine Ethernet-Schnittstelle, die sowohl 10Base-T als auch 100Base-TX (Fast-Ethernet) beherrscht. Manchmal sogar Gigabit-Ethernet. Der Spitzendurchsatz von 100 MBit/s entspricht rund 10 MByte/s.

IEEE 802.3x / Flow Control

Weil Fast-Ethernet in der Regel im Vollduplex-Modus arbeitet und damit auf CSMA/CD verzichtet, ist eine zusätzliche Flusssteuerung erforderlich. Der Grund: Wenn ein Host zu viele Datenpakete bekommt und mit der Verarbeitung nicht mehr nachkommt, dann besteht die Gefahr, dass die Datenpakete teilweise verworfen werden. Mit der Flusssteuerung kann dieser Host der Gegenstelle signalisieren, eine Sendepause einzulegen. Die betroffene Host schickt dem Verursacher ein PAUSE-Paket. Entweder an eine spezielle Multicast-MAC-Adresse oder direkt an die MAC-Adresse des Verursachers. Im PAUSE-Paket steht dann die gewünschte Wartezeit.

Beispiel: Ein Switch hat 32 Gigabit-Ports, aber nur 10 GBit/s interne Bandbreite. Mit einem PAUSE-Paket kann der Switch den Hosts mitteilen, dass sie mit einer geringeren Übertragungsrate senden sollen. Wenn die Hosts sich daran halten, dann verwirft der Switch weniger Datenpakete. So wird verhindert, dass das Netzwerk mit wiederholt gesendeten Datenpaketen überflutet wird.

Broadcastdomäne

Dank Punkt-zu-Punkt-Verbindung und Flow Control spielt das Thema Kollisionen und Kollisionsdomäne bei Ethernet keine Rolle mehr. Allerdings spricht man bei Fast Ethernet noch von einer Broadcastdomäne.
Broadcasting ist das Verhalten eines Switches, um unbekannte Empfänger zu ermitteln. Bekommt ein Switch ein Datenpaket, dessen Empfänger er keinem Port zuordnen kann, dann verhält der Switch sich für dieses eine Paket wie ein Hub und sendet es an alle Ports. Das heißt, er sendet einen Broadcast bzw. er broadcastet. In der Regel kommt dann auf einem Port das Antwortpaket und der Switch weiß dann, an welchen Port er alle weiteren Pakete schicken soll.
Die Reichweite des Broadcastings bezeichnet man als Broadcastdomäne. Sie umfasst alle Host, die auf Schicht 1 und 2 erreichbar sind.
Die Broadcastdomäne endet dort, wo der Übergang in ein anderes Netzwerk über ein anderes Protokoll erfolgt. In der Regel an einem Router.

Auto-Negotiation

Mit Auto-Negotiation können Ethernet-Hosts automatisch die Ethernet-Variante der Gegenstelle am anderen Ende der Leitung erkennen. Häufig wird Auto-Negotiation auch als Auto-Sensing bezeichnet. Dieser Begriff ist allerdings missverständlich und sollte daher nicht verwendet werden. Auto-Negotiation wurde deshalb notwendig, weil der Umstieg von 10Base-T auf 100Base-TX in der Regel in einem Mischbetrieb endete. Aus diesem Grund beherrschen Fast-Ethernet-Komponenten durchgängig Auto-Negotiation.

Um Probleme mit Auto-Negotiation zu vermeiden, sollte man die Netzwerk-Stationen entweder mit Auto-Negotiation betreiben oder auf eine feste Übertragungsart einstellen. Probleme treten in der Regel nur dann auf, wenn man Vollduplex- und Halbduplex-fähige Komponenten mischt.
Bei den Glasfaser-Varianten ist Auto-Negotiation nicht definiert. Hier muss man Voll- oder Halbduplex manuell einstellen.

Gigabit-Ethernet / 1000Base-T / IEEE 802.3z / IEEE 802.3ab

Gigabit-Ethernet gehört zu einer Familie von Netzwerktechniken, die vorwiegend in lokalen Netzwerken zum Einsatz kommen. Gigabit-Ethernet ist aber auch für die Verbindung großer Netzwerke geeignet. Gigabit-Ethernet wurde erst für Glasfaserkabel, später auch für Twisted-Pair-Kabel entwickelt und spezifiziert. Beide Varianten erlauben die Übertragung von Daten mit 1.000 MBit/s bzw. 1 GBit/s. Das ist eine Steigerung um den Faktor 10 gegenüber Fast-Ethernet mit 100 MBit/s.

Fast-Ethernet galt lange Zeit als "der" Standard für die lokale Vernetzung. Doch wer denkt, dass Fast-Ethernet mit 100 MBit/s vollkommen ausreichend ist, der irrt. Wenn Daten im Netzwerk gespeichert werden, dann ist das 100-MBit-Netz ein Flaschenhals. 1 GBit/s ist ein Muss, wenn man Server und Speichergeräte in ein Netzwerk einbinden will und viele Netzwerk-Teilnehmer darauf zugreifen sollen.
Viele verschiedene Anwendungen (z. B. Internet, Multimedia, elektronischer Dokumentenaustausch) verursachen eine hohe Netzlast. Deshalb ist es notwendig, die zentralen Netzwerk-Stationen, wie z. B. Router, Server und Switche mit mehr Bandbreite zu verbinden, als es bei den meisten Hosts nötig ist.

IEEE 802.3ab / Gigabit Ethernet über Twisted-Pair-Kabel

1000Base-T ist eine Erweiterung von IEEE 802.3z. Der Standard beschreibt auf der physikalischen Schicht des OSI-Schichtenmodells, wie und in welcher Form Daten auf dem Kabel übertragen werden. Alle weiteren Funktionen von Ethernet, dazu gehört auch das Zugriffsverfahren, sind auf dem MAC-Layer definiert.
Gigabit-Ethernet ist zu 100 MBit/s und 10 MBit/s abwärtskompatibel. Außerdem beherrscht Gigabit-Ethernet Auto-MDI/X. Das bedeutet, Gigabit-Ports erkennen automatisch eine Uplink-Verbindung. Gigabit-Switche haben deshalb keinen Uplink-Port mehr. Cross-Over-Patchkabel sind nicht mehr notwendig.

Im Netzwerkbereich spielt die Verkabelung eine wichtige Rolle. Sie ist neben den Kopplungselementen der teuerste und aufwendigste Teil der gesamten Installation. Nur ungern tauscht man eine Netzwerk-

Verkabelung aus. Vor allem, wenn es nicht dringend notwendig ist. Ein neues Übertragungssystem lässt sich in diesem Bereich leichter einführen, wenn nicht gleich die komplette Verkabelung ausgetauscht werden muss. Von Vorteil ist, dass bei der Einführung von Gigabit-Ethernet die vorhandene strukturierte Verkabelung (Twisted-Pair-Kabel) übernommen werden kann. Vorausgesetzt, die Kabel sind dafür spezifiziert.
1000Base-T wurde von Anfang an so ausgelegt, dass es mit der RJ45-Steckverbindungen benutzt werden kann. Im Gegensatz zu Fast-Ethernet braucht Gigabit-Ethernet alle vier Adernpaare eines Kabels.

Vom Grundsatz her, ist Gigabit-Ethernet für den Einsatz mit CAT5-Leitungen ausgelegt. Doch CAT5 ist nicht gleich CAT5. 1000Base-T stellt hohe Anforderungen an die Kabelinstallation. In Einzelfällen scheitert 1000Base-T auf CAT5. Wenn bei der Abnahmemessung der Verkabelung die Anforderungen von 1000Base-T noch nicht berücksichtigt wurden, dann kann man nur durch eine Nachmessung feststellen, ob eine CAT5-Verkabelung Gigabit-Ethernet-tauglich ist.
Für kurze Strecken bis 10 Meter, kann man auf alle Fälle normale CAT5-Kabel verwenden. Ab 10 Meter sollte es mindestens CAT5e sein, um eine stabile und störungsfreie Verbindung herstellen zu können. Sonst kann es passiert, dass die Gigabit-Verbindungen auf Fast-Ethernet mit 100 MBit/s zurückfallen.

IEEE 802.3bz / NBase-T (2,5GE und 5GE)

IEEE 802.3bz ist ein Ethernet-Standard für Next Generation Enterprise Access BASE-T PHY, kurz NBase-T, der Ethernet mit 2,5 GBit/s und 5 GBit/s auf Twisted-Pair-Kabeln ermöglicht.
Der Grund für die zwei Zwischenschritte zwischen 1 und 10 GBit/s ist die Anforderung, Wireless Access Points (WAP) mit Datenraten über 1 GBit/s mit nur einem Twisted-Pair-Kabel verlustfrei an ein lokales Netzwerk anzubinden.

Bei der effektiven Anbindung von WLANs mit IEEE 802.11ac der Entwicklungsstufe Wave 2 (über 1 GBit/s) müsste man zwei Gigabit-Ports mit Link Aggregation (2 GBit/s) oder auf 10-Gigabit-Ethernet mit 10 GBit/s inkl. TP-Kabel der Kategorie 6A umstellen.
Zwei Gigabit-Ports müsste man mit zwei TP-Kabeln bedienen, was den Verkabelungsaufwand verdoppelt bzw. in bestehenden Verkabelungen

nicht vorgesehen war.
Die Variante mit 10GBase-T (10-GBit/s-Ethernet, 10GE) ist viel zu teuer und erfordert TP-Kabel mit CAT6A, die nicht überall vorhanden sind. Außerdem benötigt die 10GBaseT-Technik viel mehr Energie.
Beides sind Techniken, die WAPs und Switche teurer machen und deshalb nur im Enterprise-Bereich, aber nicht im Privat-Bereich Sinn machen. Deshalb bedarf es hier Zwischenschritte, damit auf herkömmlicher CAT5-Verkabelung über 100 Meter eine Ethernet-Verbindung zwischen 1 und 10 GBit/s möglich ist.

10-Gigabit-Ethernet / 10GE / IEEE 802.3ae / IEEE 802.3an

10-Gigabit-Ethernet gehört zu einer Familie von Netzwerktechniken, die vorwiegend in lokalen Netzwerken zum Einsatz kommt. Ethernet eignet sich auch zur Verbindung großer Netzwerke. 10-Gigabit-Ethernet wurde erst für Glasfaserkabel, später auch für Twisted-Pair-Kabel entwickelt und spezifiziert. Die verschiedenen Varianten erlauben die Übertragung von Daten mit 10 GBit/s. Das ist eine Steigerung um den Faktor 10 gegenüber Gigabit-Ethernet mit 1 GBit/s.

10-Gigabit-Ethernet ist weniger ein Übertragungssystem im lokalen Netz (LAN - Local Area Network). Zwar hat 10-Gigabit-Ethernet auch in lokalen Netzwerken seine Berechtigung. Zum Beispiel für HPC-Clustering, SAN, Server-Anbindungen und Backbone-Verbindungen. Entwickelt wurde es jedoch unter anderem deshalb, um ATM in Weitverkehrsnetzen (WAN - Wide Area Network) abzulösen. 10-Gigabit-Ethernet konkurriert also auch mit SONET (Synchronous Optical Network) und SDH (Synchronous Digital Hierarchy).
Um den Standard flexibel zu halten und einen breiten Einsatz zu ermöglichen, unterstützt er gleich 7 verschiedene Glasfasertypen. 10-Gigabit-Ethernet ist praktisch unabhängig vom eingesetzten Glasfaserkabel.

Jumbo-Frame

Jumbo-Frames wurden bereits bei 1GBase-T eingeführt, sind jedoch in 10GBase-T standardisiert. Man kann sie aktivieren, ohne das es zu Problemen bekommt. In Jumbo-Frames passen bis zu 9014 Byte

Nutzdaten in ein Ethernet-Frame. Vorher waren es nur 1500 Byte. Der Anteil des Overheads an der Übertragung hat sich durch Jumbo-Frames reduziert.

10GBase-T nutzt alle vier Adernpaare des Twisted-Pair-Kabels. Die 10 GBit/s sind auf 4 Adernpaare aufgeteilt. Das sind 2,5 GBit/s pro Adernpaar. Eine solche Übertragungsrate ist mit einem binären Übertragungsverfahren nicht möglich. Deshalb werden pro Taktschritt mehrere Bit übertragen. Die Grenzfrequenz von 10GBase-T ist auf 500 MHz festgelegt. Die Maximalfrequenz ist also vom Kabel vorgegeben. Geeignet sind CAT6A-, $CAT6_A$- oder CAT7-Kabel. Mit Abstrichen in der Reichweite auch CAT6 und CAT5(e).

Kabelinstallation für 10GBase-T

Kategorie	Grenzfrequenz	Reichweite	Anmerkung
CAT5(e)	100 MHz	~ 22 m	nicht spezifiziert
CAT6	250 MHz	~ 30 m	nicht spezifiziert
CAT6A	500 MHz	~ 55 m	nicht spezifiziert
CAT7	600 MHz	100 m	

25-Gigabit-Ethernet

Mit 25GBASE-T SG (25 GBit/s) gibt es eine Arbeitsgruppe, die an einem Zwischenschritt zwischen 10GE und 40GE arbeitet. Es geht um Kostenersparnis im Rechenzentrum, wo durch Virtualisierung Server effizienter ausgelastet werden und 10GE zum Engpass wird, Link Aggregation zu aufwändig und 40GB zu teuer ist.

40- und 100-Gigabit-Ethernet / IEEE 802.3ba

40-Gigabit- und 100-Gigabit-Ethernet (40GE und 100GE) gehören zu einer Familie von Netzwerktechniken, die vorwiegend in lokalen Netzwerken zum Einsatz kommen. Die auf Ethernet basierende lokale Netzwerktechnik eignet sich auch zur Verbindung großer Netzwerke. Der

Standard IEEE 802.3ba umfasst 40-Gigabit- und 100-Gigabit-Ethernet und ist der erste Ethernet-Standard, in dem zwei Geschwindigkeitsstufen definiert sind. IEEE 802.3ba ist für Entfernungen bis 40 km ausgelegt.

Auf dem Weg zum 100-Gigabit-Ethernet ist 40 Gigabit nur ein Zwischenschritt. Der ist deshalb notwendig, weil 100 Gigabit technisch sehr anspruchsvoll und teuer in der Implementierung ist. Lange Zeit gab es nicht genug Nachfrage für höhere Geschwindigkeiten, da sich 10-Gigabit-Ports kostengünstig bündeln lassen. 100 GBit/s kann man zum Beispiel dadurch erreichen, dass 10 x 10 GBit/s gebündelt werden. Doch das ist für den Einsatz in Weitverkehrsnetzwerken nicht praktikabel und auch nicht wirtschaftlich.

Die 40-GBit-Technik ist bei optischen Weitverkehrsstrecken (WAN) seit Jahren etabliert. Mit ihr konnte der Breitbandbedarf von Netzwerk- und Datenzentren-Betreibern befriedigt werden.
Netzwerk-Betreiber würden 100-Gigabit-Ethernet zum Beispiel zur schnellen Verbindung in Rechenclustern, zum Vernetzen von Massenspeichern oder im Internet-Backbone der nächsten Generation favorisieren. Für die Zukunft müssen die Netzbetreiber den steigenden Anforderungen durch Videoübertragungen oder Cloud Computing gewachsen sein. Außerdem sinkt mit 100 Gigabit die Zahl der pro Router erforderlichen Ports. Ohne 100-Gigabit-Ports sind Datenraten über 10 GBit/s nur umständlich über mehrere parallele 10-GBit-Verbindungen möglich.

100-Gigabit-Ethernet über Kupferkabel?

Die Übertragung von 10 GBit/s über Kupfer galt schon als technisch sehr anspruchsvoll. Eine weitere Steigerung gilt als nahezu unmöglich. Kupferkabel sollen bei beiden Geschwindigkeitsstufen auf Twinax-Kabel für Strecken von maximal zehn Metern möglich sein (100GBASE-CR10). Es ist aber bereits im Gespräch, dass bei einer Kabellänge von 70 Metern 100 GBit/s auf Cat-7-Kabel machbar ist. Mit IEEE 802.3bq ist ein Standard für 40 GBit/s über Kupferkabel (40GBase-T) in Arbeit.

Das Problem: Die heutigen Chips mit einer 65-nm-Strukturbreite sind für diese Transmitter/Receiver ungeeignet. Bis es ein 100-Gigabit-Ethernet für Kupferkabel gibt, müssen noch zwei bis drei Chip-Generationen ins

Land gehen. Hinzu kommt, dass 100GE auf Twisted-Pair-Kabel, falls überhaupt technisch machbar, ökonomisch völlig unsinnig ist.

Power-over-Ethernet (PoE)

Hinter Power-over-Ethernet stehen standardisierte Verfahren, um Netzwerk-Endgeräte über das Netzwerk-Kabel mit Strom zu versorgen. Die Stromversorgung von Endgeräten in der Netzwerktechnik liegt im Einflussbereich der Hersteller der Endgeräte. Die lösen die Stromversorgung von Geräten mit geringen Leistungen meist über Steckernetzteile. Das bedeutet, neben jeder Netzwerkdose muss auch eine 230V-Steckdose sitzen.
Ethernet nimmt nicht nur für die lokale Netzwerkverkabelung, sondern auch für Sicherheitsnetzwerke eine führende Position ein. Da immer mehr Geräte über eine Ethernet-Schnittstelle verfügen, ist vorstellbar, dass man darüber auch gleich die Stromversorgung abwickelt. Mit Power-over-Ethernet (PoE) entfällt der separate Stromanschluss und Steckernetzteile für die Stromversorgung. Zum Beispiel für Webcams und WLAN-Access-Points.

PoE-Standards: IEEE 802.af / IEEE 802.3at / IEEE 802.3bt

PoE-Standard / IEEE		Leistung pro Port	nutzbare Leistung
PoE	802.3af	15,4 Watt	12,95 Watt
PoE+	802.3at	25,4 Watt	21,90 Watt
PoE++ / 4PPoE	802.3bt		70 bis 100 Watt

Der Hauptvorteil der Power-over-Ethernet-Spezifikationen besteht darin, dass die bestehende Netzwerkverkabelung mit Twisted-Pair weiterverwendet werden kann. Die physikalischen Grenzen der Netzwerkkabel wurden bei der Ausarbeitung der PoE-Standards berücksichtigt. Das bedeutet aber auch, dass sich Twisted-Pair-Kabel wegen ihres geringen Leitungsquerschnitts und der RJ45-Stecker nur für eine bestimmte maximale Leistung eignen. Die beiden Standards beschreiben exakt, wie viel Strom über das Netzwerkkabel fließen darf und sehen auch den Schutz von Altgeräten ohne PoE-Unterstützung vor.

IEEE 802.3af / Power-over-Ethernet (PoE)

Der Standard IEEE 802.3af gilt nur für 10Base-T und 100Base-TX. Das bedeutet, dass nur die Adernpaare 1/2 und 3/6 für die Datenübertragung genutzt werden und die beiden anderen Adernpaare unbenutzt sind. Vorgesehen ist deshalb, die beiden freien Adernpaare für die Energieversorgung zu nutzen. Alternativ sollen die mit Datenübertragung belegten Adern mit der Stromversorgung überlagert werden.
Weil RJ45-Stecker und Twisted-Pair-Kabel nicht für Ströme im Ampere-Bereich ausgelegt sind, wird eine Spannung zwischen 44 V und 57 Volt, im Mittel 48 Volt, verwendet, was den Anforderungen an eine Schutzkleinspannung entspricht. Je Adernpaar ist ein Strom von maximal 175 mA vorgesehen. Bei zwei Adernpaaren ist das in Summe ein Strom von 350 mA. Beim Einschalten sind kurzzeitig 400 mA erlaubt. Die maximale Leistungsaufnahme beträgt 15,4 Watt pro Switch-Port.
Durch die relativ hohe Spannung bleibt die Verlustleistung und damit die Wärmeentwicklung in den Kabeln und an den Steckerübergängen gering. Trotzdem kommt es zu Verlusten auf der Leitung. Der Standard geht davon aus, dass am Ende einer 100 Meter langen Leitung von eingespeisten 15,4 Watt etwa 12,95 Watt nutzbare Leistung übrig bleibt. Manche PoE-Switches stellen auch 30 Watt pro Port zur Verfügung. Sie arbeiten damit außerhalb der Spezifikation.
Doch schon bei einer maximalen Entnahmeleistung von 12,95 Watt eignet sich diese Technik hervorragend um Webcams, Print-Server, IP-Telefone (Voice-over-IP), WLAN-Access-Points, Handheld-Computer und sparsame Notebooks mit Strom zu versorgen. Den größten Nutzen haben Access-Points und Webcams.

IEEE 802.at / Power-over-Ethernet-Plus (PoE+ / PoE Plus)

Mit IEEE 802.at eignet sich Power-over-Ethernet auch für 1000Base-T. Gleichzeitig wird die Leistung fast verdoppelt.
IEEE 802.at verspricht eine Leistung bis 25,5 Watt pro Port. Dabei wird die Minimalspannung von 44 auf 50 Volt erhöht. Der maximale Strom wurde von 350 mA auf 600 mA erhöht. Bei diesen hohen Leistungen wird ein Cat5e/6-Kabel empfohlen. Das hat einen geringeren Widerstand.
Die 25,5 Watt Leistung steht dem Endgerät nicht direkt zur Verfügung. Man muss noch die Verluste zwischen Ethernet-Eingangsbuchse und dem Ausgang des Spannungsreglers abziehen. Man spricht von einem

Wirkungsgrad von etwa 85%, was einer Leistung von etwa 21,90 Watt entspricht.

Für PoE+ gibt es momentan kaum sinnvolle Anwendungen. Den meisten PoE-Geräten reichen 10 oder 100 MBit/s vollkommen aus. Viel interessanter ist die höhere Leistung.

IEEE 802.3bt / Four-Pair-Power-over-Ethernet (4PPoE / PoE++)

Den Standard IEEE 802.3bt bezeichnet man als Four-Pair-Power-over-Ethernet. Die Kurzschreibweise 4PPoE oder PoE++.
Bisher nutzt Power-over-Ethernet nur zwei der vier Aderpaare eines Twisted-Pair-Kabels. Mit 4PPoE werden alle Adern der vorhandenen Kabel zur Leistungsübertragung verwendet. Damit steigt die Leistung auf 70 bis 100 Watt. Der RJ45-Stecker wird wie der USB zum global normierten Steckverbinder für die elektrische Energieversorgung für Endgeräte.

Die Idee von PoE++ ist es den ganzen Arbeitsplatz mit Strom zu versorgen. Mit 100 Watt könnte man komplette Rechner mit Bildschirm inklusive Telefon über ein LAN-Kabel betreiben.

Varianten der Energieversorgung

- Endspan: direkte Versorgung durch PoE-Switch
- Midspan: Versorgung über zwischengeschaltete Quellen, Beispiel: PoE-Injektor

Varianten der Energieeinspeisung

- Mode A: Strom über von Daten genutzten Adernpaare (Phantom- oder Fern-Speisung)
- Mode B: Strom über von Daten ungenutzten Adernpaare (Spare-Pairs-Verfahren)

IEEE 802.11 / WLAN-Grundlagen

IEEE 802.11 ist eine Gruppe von Standards für ein Funknetzwerk auf Basis von Ethernet. Damit ist IEEE 802.11 das am weitesten verbreitete drahtlose Netzwerk bzw. Technik für ein Wireless Local Area Network (WLAN).

Seit 1997 gibt es mit IEEE 802.11 erstmals eine verbindliche Luftschnittstelle für lokale Funknetzwerke. Davor war der breite Einsatz lokaler Funknetzwerke wegen der fehlenden Standardisierung und der geringen Datenübertragungsrate undenkbar. Der Standard baut auf den anderen Standards von IEEE 802 auf. IEEE 802.11 ist, vereinfacht ausgedrückt, eine Art schnurloses Ethernet. IEEE 802.11 definiert die Bitübertragungsschicht des OSI-Schichtenmodells für ein Wireless LAN. Dieses Wireless LAN ist, wie jedes andere IEEE-802-Netzwerk auch, vollkommen Protokoll-transparent. Drahtlose Netzwerkkarten lassen sich deshalb ohne Probleme in jedes vorhandene Ethernet einbinden. So ist es mit Einschränkungen (Zuverlässigkeit und Geschwindigkeit) möglich, eine schnurgebundene Ethernet-Verbindung nach IEEE 802.3 durch eine WLAN-Verbindung nach IEEE 802.11 zu ersetzen.

IEEE 802.11 ist der ursprüngliche Standard, der Übertragungsraten von 1 oder 2 MBit/s ermöglicht. Darauf aufbauend wurde der Standard laufend erweitert. Hauptsächlich um die Übertragungsrate und die Datensicherheit zu erhöhen und die Zusammenarbeit zwischen den Geräten unterschiedlicher Hersteller zu verbessern.

WLAN (Wireless LAN) oder IEEE 802.11

Gelegentlich wird die Bezeichnung "Wireless LAN" und der Standard "IEEE 802.11" durcheinander geworfen. Der Unterschied ist dabei ganz einfach. "Wireless LAN" ist die allgemeine Bezeichnung für ein schnurloses lokales Netzwerk (Wireless Local Area Network). "IEEE 802.11" dagegen ist ein Standard für eine technische Lösung, die den Aufbau eines Wireless LAN ermöglicht. Es ist also durchaus denkbar, dass es noch andere Standards gibt, mit denen ein Wireless LAN aufgebaut werden kann.
Allerdings hat es sich im allgemeinen Sprachgebrauch durchgesetzt, ein

lokales Funknetzwerk, dass auf dem Standard "IEEE 802.11" basiert als Wireless LAN bzw. WLAN zu bezeichnen.

Übersicht: Übertragungsgeschwindigkeit

Standard	Frequenzen	Streams	Datenrate (brutto)
802.11	2,4 GHz	1	2 MBit/s
802.11b	2,4 GHz	1	11 MBit/s
802.11a/h/j	5 GHz	1	54 MBit/s
802.11g	2,4 GHz	1	54 MBit/s
802.11n	2,4	1 2 3 4	150 MBit/s 300 MBit/s 450 MBit/s 600 MBit/s
	5 GHz	1 2 3 4	150 MBit/s 300 MBit/s 450 MBit/s 600 MBit/s
802.11ac	5 GHz	1 2 3 4 5...8	433 MBit/s 867 MBit/s 1.300 MBit/s 1.733 MBit/s bis 6.936 MBit/s
802.11ad	60 GHz	1	4.620 MBit/s 6.757 MBit/s

Erläuterung zu den Datenraten von WLAN

Schaut man sich die Angaben der Hersteller und Händler zur Bruttodatenrate ihrer Produkte an und vergleicht die Werte, die man damit in der Praxis erreicht, riecht das fast schon nach einem Reklamationsgrund. Tatsache ist, dass die Bruttodatenraten, wie sie auf

den Produktverpackungen und vom Standard angegeben sind, in der Praxis nie erreicht werden können.

Dazu muss man wissen, dass alle WLAN-Standards des IEEE mit ihrer theoretisch maximalen Übertragungsgeschwindigkeit spezifiziert werden. In der Praxis sind die angegebenen Übertragungsraten aber viel geringer, als angegeben. So erreichen WLANs nach IEEE 802.11g mit 54 MBit/s in der Praxis selten mehr als 16 MBit/s. Ein WLAN nach IEEE 802.11n mit 150, 300, 450 und 600 MBit/s erreicht selten mehr als die Hälfte davon. Der Standard IEEE 802.11ac verspricht brutto eine Datenrate von sagenhaften 7 GBit/s. Doch diese Werte sind davon abhängig, welche Funkkanalbreite, Übertragungsart und die Anzahl der Antennen verwendet wird. Doch auch das ist reine Theorie. Denn in der Praxis muss jede Funktechnik mit weiteren Einschränkungen kämpfen. So ist die Funkkanalbreite begrenzt, ebenso die Anzahl der Antennen. Das heißt, die typischen Datenraten liegen darunter und aufgrund spezifischer Funkbedingungen in der Praxis noch weiter darunter.
Doch auch das sind nur Richtwerte. Was in der Praxis dann wirklich möglich ist, ist von den lokalen Begebenheiten abhängig. Decken, Wände, Möbel und andere Funknetzwerke stören die Funkübertragung eines WLANs. Je nach Umgebungsbedingungen, Anzahl der teilnehmenden Stationen und deren Entfernung erreicht man auch nur einen Bruchteil der typischen Datenrate.

Die Differenz zwischen der Brutto-Übertragungsgeschwindigkeit und dem, was in der Praxis tatsächlich möglich ist, ist der Tatsache geschuldet, dass es sich bei Funk um einen geteilten Übertragungskanal handelt, den mehrere Teilnehmer gleichzeitig nutzen müssen und deshalb ein spezielles Verfahren den Zugriff darauf aushandelt. Das CSMA/CA genannte Verfahren regelt wann eine Station senden darf. Die anderen Stationen müssen während dieser Zeit warten. Anschließend fällt dann noch eine Pause an. Die Funkschnittstelle ist deshalb nie zu 100% belegt. Für jeden einzelnen Teilnehmer bedeutet das, es bleibt nur ein Bruchteil der typischen Übertragungsgeschwindigkeit übrig.

WLAN-Standards von IEEE 802.11

Im September 1990 begann eine Arbeitsgruppe des IEEE an einem Standard für drahtlose Netzwerke mit 1 MBit/s im Frequenzbereich 2,4

GHz zu arbeiten. Dabei entstand ein Protokoll und Übertragungsverfahren für drahtlose Netzwerke. Der Standard IEEE 802.11 fand schnell Akzeptanz und fand eine rasche Verbreitung.
Innerhalb weniger Jahre entstanden Erweiterungen der Funktechnik, die vor allem, aber nicht nur, die Übertragungsrate auf der Funkschnittstelle steigerten.

WLAN-Sicherheit und Verschlüsselung

Funksignale bewegen sich im freien Raum. Das bedeutet, jeder kann die gesendeten Daten abhören oder stören. Um zumindest das Abhören zu verhindern, werden WLANs mit Authentifizierung und Verschlüsselung betrieben.
Ein weiterer Knackpunkt ist die Nutzung des WLANs und die Nutzung des damit bereitgestellten Internet-Anschluss durch fremde Personen. Der Betreiber eines ungesicherten WLANs kann rechtlich in die Verantwortung und damit Haftung genommen werden, wenn ihm unbekannte Personen seinen Internet-Zugang für Rechtsverletzungen missbrauchen. Dazu haben bereits die Landgerichte Hamburg (2006) und Düsseldorf (2008) geurteilt. Es gibt zwar auch gegenteiligen Urteile. Doch es empfiehlt sich, gerichtliche Auseinandersetzungen im Voraus zu vermeiden. Deshalb sollte die Verschlüsselung immer aktiviert sein. Vorzugsweise WPA2. Die älteren Verschlüsselungsverfahren WPA und WEP sollte man nicht mehr verwenden. WLAN-Geräte, die WPA2 nicht beherrschen, sollte man dringend austauschen.

WLAN-Authentifizierung

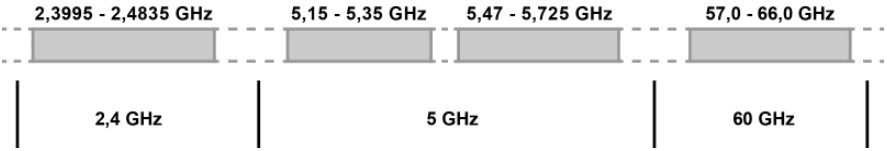
Nicht jeder soll ein WLAN nutzen dürfen. Zwar kann der Zugriff auf ein WLAN durch ein Passwort eingeschränkt werden. Doch ist das Passwort erst einmal bekannt, dann ist damit nicht nur der Zugriff, sondern auch die Verschlüsselung ungesichert.
Zusätzlich zur Verschlüsselung kann bei größeren WLANs mit vielen Nutzern eine zusätzliche Authentifizierung mit dem Protokoll IEEE 802.1x integriert werden, bei der jeder Nutzer eigene Zugangsdaten benötigt (Benutzername und Passwort). An einer zentralen Stelle kann der Zugriff auf einfache Art und Weise freigegeben oder eingeschränkt werden.

Die Entsprechenden Einstellungen stehen häufig im begrifflichen Zusammenhang mit WPA2-Enterprise oder WPA2-RADIUS.

IEEE 802.11 vs. Bluetooth

Während der Entwicklung des WLAN-Standards IEEE 802.11 und Bluetooth haben sich schnell Gemeinsamkeiten herausgestellt. Beide Funkstandards arbeiten im Frequenzband 2,4 GHz und sollen unterschiedliche Geräte über Funk miteinander verbinden. Beide Standards zeichnen sich durch individuelle Stärken aus und kommen dadurch in verschiedenen Geräten auf den Markt.
Wireless LAN übertrifft Bluetooth in seiner Reichweite und Übertragungsgeschwindigkeit und kommt deshalb in lokalen Netzwerken zum Einsatz.
Bluetooth ist mit geringen Hardwarekosten, niedrigem Stromverbrauch und Echtzeitfähigkeit in den Bereichen Sprachübertragung, Audio-Video-Lösungen und Adhoc-Verbindungen zwischen Kleinstgeräten besser geeignet. Bluetooth löst hier Irda (Infrarot) erfolgreich ab. Und Bluetooth 3.0 macht sich WLAN-Techniken zunutze, um große Datenmengen zu übertragen.

WLAN-Frequenzen und -Kanäle



Für WLANs nach IEEE 802.11 stehen drei Frequenzbereiche zur Verfügung. Der meistgenutzte Bereich liegt bei 2,4 GHz, der zweite bei 5 GHz und der dritte bei 60 GHz. Alle Frequenzbereiche sind weltweit Lizenz-frei nutzbar. Das bedeutet, dass auf privatem Grund und Boden für die Nutzung keine Gebühren bezahlt werden müssen. Das bedeutet aber auch, dass sich in diesen Frequenzbereichen auch andere Funktechniken und Funknetze tummeln. Die Geschwindigkeit und Stabilität eines Funknetzwerks mit IEEE 802.11 hängt maßgeblich von der Intensität der Nutzung anderer Funktechniken im gleichen Frequenzband ab.

	2,4 GHz	5 GHz	60 GHz
Frequenzen	Von 2,3995 bis 2,4845	Von 5,150 bis 5,350 Von 5,470 bis 5,725	Von 57,0 bis 66,0
Reichweite	akzeptabel (Haus)	begrenzt (Wohnung/Stockwerk)	gering (Raum)
Kanalbreite	20 und 40 MHz	20, 40, 80, 160 MHz	2 GHz
Nutzung	stark überfüllt	gering	selten

Hinweis: Weltweit ist die Nutzung der Frequenzbereiche für WLAN nach IEEE 802.11 unterschiedlich geregelt. Die hier gemachten Angaben beziehen sich auf Europa.

2,4 GHz (ISM)

Im Frequenzband um 2,4 GHz, das als ISM-Frequenzband (Industrial, Scientific, Medicine) bezeichnet wird, und für Anwendungen in der Industrie, Wissenschaft und Medizin reserviert ist, konkurrieren viele Standards und proprietäre Funktechniken der unterschiedlichsten Hersteller. Unglücklicherweise auch Geräte des täglichen Gebrauchs. Zum Beispiel Funkfernbedienungen und AV-Funksysteme.

Im 2,4-GHz-Band gibt es 13 Kanäle, die jeweils 5 MHz umfassen. Da man jeweils 4 Kanäle zu einem großen 20 MHz Kanal zusammenfasst, ergibt sich eine Kanalzuteilung von 1, 7 und 13 oder besser 1, 5, 9 und 13. Auf diese Weise sind jeweils zwei Kanäle unterhalb und oberhalb der eingestellten Kanalfrequenz für einen Übertragungskanal belegt.

5 GHz

Weniger in Gebrauch ist das Frequenzband um 5 GHz, mit einer nahezu weltweit verfügbaren Breite von fast 500 MHz. Es dient als Ausweich-Frequenzband, um ein WLAN zu beschleunigen. Allerdings ist dieses Frequenzspektrum weltweit nicht einheitlich geregelt, wodurch sich Unterschiede bei der Nutzung der Frequenzbereiche ergeben.

Dazu kommen auch unterschiedliche Sendeleistungen, was auch zu unterschiedlichen Reichweiten führt. In Europa (EU) darf im 5-GHz-Band mit WLAN mit maximal 200 mW Abstrahlleistung gefunkt werden (Ausnahme mit maximal 1 W in Großbritannien).

In den USA werden 3 Frequenzbänder mit jeweils 100 MHz benutzt. Effektiv stehen 12 jeweils 20 MHz breite Kanäle zur Verfügung. In Europa stehen 8 Kanäle im unteren Frequenzbereich und weitere 11 Kanäle im oberen Frequenzbereich zur Verfügung. Insgesamt ist das Frequenzspektrum in Europa 200 MHz groß (in Großbritannien sogar 455 MHz).

Es wird überwiegend von der WLAN-Industrie, aber nicht besonders intensiv genutzt. Viele preisgünstige WLAN-Router, die im 5-GHz-Band funken, nutzen lediglich den Bereich bis Kanal 48, weil darüber die lästige Dynamic Frequency Selection (DFS) zum Schutz des Wetterradars Pflicht ist. Deshalb herrscht bis Kanal 48 manchmal schon so viel Betrieb wie im ganzen 2,4-GHz-Band.
Weil der Frequenzbereich über Kanal 48 so wenig genutzt wird, gibt es bereits Begehrlichkeiten aus dem Bereich des Mobilfunks, diesen Frequenzbereich ebenfalls zu nutzen. Deshalb ist in Zukunft mit der Zunahme der Nutzung durch WLANs und Mobilfunk zu rechnen.

60 GHz

Das Frequenzband um 60 GHz hat einen rund 7 GHz breiten Funkkanal. Allerdings ist die Streckendämpfung für das Funksignal bei 60 GHz enorm. Bei dieser Frequenz erreicht die Absorption durch den atmosphärischen Sauerstoff rund 20 dB pro Kilometer (dB/km). Um genauer zu sein, der Sauerstoff erreicht hier sein Absorbationsmaximum. Die hochfrequenten Signale haben eine sehr begrenzte Reichweite, die so gut wie nicht durch Zimmerwände dringen. Hohe Geschwindigkeiten erreicht man damit in der Regel nur auf ein paar Meter. Am besten nur wenige Zentimeter und mit Sichtkontakt. Und damit ist ein WLAN bei 60 GHz ein reiner Zimmer-Funker.
Das 60-GHz-Band erstreckt sich von 57 bis 66 GHz und wird in vier Kanäle mit einer Bandbreite von 1.760 MHz unterteilt.

Unter 1 GHz

Die meisten kennen die Frequenzbereiche um 2,4 und 5 GHz. Manche auch den Bereich um 60 GHz. Dass es unlizensierte Bänder unter 1 GHz gibt, ist dabei weniger bekannt. Signale unterhalb von 1.000 MHz bzw. 1 GHz durchdringen vergleichsweise leichter Gebäude, weshalb dieser Frequenzbereich sich für das Internet der Dinge eignet, aber eben auch hart umkämpft ist.
Das Frequenzband liegt im Bereich von 863 bis 886 MHz, wobei die exakte Breite regional sehr unterschiedlich ausfallen kann.

- Funkkanalbreite: 1 bis 16 MHz
- Sendeleistung abhängig vom Land/Region: 10 mW bis 1 W
- Signalreichweite: 100 bis 1.000 Meter

Mit IEEE 802.11ah ist die Nutzung der Frequenzen unterhalb von 1 GHz vorgesehen (außerhalb der terrestrischen Rundfunkbänder). Das ist besonders in den USA und in Ländern interessant, in denen Schutzbänder frei oder einzelne TV-Kanäle freigegeben und neu zusammengefasst werden. Ob diese Frequenzbereiche von einer WLAN-Technik genutzt werden dürfen, ist natürlich eine andere Frage.

Tatsache ist jedoch, dass die Reichweite in den meisten Fällen gerade mal 200 Meter beträgt. Außerdem wird empfohlen, dass die Clients Sichtkontakt zur Basisstation haben. Beim Betrieb im Freien ist bei Regen oder hoher Luftfeuchtigkeit mit weiterer Reduzierung der Reichweite zu rechnen.

Kanalbreite

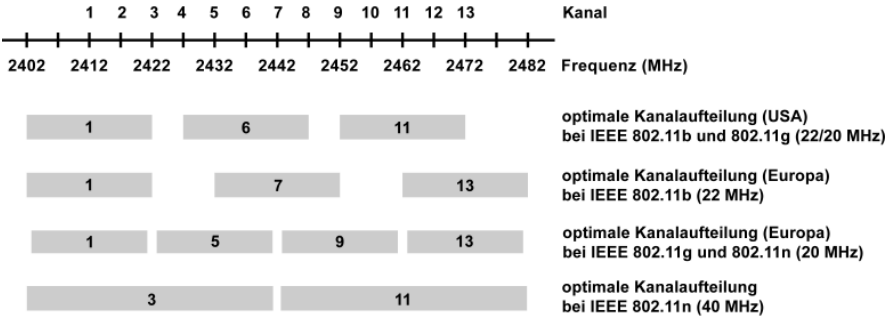
Bei WLAN gilt, dass sich alle Teilnehmer das Übertragungsmedium teilen müssen. Aufgrund der Allgemeinzuteilung darf das zur Verfügung stehende Frequenzband nicht vollständig belegt werden. Deshalb teilt man das Frequenzband zusätzlich in Kanäle ein, die aber auch nicht exklusiv genutzt, sondern mit anderen Netzen geteilt werden müssen.

Im 2,4-GHz-Frequenzband existieren insgesamt 79 schmalbandige Kanäle, die in mehrere breitbandige Kanäle zusammengefasst sind. In Europa gibt es 13, in den USA 11 und in Japan 14 solcher Kanäle. Diese

Kanäle sind allerdings eng aneinandergereiht und überlappen sich. Deshalb kann man nicht alle der 11, 13 oder 14 Kanäle verwenden, sondern je nach Kanal-Verteilung nur 3 oder 4. Und das bei einer Kanalbreite von 20 MHz. Bei einer Kanalbreite von 40 MHz würde sich die Anzahl parallel nutzbarer Kanäle halbieren.

- IEEE 802.11: bei 2,4 GHz mit 22 MHz Kanalbreite
- IEEE 802.11g und 802.11n: bei 2,4 GHz mit 20 MHz Kanalbreite
- IEEE 802.11n: bei 2,4 GHz mit 40 MHz Kanalbreite
- IEEE 802.11n: bei 5 GHz mit 20 und 40 MHz Kanalbreite
- IEEE 802.11ac: bei 5 GHz mit 80 und 160 MHz Kanalbreite
- IEEE 802.11ad: bei 60 GHz mit 2 GHz Kanalbreite

Kanal-Verteilung



Bei der Konfiguration eines oder mehrerer Access Points muss darauf geachtet werden, dass die Kanäle nicht zu breit und nicht zu dicht beieinander liegen, um eine ungewollte Überlappung zu vermeiden. Überlappungen führen zu einem engeren Kanal und damit zu einer geringeren Übertragungsrate.

Um das zur Verfügung stehende Frequenzband möglichst optimal zu nutzen, gilt es, die WLAN-Kanäle und Kanalbreite richtig zu wählen. Sinnvoll ist es, dies dem Wireless Access Points (WAP) zu überlassen. Die folgende Beschreibung geht darauf ein, wie die Frequenzbereiche um 2,4 und 5 GHz von den verschiedenen WLAN-Standards aufgeteilt werden, um das Frequenzspektrum möglichst optimal auszunutzen.

Hinweis: Gilt, wenn es im Frequenzspektrum extrem eng zu geht: Zwei WLAN-Netze mit gleichem Kanal stören sich am wenigsten. Liegen die Kanäle halb übereinander, dann nimmt das eine WLAN das andere als Störung war und versucht mit niedriger Modulation und maximaler Sendeleistung das jeweils andere zu übertönen. So stören sich die WLANs gegenseitig. Deshalb lieber einen belegten Kanal benutzen, als irgendwas dazwischen. Einen Kanal außerhalb der üblichen Kanalverteilung zu verwenden ist kontraproduktiv und senkt nur die Übertragungsrate für alle WLAN-Netze in der näheren Umgebung.

WLAN-Kanäle bei IEEE 802.11b (2,4 GHz mit 22 MHz Kanalbreite)

Bei einem WLAN mit IEEE 802.11b empfiehlt es sich, die Kanäle 1, 7 oder 13 einzustellen. Hierbei handelt es sich, bei einer Kanalbreite von 22 MHZ (DSSS), um die überlappungsfreien Kanäle, bei denen das Frequenzspektrum um 2,4 GHz optimal ausgenutzt wäre.

WLAN-Kanäle bei IEEE 802.11g und 802.11n (2,4 GHz mit 20 MHz Kanalbreite)

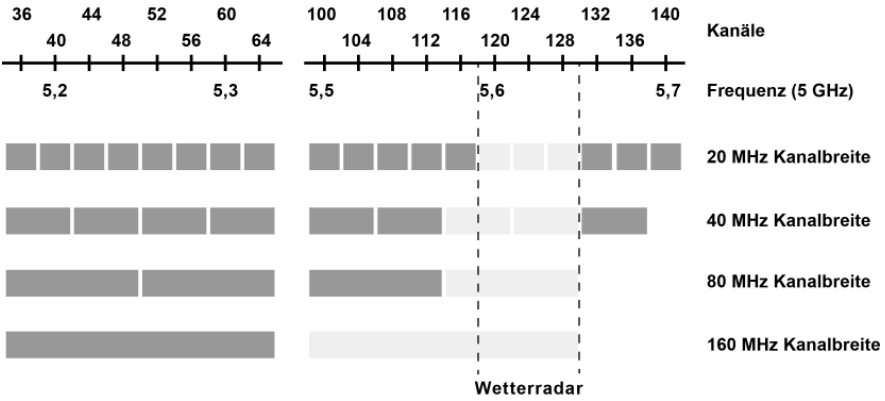
Bei einem WLAN mit IEEE 802.11g oder 802.11n ordnet man die Kanäle nach der 5er- bzw. 6er-Regel an, um mehrere Access Points optimal nebeneinander betreiben zu können.
Die 5er-Regel verwendet die Kanäle 1, 6, 11 (Kanalbelegung für USA).
Die 6er-Regel verwendet die Kanäle 1, 7, 13 (Kanalbelegung für Europa).
Damit überschneiden sich die Frequenzbereiche der Kanäle nicht und Verbindungsprobleme bleiben aus. Nur wenn die Access Points über 30 Meter auseinander stehen, darf sich die Kanalauswahl überschneiden.

Obwohl die 6er-Regel einen WLAN-Kanal mehr zulassen würde, werden WLANs mit IEEE 802.11g und 802.11n oft auf die Kanäle 1, 7 und 13 eingestellt. Hintergrund ist die Kompatibilität zu IEEE 802.11b. Weil Geräte nach IEEE 802.11b nahezu ausgestorben sein dürften, gibt es keinen Grund mehr die Kanalaufteilung 1-7-13 zu nutzen.
Bei einer Kanalbreite von 20 MHz (OFDM) und 16,25 MHz pro Träger empfiehlt es sich die Kanäle 1, 5, 9 oder 13 einzustellen. Das ermöglicht die optimale Ausnutzung des Frequenzspektrums um 2,4 GHz.

WLAN-Kanäle bei IEEE 802.11n (2,4 GHz mit 40 MHz Kanalbreite)

Bei einem WLAN mit IEEE 802.11n mit einer Kanalbreite von 40 MHz (OFDM) und 33,75 MHz pro Träger empfiehlt es sich, die Kanäle 3 (1+5) oder 11 (9+13) einzustellen.
In der Praxis vermeidet man es, ein WLAN mit IEEE 802.11n bei 2,4 GHz mit einer Kanalbreite von 40 MHz einzurichten. Dabei wäre das Frequenzspektrum mit 2 WLANs voll belegt. Damit auch WLANs mit IEEE 802.11g parallel betrieben werden können, sollten WLANs mit IEEE 802.11n auch nur mit 20 MHz Kanalbreite eingerichtet sein.

WLAN-Kanäle bei IEEE 802.11n (5 GHz mit 20 und 40 MHz Kanalbreite)



In der EU sind zwei Bereiche im 5-GHz-Frequenzband nutzbar. 5.150 bis 5.350 MHz (Kanal 36 bis 64) und 5.470 bis 5.725 MHz (Kanal 100 bis 140). In anderen Ländern liegen die Grenzen eventuell anders.
Die Nutzung des 5-GHz-Bandes setzt eine Kanalauswahlautomatik voraus, die dafür sorgt, dass die Basisstation nur die Kanäle belegt, die frei sind. Unter anderem deshalb, weil die Kanäle 120 bis 128 vom Wetter-Radar belegt sind.
Zusammenfassend kann man sagen, dass in der EU im 5-GHz-Frequenzband 16 zu je 20 MHz bzw. 7 zu je 40 MHz breite Kanäle uneingeschränkt genutzt werden dürfen. Hierbei muss man berücksichtigen, dass es lokal ein Wetterradar geben, dass das 5-GHz-Frequenzband etwas begrenzt.

Damit WLAN-Basisstationen in der EU alle Kanäle nutzen dürfen, müssen sie die Signale anderer Funksysteme erkennen und durch Kanalwechsel ausweichen können (DFS). Weiterhin gilt die Anordnung, dass nur mit DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) die Kanäle oberhalb von Kanal 48 genutzt werden dürfen. DFS ist notwendig, um bspw. den Betrieb des Wetterradars nicht zu stören.

WLAN-Kanäle bei IEEE 802.11ac (5 GHz mit 80 und 160 MHz Kanalbreite)

Im Frequenzbereich von 5 GHz sieht die IEEE 802.11ac Kanalbreiten von 20, 40, 80 und 160 MHz vor. Die Kanalbreiten 20, 40 und 80 MHz sind die Mindestanforderungen von IEEE 802.11ac. Typischerweise wird eine Kanalbreite von 80 MHz verwendet. Die Kanalbreite 160 MHz ist optional und der Nutzen in der Praxis eher fraglich. Je breiter ein Kanal, desto weniger WLANs können parallel arbeiten. Ein Kanal mit 160 MHz würde fast das ganze verfügbare Frequenzspektrum belegen. Das wäre nur in Ausnahmefällen sinnvoll.

Möchte man im 5-GHz-Frequenzband 80 MHz breite Kanäle nutzen, teilt sich das Frequenzband in 4 je 80 MHz breite Kanäle auf, wovon wegen dem Wetterradar nur 3 störungsfrei nutzbar sind.
Möchte man im 5-GHz-Frequenzband 160 MHz breite Kanäle nutzen, teilt sich das Frequenzband in 2 je 160 MHz breite Kanäle auf, wovon wegen dem Wetterradar nur eines störungsfrei nutzbar ist. Falls das Frequenzband nicht groß genug für einen 160 MHz breiten Kanal ist, kann IEEE 802.11ac auch 2 spektral getrennte 80-MHz-Kanälen zusammenfassen (Discontiguous Mode).

CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

Die Übertragungstechnik von IEEE 802.11 sieht den unkoordinierten, ungeplanten und spontanen Betrieb eines WLANs vor. In der Praxis sieht das so aus, dass jeder eine WLAN-Basisstation in Betrieb nehmen kann, ohne genaue technische Kenntnisse über deren Funktionsweise zu haben. Das bedeutet, dass die so betriebenen Funksysteme Techniken und Maßnahmen zur Koexistenz beherrschen müssen.

Durch regulative Maßnahmen wird die Fähigkeiten zur Koexistenz mehrerer Funksysteme und Funknetze und die gemeinsame Ressourcennutzung und -teilung erzwungen. Dabei ergeben sich verschiedene Schwierigkeiten, weshalb das mal gut und auch mal weniger gut funktioniert.
Aus technischer Sicht ist ein WLAN mit dem früheren Koax-Ethernet vergleichbar, wodurch sich ähnliche Techniken zur Teilung und Zugriffssteuerung auf das Übertragungsmedium ergeben.

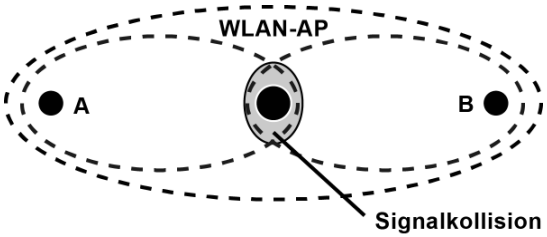
Warum CSMA/CA?

Bei WLAN gilt, dass sich alle Teilnehmer das Übertragungsmedium teilen müssen. Das heißt, dass in einem bestimmten Funkbereich (WLAN-Kanal) nur eine Übertragung störungsfrei stattfinden kann und somit immer nur ein Teilnehmer senden darf. Wer wann senden darf, muss über ein Mehrfachzugriffsverfahren geregelt werden, um den Mehrbenutzerbetrieb zu ermöglichen. Das kann man über einen zentralen Controller machen, bei dem die Teilnehmer die Berechtigung zum Senden einholen müssen oder regelt es ohne zentrale Instanz. Zum Beispiel über Listen Bevor Talk (LBT). Das heißt, senden darf ein Teilnehmer erst dann, wenn das Übertragungsmedium frei ist.

CSMA (Carrier Sense Multiple Access) ist ein solches Mehrfachzugriffsverfahren. Es sieht vor, dass jeder Teilnehmer vor dem Senden prüfen muss, ob das Übertragungsmedium frei ist. Erst wenn kein anderer Teilnehmer etwas sendet, dann ist die Übertragung erlaubt. Das schließt natürlich nicht aus, dass zwei Teilnehmer das Medium als frei erkennen und gleichzeitig senden. Dann tritt eine Kollision auf. Dabei überlagern sich die Signale. Die Daten sind in diesem Fall für den Empfänger unbrauchbar.
Beim kabelgebundenen Ethernet können die Stationen mit CSMA/CD (Carrier Sense Multiple Access/Collision Detection) die Kollision schon während der Übertragung erkennen, den Vorgang abbrechen und nach einer zufälligen Wartezeit einen erneuten Versuch starten.

In einem Funknetzwerk gibt es mehrere Probleme. Erstens lassen sich Kollisionen von Störungen nicht unterscheiden. Das zweite Problem hat mit der Reichweite von Funksignalen zu tun. So kann das eigene Signal die Signale der anderen Teilnehmer überdecken. Weil die anderen Signale

nicht in Reichweite sind, kann ein Sender nicht feststellen, ob das Signal fehlerfrei beim Empfänger ankam oder ob eine Signalkollision aufgetreten ist.
In einem WLAN kann es auch vorkommen, dass sich nicht alle WLAN-Teilnehmer kennen. Dieses Problem nennt sich Hidden-Node oder Hidden-Terminal. Besonders problematisch ist der Fall, wenn sich mehrere Teilnehmer außerhalb der Reichweite anderer Teilnehmer befinden. Dabei kann es zum fälschlichen Erkennen eines freien Kanals kommen.

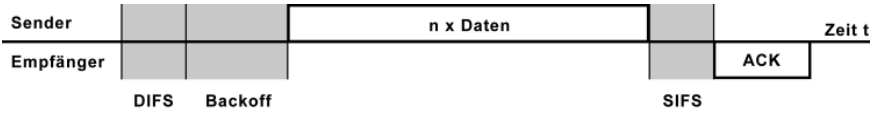


Ein Beispiel soll diese Probleme deutlich machen. So ziemlich in der Mitte eines Funknetzwerks befindet sich der Wireless Access Point (WAP), die Basisstation, über die die Wireless Clients Zugang zum Netzwerk bzw. Internet bekommen können. Die Teilnehmer A und B befinden jeweils in Reichweite zum WAP, allerdings nicht zueinander. Das heißt, A sieht B nicht und B sieht A nicht. Wenn A und B gleichzeitig senden und eine Kollisionserkennung durchführen, dann wäre für die beiden die Übertragung fehlerfrei gewesen. Allerdings überschneiden sich die Funksignale beim WAP. Und damit ist es zu einer Kollision gekommen, von der A und B nichts mitbekommen haben, weil ihre eigenen Funksignale nur eine begrenzte Reichweite haben.

Und deshalb wird im Vergleich zu den drahtgebundenen Ethernet-Varianten (mit CSMA/CD) auf eine Kollisionserkennung (Collision Detection, CD) verzichtet. Stattdessen wird ein Verfahren eingesetzt, das man als Kollisionsvermeidung (Collision Avoidance, CA) bezeichnet. Wobei das eine irreführende Bezeichnung ist.

Funktionsweise von CSMA/CA

Bevor ein WLAN-Client sendet stellt er sicher, dass der Empfänger zum Empfang bereit und das Übertragungsmedium frei ist. Dieses Vorgehen wird als Listen-Before-Talk (LBT) bezeichnet. Zu Deutsch: Hören vor dem Sprechen.
Ein WLAN-Client hört also zuerst in das Übertragungsmedium hinein, ob gerade ein anderer Teilnehmer sendet. Ist die Funkschnittstelle belegt, wartet der Teilnehmer eine zufällige Zeit ab und hört erneut in das Übertragungsmedium hinein. Erst wenn es frei ist, kann der Teilnehmer mit der Übertragung beginnen, andernfalls wird der Teilnehmer erneut eine zufällige Zeit warten und erneut prüfen.
Die zufällig Zeit, die verstreichen muss, bevor ein Gerät erneut den Funkkanal prüft liegt bei 42 bis 178 µs.



Weil eine Kollision nicht festgestellt werden kann arbeitet CSMA/CA mit Bestätigungspaketen (ACK), mit dem der Empfänger eines Pakets den Empfang beim Absender bestätigen muss. Das ACK-Paket wird genauso behandelt, wie ein normales Datenpaket. Es besteht aus dem 802.11-Header und dauert 24 µs. Das ACK-Paket wird nach einer kurzen Wartezeit (SIFS) gesendet. Erst danach gehen andere Datenpakete auf die Reise.

Nachteile durch CSMA/CA

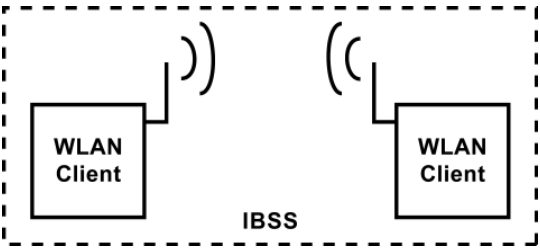
Die Sicherungsfunktionen, die durch CSMA/CA auf dem MAC-Schicht vorhanden sind, können in den oberen Protokoll-Schichten zu Problemen führen. Kommt es bereits auf der MAC-Schicht zu Datenverlusten, verzögern sich die Datenpakete auf den oberen Schichten. Das führt zu verlängerten Übertragungszeiten, die z. B. TCP/IP mit bestimmten Mechanismen zur Bestätigung von Datenpaketen durch den Empfänger erhöht. Dies führt zu erhöhtem Datenaufkommen durch die mehrfachen Bestätigungsmeldungen auf anderen Schichten. Diese Schwierigkeiten sind häufig dafür verantwortlich, dass die Performance von drahtlosen Netzen deutlich unter der von drahtgebundenen Netzwerken liegt.

WLAN-Topologie

Eine WLAN-Topologie besteht im wesentlichen aus den drahtlosen Netzteilnehmern, die als WLAN-Clients bezeichnet werden und mindestens einer WLAN-Basisstation, die als Wireless Access Point (WAP) oder einfache nur Access Point (AP) bezeichnet wird. Ein Access Point ist innerhalb eines WLANs das einzige aktive Schicht-2-Element. Vergleichbar mit einer Bridge verbindet der Access Point zwei Netzwerke mit unterschiedlichen physikalischen Schichten. Bspw. das Wireless LAN mit dem drahtgebundenen Ethernet.

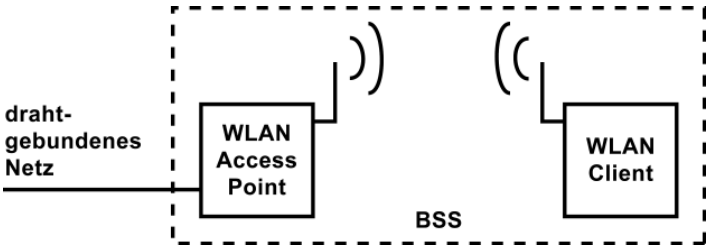
Im Folgenden sind verschiedene Topologien beschrieben, wie sie in Kombination mit Wireless LAN nach IEEE 802.11 vorkommen.

IBSS - Independent Basic Service Set (Ad-hoc)



Schon mit zwei drahtlosen Hosts lässt sich ein einfaches Wireless LAN aufbauen. Diese Topologie bezeichnet man auch als Ad-hoc-Netzwerk. Der WLAN-Standard sieht die Bezeichnung Independent Basic Service Set (IBSS) vor. Bei der Einrichtung sind keine weiteren aktiven Elemente erforderlich. Die Hosts kommunizieren direkt über ihre WLAN-Adapter. Solange sich die Hosts gegenseitig in Reichweite befinden, ist eine Kommunikation zwischen den Hosts möglich.
Der IBSS-Modus wurde nur sehr grob spezifiziert. Deshalb gibt es auch heute noch Probleme, wenn WLAN-Geräte unterschiedlicher Hersteller ad-hoc miteinander verbunden werden sollen. Außerdem ist eine sichere Verschlüsselung im IBSS-Modus nicht möglich.
Diese Art der Vernetzung ist für ein WLAN mit IEEE 802.11 eher unüblich. Eine Ad-hoc-Vernetzung ist mit Bluetooth einfacher und sicherer realisierbar.

BSS - Basic Service Set

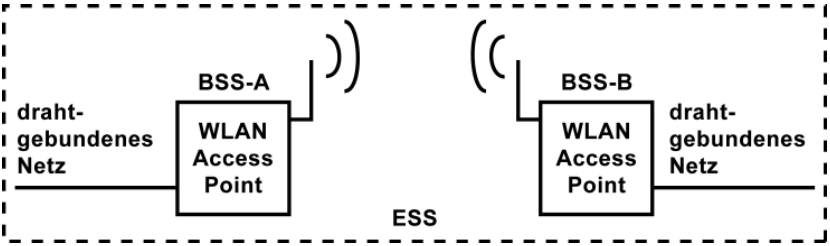


Das Basic Service Set (BSS) ist der typische Betrieb eines WLANs. Hier bildet der Wireless Access Point den Übergang vom drahtgebundenen ins drahtlose Netzwerk. Er stellt innerhalb einer Funkzelle den Zugriff auf das drahtgebundene Netzwerk und umgekehrt her. Der Access Point übernimmt dabei die Aufgabe einer Bridge. Er erlaubt es sogar, Protokolle, die das WLAN unnötig überlasten würden, herauszufiltern. Der Access Point versorgt eine Funkzelle (räumliche Ausbreitung der Funksignale), in der er eine festgelegte Übertragungsrate garantiert. Alle Funkteilnehmer müssen sich jedoch diese Übertragungsrate teilen.
Die Übertragungsrate in einem WLAN ist stark von der Lage und Ausrichtung aller Geräte und der Umgebung abhängig. Hier spielen schwankende Einflüsse, wie die Feuchtigkeit in der Luft und der Bausubstanz eine große Rolle. Einen Access Point stellt man möglichst so auf, dass keine Wände oder andere Hindernisse zwischen Access Point und den WLAN-Clients liegen. Die Aufstellhöhe spielt dabei keine Rolle.
Einzelne WLAN-Netze werden über ihre ESSID (Extended Service Set Identifier) bzw. SSID (Service Set Identifier) identifiziert.
Funkzellen, die zusätzlich QoS unterstützen werden als QBSS bezeichnet.

ESS - Extended Service Set / IEEE 802.11c / Wireless Bridging

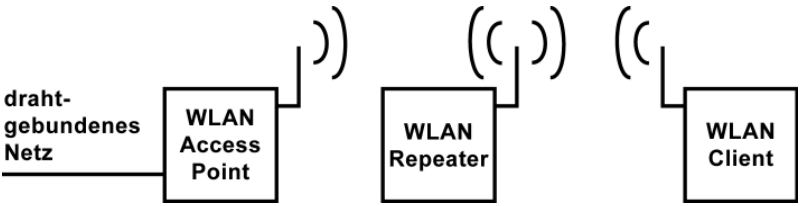
Wenn mehrere Access Points in Form von zwei oder mehreren Basic Service Sets (BSS-A und BSS-B) zueinander eine Funkverbindung herstellen, dann nennt sich das Extended Service Set (ESS).
Diese Topologie sieht vor, dass man die Reichweite eines kabelgebundenen Netzwerks erhöht. Bei einer Infrastruktur auf Basis von 10Base-T/100Base-TX dürfen die einzelnen Kabelsegmente eine Maximallänge von 100 Metern haben. Mit Wireless LAN besteht die Möglichkeit, Bereiche zu verbinden, die mit der herkömmlichen

Verkabelung nicht erreicht werden können.
Die Reichweite im Freien liegt bei guten Bedingungen zwischen 100 und 300 Metern. Reicht das nicht aus, so lässt sich mit zwei gerichteten Antennen einige Kilometer überbrücken. Und das gebühren- und genehmigungsfrei. Auch über Grundstücksgrenzen hinweg.



IEEE 802.11c ist der Standard zur drahtlosen Kopplung zweier Netzwerk-Topologien über WLAN. Das Bridging erfolgt mit zwei Access Points. Hierbei handelt es sich dann um eine dedizierte Funkverbindung. Die Identifikation der Gegenstelle erfolgt über die MAC-Adresse. Anmeldeversuche gewöhnlicher drahtloser Endgeräte werden verweigert. Die Norm 802.11c ist für die breite Masse ohne Bedeutung. Es handelt sich lediglich um eine Veränderung der Norm 802.1d (MAC-Layer-Bridging) zwecks Koppelung mit 802.11-Datenframe (auf der Sicherungsschicht).
Zwei APs, die mit 802.11c arbeiten ersetzen mit der Funkverbindung eine Kabel-Verbindung.

WDS - Wireless Distribution System (WLAN-Repeater)



WDS, neben Wireless Distribution System auch Wireless Distributed System genannt, bezeichnet die drahtlose Verbindung mehrerer Wireless Access Points untereinander. Es handelt sich dabei um die Funktion eines WLAN-Repeaters innerhalb eines WLAN-Netzwerks.

Ein als WDS konfigurierter Access Point ist eine WLAN-Basisstation, die schwache Funksignale empfängt, neu aufbereitet und verstärkt wieder abstrahlt. WLAN-Repeater vergrößern im Prinzip die Reichweite einer einzelnen Basisstation, die sie über ihre Hardware-Adresse (MAC) identifizieren. Bei der Repeater-Funktion handelt es sich praktisch um eine Funkverlängerung. Der WLAN-Repeater verteilt dabei die Datenpakete per Broadcast an alle WLAN-Teilnehmer und erzeugen damit eine Datenflut im WLAN.
Da Access Point und Repeater die gleiche SSID haben, können sich die WLAN-Clients wahlweise mit dem Repeater oder dem Access Point verbinden. Je nach dem welches Funksignal stärker ist.

IEEE 802.11b / WLAN mit 11 MBit

IEEE 802.11b ist ein Standard für ein Wireless LAN mit einer Übertragungsrate von maximal 11 MBit/s aus dem Jahr 1999. Der Standard benützt das 2,4-GHz-Frequenzband, wofür keine langwierigen Zulassungen notwendig sind. Die WLAN-Geräte dieses Standards haben sich sehr schnell, auch wegen des günstigen Preises, durchgesetzt.
Die tatsächliche Transferrate beträgt in der Praxis maximal 5 MBit/s. Je nach Umgebungsbedingungen und dem Abstand zwischen den Stationen reduziert sich die Übertragungsrate erheblich.
Die Reichweite in Gebäuden beträgt in Abhängigkeit des Baustoffs für Wände und Decken um die 20 bis 30 Meter.

Hinweis: WLAN-Geräte, die dem Standard IEEE 802.11b entsprechen, sind veraltet. Man sollte sie nicht mehr verwenden. Der Hauptgrund ist die mangelhafte Verschlüsselung. Zudem geht der Datendurchsatz zurück, wenn ein 802.11b-Gerät sich an einem 802.11g- oder 802.11n-Access-Point anmeldet. Der Kompatibilitätsmodus geht auf Kosten der Geschwindigkeit. Auch für die anderen Geräte.

IEEE 802.11g / WLAN mit 54 MBit

IEEE 802.11g ist ein Standard für ein Wireless LAN mit einer Übertragungsrate von maximal 54 MBit/s aus dem Jahr 2003. IEEE 802.11g ist der Nachfolger von IEEE 802.11b mit einem verbesserten Modulationsverfahren. Der Standard verwendet dafür das 2,4-GHz-

Frequenzband, für dessen Nutzung keine Zulassung notwendig ist. Allerdings sind wie im WLAN nach IEEE 802.11b mit allen Nachteilen in diesem Frequenzband zu rechnen. Vor allem Störungen durch andere Funkdienste, z. B. Bluetooth oder Funk-Fernbedienungen.

Kompatibilität zu IEEE 802.11b

Der besondere Vorteil von IEEE 802.11g ist die Abwärtskompatibilität zu IEEE 802.11b. Damit kann eine bestehende WLAN-Infrastruktur weitergenutzt werden, während einzelne bandbreitenbedürftige Segmente auf IEEE 802.11g umgestellt werden können. Die Abwärtskompatibilität zu 802.11b wird durch die CCK-Modulation (Complementary Code Keying) sichergestellt. Werden in einem 802.11g-WLAN Geräte mit 802.11b-Standard genutzt, wird die Datenrate automatisch auf 11 MBit/s reduziert. Werden Geräte ausschließlich mit 802.11g eingesetzt, ermöglicht die OFDM-Übertragungstechnik, abhängig von der Qualität der Funkverbindung, Brutto-Übertragungsraten von 6 bis 54 MBit/s. Geräte, die nur 11b unterstützen, können 802.11g-WLANs nicht erkennen.

Im WLAN-Standard 802.11g war die Kompatibilität zu 802.11b gefordert. Deshalb beherrscht die 802.11g-Hardware auch die Datenraten bis 11 MBit/s. Da 802.11g ein anderes Modulationsverfahren benutzt als 802.11b, kann die 802.11b-Hardware nicht erkennen, ob das Medium durch 802.11b-Hardware belegt ist. Um Kollisionen zu vermeiden, stellt die 802.11g-Station bei anwesenden 802.11b-Stationen ihren Datenpaketen ein 802.11b-kompatibles CTS-Steuerpaket (Clear-to-Send) voran. Das CTS-Paket reserviert das Medium für eine bestimmte Zeit. Es ist aber genauso lang, wie ein normales Datenpaket und drückt so die Datenrate. Das passiert immer dann, wenn 802.11g- und 802.11b-Stationen sich den selben Funkkanal teilen.

IEEE 802.11a / IEEE 802.11h / IEEE 802.11j

IEEE 802.11a ist eine Spezifikation für Wireless LAN aus dem Jahr 1999 mit einer theoretischen Übertragungsgeschwindigkeit von 54 MBit/s. Das ist 5 mal schneller, als IEEE 802.11b mit maximal 11 MBit/s. IEEE 802.11a gilt als Alternative zu IEEE 802.11g, das ebenso 54 MBit/s übertragen kann.

Der Grund für die parallele Entwicklung von 802.11a und 802.11g, liegt in der hohen Auslastung des 2,4-GHz-Bandes, in dem IEEE 802.11b und 802.11g funken. Drahtlose Fernbedienungen, AV-Brücken, Fernsteuerungen und viele private WLANs teilen sich die begrenzte Bandbreite im 2,4-GHz-Frequenzbereich. Mit IEEE 802.11a kann man mit einem WLAN auf das kaum genutzte 5-GHz-Band ausweichen. Allerdings ist dort, wegen der höheren Dämpfung, die Reichweite und damit der Datendurchsatz geringer. Doch die geringere Auslastung kompensiert das wieder.

Während in den USA die Spezifikation IEEE 802.11a gilt, gibt es für Europa und Japan die Spezifikationen IEEE 802.11h und IEEE 802.11j, die jeweils die nationale Begebenheiten berücksichtigen.

IEEE 802.11n / WLAN mit 150 MBit/s

IEEE 802.11n ist die Spezifikation für ein WLAN mit Übertragungsraten von 150, 300, 450 und 600 MBit/s. Für IEEE 802.11n wurde Ende 2003 eine Arbeitsgruppe eingerichtet, um einen WLAN-Standard zu schaffen, der eine Nettoübertragungsrate von mindestens 100 MBit/s erreicht. Wie bei Fast-Ethernet sollten im WLAN auch 100 MBit/s möglich sein. In der Praxis ist mit 120 MBit/s (bei 300 MBit/s brutto) und 240 MBit/s (bei 600 MBit/s brutto) zu rechnen.
Erreicht werden diese Geschwindigkeiten mit mehreren Antennen und Signalverarbeitungseinheiten (MIMO), die Verdopplung der Funkkanal-Bandbreite auf 40 MHz, sowie die parallele Nutzung des 2,4- und 5-GHz-Frequenzbandes.

2006 gab es bereits den ersten Entwurf eines Standards mit der Bezeichnung Pre-11n bzw. 11n-Draft. Obwohl es nur ein Entwurf war, war Ende 2006 die erste Pre-11-Hardware erhältlich. Der Grund für die rasche Umsetzung eines noch nicht verabschiedeten Standards, war die Nachfrage nach schnellerem WLAN. Zwischen Februar 2007 und September 2008 kam es zu weiteren Versionen (Draft 2.0 bis Draft 7.0). Bei den meisten kommerziellen Produkten ist die technische Spezifikation für Draft 2.0 die Basis.
Die endgültige Standardisierung verzögerte sich im Lauf der Zeit immer wieder. Offiziell wurde der Standard IEEE 802.11n im September 2009 verabschiedet.

Techniken zur grundlegenden Verbesserung der Übertragungsrate

- Antennengruppen mit MIMO (Multiple Input Multiple Output)
- Spatial Multiplexing mit Space Time Block Coding (STBC)
- Antennen-Diversity (Signal von der Antennen mit dem besseren Empfang abgreifen)
- verbesserte OFDM-Modulation mit maximal 65 MBit/s in einem 20-MHz-Kanal (nur 54 MBit/s bei 802.11g)
- Kanalbündelung
- Transmit Beamforming
- Packet Aggregation (Zusammenfassen von Paketen)
- RIFS (Reduced InterFrame Spacing)
- Greenfield-Mode (Abschaltung der 11a-, 11b- und 11g-Unterstützung)

Bei IEEE 802.11n soll der Datendurchsatz über 100 MBit/s durch einen höheren Durchsatz auf der MAC-Schicht (Media Access Control) und einem geringeren Overhead erreicht werden. Deutliche Verbesserungen sollen adaptive MACs bringen, die die Bandbreite unter allen Teilnehmern besser aufteilt.

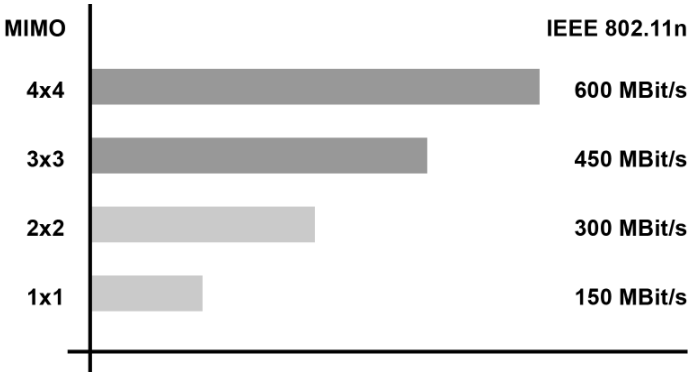
Transmit Beamforming (Sendestrahlsteuerung), Receive Combining und breite Hochfrequenzkanäle sollen die Funkverbindung verbessern und mehr Datendurchsatz bringen. Je nach Anwendung oder lokaler Frequenzvergabe (abhängig von der Regulierung) sollen 10, 20 oder 40 MHz breite HF-Kanäle möglich sein. Die WLAN-Geräte prüfen, ob diese Kanäle für die Datenübertragung frei sind. Bluetooth-Geräte in der Nähe können den WLAN-Geräten mitteilen nur einen Kanal zu nutzen. So bleibt auch für gleichzeitige Bluetooth-Funkverbindungen noch genug Bandbreite übrig.

Da die Funkschnittstelle einer ständigen Veränderung unterliegt werden vor der Nutzdatenübertragung Trainingssequenzen übertragen. Mit Hilfe von Pilottönen innerhalb der Nutzdaten erfolgt dann eine dynamische Feinabstimmung der Signalverarbeitung. Der Einsatz in Räumen soll die Reflektionen (mehrfache Empfangssignale) für mehr Datendurchsatz ausnutzen.

Frequenzen und Kanäle

IEEE 802.11n beherrscht sowohl das 2,4-GHz- wie auch das 5-GHz-Band. Das bedeutet, es stehen zwei Frequenzbänder zur Verfügung. Doch Vorsicht, die meisten billigen 11n-Geräte beherrschen nur das 2,4-GHz-Band.
Im 2,4-GHz-Band gibt es 13 Kanäle, die jeweils 5 MHz umfassen. Da man jeweils 4 Kanäle zu einem großen 20 MHz Kanal zusammenfasst, ergibt sich eine Kanalzuteilung von 1, 7 und 13 oder besser 1, 5, 9 und 13. Auf diese Weise sind jeweils zwei Kanäle unterhalb und oberhalb der eingestellten Kanalfrequenz für einen Übertragungskanal belegt.
Im 5-GHz-Band sind 19 verschiedene nicht überlappende Kanäle mit jeweils 20 MHz Kanalbreite nutzbar.

Übertragungsgeschwindigkeit



Alle vorhergehenden WLAN-Spezifikationen des IEEE wurden mit der theoretisch maximalen Übertragungsgeschwindigkeit abgesegnet. So erreichen WLANs nach IEEE 802.11g mit 54 MBit/s in der Praxis selten mehr als 20 MBit/s und IEEE 802.11b mit 11 MBit/s selten mehr als 5 MBit/s.
Auch bei IEEE 802.11n ist es nicht anders. Hier sollen brutto 150, 300, 450 und 600 MBit/s erreicht werden. Bei einer guten Funkverbindung sollte davon netto rund die Hälfte übrig bleiben. Was in der Praxis dann wirklich möglich ist, ist von den lokalen Gegebenheiten abhängig. Wände, Möbel und andere Netzwerke stören die Funkübertragung. Einfache WLAN-Geräte mit brutto 150 MBit/s erreichen in der Praxis nur eine

Geschwindigkeit von maximal 60 MBit/s. Sie kommen ohne die Mehrantennentechnik MIMO aus und übertragen somit nur einen Datenstrom. Sie sind mit dem Logo von IEEE 802.11a/g mit dem Untertitel "with some n features" gekennzeichnet. In den meisten Fällen ist das mehr als ausreichend. Die Übertragungsgeschwindigkeit in einem WLAN mit IEEE 802.11n wird nur bei besonders schnellen Internet-Anschlüssen oder der Übertragung großer Datenmengen im heimischen Netzwerk ausgereizt.
Dualband-WLAN-Basisstationen, die in den Frequenzbereichen 2,4 und 5 GHz funken können, transportieren maximal 300 MBit/s (brutto), was in der Praxis zwischen 70 und 100 MBit/s entspricht.
In der Praxis kann man davon ausgegangen, dass WLANs mit IEEE 802.11n zwei- bis viermal schneller sind als WLANs mit IEEE 802.11g.

Hinweis: Die maximale Brutto-Übertragungsgeschwindigkeit von IEEE 802.11n liegt bei 450 MBit/s. 600 MBit/s ist zwar definiert, dazu werden aber aktuell keine Produkte angeboten.

Kompatibilität zu IEEE 802.11b und 802.11g

Die etablierte IEEE 802.11b/g-Technik soll durch IEEE 802.11n nicht veralten, sondern nahtlos eingebunden werden. Die parallele Nutzung von WLANs mit 802.11g und 802.11n schließt sich nicht aus.
Aber, ein WLAN mit 802.11n, das einen 40-MHz-Kanal nutzt, könnte für bestehende WLANs mit 802.11g zum Problem werden. Der Grund, im 2,4-GHz-Frequenzband geht es recht eng zu. Hier tummeln sich noch weitere Funktechniken. Aus diesem Grund ist davon auszugehen, dass ein 40-MHz-Kanal nur im 5-GHz-Frequenzband möglich sein wird. Schon allein deshalb, um die Kompatibilität zu WLANs mit 802.11g nicht zu gefährden.
Damit man überhaupt die Vorteile von IEEE 802.11n nutzen und von der Geschwindigkeitssteigerung profitieren kann, sollte der Kompatibilitätsmodus zu 802.11b und 802.11g abgeschaltet werden. Im Optimalfall richtet man den WLAN-Router oder Access Point so ein, dass er mit 802.11g im 2,4-GHz-Band und mit 802.11n im 5-GHz-Band arbeitet. Allerdings haben nicht alle Access Points diese Möglichkeiten.

MIMO - Multiple Input Multiple Output

MIMO sieht vor, mehrere Sende- und Empfangsantennen zu verwenden. Vom Prinzip her wird der Frequenz-Zeit-Matrix eine dritte Dimension, der Raum, hinzugefügt. Mehrere Antennen verhelfen dem Empfänger zu räumlichen Informationen, was zur Steigerung der Übertragungsrate durch Spatial Multiplexing genutzt werden kann. Dabei werden mehrere Datenströme parallel in einem Funkkanal übertragen. Die parallele Signalverarbeitung bringt verbesserten Signalempfang und vermindert die Nachteile durch Mehrwegeempfang, der durch reflektierte Signale entsteht. Insgesamt verbessert sich die Leistung des ganzen Funksystems durch MIMO erheblich.

IEEE 802.11ac / Gigabit-WLAN

IEEE 802.11ac ist ein Funknetz-Standard, der manchmal als 5G Wifi bezeichnet wird. IEEE 802.11ac wurde im November 2013 als Standard verabschiedet. Es handelt sich um den fünften WLAN-Standard nach 802.11, 802.11b, 802.11g/11a und 802.11n.
IEEE 802.11ac sieht Übertragungsgeschwindigkeiten im Gigabit-Bereich vor. Genau genommen definiert der Standard eine maximale Datenrate von rechnerisch 6.936 MBit/s. Die Beschleunigung bei IEEE 802.11ac erfolgt durch die Optimierung des Übertragungsprotokolls, breitere Kanäle im Frequenzspektrum bei 5 GHz und bessere Modulationsverfahren. Da 802.11ac nur für 5 GHz spezifiziert ist gilt 802.11n weiterhin für 2,4 GHz und wird parallel genutzt.

Technische Merkmale

IEEE 802.11ac bringt im Vergleich zum Vorgänger IEEE 802.11n keine wesentlichen Neuerungen. Statt dessen erreicht man die höhere Übertragungsrate durch breitere Übertragungskanäle (bis 160 MHz), mehr parallele Sende- und Empfangseinheiten (8 x 8), eine effizientere Modulation (256QAM) und Multi-User-MIMO. Ein weiterer Vorteil von 11ac ist die bessere Ausleuchtung.

- Kanalbreiten von 20, 40, 80 und 160 MHz
- Modulationsverfahren 256QAM kodiert pro Übertragungsschritt 8 Bit

- bis zu 8 simultan nutzbare Antennen
- Multiuser-MIMO (MU-MIMO) unterstützt mehrere Clients pro Basisstation

Frequenzen und Kanäle

Ein WLAN mit IEEE 802.11ac arbeitet im Funkspektrum von 5 GHz, für das es weltweit eine Allgemeinzuteilungen gibt. In der EU sind folgende Bereiche im 5-GHz-Frequenzband freigegeben.

- 5.150 bis 5.350 MHz (Kanal 36 bis 64)
- 5.470 bis 5.725 MHz (Kanal 100 bis 140)

In anderen Regionen auf der Welt sieht es anders aus. In der Regel dürfte genug Platz für mehrere parallel betriebene 11ac-WLANs sein.
Im Frequenzbereich von 5 GHz sieht die IEEE 802.11ac Kanalbreiten von 20, 40, 80 und 160 MHz vor. Die Kanalbreiten 20, 40 und 80 MHz sind die Mindestanforderungen von IEEE 802.11ac. Typischerweise wird eine Kanalbreite von 80 MHz verwendet. Die Kanalbreite 160 MHz ist optional und der Nutzen in der Praxis eher fraglich. Je breiter ein Kanal, desto weniger WLANs können parallel arbeiten. Ein Kanal mit 160 MHz würde fast das ganze verfügbare Frequenzspektrum belegen. Das wäre nur in Ausnahmefällen sinnvoll.

DFS - Dynamic Frequency Selection

Damit WLAN-Basisstationen in Europa und in vielen anderen Ländern im Frequenzband um 5 GHz alle 19 Kanäle zu je 20 MHz oder mehr Breite nutzen dürfen, müssen sie die Signale anderer Funksysteme erkennen und durch Kanalwechsel ausweichen können. Ohne DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) dürfen WLAN-Geräte nur die untersten vier Kanäle 36 bis 48 (5.150 bis 5.250 MHz) verwenden, was einem 80-MHz-Frequenzblock (4 x 20-MHz-Kanäle) entspricht. In Europa ist das deshalb notwendig, um bspw. den Betrieb des regionalen Wetterradars auf den Kanälen Kanäle 120 bis 128 nicht zu stören.

DFS erkennt andere Funksysteme und weicht ihnen durch den Wechsel auf andere Kanäle aus. Mit TPC steuern die Access-Points ihre Sendeleistung dynamisch. So werden bei guter Funkverbindung die Daten

mit geringerer Sendeleistung gesendet.
Leider ignorieren einige WLAN-Hersteller DFS und TPC und sparen sich die Zusatzkosten bei der Prüfung. Somit gibt es Geräte auf dem Markt, die nur unvollständig 5-GHz-fähig sind. Diese Geräte arbeiten nur auf den Kanälen 36 bis 48. Dabei ist DFS nichts neues. Es ist bereits in IEEE 802.11h enthalten. Ebenso bei IEEE 802.11n, das sowohl im 2,4-GHz- als auch im 5-GHz-Band arbeiten kann.

Das Fehlen von DFS ist aus zwei Gründen ein Ärgernis. Wenn ein Router oder Access Point mit 802.11ac und einem breiten 80-MHz-Signal die Kanäle 36 bis 48 komplett belegt. Und dann ein Nachbar auch so einen Router verwendet, dann müssen sich beide WLAN-Betreiber diese Bandbreite teilen. Von schnellem WLAN kann dann keine Rede mehr sein.
Der zweite Knackpunkt betrifft WLAN-Clients und -Adapter, die den Bereich über Kanal 48 nicht nutzen können. Hat ein Access Point das WLAN auf einem höheren Kanal aufgebaut, dann kann ein Notebook oder Smartphone ohne DFS/TPC-Unterstützung keine Verbindung zu diesem Access Point aufbauen.

Modulationsverfahren 256QAM

Wie alle modernen Funksysteme nutzt IEEE 802.11ac OFDM, um den Frequenzbereich in zahlreiche, individuell modulierte Subträger zu unterteilen. Im besten Fall unterstützen die Geräte hochwertige Modulationsverfahren. Zum Beispiel 256QAM mit 256 Stufen. Das sind 8 Bit pro Übertragungsschritt. Im Vergleich dazu überträgt 64QAM nur 6 Bit pro Übertragungsschritt.

Bis zu 8 MIMO-Streams

MIMO sieht vor, mehrere Sende- und Empfangsantennen zu verwenden. Bei IEEE 802.11ac bis zu 8 Stück. Das bedeutet bis zu 8 gleichzeitige Datenströme. Mit jedem Datenstrom wird die Übertragungsrate erhöht. Es ist jedoch kaum damit zu rechnen, dass Access-Points mit mehr als 3 oder 4 Datenströmen auf den Markt kommen. Der Datendurchsatz steigt mit jedem weiteren Datenstrom nicht zwangsläufig an. Dafür steigt der Hardware-Aufwand, die Anzahl der Antennen, der Rechenaufwand zur

Signaltrennung und der Energieverbrauch. Insbesondere mobile Geräte müssen mit einem, höchstens zwei Datenströmen auskommen.

MU-MIMO - Multi-User-MIMO

IEEE 802.11ac sieht auch eine Erweiterung für Multi-User-MIMO (MU-MIMO) vor, bei der mehrere Antennen an unterschiedliche WLAN-Clients Daten senden. Sinnvoll sind hier vier oder mehr Antennen, bei Basisstationen, die mehrere Clients versorgen müssen. Mehrere Antennen versorgen gleichzeitig mehrere Clients. Dazu müssen aber auch die Clients MU-MIMO-fähig sein.

Beamforming

Beamforming ist bereits seit IEEE 802.11n spezifiziert, aber leider zu ungenau. Herstellerübergreifendes Beamforming hat selten funktioniert. In IEEE 802.11ac ist Beamforming genauer spezifiziert.
Per Beamforming kann eine Basisstation das Funksignal in eine bestimmte Richtung senden und so die Verbindung zu einem bestimmten Client deutlich verbessern. Beim Beamforming senden mehrere Antennen das gleiche Signal mit einem zeitlichen Versatz. Dabei entsteht eine Richtwirkung, die die Sendeenergie auf einen Client fokussiert. Dabei verbessert sich die Qualität der Funkverbindung, was eine höhere Modulationsstufe erlaubt und somit die Übertragungsrate erhöht.

Übertragungsgeschwindigkeit

In der Theorie lassen sich mit IEEE 802.11ac fast 7 GBit/s übertragen. Doch dazu müssten die beteiligten Geräte die Maximalwerte aller spezifizierten Leistungsparameter vollständig unterstützen und miteinander kombinieren. In der Praxis ist das fast unmöglich. Die theoretische Übertragungsrate hängt von verschiedenen Faktoren ab:

- Anzahl der gleichzeitigen Datenströme mit MIMO (1 bis 8)
- Breite des Kanals (20, 40, 80 oder 160 MHz)
- Modulationsverfahren (64QAM, 256QAM)

Kombiniert man die maximal spezifizierten Leistungsparameter, dann kommt man rechnerisch auf insgesamt 6.936 MBit/s (rund 7 GBit/s).

- 433 MBit/s (5 GHz) = 1 x MIMO + 80 MHz Kanal + 256QAM
- 867 MBit/s (5 GHz) = 2 x MIMO + 80 MHz Kanal + 256QAM
- 1.300 MBit/s (5 GHz) = 3 x MIMO + 80 MHz Kanal + 256QAM
- 1.700 MBit/s (5 GHz) = 4 x MIMO + 80 MHz Kanal + 256QAM
- 3.464 MBit/s (5 GHz) = 8 x MIMO + 80 MHz Kanal + 256QAM
- 6.936 MBit/s (5 GHz) = 8 x MIMO + 160 MHz Kanal + 256QAM

Berechnung: In der Praxis kommt man mit einem Datenstrom mit einer Antenne, bei einem 80 MHz breiten Kanal und dem Modulationsverfahren 256QAM auf 433 MBit/s. Mit der Mehrantennen-Technik MIMO und zwei räumlich getrennten Datenströmen kommt man auf 867 MBit/s. Mit drei Datenströmen steigt die Datenrate auf rund 1.300 MBit/s brutto. Arbeitet man mit vier Datenströmen, kommt man auf eine Datenrate von rund 1.700 MBit/s.

Diese Werte (gerundet) setzten voraus, dass sowohl der Access Point als auch die WLAN-Clients alle technischen Voraussetzungen erfüllen. Wenn ein WLAN-Client nur vier Datenströme beherrscht, dann erreicht der Datenaustausch auch nur die Geschwindigkeit, die für den WLAN-Client möglich ist.
Die erwähnten 8 Sende- und Empfangseinheiten (8 x MIMO) setzen die entsprechende Anzahl von Antennen und die unterstützende Elektronik voraus. Das ist in mobilen und Akku-betriebenen Geräten schwer möglich. Doch gerade diese Geräteklassen sind auf schnelle Funktechniken angewiesen. Dem gegenüber steht der mangelnde Platz und begrenzter Energieversorgung. Deshalb werden Übertragungsgeschwindigkeiten im GBit-Bereich bei mobilen Geräten die Ausnahme bleiben.

WLAN-Geräte mit IEEE 802.11ac können ihre Geschwindigkeit auch nur auf kurzen Distanzen und ohne Hindernisse ausspielen. Funksignale im 5-GHz-Frequenzband werden von Wänden und Decken viel stärker ausgebremst als die 2,4-GHz-Frequenzband. Das ist kein Problem, dann WLAN-Geräte mit IEEE 802.11ac können auch die älteren Standards bei 2,4 GHz.

In der Praxis sollte man damit rechnen, dass sich die hier genannten Bruttowerte etwa halbieren. Eine angestrebte Datenrate von über 1 GBit/s

ist nur dann möglich, wenn die Funkbedingungen optimal sind. Und das ist selten so.

IEEE 802.11ad - Wireless Gigabit (WiGig)

IEEE 802.11ad wird als Wireless Gigabit, kurz WiGig, bezeichnet und liegt seit 2012 als Standard vor. Es handelt sich dabei um eine Spezifikation für eine schnelle drahtlose Verbindung auf Basis von WLAN nach IEEE 802.11. Die typische Anwendung ist allerdings nicht die Vernetzung von Computern, sondern das Verbinden von digitalen Videosystemen oder auch Computer-Peripherie. Zum Beispiel zwischen einem Fernseher und einem Mediaplayer (DVD, Blu-ray) oder einem Computer und einem Drucker. So eine Art Wireless USB oder Wireless PCIe.

Was genau aus IEEE 802.11ad wird, das ist aber noch nicht sicher. Angedacht sind Punkt-zu-Punkt-Funkverbindungen mit Übertragungsgeschwindigkeiten im Gigabit-Bereich. Um das zu erreichen wird auf Abwärtskompatibilität zu allen vorhergehenden WLAN-Standards verzichtet.
Ebenso findet mit IEEE 802.11ad ein Frequenzwechsel auf 60 GHz statt. Hier sind auf mehreren 2 GHz breiten Kanälen jeweils bis zu 7 GBit/s brutto machbar.
Obwohl IEEE 802.11ad noch keine Marktbedeutung hat, sind schon einige Firmen dabei die Geschwindigkeit auf bis zu 20 GBit/s hochzutreiben.
Denkbar wäre auch, dass in Zukunft ein Funknetz auf Basis von IEEE 802.11ad mit weiteren Optimierungen und breiteren Kanälen bis zu 100 GBit/s Übertragungsrate haben kann.

IEEE 802.11ax / High Efficiency WLAN

IEEE 802.11ax ist ein Standard für ein High Efficiency WLAN mit Übertragungsgeschwindigkeiten im Gigabit-Bereich. Es handelt sich um den sechsten WLAN-Standard nach 802.11, 802.11b, 802.11g/11a, 802.11n und 802.11ac. Das Ziel von IEEE 802.11ax ist, die Effizienz des WLAN-Protokolls bei hoher Teilnehmerdichte zu verbessern. Damit ist eine Geschwindigkeitsvervierfachung gegenüber dem Vorgänger IEEE 802.11ac vorgesehen.

Inzwischen erstreckt sich das Einsatzgebiet von WLAN nicht nur auf mobile Geräte, sondern auch auf Fernseher, Settop- und Streaming-Boxen. Das größte Datenvolumen entsteht dabei durch Streaming-Anbieter und -Konsumenten, die immer schnellere Übertragungsraten fordern. Doch mit dem Vorgänger IEEE 802.11ac hat man bereits die Grenze, was die technische Machbarkeit bei Kanalbreite und Modulationsverfahren angeht, erreicht.

Eine noch höhere Geschwindigkeit zu realisieren, ist also nicht so einfach. Deshalb ist man daran interessiert, den Unterschied zwischen der rechnerischen Datenübertragungsrate (Brutto) und der vom Anwender gefühlten Geschwindigkeit zu reduzieren. Es geht also um die Erhöhung der Effizienz beim Betrieb vieler WLAN-Stationen am gleichen Ort. Genau genommen geht es um die Erhöhung des flächenbezogenen Durchsatzes in Bits pro Quadratmeter (Bit/s/m^2).

Ideen für ein High Efficiency WLAN

- Künftig wird man vielleicht auf die rückwärtskompatible Unterstützung von IEEE 802.11 und IEEE 802.11b verzichten. Das bedeutet, dass die Übertragungsarten Frequency Hopping Spread Spectrum (FHSS, 1/2 MBit/s) und Direct Sequence Spread Spectrum (DSSS, 11 MBit/s) aus dem Standard fliegen. Parallel dazu ist die Arbeitsgruppe 802.11mc mit der Wartung der Norm beauftragt.
- IEEE 802.11ac soll mit seiner feinerstufigen Modulation (QAM256) auf das 2,4-GHz-Spektrum übertragen werden.
- Im 2,4-GHz-Spektrum sollen nur noch die Kanäle 1, 6 und 11 unterstützt werden. So sollen Beeinträchtigungen durch sich gegenseitig störende Signale, durch sich überlappende Kanäle, vermieden werden.
- IEEE 802.11ax wird auf OFDMA setzen und damit LTE ähnlicher werden.

WLAN-Sicherheit

In Netzwerken mit Leitungen und Kabel setzt das Abhören der Kommunikation das physikalische Anzapfen der Leitung voraus. Da Netzwerkkabel in der Regel innerhalb gesicherter Gebäude und verdeckt

verlaufen, ist das Abhören von Anfang an erschwert.
In einem Funknetz sieht das ganz anders aus. Hier dient der freie Raum als Übertragungsmedium. Die Reichweite der Datenübertragung wird hier nur durch die Stärke der Funksignale begrenzt. Sobald ein drahtloses Gerät seine Daten sendet, benötigt ein Angreifer nur ein Empfangsgerät, dass sich in Reichweite der Funksignale befindet, um Daten empfangen zu können.
Gleichzeitig besteht die Gefahr, dass nicht autorisierte Personen die WLAN-Infrastruktur benutzen oder Zugang zu einem Netzwerk erhalten. Deshalb sind Sicherheitsvorkehrungen zu treffen. Konkret die Verschlüsselung der Datenpakete und die Authentifizierung von Benutzern und WLAN-Clients.

Am Anfang der WLAN-Entwicklung war der IEEE-Standard 802.11 ein einziges Sicherheitsrisiko. Der Zugang zum WLAN war offen, also ohne Authentifizierung des Benutzers und die Datenübertragung war unverschlüsselt und somit für jeden einsehbar. Beides ist aus Sicherheitsgründen völlig inakzeptabel. Ganz egal, ob in einem privaten Netzwerk oder in einem Unternehmensnetzwerk.

Um ein WLAN sicher zu betreiben ist die Authentifizierung des Benutzers und die Verschlüsselung der Datenübertragung notwendig. Die deutsche Rechtsprechung sieht die Authentifizierung und Verschlüsselung eines WLANs zwingend vor. Wer ein WLAN unzureichend gesichert betreibt, gilt im Falle einer Rechtsverletzung über seinen Internet-Anschluss als Störer und wird demzufolge in Haftung genommen.
Wer einen WLAN-Router oder Access Point betreibt sollte darauf achten, dass die Authentifizierung und Verschlüsselung immer eingeschaltet ist.

Wegen der Erfordernis von Verschlüsselung und Authentifizierung in WLANs wurde in einem Schnellschuss WEP entwickelt. Doch schnell stellte sich heraus, dass es sich mit einfachen Mitteln knacken lässt. Die Schwachstellen wurden mit dem Nachfolger WPA Großteils eliminiert. Parallel entwickelte das IEEE den Standard IEEE 802.11i mit einem sicheren Verschlüsselungsverfahren auf Basis von AES. Aus dem Standard IEEE 802.11i ist WPA2 entstanden. WPA2 gilt als hinreichend sicher und ist gegenüber WEP und WPA zu bevorzugen.
WPS dient der einfacheren Authentifizierung per Pin oder Button, um einen WLAN-Client an einem per WPA- oder WPA2-gesicherten WLAN

anzumelden. Leider führt diese Vereinfachung dazu, dass die Authentifizierung unsicherer wird, solange WPS aktiviert ist.

- WEP (unsicher und veraltet)
- WPA (sicher und veraltet)
- WPA2 (sicher und aktuell)
- WPS (unsicher und aktuell)

WPA - WiFi Protected Access

WPA ist der Nachfolger von WEP zur Authentifizierung und Verschlüsselung von WLANs. Noch vor der offiziellen Verabschiedung von IEEE 802.11i, brachte die Herstellervereinigung Wi-Fi Alliance im Jahr 2003 auf Basis eines Entwurfs von IEEE 802.11i ein eigenes Verfahren mit der Bezeichnung "WiFi Protected Access" (WPA) heraus. Damit sollte Schaden und Imageverlust der WLAN-Technik verhindert werden, der durch die fehlenden Sicherheitsfunktionen entstanden war. Der entstehende Markt für kabellosen Netzwerke und die damit verbundenen Einnahmen sollten nicht gefährdet werden.

WPA basiert auf WEP-Hardware (RC4, XOR, ...) damit ein einfaches Software-Update einen Wireless Access Point von WEP auf WPA aktualisiert werden kann. WPA verwendet für die Verschlüsselung TKIP (Temporal Key Integrity Protocol). TKIP setzt auf den RC4-Algorithmus mit einer verbesserten Schlüsselberechnung (Fast Packet Keying, FPK). Allerdings ist das im Vergleich zu RC4 auch nicht wirklich sicherer. Aus diesem Grund wurde WPA nur übergangsweise eingesetzt und heute durchgängig WPA2 empfohlen.

Sicherheitskonzept von WPA

- Trennung von
- Benutzer-Authentifizierung
- Nachrichten-Verschlüsselung
- Integritätssicherung
- Schlüssel-Management
- Schlüssel werden regelmäßig neu erstellt
- verschiedene Schlüssel für verschiedene Anwendungen

- Master Key bildet nur die Grundlagen für die Schlüsselerzeugung

Schwachstellen von WPA

- TKIP basiert auf RC4, was gegen Known-Plaintext-Angriffe anfällig ist.
- ARP-Spoofing möglich.
- Passwort kann per Wörterbuchangriff erraten werden (Dictionary Attack). Deshalb sind schwache Passwörter, die zu kurz, zu einfach und zu wenig unterschiedliche Zeichen enthalten, nicht sicher.

WPA2 - WiFi Protected Access 2 / IEEE 802.11i

WPA2 (WiFi Protected Access 2) bzw. IEEE 802.11i ist ein Standard aus dem Jahr 2004 für die Authentifizierung und Verschlüsselung von WLANs, die auf den IEEE-Spezifikationen 802.11 basieren. Der Entwurf für ein standardisiertes Verschlüsselungsverfahren war deshalb notwendig, weil die Verschlüsselung mit WEP nicht wirklich sicher war. IEEE 802.11i sollte die groben Sicherheitsmängel von WEP beseitigen.

Nach der Verabschiedung von IEEE 802.11i erweiterte die Herstellervereinigung Wi-Fi Alliance den vorausgegangenen Standard WPA um eine zweite Version. Damit basiert WPA2 auf dem Standard IEEE 802.11i. Zu beachten ist, dass WPA2 mit IEEE 802.11i nicht identisch ist. WPA2 enthält nur einen Teil von IEEE 802.11i.

Sicherheitskonzept von WPA2

- Sicherheitskonzept von WPA übernommen und erweitert.
- Verschlüsselung: AES statt TKIP (RC4).
- Schwachstelle: TKIP als Fallback (schlecht).

Der wesentliche Unterschied zwischen WPA und WPA2 ist die Verschlüsselungsmethode. Während WPA das weniger sichere TKIP verwendet, kommt in WPA2 das sichere AES zum Einsatz.
AES (Advanced Encryption Standard) ist der Nachfolger des veralteten DES (Data Encryption Standard). In der Regel bringt AES mehr

Datendurchsatz als TKIP. Moderne WLAN-Chipsätze enthalten einen Hardware-Beschleuniger für AES. Bei TKIP muss in der Regel der interne Prozessor die Arbeit erledigen.

WPA-Variante		WPA	WPA2
Personal Mode	Authentifizierung	PSK	PSK
	Verschlüsselung	TKIP/MIC	AES-CCMP
Enterprise Mode	Authentifizierung	802.1x/EAP	802.1.x/EAP
	Verschlüsselung	TKIP/MIC	AES-CCMP

WPA2 Enterprise Mode

Der WPA2 Enterprise Mode ist mit IEEE 802.11i fast identisch. Der Unterschied ist die fehlende Funktion Fast Roaming, die für VoIP-, Audio- und Video-Anwendungen interessant ist. Mit dieser Funktion wird der Wechsel zwischen zwei Access Points (AP) schneller durchgeführt. Die Verbindung verläuft damit unterbrechungsfrei.
Wesentlicher Bestandteil ist die Authentifizierung per RADIUS.

WPA2 Personal Mode

Der WPA2 Personal Mode ist eine abgespeckte WPA2-Variante, die hauptsächlich in SOHO-Geräten für Privatanwender und kleine Unternehmen gedacht ist. Die Authentifizierung erfolgt mit ein Pre-Shared-Key (Passwort).

WPS - WiFi Protected Setup

WPS ist eine Spezifikation des Industriekonsortiums WiFi Alliance (WFA) hinter der sich eine Konfigurationsautomatik verbirgt. WPS erleichtert die WLAN-Konfiguration von WLAN-Clients. Die Konfiguration erfolgt entweder per Knopfdruck (WPS-PBC) oder Pin-Eingabe (WPS-PIN).
Die Hauptschwierigkeit bei der Konfiguration eines WLAN-Clients ist die Eingabe des WLAN-Passworts (Pre-Shared-Key), welches im Access

Point hinterlegt ist. WPS vereinfacht und automatisiert diese Umständlichkeit.

Eigenschaften von WPS

- Authentifizierung des WLAN-Clients gegenüber dem WLAN-AP
- Authentifizierung des WLAN-AP gegenüber dem WLAN-Client
- Automatische Konfiguration des WLAN-Clients mit dem WLAN-Passwort

Authentifizierung nach Knopfdruck (WPS-PBC)

Beim WPS-PBC-Verfahren drückt man einen Knopf am WLAN-Router oder aktiviert den WPS-Authentifizierungsmechanismus in der Administrations-Oberfläche des WLAN-Routers. Dabei wird die WPS-Anmeldephase gestartet. Der erste WLAN-Client, der sich daraufhin per WPS anmeldet, bekommt das Passwort für die WLAN-PSK-Authentifizierung.
Das bedeutet, dass für einen kurzen Moment das WLAN für eine WPS-Authentifizierung und Passwort-Übergabe offen ist. Das mag unsicher erscheinen. Allerdings ist die WPS-PBC-Methode praktisch nicht angreifbar. Der Angreifer hat dabei das Problem, dass er nicht weiß, ab wann das Zeitfenster gilt. Er müsste also dauernd eine WPS-Authentifizierung vornehmen. Da man als WLAN-Nutzer nicht ständig neue WLAN-Clients authentifiziert, ist ein solcher Angriff eher unwahrscheinlich. Der Angreifer wird eher eine andere Angriffsmethode wählen.
Allein dadurch, dass WPS-PBC nur bei Bedarf aktiviert ist, ist es sicherer als die WPS-Pin-Methode, die immer aktiv und deshalb auch immer angreifbar ist.

Authentifizierung per Zahleneingabe (WPS-Pin)

Die Authentifizierung per WPS-Pin sieht die Eingabe einer achtstelligen Zahlenfolge auf dem WLAN-Client vor. Gerade bei Smartphones ist das eine echte Erleichterung, weil man hier eine kleine Tastatur hat, bei der die Passwort-Eingabe ziemlich fummelig sein kann. Vor allem, wenn man ein kompliziertes WLAN-Passwort mit Buchstaben, Zahlen und Sonderzeichen hat.

Die WPS-Pin-Methode sieht vor, dass das WLAN-Passwort dem WLAN-Client mitgeteilt wird, wenn eine korrekte WPS-Pin eingegeben wurde. Dabei übermittelt der WLAN-Router dem Client ein Einrichtungspaket mit dem WLAN-Passwort.

Ablauf der Authentifizierung per WPS-Pin

1. Der WLAN-Client bittet den WLAN-AP um eine WPS-Pin-Authentifizierung.
2. Anschließend tauschen beide den Schlüssel für die Transport-Verschlüsselung per Diffie-Hellman aus.
3. Die Authentizität des WLAN-APs muss vom Client geprüft werden, weil sich ein fremder AP die Pin abgreifen könnte. Das heißt, der Client muss sicherstellen, dass er mit dem richtigen AP die WPS-Authentifizierung durchläuft und nicht mit einem AP, der zufällig den gleichen Namen hat.
4. Der AP packt je eine vierstellige Pin-Hälfte (mit Zufallszahl gehasht), der insgesamt achtstelligen Pin, in einen verschlüsselten Container und schickt sie an den WLAN-Client. Der kann damit allerdings noch nichts anfangen.
5. Der Client schickt jetzt die erste Hälfte seiner Pin transportverschlüsselt an den AP.
6. Wenn dieser erste Teil der Pin korrekt ist, dann schickt der AP die Zufallszahl für die erste Pin an den Client.
7. Der Client kann daraufhin die erste Pin (mit Zufallszahl gehasht) verifizieren. Er weiß dann, ob er mit dem richtigen AP verbunden ist.
8. Dann schickt der Client die zweite Hälfte seiner Pin transportverschlüsselt an den AP.
9. Wenn auch der zweite Teil der Pin korrekt ist, dann bekommt der WLAN-Client vom AP die zweite Zufallszahl und das WLAN-Passwort.
10. Mit der zweiten Zufallszahl verifiziert der Client auch den zweiten Teil der Pin, die er vom AP bekommen hat.
11. Wenn diese korrekt ist erfolgt die Anmeldung mit dem WLAN-Passwort per WPA/WPA2.

Wie sicher ist WPS?

Die WPS-Pin-Methode könnte sicher sein, wenn die WLAN-Router-Hersteller die WPS-Spezifikation richtig und vollständig implementieren würden.
Die Spezifikation fordert unter anderem ein kleines Display am WLAN-Router, dass eine einmal gültige WPS-Pin anzeigt. Und das auch nur bei Bedarf. In der Praxis haben WLAN-Router kein solches Display, sondern eine statische WPS-Pin, die im schlechtesten Fall auf der Rückseite des Geräts im Typenschild zu finden ist. In der WPS-Spezifikation wird jedoch von einer statischen WPS-Pin explizit abgeraten. Nur halten sich die wenigsten Hersteller daran und das widerspricht sogar anerkannten Sicherheitsstandards.

Wenn man nicht weiß, ob das WPS-Verfahren des eigenen WLAN-Routers gegen irgendeinen Angriff anfällig ist, sollte man WPS generell im Router deaktivieren. Allein schon deshalb, weil man nicht weiß, ob es in Zukunft nicht noch weitere Verfahren und Angriffe gibt, um WPS auszuhebeln.
Die beschriebenen Probleme kann man vermeiden, wenn man WPS-PBC einsetzt. Bei dieser Methoden wird eine entsprechende WPS-Taste am WLAN-Router vorausgesetzt.

HomePlug-Powerline

HomePlug-Powerline ist eine Technik, mit der die Leitungen eines hausinternen Stromnetzes als Datennetz verwendet werden können. Mit einfachsten Mitteln kann ein Netzwerk über die vorhandenen Stromkabel aufgebaut werden. Es müssen keine neuen Leitungen gezogen werden. Und die Konfiguration der Geräte ist mit der beiliegenden Software fast ein Kinderspiel.

Die HomePlug-Powerline-Alliance ist eine Initiative einiger Unternehmen mit dem Ziel, die Entwicklung, Standardisierung und Spezifikation neuer, leistungsfähiger Powerline-Komponenten voranzutreiben. Die HomePlug-Powerline-Adapter verschiedener Generationen sind untereinander kompatibel.

HomePlug-Powerline-Adapter

Der HomePlug-Powerline-Adapter ist die technische Einrichtung, die den Übergang von einem Datennetz in das Stromnetz darstellt. Mit HomePlug-Powerline-Adapter wird das hausinterne Stromnetz in ein Daten-Netzwerk verwandelt. Und das an jeder Steckdose innerhalb der Haus- bzw. Wohnungsverkabelung. Damit wird jede Steckdose automatisch zum Netzwerkanschluss.
In der einfachsten Variante werden die PCs über HomePlug-Powerline-Adapter für Ethernet oder USB mit dem Stromnetz verbunden. Die Datenkommunikation ist dann über die Stromleitungen in der ganzen Wohnung oder Haus möglich.
Es gibt auch Powerline-WLAN-Adapter, die in eine Steckdose gesteckt werden und als WLAN-Access-Point fungieren. So lassen sich auch WLAN-Geräte an das Powerline-Netz anbinden.
Die Adapter gibt es in den Geschwindigkeitsvarianten 28, 85, 200, 500, 1.200 und 1.800 MBit/s. Über einem Router kann jeder PC gleichzeitig Zugang zum Internet haben.

Das internationale DSL-Forum hat HomePlug AV als die Inhouse-Technik gewählt, die von den nach DSL-Forum-Normen zugelassenen DSL-Modems/-Routern unterstützt wird. Das DSL-Forum ist eine internationale Industrievereinigung, die die Normen für den gesamten DSL-Markt festlegt.

HomePlug AV

HomePlug AV erreicht auf einem 26 MHz breiten Kanal (2 bis 28 MHz) theoretisch 200 MBit/s. Doch die Dämpfung steigt mit der Frequenz. Die Höchstgeschwindigkeit kommt dann nur auf kurzen Strecken zustande. In typischen Wohnungen erreicht man 20 bis 80 MBit/s netto.

HomePlug AV2

HomePlug AV2 erreicht seinen höheren Datendurchsatz von 500 MBit/s durch Detailverbesserungen und ein doppelt so breites Frequenzband von 2 bis 85 MHz. Manche Geräte nutzen den Frequenzbereich nur bis 68 MHz, um Störungen von UKW zu vermeiden.
Optimiert wird das Übertragungsverfahren mit Diversity und einem

verbesserten Modulationsverfahren. Die Optimierungen greifen allerdings nur bei optimalen Verbindungen. Schlechte Powerline-Verbindungen kommen mit HomePlug AV2 auf nur etwa 10 bis 50 Prozent mehr Durchsatz.
Im praktischen Einsatz erreichen HomePlug-AV2-Adapter damit bis zu 150 MBit/s auf der Stromleitung.

In sogenannte Gigabit-Powerline-Adaptern steckt die Technik des Chipentwicklers Gigle, der von der Firma Broadcom übernommen wurde. Die Gigle-Technik benutzt ein Frequenzband von 55 bis 305 MHz und erreicht damit bis zu 900 MBit/s auf der Stromleitung.
Obwohl man anhand der Bruttodatenrate mehr erwarten dürfte übertragen die Adapter mit der proprietären Gigle-Technik nur selten mehr als die HomePlug-AV2-Adapter.

HomePlug AV1200 und AV1800

Durch den Einsatz von MIMO (bekannte von WLAN) kann die Powerline-Technik zwei Datenströme im selben Frequenzband gleichzeitig übertragen. Dabei ergibt sich eine maximale Bruttodatenrate von 1.200 MBit/s (AV1200) im Frequenzband von 2 bis 68 MHz. Unter günstigen Bedingungen erreicht man damit etwa 400 MBit/s.
Mit AV1800 (1.800 MBit/s) erfolgt die Übertragung in einem breiteren Frequenzband von 2 bis 86 MHz.

Powerline als Vernetzungsalternative

Powerline ist ein Netzwerk aus der Steckdose. Statt WLAN oder Netzwerkverkabelung zu installieren könne auch hausinterne oder wohnungsinterne Stromleitungen zur Vernetzung zweier oder mehrerer PCs genutzt werden. Die PCs können überall dort stehen, wo eine Steckdose vorhanden ist. In der einfachsten Variante werden die PCs über HomePlug-Powerline-Adapter für Ethernet oder USB mit dem Stromnetz verbunden. Die Datenkommunikation ist dann über die Stromleitungen in der ganzen Wohnung oder Haus möglich.
Es gibt auch Powerline-WLAN-Adapter, die in eine Steckdose gesteckt werden und als WLAN-Access-Point fungieren. So lassen sich auch WLAN-Geräte an das Powerline-Netz anbinden.

HomePlug-Powerline eignet sich insbesondere dann, wenn eine Neuverkabelung aufgrund des Aufwands nicht in Frage kommt und alle anderen Vernetzungstechniken, wie WLAN oder 10BaseT über Telefonleitungen nicht zuverlässig funktioniert.

- Einfache Vernetzung mehrerer PCs.
- Internet-Zugang für einen oder mehrere PCs.
- Erhöhung der Reichweite von WLAN durch Einstecken an jeder Steckdose.

TCP/IP

IP – Internet Protocol Version 4

IP – Internet Protocol Version 6

TCP – Transmission Control Protocol

UDP – User Datagramm Protocol

TCP/IP

TCP/IP ist eine Protokoll-Familie für die Vermittlung und den Transport von Datenpaketen in einem dezentral organisierten Netzwerk. Es wird im LAN (Local Area Network) und im WAN (Wide Area Network) verwendet. Der Erfolg des Internets ist zum großen Teil auch den Protokollen rund um TCP/IP zu verdanken.

Schicht	Dienste und Protokolle
Anwendung	Anwendungen
Transport	TCP - Transmission Control Protocol
Internet	IP - Internet Protocol
Netzzugang	Übertragungssystem

Die Abkürzung TCP/IP steht für die beiden Protokolle Transmission Control Protocol (TCP) und Internet Protocol (IP).
Das Internet Protocol (IP) ist auf der Vermittlungsschicht (Schicht 3) des OSI-Schichtenmodells angeordnet. Das Transmission Control Protocol (TCP) ist auf der Transportschicht (Schicht 4) des OSI-Schichtenmodells angeordnet. Innerhalb des DoD-Schichtmodells bildet TCP/IP das Rückgrad für alle Kommunikationsverbindungen.

Aufgaben und Funktionen von TCP/IP

Die zentrale Aufgabe von TCP/IP ist dafür Sorgen zu tragen, dass Datenpakete innerhalb eines dezentralen Netzwerks beim Empfänger ankommen. Dafür stellt TCP/IP die folgenden zentralen Funktionen bereit.

- Logische Adressierung / Logical Addressing (IP)
- Wegfindung / Routing (IP)
- Fehlerbehandlung und Flussteuerung / Error Control and Flow Control (TCP)
- Anwendungsunterstützung / Application Support (TCP)
- Namensauflösung / Name Resolution (DNS)

Die Besonderheiten und Probleme der paketorientierten Datenübertragung sind sehr vielfältig und erfordern deshalb spezielle Lösungen und Funktionen, die an dieser Stelle nicht alle berücksichtigt werden. Die folgende Darstellung und Beschreibung ist also nur eine Auswahl der wichtigsten Funktionen.

Logische Adressierung / Logical Addressing (IP)

In einem einfachen, lokalen Netzwerk empfängt jeder Netzwerk-Adapter jedes Datenpaket. Das ist dann der Fall, wenn sich prinzipbedingt alle Netzwerk-Teilnehmer das Übertragungsmedium teilen müssen (z. B. bei WLAN oder Ethernet). Bei Netzwerken mit wenigen Teilnehmern ist das eine praktikable Lösung. Doch in einem Netzwerk mit vielen Tausend oder sogar Millionen Teilnehmern ist das wenig sinnvoll. Ob ein Datenpaket seinen richtigen Empfänger erreicht, wäre dann dem Zufall überlassen.
Deshalb bedarf es einer Möglichkeit das Netzwerk physikalisch (Topologie) und logisch (Adressierung) zu strukturieren. Innerhalb von TCP/IP übernimmt IP die logische Adressierung von Netzwerken und deren Teilnehmern. Dabei gelangen Datenpakete nur in das Netz, in das sie gehören. Die Verfahren der Adressierung sind zum Beispiel fest definierte Netzklassen, Subnetting und CIDR.

Wegfindung / Routing (IP)

Während die logische Adressierung durch IP dafür sorgt, dass ein großes Netzwerk in Segmente geteilt wird, sorgt Routing als eine Art Wegfindung dafür, dass ein Datenpaket sein Ziel über die einzelnen Netzwerk-Segmente erreicht. Für jedes einzelne Datenpaket wird in jedem Netzknoten auf dem Weg vom Sender zum Empfänger, der nächste Netzknoten ermittelt. Auf diese Weise findet ein Datenpaket den Weg zu seinem Empfänger, auch wenn der in einem unbekannten Netzwerk-Segment liegt.

Fehlerbehandlung und Flussteuerung / Error and Flow Control (TCP)

Durch TCP stehen Sender und Empfänger ständig in Kontakt zueinander (Verbindungsmanagement). Obwohl es sich eher um eine virtuelle

Verbindung handelt, werden während der Datenübertragung ständig Kontrollmeldungen ausgetauscht, weshalb man von einer verbindungsorientierten Kommunikation spricht. Wird ein Fehler festgestellt, wird das betreffende Datenpaket erneut übertragen. Zusätzlich ist eine Daten-Flusssteuerung notwendig, um die verfügbare Übertragungsgeschwindigkeit auszunutzen. Weil es im Internet für eine Ende-zu-Ende-Verbindung keinen exklusiven Kanal mit fester Übertragungsgeschwindigkeit gibt, bedarf es hier einer automatischen Anpassung.

Anwendungsunterstützung / Application Support (TCP)

Ähnlich wie Rechner mit IP-Adressen in Netzwerken adressiert werden, bedarf es einer Unterscheidung der Kommunikationsverbindungen zwischen spezifischen Anwendungen, die gemeinsam auf einem Rechner laufen. TCP- und UDP-Ports (Nummern) bilden eine Software-Abstraktion, um spezifische Anwendungen und deren Kommunikationsverbindungen voneinander unterscheiden zu können.

Namensauflösung / Name Resolution (DNS)

In einem TCP/IP-Netzwerk werden Verbindungen zwischen den Netzwerk-Teilnehmern mit IP-Adressen aufgebaut. Eine IP-Adresse hat ursprünglich die binären Form bzw. Schreibweise und ist damit eine Folge von 1en und 0en, mit denen elektronische Schaltungen und digitale Programme arbeiten. Zur besseren Lesbarkeit werden IP-Adressen in der dezimalen (IPv4) oder hexadezimalen (IPv6) Schreibweise dargestellt. Doch weder die Bitfolge, noch eine andere Schreibweise sind für das menschliche Gehirn einfach zu erfassen und zu merken. Der Mensch verwendet lieber Namen um eine Sache zu benennen und zu identifizieren. Deshalb werden statt IP-Adressen eher Namen zur Adressierung auf der Anwendungsebene verwendet. Damit eine Verbindung auf IP-Ebene möglich ist, ist eine Namensauflösung notwendig. Gemeint ist, dass zu einem Computer- oder Domain-Namen eine zugehörige IP-Adresse ermittelt werden muss. Man bezeichnet das als Namensauflösung.

Vorteile von TCP/IP

TCP/IP hat mehrere entscheidende Vorteile. Jede Anwendung ist mit TCP/IP in der Lage über jedes Netzwerk Daten zu übertragen und auszutauschen. Dabei ist es egal, wo sich die Kommunikationspartner befinden. Das Internet Protocol (IP) sorgt dafür, dass das Datenpaket sein Ziel erreicht und das Transmission Control Protocol (TCP) steuert die Datenübertragung und sorgt für die Zuordnung von Datenstrom und Anwendung.

Für die Anwendungen soll die Art und Weise der physikalischen und logischen Datenübertragung keine Rolle spielen. Der Anwender soll sich auch nicht um Verbindungsaufbau und -abbau kümmern müssen. So lange der Anwender eine korrekte Adresse kennt, wird sich TCP/IP um den Verbindungsaufbau, -abbau und die Übertragung zum Ziel kümmern. Ganz egal welche Anwendung oder welcher Übertragungsweg verwendet wird.

- TCP/IP ist ein weltweit gültiger Standard und an keinen Hersteller gebunden.
- TCP/IP kann auf einfachen Computern und auf Supercomputern implementiert werden.
- TCP/IP ist in LANs und WANs nutzbar.
- TCP/IP macht die Anwendung vom Übertragungssystem unabhängig.

Nachteile von TCP/IP

Allerdings ist TCP/IP alles andere als eine effiziente Methode um Daten zu übertragen. Die Daten werden in kleine Datenpakete aufgeteilt. Damit der Empfänger eines Datenpakets weiß, was er damit machen soll, wird dem Datenpaket ein Kopfdatensatz, der als Header bezeichnet wird, vorangestellt. Pro Datenpaket ergibt sich ein Verwaltungsanteil von mindestens 40 Byte pro TCP/IP-Datenpaket. Nur wenn Datenpakete von mehreren kByte gebildet werden, bleibt der Verwaltungsanteil im Vergleich zu den Nutzdaten (Payload) gering.

Wenn die Anwendung bestimmte Anforderungen an das Übertragungssystem stellt, dann lässt sich das nur sehr schwer zu

realisieren. Die systeminterne Kommunikation zwischen Anwendung und Übertragungssystem über TCP/IP hinweg ist nicht vorgesehen.
Auch lässt sich ein koordinierten Austausch von Verbindungsqualität und -anforderungen zwischen Netzknoten nur sehr schwer netzüberbreifend realisieren. Es gibt zwar Quality of Service (QoS). Doch das ist optional und erfordert die Kontrolle über das Netzwerk, was in einem dezentral organisierten Netzwerk, wie dem Internet, nicht vorgesehen ist.

Man spricht in diesem Zusammenhang auch von Netzneutralität. Die Netzneutralität fordert, dass jedes Paket gleich behandelt wird. Das hat den Nachteil, dass bestimmte Datenpakete nicht priorisiert werden können. Das hat wiederum die Konsequenz, dass bestimmte Anwendungen im Internet mit TCP/IP nicht gut funktionieren.

IPv4 - Internet Protocol Version 4

Das Internet Protocol, kurz IP, wird im Rahmen der Protokollfamilie TCP/IP zur Vermittlung von Datenpaketen verwendet. Es arbeitet auf der Schicht 3 des OSI-Schichtenmodells und hat maßgeblich die Aufgabe, Datenpakete zu adressieren und in einem dezentralen, verbindungslosen und paketorientierten Netzwerk zu übertragen. Dazu haben alle Netzwerk-Teilnehmer eine eigene IP-Adresse im Netzwerk. Sie dient nicht nur zur Identifikation eines Hosts, sondern auch des Netzes, in dem sich der jeweilige Host befindet.

Das Internet Protocol (IP) im TCP/IP-Protokollstapel

<table>
<tr><td>Schicht</td><td colspan="4">Dienste / Protokolle / Anwendungen</td></tr>
<tr><td>Anwendung</td><td>HTTP</td><td>IMAP</td><td>DNS</td><td>SNMP</td></tr>
<tr><td>Transport</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td>Internet</td><td colspan="4">IP (IPv4 / IPv6)</td></tr>
<tr><td>Netzzugang</td><td colspan="4">Ethernet, WLAN, ...</td></tr>
</table>

Neben IPv4 gibt es noch IPv6. Beide Protokolle arbeiten in der Regel parallel, was als Dual Stack bezeichnet wird.

Aufgaben und Funktionen von IPv4

- Logische Adressierung (IPv4-Adresse)
- IPv4-Konfiguration
- IPv4-Header
- IP-Routing
- Namensauflösung

IPv4-Adressen

Die wichtigste Aufgabe von IP (Internet Protocol) ist, dass jeder Host in einem dezentralen TCP/IP-Netzwerk gefunden werden kann. Dazu wird jedem Hardware-Interface (Netzwerkkarte oder -adapter) eine logische IPv4-Adresse zugeteilt.
Die IPv4-Adresse ist mit den Angaben zu Straße, Hausnummer und Ort einer Anschrift vergleichbar.

Aufbau einer IPv4-Adresse

Damit die IPv4-Adresse von Hardware und Software einfach verarbeitet werden kann, liegt sie in einem Bitcode bzw. einer Bitfolge aus Einsen (1) und Nullen (0) vor. Sie ist somit maschinenlesbar. Die Bitfolge hat 32 Stellen bzw. ist 4 Byte (32 Bit) groß.

Schreibweise	Beispiel-Adresse			
Binär/Dual	0111 1111	0000 0000	0000 0000	0000 0001
Hexadezimal	7F	00	00	01
Dezimal	127	0	0	1

Zur einfacheren Lesbarkeit und auch zur Segmentierung werden die 32 Bit einer IPv4-Adresse in jeweils 8 Bit (1 Byte) aufgeteilt und durch einen Punkt voneinander getrennt. Dabei kann jedes Byte durch die achtstellige 1er- und 0er-Folge einen dezimalen Wert von 0 bis 255 annehmen. Das sind 256 Werte pro Stelle. Die binäre IPv4-Adresse 01111111.00000000.00000000.00000001 ergibt die IPv4-Adresse 127.0.0.1.

Obwohl die dezimale Schreibweise üblich ist, können IPv4-Adressen auch als hexadezimale Zahl oder Oktalzahl angegeben werden. Beides ist in der Praxis unüblich und deshalb wenig sinnvoll. Die Besonderheit bei IPv4-Adressen in oktaler Schreibweise ist die Kennzeichnung mit einer führenden Null. Betriebssysteme wie zum Beispiel ab Windows 8.1, Ubuntu 13.10 und Mac OS X 10.9 halten sich an diese Regel. Das bedeutet, gibt man in die Browser-Adresszeile eine IPv4-Adresse mit führender Null ein, dann wird eine oktale Zahl angenommen und in die dezimale Darstellung umgerechnet. Anschließend wird eine Verbindung zu dieser Adresse aufgebaut. Aus diesem Grund sollte man führende Nullen bei der dezimalen Schreibweise von IPv4-Adressen generell weglassen.

- Falsche Schreibweise: 127.000.000.001
- Richtige Schreibweise: 127.0.0.1

Struktur im IPv4-Adressraum

Der IPv4-Adressraum umfasst 32 Bit und reicht von 0.0.0.0 bis 255.255.255.255. Rein rechnerisch ergibt sich aus einer 32-Bit-Adresse eine Anzahl von 2 hoch 32 Adressen. Das entspricht über 4 Milliarden Adressen. Als man den Adressraum definierte, entsprach das damals ungefähr der Weltbevölkerung. Damals war es undenkbar, dass jeder Mensch irgendwann mal eine IPv4-Adresse brauchen, geschweige denn, dass jemand ein persönliches Endgerät (Smartphone) mit einer IPv4-Adresse mit sich herumtrage würde.

Für jede IP-Adresse müsste ein IP-Router wissen, wo sich der entsprechende Host befindet. Das wäre bei 4 Milliarden IPv4-Adressen ein sehr großer Datenbestand, der bei jedem Datenpaket erneut durchlaufen werden müsste, um den Host zu finden. Außerdem müsste jeder Router auf dem Weg zum Host den Vorgang wiederholen. Das würde viel Rechenleistung und Speicherkapazität voraussetzen, die in der Anfangszeit von TCP/IP undenkbar war. Aus diesem Grund hat man dem IPv4-Adressraum eine gewisse Struktur gegeben, um die Routing-Entscheidungen in den Routern einfacher zu machen. Insbesondere vor dem Hintergrund, dass damals die Verfügbarkeit von Rechenleistung und Speicher geringer war.

Im Prinzip hat man sich eine Art Verzeichnis überlegt, wo drin steht, wo sich eine IPv4-Adresse im Netzwerk befindet. Bei Telefonnummern kennen wir die Aufteilung in Ländervorwahl, Ortsvorwahl und Teilnehmerrufnummer. So eine Struktur hatte man sich auch bei IPv4-Adressen vorgestellt. Damit IP-Router möglichst effizient arbeiten können, wurden IPv4-Adressen anfangs hierarchisch zugeteilt. Das hat aber nicht sehr lange funktioniert. Wegen einem zu geringen Adressraum gilt die regionale Zuteilung, wie bei Telefonnummer, nicht mehr.

	Netzadressen	Hostadresse	Subnetzmaske/CIDR
IPv4-Adresse	xxx	.yyy.yyy.yyy	255.0.0.0 /8
Subnetzmaske	255	.0.0.0	
IPv4-Adresse	xxx.xxx	.yyy.yyy	255.255.0.0 /16
Subnetzmaske	255.255.	.0.0	
IPv4-Adresse	xxx.xxx.xxx	.yyy	255.255.255.0 /24
Subnetzmaske	255.255.255	.0	

Trotzdem bilden IPv4-Adressen eine Hierarchie ab. Jede IPv4-Adresse besteht im Prinzip aus zwei Teilen. Dem Netz (Subnetz) bzw. der Netzadresse (Netz-ID) und dem Host bzw. der Hostadresse (Host-ID). Beide Teile werden in der IP-Adresse abgebildet.
Für das IP-Routing ist nur die Netzadresse wichtig. Und die Hostadresse ist nur für den Router wichtig, in dessen Netz sich der Host befindet.
Bei einer IPv4-Adresse ist der vordere Teil die Netzadresse und der hintere Teil die Hostadresse. Die Teilung findet typischerweise an einem Punkt (".") statt. Aber nicht immer. An welcher Stelle genau die IPv4-Adresse in Netz und Host geteilt wird, dass entscheidet die Netzklasse, die Subnetzmaske oder das CIDR-Suffix.

Durch die Strukturierung entstanden jedoch Lücken im Adressraum, der nicht genutzt wird und der im Prinzip auch nie genutzt werden kann. Das Entstehen von Lücken nennt man Fragmentierung des IPv4-Adressraums. Das hat dazu geführt, dass ein Teil des Adressraums nicht nutzbar ist. Dazu gehört zum Beispiel der Adressbereich von 0.0.0.0 bis 0.255.255.255.

In den nutzbaren Adressbereichen ist die erste und letzte Adresse eines Subnetzes immer durch das ganze Netz (".0") und die Broadcast-Adresse (".255") belegt. Welche das genau sind, hängt von der Aufteilung der Subnetze ab. Beispielsweise sind bei einem /28-Netz mit insgesamt 16 IPv4-Adressen (2 hoch 4 gleich 16) deshalb nur 14 IPv4-Adressen nutzbar. Im kleinsten Netz (/30) mit vier IPv4-Adressen sind sogar nur zwei IPv4-Adressen nutzbar. Die anderen zwei sind durch die Strukturierung (Netz- und Broadcast-Adresse) verschwendet.

Vergabe von IPv4-Adressen

IPv4-Adressen sind begrenzt und müssen offiziell beantragt und zugeteilt werden. Man kann also nicht irgendeine IPv4-Adresse verwenden.
Die Adressvergabe folgte ursprünglich einer regionalen Hierarchie. Das heißt, der IPv4-Adressraum wurde in Regionen aufgeteilt. Man hat dazu Regional Internet Registries (RIR) mit der Aufgabe betraut IPv4-Adressen zu vergeben. In Europa und dem Mittleren Osten ist dafür das RIPE NCC zuständig.
Leider kam es wegen der unbedachten Vergabepraxis von Adressbereichen in den Anfangsjahren und dem unvorhersehbaren Wachstum des Internets dazu, dass wir heute an IPv4-Adressen-Knappheit leiden. Deshalb ist man, in mit IPv4-Adressen unterversorgten Gebieten, auf die Einführung von IPv6 angewiesen.

IPv4-Netzklassen

Das Prinzip der IPv4-Netzklassen oder auch die englische Bezeichnung "classful network" definiert eine feste Unterteilung des IPv4-Adressraums in Teilnetze bzw. Subnetze. Dadurch kann die Größe eines Netzwerks und dessen Adresse aus der IPv4-Adresse abgeleitet werden. Mit der Netzklasse wird aber nicht die tatsächliche Größe eines Netzwerks angegeben, sondern nur wie viele Adressen es maximal umfassen kann.

Die Netzklasse definiert, an welcher Stelle in der IPv4-Adresse die Trennung zwischen Netz- und Hostadresse stattfindet.

- Class A: 8 Bit Netz (y) und 24 Bit Host (x): yyy.xxx.xxx.xxx
- Class B: 16 Bit Netz (y) und 16 Bit Host (x): yyy.yyy.xxx.xxx
- Class C: 24 Bit Netz (y) und 8 Bit Host (x): yyy.yyy.yyy.xxx

- Class D: für Multicast reserviert, lokal nutzbar
- Class E: reserviert, nur teilweise benutzt

Dieses starre Netzklassen-Modell ist aber reichlich unpraktisch. Es führt dazu, dass zu große Adressbereiche pauschal vergeben werden (müssen), auch wenn die nutzende Organisation die Anzahl der Adressen gar nicht wirklich braucht. Umgekehrt bekommen kleine Organisationen nur einen kleinen Adressbereich, obwohl sie vielleicht einen größeren bräuchten. Das Prinzip der Netzklassen wird heute nur noch in Randbereichen angewendet. Maßgeblich ist heute Subnetting und CIDR. Von Netzklassen spricht man heute nur noch in Bildung und Lehre. Das Prinzip der Netzklassen wurde im Jahr 1993 von CIDR (Classless Inter-Domain Routing) ersetzt und spielt deshalb in der Praxis heute keine Rolle mehr.

Subnetting und Supernetting

Durch Subnetting kann man große IPv4-Adressbereiche, die ehemals einer Netzklasse fest zugewiesen gewesen sind (Netzklasse bestimmt die Größe eines Netzwerks), in mehrere kleine IPv4-Adressbereiche aufteilen. Supernetting macht es genau umgekehrt. Durch Supernetting kann man mehrere kleine IPv4-Adressbereiche, in einen größeren IPv4-Adressbereich umwandeln.

Jede IPv4-Adresse besteht aus zwei Teilen. Jeder Teil hat eine bestimmte Bedeutung. Der vordere Teil ist die Adresse für das Netzwerk, indem sich der Host befindet. Der hintere Teil ist die Adresse für den Host. Wo sich die IPv4-Adresse teilt, wird beim Subnetting von der Subnetzmaske bzw. Subnetmask (engl.) bestimmt. Die Subnetzmaske besteht ebenso wie die IPv4-Adresse aus 32 Bit. Die Darstellung der Subnetzmaske entspricht jedoch einer geschlossenen Kette beginnend mit Einsen und abschließenden Nullen. Ein Beispiel: 11111111 11111111 11111111 00000000. Das entspricht in der Dezimaldarstellung 255.255.255.0. Legt man die Subnetzmaske wie eine Maske über die IP-Adresse ergibt sich die Teilung in Netzadresse und Hostadresse an der Stelle, wo sich der Wechsel von "1" auf "0" befindet.

CIDR - Classless Inter-Domain Routing

CIDR (Classless Inter-Domain Routing) ist trotz der Namensgebung kein Routing-Protokoll, sondern ein Verfahren, um den IPv4-Adressraum effizienter zu nutzen. CIDR wurde 1993 eingeführt, um das Konzept der Netzklassen abzulösen. Mit CIDR fällt die feste Zuordnung zwischen IPv4-Adresse und einer bestimmten Netzklasse weg. Vor CIDR hat die Netzklasse definiert, welcher Teil der Netzteil und welcher der Hostteil einer IPv4-Adresse ist. Mit CIDR steckt diese Information in einem Suffix.

Vereinfacht ausgedrückt ist das Suffix eine Schreibweise, die die Subnetzmaske abkürzt. Das Suffix gibt die Anzahl der aufeinander folgenden 1er Bits in der Subnetzmaske an.

Schreibweise mit Subnetzmaske	Binäre Schreibweise (Subnetzmaske)	Verkürzte Schreibweise mit CIDR-Suffix
10.0.0.1 (255.0.0.0)	11111111.00000000.00000000.000000	10.0.0.1/8
192.168.0.1 (255.255.255.0)	11111111.11111111.11111111.00000000	192.168.0.1/24

Reservierte Subnetze und nicht verfügbare IPv4-Adressen (Reserved IP Adresses)

Im theoretisch möglichen Adressbereich von 0.0.0.0 bis 255.255.255.255 sind bestimmte Adressen und Subnetze für spezielle Anwendungen reserviert oder gesperrt. Die Kenntnis über diese Adressen oder Adressbereiche ist deshalb wichtig, um eine fehlerhafte IPv4-Konfiguration zu vermeiden oder zu erkennen.

- Die erste und letzte IPv4-Adresse eines Subnetzes sind reserviert
  - x.x.x.0: Netz- oder Subnetz-Adresse
  - x.x.x.255: Broadcast-Adresse

- Nicht routbare IPv4-Adressen
    - 0.0.0.0/8 (0.0.0.0 bis 0.255.255.255): Standard- bzw. Default-Route im Subnetz (Current Network).
    - 127.0.0.0/8 (127.0.0.0 bis 127.255.255.255): Reserviert für den Local Loop bzw. Loopback.
- Private IPv4-Adressen
    - 10.0.0.0/8 (10.0.0.0 bis 10.255.255.255): Reserviert für die Nutzung in privaten Netzwerken. Nicht im Internet routbar.
    - 172.16.0.0/12 (172.16.0.0 bis 172.31.255.255): Reserviert für die Nutzung in privaten Netzwerken. Nicht im Internet routbar.
    - 192.168.0.0/16 (192.168.0.0 bis 192.168.255.255): Reserviert für die Nutzung in privaten Netzwerken. Nicht im Internet routbar.
    - 169.254.0.0/16 (169.254.0.0 bis 169.254.255.255): Link-local Adresses für IPv4LL.
- Class D (Multicast)
    - 224.0.0.0 bis 239.255.255.255: Nicht im Internet, sondern nur lokal in den eigenen Netzen routbar.
- Class E (reservierte Adressen)
    - 240.0.0.0 bis 255.255.255.255: Alte IPv4-Stacks, die nur mit Netzklassen arbeiten, kommen damit nicht klar.

Localhost oder Local Loop

Der gesamte Adressbereich von 127.0.0.0 bis 127.255.255.255 ist für den Local Loop bzw. Loopback reserviert.
Die IPv4-Adresse 127.0.0.1 hat jeder IPv4-Host. Diese IPv4-Adresse wird auch als Localhost (Namensauflösung: localhost) bezeichnet. Es handelt sich dabei um ein virtuelles Interface. Das aber keiner Hardware zugeordnet ist. Dieses virtuelle Interface wird von Anwendungen verwendet, die über das Netzwerk kommunizieren wollen/müssen, dabei aber nicht das lokale Netzwerk in Anspruch nehmen können/wollen.
Wird ein Datenpaket mit der Ziel-Adresse 127.0.0.1 verschickt, so wird sie an den Absender selber verschickt. Diese IPv4-Adresse kann zum Testen verwendet werden. Zum Beispiel, ob TCP/IP oder eine darüber erreichbare Anwendung korrekt installiert und konfiguriert ist.

Local Link Addresses (IPv4LL)

Beim Adressbereich von 169.254.0.0 bis 169.255.255.255 (169.254.0.0/16) handelt es sich um link-lokale IPv4-Adressen. Dieser Adressbereich wird von Rechnern genutzt, bei denen die automatische IPv4-Konfiguration per BOOTP oder DHCP fehlgeschlagen ist. Durch die Selbstzuweisung link-lokaler IPv4-Adressen sind alle Rechner im selben Adressbreich in einem gemeinsamen lokalen Netzwerk in der Lage miteinander zu kommunizieren.

Netz-Adressen und Broadcast-Adressen

Eine IPv4-Adresse, deren letzte Stelle eine "0" ist, ist keine gültige IPv4-Adresse (z. B. 127.0.0.0). Es handelt sich dabei um die Adresse eines ganzen Subnetzes, nicht eines einzelnen Hosts.
Eine IPv4-Adresse, deren letzte Stelle eine "255" ist (z. B. 127.0.0.255), ist ebenso keine gültige IPv4-Adresse. Es ist eine Broadcast-Adresse für das Netz 127.0.0.0. Die Datenpakete mit dieser Zieladresse werden in diesem Netz an alle Hosts geschickt und nicht an einen einzelnen Host.

Eine Broadcast-Adresse innerhalb eines Netzwerkes dient dazu, eine Nachricht an alle Hosts innerhalb des Netzwerks zu schicken. Beispielsweise um Dienste im Netzwerk aufzuspüren. Zum Beispiel DHCP für die IPv4-Konfiguration, Datei- und Druckerfreigaben oder einen Gaming-Server.

Hinweis: Durch die Einschränkung von 0 bis 255 hat ein Klasse-C-Subnetz bzw. 24er CIDR-Suffix zwar 256 Adressen (von .0 bis .255), aber abzüglich der Netz-Adresse x.x.x.0 und der Broadcast-Adresse x.x.x.255 nur maximal 254 adressierbare Host-Adressen.

Private IP-Adressen / Address Allocation for Private Internets (RFC1918)

IPv4-Adressen sind begrenzt und müssen offiziell beantragt und zugeteilt werden. Man kann also nicht irgendeine IPv4-Adresse verwenden. Allerdings gibt es für die private und nicht-öffentliche Nutzung von TCP/IP spezielle Adressräume, die innerhalb von privaten Netzen frei zur Verfügung stehen und nicht im öffentlichen Internet geroutet werden.

Wenn man nun ein privates lokales Netzwerk aufbauen möchte, verwendet man solche privaten IPv4-Adressen, wenn man zu wenige oder keine öffentlichen IPv4-Adressen hat. Die privaten IPv4-Adressen haben aber den Nachteil, dass sie nur im jeweiligen lokalen Netzwerk gültig sind und nicht in öffentliche Netzen geroutet werden. Datenpakete mit privaten IPv4-Adressen verbleiben in den lokalen Netzwerken. Umgekehrt heißt das auch, dass Hosts, die nur eine private IPv4-Adresse haben, nicht direkt aus dem Internet erreichbar sind.

Von	Bis	Subnetzmaske	Hosts	Netzklasse
10.0.0.0	10.255.255.255	255.0.0.0	16.777.214	A
172.16.0.0	172.31.255.255	255.255.0.0	65.534	B
192.168.0.0	192.168.255.255	255.255.255.0	254	C

Wenn ein lokaler Host mit dem Internet verbunden werden soll, dann benötigt er eine öffentliche IPv4-Adresse. Leider hat die großzügige Zuteilung der öffentlichen IPv4-Adressen dazu geführt, dass es keine öffentlichen IPv4-Adressen für jeden Host gibt. Bei Internet-Zugängen löst man die Problematik mit NAT. Dabei bekommt nur der Internet-Zugangs-Router eine öffentliche IPv4-Adresse und alle anderen Hosts in seinem Netzwerk eine private IPv4-Adresse. Das NAT-Protokoll sorgt nun dafür, dass sich mehrere lokale Hosts eine öffentliche IP-Adresse teilen können.

IPv4-Konfiguration

Damit ein Netzwerk-Teilnehmer in einem TCP/IP-Netzwerk teilnehmen kann benötigt er zumindest eine IP-Adresse. Diese sollte zumindest im lokalen Netzwerk einmalig sein (private IPv4-Adresse). Zusätzlich bedarf es der Angabe einer Subnetzmaske, damit der Host weiß, in welches Netz er gehört. Damit eine Kommunikation ins öffentliche Netzwerk möglich ist, bedarf es auch noch der IPv4-Adresse des Standard-Gateways (Default-Gateway). Damit die Auflösung von Domain- oder Computer-Namen möglich ist, muss auch noch die IPv4-Adresse eines DNS-Servers. Erst mit diesen vier Angaben ist eine IPv4-Konfiguration vollständig.

Bei der IPv4-Konfiguration sorgt man dafür, dass ein IP-Host diese Parameter erhält, damit er das TCP/IP-Netzwerk nutzen kann.

- IPv4-Adresse
- Subnetzmaske
- IPv4-Adresse des Standard-Gateways (für Verbindungen ins öffentliche Netzwerk)
- IPv4-Adresse des DNS-Servers (für die Auflösung von Domain- und Computer-Namen)

Es gibt mehrere Möglichkeiten die IPv4-Konfiguration vorzunehmen. Man unterscheidet in der Regel zwischen manuell (fest/statisch) und automatisch (APIPA) oder halbautomatisch (BOOTP oder DHCP) bzw. zwischen statisch und dynamisch.

- Manuelle IPv4-Konfiguration (manuell/statisch)
- Autokonfiguration mit IPv4LL (automatisch/dynamisch)
- Autokonfiguration mit BOOTP (halbautomatisch/dynamisch)
- Autokonfiguration mit DHCP (halbautomatisch/dynamisch)

Manuelle IPv4-Konfiguration (fest/statisch)

Die manuelle IPv4-Konfiguration bezeichnet man auch als feste oder statische IPv4-Konfiguration, weil hier die Parameter manuell in die Konfigurationsoberfläche des jeweiligen Hosts eingetragen werden. Dabei muss der Systemadministrator vorher die Parameter festlegen. Die Parameter sind systembedingt vorgegeben oder der Administrator muss sie festlegen (statisch). Wenn sich die Parameter ändern, dann muss die statische Konfiguration manuell geändert werden.

Die Vorteile der manuellen IPv4-Konfiguration sind, dass der Administrator sicherstellen kann, dass sich die Konfiguration nachträglich nicht verändert. Das ist beispielsweise dann sinnvoll, wenn andere Netzwerk-Teilnehmer auf festgelegte IP-Adressen angewiesen sind, die zum Beispiel zu Servern oder Gateways gehören.

Ein Nachteil ist, dass die manuelle IPv4-Konfiguration fehleranfällig ist. Außerdem muss eine Verwaltung der IPv4-Adressen erfolgen, um zu

vermeiden, dass bereits vergebene IPv4-Adressen doppelt verwendet werden.
Außerdem muss eine manuelle Konfiguration bei jedem Netzwerk-Teilnehmer erneut erfolgen, wenn sich ein Parameter der IPv4-Konfiguration ändern. Beispielsweise die Adressen von Standard-Gateway oder DNS-Server.

Um die Nachteile der manuelle Konfiguration zu vermeiden, wird üblicherweise DHCP für die halbautomatische IPv4-Konfiguration verwendet. Es handelt sich dabei um ein Protokoll, dass IPv4-Adressen in einem TCP/IP-Netzwerk verwaltet und gleichzeitig die IPv4-Konfiguration im Netzwerk verteilt. Mit DHCP ist jeder Netzwerk-Teilnehmer in der Lage sich selber zu konfigurieren.

IPv4-Autokonfiguration mit IPv4LL (APIPA oder Bonjour)

In einem einfachen lokalen Netzwerk ist es nicht erforderlich, dass Clients und Server in einem Netzwerk manuell konfiguriert werden müssen. Wenn keine manuelle Konfiguration erfolgt und kein DHCP-Server verfügbar oder erreichbar ist (Timeout), dann konfigurieren sich die IPv4-Hosts selber.
Ein Host teilt sich dann selber eine link-lokale Adresse aus dem Adressbereich von 169.254.0.0 bis 169.255.255.255 (IPv4LL-Adressen: 169.254.0.0/16) zu.

Diese Art der Autokonfiguration ist unterschiedlich implementiert. Das Verfahren ist Teil von Bonjour (Zeroconf) von Apple und APIPA von Microsoft. Unter Windows, Linux und Mac OS X sollte es also funktionieren.
Weil man sich ursprünglich nicht darauf verlassen konnte, dass das funktionierte, hat man BOOTP und DHCP entwickelt, um eine dynamische IPv4-Konfiguration (Autokonfiguration) zu realisieren.

BOOTP

Ursprünglich war die Idee, dass ein Boot PROM auf einer Netzwerkkarte dafür sorgte, dass das Betriebssystem über das Netzwerk geladen wird, wenn der PC eingeschaltet wurde. In dem Fall war die IP-Adresse des BOOTP-Servers statisch festgelegt.

Das Bootstrap-Protocol (BOOTP) sieht vor, dass sich ein Computer ohne Festplatte zuerst eine IP-Adresse vom BOOTP-Server zuweisen lässt, um danach das Betriebssystem aus dem Netzwerk zu laden.

Die Autokonfiguration durch BOOTP kann auch ohne das Laden des Betriebssystems erfolgen. Leider hat das Verfahren verschiedene Nachteile. Im Prinzip findet keine Verwaltung der IP-Adressen statt. Die Vergabe von IP-Adressen kann man nicht steuern. Außerdem gibt es keinen Timeout-Mechanismus für die Nutzung von IP-Adressen. Auch kann eine IP-Adresse nicht zurückgegeben werden.
Wegen dieser Umstände kann es passieren, dass der BOOTP-Server eine IPv4-Adresse vergibt, die noch vergeben ist. Doppelt vergebene IP-Adressen führen zu Fehlfunktionen im Netzwerk. Je mehr Hosts sich einen Adressbereich teilen müssen, desto wahrscheinlicher wird eine IP-Adresse mehrfach vergeben, was es zu vermeiden gilt. Aus diesem Grund wurde DHCP entwickelt.

DHCP

DHCP basiert auf BOOTP und stammt von Microsoft. Es ist ein Protokoll, um IP-Adressen in einem TCP/IP-Netzwerk zu verwalten und an die Stationen im Netzwerk zu verteilen. Dafür ist im Netzwerk ein DHCP-Server zuständig, über den sich jeder Netzwerk-Teilnehmer eine IP-Konfiguration besorgen kann und sich somit halbautomatisch konfiguriert.

Die Besonderheit von DHCP ist, dass es nicht nur die IP-Adresse verteilt, sondern gleich die ganze IP-Konfiguration mit Subnetzmaske, Standard-Gateway, DNS-Server und Bedarfsweise weiteren optionalen Netzwerk-Adressen und -Parametern.
Außerdem verfügt DHCP über einen Lease-Mechanismus zur Verwaltung und Vergabe von IP-Adressen. DHCP merkt sich nicht nur welcher Host welche IP-Adresse hat, sondern versieht sie mit einer Begrenzung der Nutzungsdauer. Eine IP-Adresse kann also erneut vergeben werden, wenn die Zeit abgelaufen ist. Der DHCP-Client muss sich vor Ablauf der sogenannten Lease-Time eine neue IP-Konfiguration besorgen.

Als Anwender ist man natürlich auf die Funktion des DHCP-Servers angewiesen. Deshalb ist das eine kritische Komponente in einem TCP/IP-

Netzwerk. Aus diesem Grund wird bei besonders kritischen Teilen in einem Netzwerk die IPv4-Konfiguration manuell vorgenommen. Um zu verhindern, dass ein Netzwerk durch den Ausfall eines DHCP-Servers betroffen ist, betreibt man in größeren Netzwerken mehrerer DHCP-Server.

Statische IPv4-Konfiguration per DHCP?

Man kann in einem DHCP-Server einstellen, dass ein Netzwerk-Teilnehmer immer die selbe IPv4-Adresse hat. Man legt dazu in der DHCP-Server-Konfiguration fest, welche MAC-Adresse welche IPv4-Adresse bekommen soll. Auf diese Weise bekommt ein per DHCP anfragender Host immer die selbe IPv4-Adresse. Sie ist dann praktisch statisch.
Wenn jetzt der DHCP-Server ausfallen sollte und sich dieser Server eine neue IPv4-Konfiguration besorgt, dann kann es passieren, dass der Server nicht mehr verfügbar ist, weil er keine IPv4-Konfiguration bekommen kann. Es sei denn, er verwendet die alte IPv4-Konfiguration weiter.

Wer Server und Gateways betreibt, der wird bei der IP-Konfiguration nichts dem Zufall überlassen wollen, weil er bei deaktiviertem oder ausgefallenem DHCP-Server nicht mehr auf den Server kommt, oder die darauf laufenden Dienste nicht mehr erreichbar sind.

Abhilfe schafft man nur dadurch, dass man mehrere DHCP-Server betreibt. Man kann durchaus mehrere DHCP-Server parallel laufen lassen, solange man einen zum Master erklärt und dafür sorgt, dass sie den Adress-Pool untereinander abgleichen.

IP-Routing

Das Internet Protocol (IP) ist ein routingfähiges Protokoll und sorgt dafür, dass Datenpakete über Netzgrenzen hinweg einen Weg zu anderen Hosts finden. Es kann die Daten über jede Art von physikalischer Verbindung oder Übertragungssystem vermitteln. Der hohen Flexibilität steht ein hohes Maß an Komplexität bei der Wegfindung vom Sender zum Empfänger gegenüber. Der Vorgang der Wegfindung wird Routing genannt.

Das Routing ist ein Vorgang, der den Weg zur nächsten Station eines Datenpakets bestimmt. Im Vordergrund steht die Wahl der Route aus den verfügbaren Routen, die in einer Routing-Tabelle gespeichert sind.

Parameter und Kriterien für Routing

Verschiedene Parameter und Kriterien können für die Wahl einer Route von Bedeutung sein:

- Verbindungskosten
- notwendige Bandbreite
- Ziel-Adresse
- Subnetz
- Verbindungsart
- Verbindungsinformationen
- bekannte Netzwerkadressen

Warum ist Routing notwendig?

Das grundlegende Verbindungselement in einem Ethernet-Netzwerk ist der Hub oder Switch. Daran sind alle Netzwerk-Teilnehmer angeschlossen. Wenn ein Host Datenpakete verschickt, dann werden die Pakete im Hub an alle Stationen verschickt und von diesen angenommen. Jedoch verarbeitet nur der adressierte Host die Pakete weiter. Das bedeutet aber auch, dass sich alle Hosts die Gesamtbandbreite dieses Hubs teilen müssen (z. B. 10 MBit oder 100 MBit). Obwohl die physikalische Struktur und Verkabelung des Hubs ein Stern mit Punkt-zu-Punkt-Verbindungen ist, entspricht die logische Struktur einem Bus. Also eine einzige Leitung, an der alle Netzwerk-Teilnehmer angeschlossen sind. Wollen nun zwei oder mehr Hosts gleichzeitig senden, kommt es zu einer Kollision, die zu einer allgemeinen Sendepause auf dem Bus führt. Danach versuchen die Hosts erneut zu senden, bis die Übertragung erfolgreich war. Dieses Verfahren nennt man CSMA/CD. Die maximale Anzahl von Hosts an einem Ethernet-Bus ist 1.023. Je mehr Hosts an einem Hub angeschlossen sind, desto häufiger kommen Kollisionen vor, die das Netz überlasten.

Um die Nachteile von Ethernet in Verbindung mit CSMA/CD auszuschließen, wählt man als Kopplungselement einen Switch und nutzt

Fast Ethernet (kein CSMA/CD mehr). Der Switch merkt sich die Hardware-Adressen (MAC-Adressen) der Stationen und leitet die Ethernet-Pakete nur an den Port, hinter dem sich die Station befindet. Ist einem Switch die Hardware-Adresse nicht bekannt, leitet er das Datenpaket an alle seine Ports weiter (Broadcast) und funktioniert in diesem Augenblick wie ein Hub. Neben der begrenzten Speichergröße des Switches machen sich viele unbekannte Hardware-Adressen negativ auf die Performance eines Netzwerks bemerkbar.

Zum Verbinden großer Netzwerke eignet sich weder ein Hub noch ein Switch. Aus diesem Grund wird ein Netzwerk durch Router und IP-Adressen in logische Segmente bzw. Subnetze unterteilt.
Die Adressierung durch das Internet Protocol ist so konzipiert, dass der Netzwerkverkehr innerhalb der Subnetze bleibt und erst dann das Netzwerk verlässt, wenn das Ziel in einem anderen Netzwerk liegt.

Insbesondere folgende Probleme in einem Ethernet-Netzwerk machen IP-Routing notwendig:

- Vermeidung von Kollisionen und Broadcasts durch Begrenzung der Kollisions- und Broadcastdomäne
- Routing über unterschiedliche Netzarchitekturen und Übertragungssysteme
- Paket-Filter und Firewall
- Routing über Backup-Verbindungen bei Netzausfall

IP-Routing-Algorithmus

Der IP-Routing-Algorithmus gilt nicht nur für IP-Router, sondern für alle Host, die IP-Datenpakete empfangen können. Die empfangenen Datenpakete durchlaufen diesen Algorithmus bis das Datenpaket zugeordnet oder weitergeleitet werden kann.

An erster Stelle des Routing-Algorithmus steht die Frage "Ist das Datenpaket für mich?". Wenn die Ziel-Adresse des Datenpakets mit der eigenen IP-Adresse übereinstimmt, dann hat das Datenpaket sein Ziel erreicht und kann verarbeitet werden.
Wenn die Adresse nicht übereinstimmt, dann wird die zweite Frage gestellt: "Ist das Datenpaket für mein Subnetz?". Dabei wird die

Zieladresse mit der Subnetzmaske maskiert. Anhand des verbleibenden Adressanteils wird festgestellt, ob das Datenpaket in den eigenen Netzabschnitt (Subnetz oder Subnet) gehört.
Stimmt auch das Subnetz nicht, wird die dritte Frage gestellt: "Ist mir die Route zum Empfänger des Datenpakets bekannt?". Manchmal wissen die Hosts die Route für bestimmte IP-Adressen. Wenn die Route bekannt ist, wird das Datenpaket über diese Route weitergeleitet.
Ist die Route nicht bekannt wird die vierte Frage gestellt: "Ist mir ein Standard-Gateway bekannt, wohin ich das Datenpaket weiterleiten kann?". Das Standard-Gateway ist in der Regel ein Router, der eingehende Datenpakete anhand der Zieladresse und einigen Regeln an seine Routing-Ausgänge verteilt. Ist kein Standard-Gateway vorhanden führt das zu einer Fehlermeldung. Das Datenpaket wird verworfen.

DHCP - Dynamic Host Configuration Protocol

DHCP ist ein Protokoll, um IP-Adressen in einem TCP/IP-Netzwerk zu verwalten und an die anfragenden Hosts zu verteilen. Mit DHCP ist jeder Netzwerk-Teilnehmer in der Lage sich selber automatisch zu konfigurieren.

Warum DHCP?

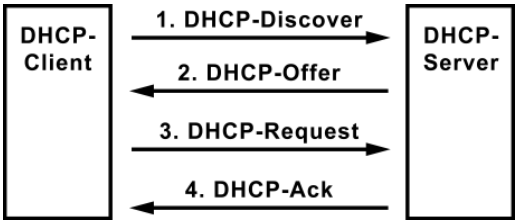
Um ein Netzwerk per TCP/IP aufzubauen ist es notwendig an jedem Host eine IP-Konfiguration vorzunehmen. Für ein TCP/IP-Netzwerk müssen folgende Einstellungen an jedem Host vorgenommen werden:

- Vergabe einer eindeutigen IP-Adresse
- Zuweisen einer Subnetzmaske (Subnetmask)
- Zuweisen des zuständigen Default- bzw. Standard-Gateways
- Zuweisen des zuständigen DNS-Servers

In den ersten IP-Netzen wurden IP-Adressen noch von Hand vergeben und fest in die Systeme eingetragen. Die dazu erforderliche Dokumentation war jedoch nicht immer fehlerfrei und schon gar nicht aktuell und vollständig. Der Ruf nach einer einfachen und automatischen Adressverwaltung wurde deshalb besonders bei Betreibern großer Netze laut. Hier war durch die manuelle Verwaltung und Konfiguration sehr viel

Planungs- und Arbeitszeit notwendig. Um für die Betreiber der immer größer werdenden Netze eine Erleichterung zu verschaffen wurde DHCP entwickelt.
Mit DHCP kann jede IP-Host die IP-Adresskonfiguration von einem DHCP-Server anfordern und sich selber automatisch konfigurieren. So müssen IP-Adressen nicht mehr manuell verwaltet und zugewiesen werden.

Funktionsweise von DHCP



Die Funktionsweise von DHCP entspricht der Client-Server-Architektur. Der DHCP-Client fragt beim DHCP-Server nach einer IP-Konfiguration. Der DHCP-Server verfügt über einen Pool von IP-Adressen, die er den DHCP-Clients zuteilen kann. Bei größeren Netzen muss der DHCP-Server zudem wissen, welche Subnetze und Standard-Gateways es gibt. In der Regel ist der DHCP-Server ein Router.
Wird ein Host mit einem aktivierten DHCP-Client gestartet, wird ein funktional eingeschränkter Modus des TCP/IP-Stacks gefahren. Dieser hat keine gültige IP-Adresse, keine Subnetzmaske und kein Standard-Gateway. Das einzige, was der Client machen kann, ist IP-Broadcasts verschicken.

DHCP-Discover: Der DHCP-Client verschickt ein UDP-Paket mit der Ziel-Adresse 255.255.255.255 und der Quell-Adresse 0.0.0.0. Dieser Broadcast dient als Adressanforderung an alle verfügbaren DHCP-Server. Im Optimalfall gibt es nur einen DHCP-Server. So vermeidet man Konflikte bei der Adressvergabe.

DHCP-Offer: Der DHCP-Server antwortet auf den Broadcast mit einer freien IP-Adresse und weiteren Parametern, um die IP-Konfiguration zu vervollständigen. Jeder angesprochene DHCP-Server schickt ein UDP-Paket mit folgenden Daten zurück:

- MAC-Adresse des Clients
- mögliche IP-Adresse
- Laufzeit der IP-Adresse/-Konfiguration (Lease-Time)
- Subnetzmaske
- IP-Adresse des DHCP-Servers / Server-ID

DHCP-Request: Aus der Auswahl von evt. mehreren DHCP-Servern sucht sich der DHCP-Client eine IP-Adresse heraus. Daraufhin verschickt er eine positive Meldung an den betreffenden DHCP-Server. Alle anderen Server erhalten die Meldung ebenso und gehen von der Annahme der IP-Adresse zugunsten eines anderen Servers aus.

DHCP-Acknowledgement: Anschließend muss die Vergabe der IP-Adresse vom DHCP-Server bestätigt werden. Doch nicht nur die Daten zum TCP/IP-Netzwerk kann DHCP an den Client vergeben. Sofern der DHCP-Client weitere Angaben auswerten kann, übermittelt der DHCP-Server weitere Optionen.

Sobald der DHCP-Client die Bestätigung erhalten hat, speichert er die Daten lokal ab. Abschließend wird der TCP/IP-Stack vollständig gestartet.

DHCP-Refresh

In der DHCP-ACK-Nachricht ist die Lease-Time (Leihdauer) angegeben, die aussagt, wie lange der Client die zugewiesene IP-Konfiguration verwenden darf. Nach der Hälfte der Lease-Time muss der standardkonforme Client einen erneuten DHCP-REQUEST sendet. In der Regel wird der DHCP-Server ein DHCP-ACK mit identischen Daten und einer aktualisierten Lease-Time schicken. Damit gilt die Nutzung der IP-Adresse als verlängert.

Aber was ist, wenn der DHCP-Server nicht antwortet und somit die aktuelle IP-Konfiguration nicht bestätigt/verlängert wird. Beispielsweise, weil der DHCP-Server ausgefallen ist oder vom Netz genommen wurde. In diesem Fall wird der Client die IP-Konfiguration ohne Einschränkungen weiter verwenden, bis die Lease-Time endgültig abgelaufen ist. Allerdings wird er vor dem Ablauf noch mal versuchen, eine Verlängerung der IP-Konfiguration von diesem DHCP-Server zu erhalten.

Wenn dieser DHCP-Server nicht mehr erreichbar ist, weil vielleicht inzwischen ein anderer DHCP-Server zuständig ist, dann wird der Client noch vor dem endgültigen Ablauf der Lease-Time mit einem erneuten DHCP-DISCOVER versuchen, eine Adresszuweisung von einem anderen DHCP-Server zu erhalten.

DHCP-Not Acknowledged

Sollte der DHCP-Server keine Adressen mehr zur Verfügung haben oder während des Vorgangs ein anderer Client diese Adresse zugesagt bekommen haben, sendet der DHCP-Server ein DHCPNAK (DHCP-Not Acknowledged).

Was passiert, wenn der Client keine IPv4-Konfiguration bekommt?

Zuerst die Gründe:

- Der Client ist mit keinem Netzwerk verbunden.
- Der Client ist verbunden, es existiert aber kein DHCP-Server in dem Netzwerk.
- Der DHCP-Server ist ausgeschaltet, deaktiviert oder nicht mit dem Netzwerk verbunden.
- Der DHCP-Server hat keine freien IP-Adressen mehr.
- Der DHCP-Server ist fehlerhaft konfiguriert.

In jedem dieser Fälle wird der Client sich eine eigene IPv4-Adresse aus dem link-lokalen Adressbereich (169.254.0.0/16) zuteilen. Damit ist die Kommunikation zumindest innerhalb des link-lokalen Netzwerks möglich.
Bei IPv6 erzeugt sich der Client automatisch eine link-lokale IPv6-Adresse per SLAAC.

NAT - Network Address Translation

NAT (Network Address Translation) ist ein Verfahren, dass in IP-Routern eingesetzt wird, die lokale Netzwerke mit dem Internet verbinden. Weil Internet-Zugänge in der Regel nur über eine einzige öffentliche und damit

routbare IPv4-Adresse verfügen, müssen sich alle anderen Hosts im lokalen Netzwerk mit privaten IPv4-Adressen begnügen. Private IP-Adressen dürfen zwar mehrfach verwendet werden, aber besitzen in öffentlichen Netzen keine Gültigkeit. Hosts mit einer privaten IPv4-Adresse können somit nicht mit Hosts außerhalb des lokalen Netzwerks kommunizieren.

Damit trotzdem alle Computer mit privater IPv4-Adresse Zugang zum Internet bekommen können, muss der Internet-Zugangs-Router in allen ausgehenden Datenpaketen die private IPv4-Adresse der lokalen Hosts durch seine eigene, öffentliche IPv4-Adresse ersetzen. Damit die eingehenden Datenpakete dem lokalen Host zugeordnet werden können, speichert der Router zusätzliche die Port-Nummern der TCP-Verbindungen in einer sogenannten NAT-Tabelle.

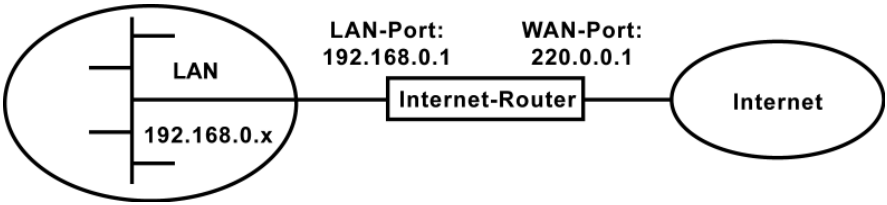
In Verbindung mit den privaten IPv4-Adressen wird NAT eingesetzt, damit über die Netzgrenzen hinweg Daten ausgetauscht, E-Mails verschickt und empfangen, sowie auf das World Wide Web (WWW) zugegriffen werden können.
NAT ist allerdings nur eine Notlösung, um die Adressknappheit von IPv4 zu umgehen. Um die damit einhergehenden Probleme zu lösen muss langfristig auf ein Internet-Protokoll mit einem größeren Adressraum umgestellt werden. IPv6 ist ein solches Protokoll.

Warum NAT?

Die ersten IPv4-Netze waren anfangs eigenständige Netz ohne Verbindung nach außen. Hier begnügte man sich mit IPv4-Adressen aus den privaten Adressbereichen. Parallel dazu kam es bereits Ende der 1990er Jahre zu Engpässen bei öffentlichen IPv4-Adressen. Die steigende Anzahl der Einwahlzugänge über das Telefonnetz mussten mit IPv4-Adressen versorgt werden.
Bis heute bekommt ein Internet-Anschluss nur eine IPv4-Adresse für ein Gerät. Damals war es undenkbar, dass an einem Internet-Anschluss ein ganzes Heimnetzwerk betrieben wird. Wenn ein Haushalt einen PC per Modem an das Telefonnetz angeschlossen und sich ins Internet eingewählt hat, dann war das schon etwas besonderes.

Heute betreibt jeder Haushalt mit Internet-Zugang sein eigenes lokales Netzwerk, in dem jedes Endgerät eine IPv4-Adresse braucht. In solchen Fällen bekommen die Geräte IPv4-Adressen aus den privaten Adressräumen 10.0.0.0/8, 192.168.0.0/16 oder 172.16.0.0/12 zugeteilt, um die wenige öffentlichen IPv4-Adressen einzusparen.
Allerdings sind private IPv4-Adressen nicht routbar. Das heißt, mit ihnen kann man keine Verbindung ins Internet aufbauen. Deshalb wurde mit NAT ein Verfahren eingeführt, bei dem in ausgehenden Datenpaketen die private IP-Adresse gegen eine öffentliche IP-Adresse ausgetauscht wird.

SNAT - Source Network Address Translation



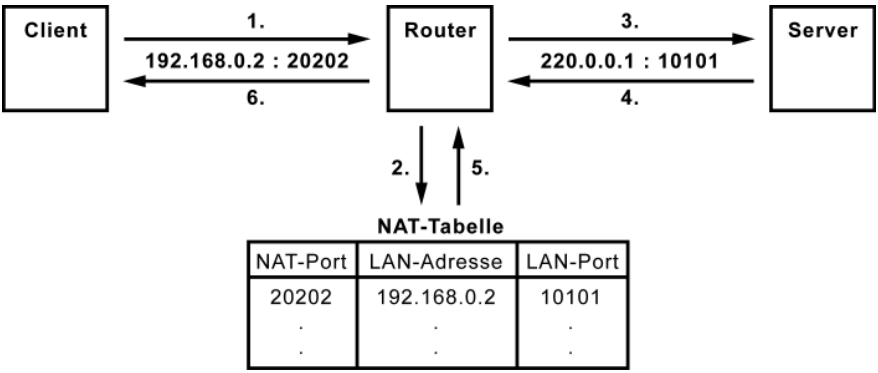
Der Betrieb eines NAT-Routers ist üblicherweise an einem gewöhnlichen Internet-Anschluss. Zum Beispiel über DSL oder Kabelmodem. Der eingesetzte Router dient als Zugang zum Internet und als Standard-Gateway für das lokale Netzwerk. In der Regel wollen über den Router mehr Geräte ins Internet, als öffentliche IP-Adressen zur Verfügung stehen. In der Regel nur eine einzige.
Beispielsweise bekommt der Router des lokalen Netzwerks die öffentliche IP-Adresse 222.0.0.1 für seinen WAN-Port vom Internet Service Provider (ISP) zugewiesen. Weil nur eine öffentliche IP-Adresse vom Internet-Provider zugeteilt wurde, bekommen die Stationen im LAN private IP-Adressen aus speziell dafür reservierten Adressbereichen zugewiesen. Diese Adressen sind nur innerhalb des privaten Netzwerks gültig. Private IP-Adressen werden in öffentlichen Netzen nicht geroutet. Das bedeutet, dass Stationen mit privaten IP-Adressen keine Verbindung ins Internet bekommen können. Damit das trotzdem funktioniert, wurde NAT entwickelt.

Innerhalb des lokalen Netzwerks hat der Router die IP-Adresse 192.168.0.1, die für den LAN-Port gilt und über die der Router im LAN direkt erreichbar und konfiguriert ist. Gleichzeitig handelt es sich dabei

um die Adresse des Standard-Gateways und zum Beispiel des lokalen DNS-Servers. Der Router ist also das Standard-Gateway über das alle Verbindung laufen. Mit seiner öffentlichen IP-Adresse tritt der Router als Stellvertreter für alle Stationen seines lokalen Netzwerks (LAN) auf.

Wenn ein Datenpaket mit einer Ziel-Adresse außerhalb des lokalen Netzwerks adressiert ist, dann ersetzt der Router die Quell-Adresse durch seine öffentliche IP-Adresse. Die Port-Nummer (TCP oder UDP) wird durch eine andere Port-Nummer ersetzt. Um später die Antwortpakete der richtigen Station zuordnen zu können führt der Router eine Tabelle mit den geänderten Quell-Adressen und den dazugehörigen Port-Nummern. Wenn also Pakete mit einer bestimmten Port-Nummer zurück kommen, dann ersetzt NAT die Ziel-Adresse durch die richtige Adresse und Port-Nummer.
In der NAT-Tabelle hat jeder Eintrag auch eine Zeitmarkierung. Nach einer bestimmten Zeit der Inaktivität wird der betreffende Eintrag gelöscht. Auf diese Weise wird sichergestellt, dass keine Ports offen bleiben.
Weil dieses Verfahren die Absender-Adresse (Source) jedes ausgehenden Datenpakets ändert, nennt man dieses Verfahren Source NAT (SNAT). SNAT bezeichnet man in der Regel einfach als NAT.

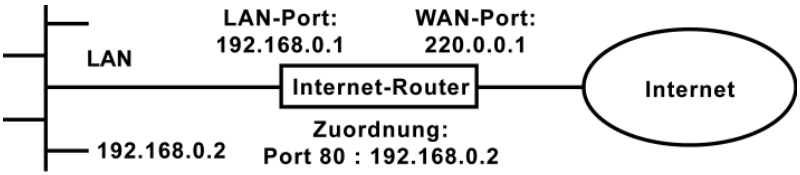
Ablauf von SNAT



1. Der Client schickt seine Datenpakete mit der IP-Adresse 192.168.0.2 und dem TCP-Port 10101 an sein Standard-Gateway, bei dem es sich um einen NAT-Router handelt.

2. Der NAT-Router tauscht IP-Adresse (LAN-Adresse) und TCP-Port (LAN-Port) aus und speichert beides mit der getauschten Port-Nummer (WAN-Port) in der NAT-Tabelle.
3. Der Router leitet das Datenpaket mit der WAN-Adresse 220.0.0.1 und der neuen TCP-Port 20202 ins Internet weiter.
4. Der Empfänger (Server) verarbeitet das Datenpaket und schickt seine Antwort zurück.
5. Der NAT-Router stellt nun anhand der Port-Nummer 20202 (WAN-Port) fest, für welche IP-Adresse (LAN-Adresse) das Paket im lokalen Netz gedacht ist.
6. Er tauscht die IP-Adresse und die Port-Nummer wieder aus und leitet das Datenpaket ins lokale Netz weiter, wo es der Client entgegen nimmt.

DNAT - Destination Network Address Translation (Port-Forwarding)



NAT setzt dynamisch eine öffentliche IP-Adresse auf mehrere private IP-Adressen um. Jede ausgehende Verbindung wird mit IP-Adresse und Portnummer festgehalten. Anhand der Portnummer kann NAT eingehende Datenpakete einer lokalen Station zuordnen. Diese Zuordnung ist allerdings nur für kurze Zeit gültig. Das bedeutet, dass Verbindungen nur aus dem lokalen Netzwerk ins öffentliche Netz aufgebaut werden können, nicht umgekehrt.
Wenn man doch einen Host innerhalb des lokalen Netzwerks dauerhaft aus dem öffentlichen Netz erreichbar machen will, dann ist das nur über einen Umweg möglich. Das Verfahren nennt sich Destination NAT (DNAT), allgemein als Port-Forwarding oder auch Port-Weiterleitung bekannt. Dabei wird in der Router-Konfiguration ein TCP-Port fest einer IP-Adresse zugeordnet. Daraufhin leitet der Router alle auf diesem Port eingehenden Datenpakete an diesen Host weiter.
Vorsicht ist beim Freischalten von TCP-Ports (Port-Forwarding) geboten. Wer keine Server-Dienste im Internet zur Verfügung stellt, sollte alle

TCP-Ports des Routers (von 0 bis 1.023) sperren. Gut vorkonfigurierte Router haben das schon automatisch eingestellt.
Wer auf Port-Forwarding nicht verzichten kann, sollte aus Sicherheitsgründen eine demilitarisierte Zone (DMZ) einrichten und so den Datenverkehr aus dem Internet aus dem lokalen Netzwerk heraus halten.

Probleme durch NAT

Durch den Einsatz von NAT wird das Ende-zu-Ende-Prinzip aufgegeben. Und damit gehen auf Anwendungsebene dezentrale Strukturen verloren oder können erst gar nicht entstehen. Durch NAT können nur noch die, die über öffentliche IPv4-Adressen und in der Regel auch über das notwendige Kleingeld verfügen, Dienste im Internet anbieten.

Ein Problem ist, dass die Anwendungen und Anwendungsprotokolle nichts davon wissen, wenn sie auf einem Host laufen, der nur eine private IPv4-Adresse hat. Solange Protokolle und Anwendungen nach dem Client-Server-Prinzip arbeiten stellt das noch kein Problem dar. Wenn jedoch eine Anwendung dem Ende-zu-Ende-Prinzip folgt, dann bedarf es Hilfskonstruktionen, damit Hosts mit privater IPv4-Adresse erreichbar sind.
Für viele Protokolle existieren Umgehungsmechanismen für NAT, die jedoch die Komplexität und Fehleranfälligkeit steigern und viele Systeme und Anwendungen von deren Verfügbarkeit abhängig machen. Dadurch werden viele Internet-Anwendungen und -Dienste komplizierter, was insgesamt auch zu mehr Sicherheitslücken führt.

Beispiel: Bei der Internet-Telefonie (VoIP) mit der Signalisierung per SIP oder H.323 ist keine direkte Verbindung zu einem VoIP-Telefon möglich. Hierbei bedarf es zentraler Gateways, an denen sich die VoIP-Telefone anmelden und regelmäßig Kontakt herstellen müssen, damit das Telefon durch NAT-Router erreichbar bleibt.
Probleme gibt es auch bei FTP, Messaging und Push Notifications. Hier wird vorausgesetzt, dass der Client direkt erreichbar ist, was er wegen der privaten IPv4-Adresse nicht ist.

Die meisten bidirektionalen Kommunikationsprotokolle lösen das so, dass der Client in regelmäßigen Abständen Datenpakete aus dem lokalen

Netzwerk heraus zu einem zentralen Server oder Gateway schickt, um die Einträge in der NAT-Tabelle seines Internet-Zugangs-Routers aktuell zu halten.
Bei einer hohen Anzahl ausgehender Verbindungen können NAT-Tabellen überlaufen. Das bedeutet, dass einzelne Verbindungen aus der NAT-Tabelle fliegen und demzufolge Verbindungen abbrechen können.

Die Einträge in der NAT-Tabelle des Routers sind nur für eine kurze Zeit gültig. Für eine Anwendung, die nur sehr unregelmäßig Daten austauscht, bedeutet das, dass ständig die Verbindung abgebrochen wird und dadurch die Erreichbarkeit eingeschränkt ist. Das hat zur Folge, dass diese Anwendung unter Umständen in einer NAT-Umgebung nicht funktioniert. Und somit kann sich diese Anwendung im Internet nicht durchsetzen. Den die meisten Clients befinden sich typischerweise in einer NAT-Umgebung.
Um dauerhaft ein Loch in den NAT-Router zu bekommen, wird mit Port-Forwarding (DNAT) gearbeitet. Das bedeutet, dass ein eingehendes Datenpaket mit einem bestimmten TCP-/UDP-Port an eine bestimmte IP-Adresse im lokalen Netzwerk geschickt wird.

Probleme mit NAT gibt es auch da, wo innerhalb des Protokolls die IPv4-Adresse des Hosts mitgeteilt wird. Wenn zum Beispiel bei verschlüsselten IPv4-Paketen eine Checksumme über die IPv4-Adresse zur Integritätskontrolle gebildet wird. Aber durch den Einsatz von NAT werden die Adressen im IPv4-Header geändert. Dadurch scheitern Protokoll, die darauf angewiesen sind, dass die Integrität des IPv4-Headers erhalten bleibt. Zum Beispiel IPsec für VPN.

Wegen den Auswirkungen durch NAT haben sich zentralistische Dienste wie Skype, Facebook und YouTube entwickelt, die die Inhalte aller Internet-Teilnehmer stellvertretend bereitstellen. Diese Dienste haben dadurch die Kontrolle über persönliche Daten gewonnen und können auf Basis derer beliebige Geschäftsmodelle betreiben.

ARP - Address Resolution Protocol

Das Address Resolution Protocol (ARP) arbeitet auf der Schicht 2, der Sicherungsschicht, des OSI-Schichtenmodells und setzt IP-Adressen in Hardware- und MAC-Adressen um. Alle Netzwerktypen und -topologien

benutzen Hardware-Adressen um die Datenpakete zu adressieren. Damit ein IP-Paket innerhalb eines lokalen Netzwerks zugestellt werden kann, muss die Hardware-Adresse des Ziels bekannt sein.
Jede Netzwerk-Adapter besitzt eine einzigartige und eindeutige Hardware-Adresse, die fest auf dem Adapter eingestellt ist.

Bevor nun ein Datenpaket verschickt werden kann, muss durch ARP eine Adressauflösung erfolgen. Dazu sendet der Host einen ARP-Request mit der MAC-Adresse "FF-FF-FF-FF-FF-FF". Das ist ein MAC-Broadcast an alle Systeme im Netzwerk. Diese Meldung wird von jedem Netzwerk-Interface entgegengenommen und ausgewertet. Das Ethernet-Frame enthält die IP-Adresse des gesuchten Hosts. Fühlt sich ein Host mit dieser IP-Adresse angesprochen, schickt er ein ARP-Reply an den Sender zurück. Die gemeldete MAC-Adresse wird dann im lokalen ARP-Cache des Senders gespeichert. Dieser Cache dient zur schnelleren ARP-Adressauflösung.
Eine Variante von ARP ist das RARP-Protokoll. Das wird verwendet, wenn die MAC-Adresse bekannt ist und die IP-Adresse gesucht wird.

Häufig findet man in anderen Dokumentationen, das ARP ein Schicht-3-Protokoll ist. Allerdings sind ARP und auch RARP für die Adressauflösung zuständig, was eigentlich keine Aufgabe der Schicht 3 ist. Da ARP und IP eng verzahnt sind, wäre ARP zwischen Schicht 3 und Schicht 2 richtig zugeordnet.

ICMP - Internet Control Message Protocol

Das Internet Control Message Protocol (ICMP) ist Bestandteil des Internet Protocols (IP). Es wird aber als eigenständiges Protokoll behandelt, das zur Übermittlung von Meldungen über IP dient. Hauptaufgabe von ICMP ist die Übertragung von Statusinformationen und Fehlermeldungen der Protokolle IP, TCP und UDP. Die ICMP-Meldungen werden zwischen Rechnern und aktiven Netzknoten, z. B. Routern, benutzt, um sich gegenseitig Probleme mit Datenpaketen mitzuteilen. Ziel ist, die Übertragungsqualität zu verbessert.

Hinweis: Die Übertragung über IP ist unsicher. Gehen Meldungen von ICMP verloren, dann löst das keine Fehlermeldung aus. Von diesem Paketverlust bekommt niemand etwas mit.

Anwendung von ICMP

Die meisten Internet- und Netzwerk-Benutzer kommen mit ICMP selten in Kontakt. Die meisten ICMP-Meldungen werden von Hosts im Netzwerk verursacht, die Probleme mit IP-Paketen des auslösenden Hosts mitteilen wollen.

Jedes Betriebssystem mit TCP/IP hat Tools, die ICMP nutzen. Zwei bekannte Tools sind Ping und Trace Route. Beides sind sehr einfache Programme, die zur Analyse von Netzwerk-Problemen gedacht sind und damit wesentlich zur Problemlösung beitragen können.

IPv6 - Internet Protocol Version 6

IPv6 ist als Internet Protocol (Version 6) für die Vermittlung von Datenpaketen durch ein paketvermittelndes Netz, die Adressierung von Netzknoten und -stationen, sowie die Weiterleitung von Datenpaketen zwischen Teilnetzen zuständig. Mit diesen Aufgaben ist IPv6 der Schicht 3 des OSI-Schichtenmodells zugeordnet.
Die Aufgabe des Internet-Protokolls besteht im Wesentlichen darin, Datenpakete von einem System über verschiedene Netzwerke hinweg zu einem anderen System zu vermitteln (Routing).

IPv6 ist der direkte Nachfolger von IPv4 und Teil der Protokollfamilie TCP/IP. Seit Dezember 1998 steht IPv6 bereit und wurde hauptsächlich wegen der Adressknappheit und verschiedener Unzulänglichkeiten von IPv4 entwickelt spezifiziert. Da weltweit immer mehr Menschen, Maschinen und Geräte an das Internet mit einer eindeutigen Adresse angeschlossen werden sollen, reichen die 4 Milliarden IPv4-Adressen nicht mehr aus.

Warum IPv6?

IPv6 gilt als Wunderwaffe gegen so manche Probleme mit Netzwerkprotokollen und gleichzeitig wird es als Teufelszeug verdammt, das wieder neue unbekannte Probleme hervorruft. Eine Tatsache ist, dass Administratoren, Programmierer und Hersteller IPv6 neu lernen müssen. Viele Rezepte aus der IPv4-Welt taugen unter IPv6 nicht mehr. Erschwerend kommt hinzu, dass es bei IPv6 allen Beteiligten an

Erfahrung fehlt. IPv6-Gurus, die man bei einem großen Problem befragen kann, gibt es nicht so viele.

Bei IPv6 ist das Ende-zu-Ende-Prinzip konsequent weiter gedacht. Ein Interface kann mehrere IPv6-Adressen haben und es gibt spezielle IPv6-Adressen, denen mehrere Interfaces zugeordnet sind.
IPv6 löst also nicht nur die Adressknappheit, sondern bietet auch Erleichterungen bei der Konfiguration und im Betrieb. Die zustandslose IPv6-Konfiguration und verbindungslokalen Adressen, die bereits nach dem Computerstart verfügbar sind, vereinfachen die Einrichtung und den Betrieb eines lokalen Netzwerks.
Damit das gelingt sind Planer und Errichter von IP-Netzen gefordert sich eine neue Denkweise anzueignen.

Internet Protocol Version 5 (IPv5)?

IPv5 hieß offiziell ST-2 (Internet Stream Protocol Version 2) und war ein experimentelles Protokoll für Echtzeit-Datenströme. ST-2 sollte ursprünglich Audio und Video per Multicast übertragen. Dadurch sollten die Bandbreitenreservierungsvorteile von ATM in die IP-Netze gelangen. Zur Serienreife hat es nicht gereicht. Deshalb gab es auch kein IPv5 im praktischen Einsatz. Und ST-2 wurde von RSVP (Resource Reservation Protocol) zur Bandbreitenanforderung bei Routern abgelöst.

Parallelbetrieb von IPv4 und IPv6 (Dual-Stack)

IPv4 hat keine Zukunft mehr und ein zügiger Wechsel zu IPv6 erscheint notwendig. Gleichzeitig muss nicht nur IPv6 eingeführt, sondern auch IPv4 parallel betrieben werden. Man bezeichnet diesen Betriebszustand als "Dual Stack".
Der Betrieb beider Protokolle muss erfolgen, bis alle Rechner auf der Welt IPv6 beherrschen. Und das kann dauern. Es gibt viele Netzwerk-Komponenten, die kein IPv6 unterstützen und erst gegen IPv6-fähige Komponenten ausgetauscht werden müssen. Auf der anderen Seite ist der Markt für IPv6 noch nicht groß genug, dass sich die Entwicklung von IPv4-vergleichbaren Produkten mit IPv6 lohnt.
Aber an IPv6 führt letztlich kein Weg vorbei. Sonst läuft man Gefahr den Anschluss an die technische Entwicklung zu verpassen.

Vorteile von IPv6

Für viele ist IPv6 einfach nur ein IPv4 mit längeren Adressen. Doch diese Ansicht ist völlig falsch. IPv6 ist ein Protokoll mit vielen neuen Funktionen. Die Erfahrungen, die jemand aus der IPv4-Welt mitbringt, lassen sich nur bedingt auf IPv6 übertragen.

- längere Adressen und dadurch ein größerer Adressraum
- mehrere IPv6-Adressen pro Host mit unterschiedlichen Gültigkeitsbereichen
- Autokonfiguration der IPv6-Adressen möglich
- Multicast durch spezielle Adressen
- schnelleres Routing
- Punkt-zu-Punkt-Verschlüsselung mit IPsec
- Quality of Service
- Datenpakete bis 4 GByte (Jumbograms)

IPv6-Adressen und Adressraum

Eine IPv6-Adresse besteht aus 128 Bit. Diese Adresslänge erlaubt eine unvorstellbare Menge von 2 hoch 128 oder 3,4 x 10 hoch 38 Adressen. Damit haben IPv6-Adressen genügend Raum, um möglichst viele Netzwerk-Topologien abbilden zu können. Gleichzeitig geht es auch darum, das Routing zu vereinfachen.

IPv6-Autokonfiguration (SLAAC / DHCPv6)

IPv6 ermöglicht eine vollständige Autokonfiguration durch einen Host mit IPv6-Adresse, Standard-Gateway und DNS-Server. Hierbei muss man anmerken, dass ein IPv6-Host in der Regel mehrere IPv6-Adressen hat und diese und alle anderen Parameter für eine vollständige Autokonfiguration auf unterschiedlichen Wegen bekommen kann. Selbstverständlich ist auch eine manuelle, das heißt, statische IPv6-Konfiguration möglich.

Address Selection

Address Selection ist ein Verfahren, welches darüber entscheidet, welche IP-Adresse verwendet wird. Wenn ein Host sowohl eine IPv4- als auch eine IPv6-Adresse hat (Dual Stack), dann stellt sich die Frage, welche er verwendet? Und wenn ein Host eine IPv6-Adresse verwendet, welche davon? Die link-lokale, die globale oder eine temporäre IPv6-Adresse?

Multicast

IPv6 fasst Netzwerkknoten, Router, Zeit-Server und andere Dienste bzw. Dienste-Anbieter in Multicast-Gruppen zusammen. Jede Gruppe ist über eine eigene Adresse erreichbar. Das bedeutet, man kann in einem lokalen Netzwerk einen zentralen Dienst ansprechen, ohne die IPv6-Adresse des Hosts zu wissen. Ein beliebiger Host kann sich einer Multicast-Gruppe zugewiesen fühlen und Pakete an eine Multicast-Adresse verarbeiten.

NDP und ICMPv6

Neighbor Discovery Protocol, kurz NDP, ist das IPv6-Protokoll zum Austausch link-lokal relevanter Nachrichten wie Router Discovery und Neighbor Discovery. Die Übertragung der NDP-Nachrichten erfolgt mit ICMPv6.

IPsec

IPsec ist eine Erweiterung des Internet-Protokolls (IP) um Verschlüsselungs- und Authentifizierungsmechanismen. Damit erhält das Internet-Protokoll die Fähigkeit IP-Pakete kryptografisch gesichert über öffentliche und unsichere Netze zu transportieren.
IPsec wurde von der Internet Engineering Task Force (IETF) als Bestandteil von IPv6 entwickelt und später auch für IPv4 spezifiziert.

Multihoming

Ein an einem lokalen Netzwerk angeschlossenes Interface gilt dann als "multihomed", wenn es mehrere globale IPv6-Adressen hat, die unterschiedliche Präfixe aufweisen. Das heißt, dass das lokale Netzwerk über mehrere ISPs an das Internet angebunden ist. Dabei haben die

Interfaces Adressen von jedem beteiligten ISP. Dies dient nicht nur der Redundanz. Es kann auch durch die Wahl der Absenderadresse das zum Übertragen verwendete Netz bestimmt werden.

Renumbering

Die Mechanismen zur "stateless" Autokonfiguration erlauben das Hinzufügen und Entfernen von globalen Präfixen und somit die Rekonfiguration eines Netzwerks im laufenden Betrieb.
Dank Renumbering lässt sich ein Interface relativ einfach mit neuen Adressen bestücken. Sei es um ein neues Adressschema einzuführen oder den Provider zu wechseln. Ein Interface wird in einen multihomed-ähnlichen Zustand gebracht. Gleichzeitig lässt man die Gültigkeit der alten Adressen langsam auslaufen.
Dazu kann man mehrere Netzzugangsrouter unterschiedlich Konfigurieren. Über Router Advertisements kann ein den Hosts sagen "priorisiere mich" und ein anderer Router "benutze mich nicht". Auf diese Weise kann man einen neuen Router in Betrieb und einen anderen außer Betrieb nehmen. Kleine SoHo-Router können das natürlich nicht.

Flow Labels

Flow Labels sind Kennzeichnungen für IP-Pakete, anhand derer Router oder Paketfilter, Pakete unterschiedlich behandeln können. Nach welchen Kriterien ein Flow Label vergeben wird, ist im Einzelfall festzulegen. Idealerweise sollten alle Pakete mit gleichem Flow Label auch gleich behandelt werden.
Flow Labels ersetzen kein MPLS und für QoS gibt es ein eigenes Feld. Ob es in der Zukunft eine Rolle spielt, das muss sich erst noch zeigen.

Mobile IPv6

Mobile IPv6 erlaubt es zwischen verschiedenen Netzen umher zuwandern, ohne dabei die Verbindung auf IP-Ebene zu verlieren. Es geht darum, unterbrechungsfrei zu kommunizieren, auch wenn man das Netz und damit der Präfix wechselt. Es ist eine Art Handover auf der IP-Ebene.

Jumbograms

Die Nutzdatenlänge wird im Header vermerkt, das entsprechende Feld kann aber keine Werte jenseits von 65.535 annehmen. Mit der Jumbo Payload Option im zugehörigen Extension Header sind auch Nutzdaten bis knapp unter 4 Gigabyte möglich. Das setzt allerdings voraus, dass man Path-MTU-Pakete dieser Größe zulässt. Es bringt nichts große Paketlängen zu definieren, wenn die zu übertragenden Router deswegen einen Fehler zurückmelden. Jumbograms sind also nur für spezielle Anwendungen und unter Umständen nur in lokalen Netzwerken sinnvoll.

Übergangsverfahren von IPv4 auf IPv6

Mit der praktischen Umsetzung von IPv4 auf IPv6 hapert es, weil es unmöglich ist, alle Netzwerk-Geräte auf einmal IPv6-fähig zu machen. Damit der Wechsel leichter geht und Investitionen in alte IPv4-Technik nicht obsolet werden, gibt es verschiedene Verfahren, die den Übergang von IPv4 nach IPv6 erleichtern sollen.

IPv6-Adressen

Eine IPv6-Adresse ist eine Netzwerk-Adresse, die einen Host eindeutig innerhalb eines IPv6-Netzwerks logisch adressiert. Die Adresse wird auf IP- bzw. Vermittlungsebene (des OSI-Schichtenmodells) benötigt, um Datenpakete verschicken und zustellen zu können. Im Gegensatz zu anderen Adressen hat ein IPv6-Host mehrere IPv6-Adressen, die unterschiedliche Gültigkeitsbereiche haben.
Konkret bedeutet das, dass wenn von IPv6-Adressen die Rede ist, dass nicht immer klar ist, welchen Gültigkeitsbereich diese IPv6-Adressen aufweisen. Grob unterscheidet man zwischen verbindungslokalen und globalen IPv6-Adressen. Die verbindungslokale IPv6-Adresse ist nur im lokalen Netzwerk gültig und wird nicht geroutet. Die globale IPv6-Adresse ist über das lokale Netzwerk hinaus im Internet gültig.

Eine IPv6-Adresse hat eine Länge von 128 Bit. Diese Adresslänge erlaubt eine unvorstellbare Menge von 2^{128} oder $3{,}4 \times 10^{38}$ IPv6-Adressen. Das sind 340.282.366.900.000.000.000.000.000.000.000.000 IPv6-Adressen, also rund 340 Sextillionen Adressen. Bei IPv4 spricht man von rund 4,3 Milliarden Adressen.

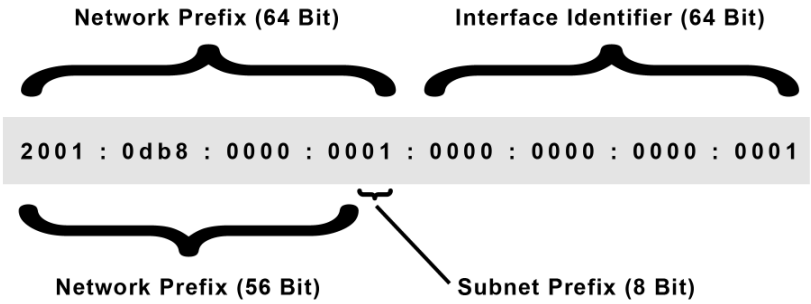
Der Adressraum von IPv6 reicht aus, um umgerechnet jeden Quadratmillimeter der Erdoberfläche inklusive der Ozeane mit rund 600 Billiarden Adressen zu pflastern. Weil man mit dieser großen Menge an Adressen verschwenderisch umgehen darf, spart man sich eine aufwendige Verwaltung, wie es bei IPv4-Adressen notwendig ist.

Segmentierung

Einer der Gründe für den Wechsel von IPv4 auf IPv6 ist der größere Adressbereich von IPv6. Doch warum gleich 128 Bit Adressbreite? Der Grund ist der, dass die IP-Adressen lang genug sein sollten, um den gesamten Adressraum großzügig segmentieren bzw. aufteilen zu können. Es sollen möglichst alle Netzwerk-Topologien berücksichtigt werden können. Gleichzeitig soll das Routing vereinfacht werden.

Damit Router effizient arbeiten können, müssen Adressen hierarchisch strukturiert vergeben werden. Damit alle Ebenen der Hierarchie abgebildet werden können, muss die IP-Adresse lang genug sein. Wünschenswert wäre es, wenn dann auch noch genug Raum für zukünftige Entwicklungen übrig bleibt. Deshalb akzeptiert man bei der Segmentierung von IPv6-Adressen auch einen relativ großen Verschnitt.

IPv6-Adresse im Detail

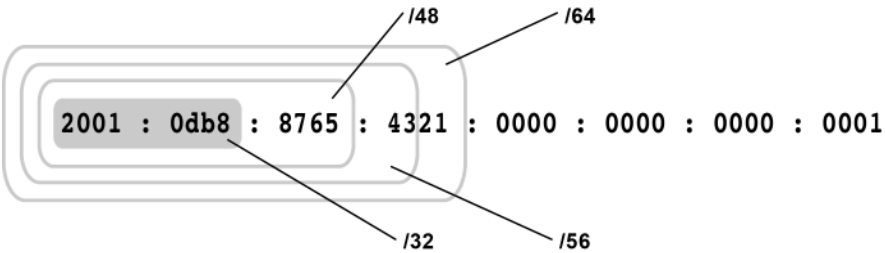


Eine IPv6-Adresse besteht aus 128 Bit. Wegen der unhandlichen Länge werden die 128 Bit in 8 mal 16 Bit unterteilt. Je 4 Bit werden als eine hexadezimale Zahl dargestellt. Je 4 Hexzahlen werden gruppiert und durch einen Doppelpunkt (":") getrennt. Um die Schreibweise zu

vereinfachen lässt man führende Nullen in den Blöcken weg. Eine Folge von 8 Nullen kann man durch zwei Doppelpunkte ("::") ersetzen.

Eine IPv6-Adresse besteht aus zwei Teilen. Dem Network Prefix (Präfix oder Netz-ID) und dem Interface Identifier (Suffix, IID oder EUI).
Der Network Prefix kennzeichnet das Netz, Subnetz bzw. Adressbereich. Der Interface Identifier kennzeichnet einen Host in diesem Netz. Er wird aus der 48-Bit-MAC-Adresse des Interfaces gebildet und dabei in eine 64-Bit-Adresse umgewandelt. Es handelt sich dabei um das Modified-EUI-64-Format.
Auf diese Weise ist das Interface unabhängig vom Network Prefix eindeutig identifizierbar.

Segmentierung: Präfix und Präfixlänge



Die von IPv4 bekannte Netzmaske bzw. Subnetzmaske fällt bei IPv6 ersatzlos weg. Um trotzdem eine Segmentierung und Aufteilung von Adressbereichen bzw. Subnetzen vornehmen zu können, wird die Präfixlänge definiert und mit einem "/" (Slash) an die eigentliche IPv6-Adresse angehängt. Der hierarchische Aufbau des Präfix soll das Routing mit IPv6 vereinfachen.
Standardmäßig ist "/64" die Präfixlänge. Es gibt jedoch weitere typische Präfixe, die 32, 48 und 56 Bit lang sind. Das hat etwas mit der Zuteilung von Präfixen zu tun. Wer eigene Netze betreiben möchte, der bekommt von seinem Provider einen kürzeren Präfix als /64 und erhält damit mehr Adressraum.

Das bedeutet, dass jedes noch so kleine Netzwerk mindestens ein Subnetz zugewiesen bekommt. In diesem Subnetz können jeweils gigantische 2^{64}, also über 18 Trillionen Einzeladressen vergeben werden. Das bedeutet, dass die Anwender sich den Einsatz von privaten IP-Adressen und

Verfahren wie NAT sparen können. Der Adressüberfluss von IPv6 macht es möglich.

Mit IPv6 lassen sich Altlasten in der Netzaufteilung beseitigen und Dank des großen Adressraums den IPv6-Adressplan großzügig neu gestalten. Da jeder Host mehrere IPv6-Adressen haben kann, wäre es denkbar, dass jeder Dienst oder jede Anwendung auf einem Server eine eigene IPv6-Adresse bekommt. Innerhalb desselben Subnetzes kann ein Dienst dann beliebig auf eine andere Hardware wechseln, ohne dass sich die IPv6-Adresse des Dienstes ändern muss.

Hinweis: Die IPv6-Autokonfiguration funktionieren nicht mit weniger als 64 Bit im Interface Identifier. Das heißt natürlich nicht, dass es nicht doch jemand versucht. Aber dann gibt es zum Beispiel Probleme beim Generieren der globalen IPv6-Adresse, weil dieser Mechanismus davon ausgeht, dass er 64 Bit selber zuteilen darf. Wenn die Mechanismen der Autokonfiguration nicht mehr funktionieren, muss man IPv6-Adressen von Hand konfigurieren oder per DHCPv6 zuteilen. Erfahrungsgemäß ist es keine gute Idee damit zu experimentieren.

Adressvergabe durch IPv6-Provider (Zuteilung des Präfixes)

Der ursprüngliche Plan zur Aufteilung des Adressraums war, dass jeder Kunde ein /48er-Netz bekommen sollte. Dass das zu großzügig ist, hat man schnell erkannt und ist deshalb zu längeren Präfixen übergegangen. Entweder /56 oder /64. /56 sollte normal sein, weil man davon ausgehen muss, dass ein Kunden mehrere Netze betreibt. Unter Umständen auch im Heimbereich. Insbesondere kleine Unternehmen haben dann mehr Spielraum, ohne Einschränkungen hinnehmen zu müssen. Enterprise-Kunden, die eigene Netze betreiben, bekommen von ihrem Provider in der Regel /48-Netze. Große Netzbetreiber und Provider bekommen generell /32er-Netze zugeteilt. Größere Netzbetreiber bekommen auch noch größere Netze.

IPv6-Address-Scopes (Gültigkeitsbereiche)

IPv6 unterscheidet sich von IPv4 nicht nur durch längere Adressen, sondern auch durch Gültigkeitsbereiche (Address Scopes) für diese Adressen. Das heißt, jede IPv6-Adresse hat einen sogenannten Scope bzw.

Gültigkeitsbereich. Der Scope ist der Teil eines Netzwerks in dem die zugehörige Adresse als gültig anerkannt und geroutet wird.

Während man bei IPv4 nur zwischen privaten und öffentlichen Adressen unterscheidet, können IPv6-Adressen vielschichtiger sein.

- Host-Scope
- Link-Local-Scope
- Unique-Local-Scope
- Site-Local-Scope (veraltet)
- Global-Scope
- Multicast-Scope

Die beiden wichtigsten Scopes sind der Link-Local-Scope und Global-Scope. Nur IPv6-Pakete mit einer globalen Absender-Adresse werden außerhalb des lokalen Netzwerks geroutet.

Privacy Extensions (RFC 4941)

Weil eine globale IPv6-Adresse wegen dem einmaligen Interface Identifier Bedenken bezüglich Datenschutz und Privatsphäre hervorrufen, wurde "Privacy Extensions" eingeführt, um die Bedenken zu zerstreuen. Deshalb sind Privacy Extensions standardmäßig aktiviert. Sind Privacy Extensions aktiviert, dann bekommt jede Schnittstelle mindestens eine zusätzliche temporär globale IPv6-Adresse, deren Interface Identifier zufällig erzeugt wird und regelmäßig wechselt. Der zufällige Interface Identifier lässt dann keinen Rückschluss mehr auf den Host zu. Temporär globale IPv6 Adressen haben nur eine begrenzte Zeit Gültigkeit. Wenn Privacy Extensions aktiv sind, dann eignet sich eine IPv6-Adresse nicht mehr zur Identifikation eines bestimmten Hosts.

Schreibweise/Notation von IPv6-Adressen

IPv6-Adressen bestehen aus insgesamt 128 Bit woraus sich eine Menge von 2^{128} möglichen Adressen ergibt. Die vorderen 64 Bit sind der Präfix bzw. Network-ID. Vereinfacht ausgedrückt, ist das die IPv6-Adresse des Subnetzes, in dem sich ein Host befindet.

Die hinteren 64 Bit werden als Interface Identifier (IID) bezeichnet. Das ist der Host-Adressanteil einer IPv6-Adresse.

Wegen der unhandlichen Länge werden die 128 Bit in 8 mal 16 Bit (2 Byte) unterteilt. Je 4 Bit werden als eine hexadezimale Zahl dargestellt. Je 4 Hexzahlen werden gruppiert und durch einen Doppelpunkt (":") voneinander getrennt.

Uneinheitlichkeit der Notation

Weil IPv6-Adressen sehr lang sein können, werden sie in der Regel gekürzt. Leider ergeben sich dabei viele unterschiedliche Schreibweisen. Die folgenden Schreibweisen sind Repräsentationen der gleichen IPv6-Adresse.

- 2001 : 0db8 : 0000 : 0000 : 0001 : 0000 : 0000 : 0001
- 2001 : db8 : 0 : 0 : 1 : 0 : 0 : 1
- 2001 : db8 : 0 : 0 : 1 : : 1
- 2001 : DB8 : 0 : 0 : 1 : : 1
- 2001 : db8 : : 1 : 0 : 0 : 1

Die einzige korrekte Schreibweise nach den verbindlichen Notationsregeln in RFC 5952 ist die letzte.

Verbindliche Notationsregeln

Um zu viele unterschiedliche Schreibweise zu vermeiden wurden folgende verbindliche Notationsregeln in RFC 5952 definiert:

1. Alle alphabetischen Zeichen werden grundsätzlich klein geschrieben.
2. Alle führenden Nullen eines Blocks werden grundsätzlich weggelassen.
3. Ein einzelner 4er Nullerblock wird zu einer "0" zusammengefasst.
4. Aufeinanderfolgende 4er Nullerblöcke werden durch zwei Doppelpunkte ("::") gekürzt.
5. Sind mehrere gleichwertige Kürzungen möglich, ist die erste von Links beginnend zu wählen.

Es wird empfohlen diese Notationsregeln einzuhalten, um Fehler und Fehlinterpretationen aufgrund unterschiedlicher Schreibweise zu vermeiden.

- Beispiel: 2001 : 0000 : 0000 : 0000 : 0001 : 0000 : 0000 : 0001
- Falsche Kürzung: 2001 : : 1 : : 1
- Richtige Kürzung: 2001 : : 1 : 0 : 0 : 1

Schreibweise der IPv6-Adresse in der URL

In URLs sind IPv6-Adressen problematisch, weil in URLs der Doppelpunkt (":") als Trennzeichen zwischen Host-Adresse (Domain-Name oder IP-Adresse) und Portnummer (optional) verwendet wird. Deshalb müssen IPv6-Adressen in eckige Klammern gesetzt werden ("[]"), wenn sie in URLs verwendet werden. Die Portnummer muss hinter der schließenden Klammer, mit einem Doppelpunkt abgetrennt, stehen.

- Beispiel: http://[2001:db8::1%25eth0]/

Weiterhin dient in URLs das Prozentzeichen (%) für die Kennzeichnung der hexadezimalen Zeichencodierung. Innerhalb der URL muss das Prozentzeichen durch seinen eigenen Hex-Code "%25" ersetzt werden (RFC 6874). Das ist dann notwendig, wenn man die Verbindung über eine bestimmte Schnittstelle erzwingen will.

Schreibweise der IPv6-Adresse im UNC-Pfad

UNC-Pfade dürfen nach der Definition von Microsoft keine Doppelpunkte enthalten. Für die Schreibweise von IPv6-Adressen ergeben sich dadurch Schwierigkeiten. Hier sind Doppelpunkte (":") als Trennzeichen vorgesehen. Um das Problem zu umgehen hat Microsoft einen Workaround definiert.

- Normale UNC-Schreibweise: \\2001:db8::1\share
- Angepasste UNC-Schreibweise: \\2001-db8--1.ipv6-literal.net\share

IPv6-Autokonfiguration

Ein IPv6-Host kann mehrere IPv6-Adressen haben. Wenn IPv6 im Host aktiviert ist, dann hat er zumindest eine link-lokale bzw. verbindungslokale Adresse. Wenn zusätzlich der Netzzugang und der Netzzugangsrouter IPv6-fähig sind, dann hat ein Host noch eine zweite IPv6-Adresse. Das ist die globale Adresse. Wenn Privacy Extensions im Host aktiviert ist, dann hat er noch zusätzlich eine temporäre globale Adresse, die für externe Verbindungen genutzt wird. Da temporäre Adressen irgendwann ihre Gültigkeit verlieren, kann ein Host auch mehrere temporäre Adressen haben.

- link-lokale IPv6-Adresse
- globale IPv6-Adresse
- (mehrere) temporäre globale IPv6-Adressen

Zu einer vollständigen IPv6-Konfiguration gehören aber nicht nur die IPv6-Adressen des Hosts, sondern mindestens noch die IPv6-Adressen des Standard-Gateways und eines DNS-Servers. Weitere Bestandteile der IPv6-Konfiguration sind netzabhängig und werden hier nicht berücksichtigt.

Die Fragestellung ist, wie kommt ein IPv6-Host an seine IPv6-Adressen und die anderen Teile der IPv6-Konfiguration, wie zum Beispiel das Standard-Gateway und der DNS-Server?

Woher bekommt ein Host seine link-lokale IPv6-Adresse?

Standardmäßig ist es so, dass wenn ein IPv6-Client gestartet wird, dann weist er sich selber eine link-lokale IPv6-Adresse zu. Verbindungen in andere Netze, zum Beispiel ins Internet, sind mit dieser link-lokalen IPv6-Adresse nicht möglich. Sie ist nur im lokalen Netz gültig. Vergleichbar, aber nicht ganz identisch, mit einer privaten IPv4-Adresse.

Die ersten 64 Bit einer link-lokalen IPv6-Adresse sind fest vorgegeben. Davon sind die ersten 16 Bit "fe80". Weitere 48 Bit werden mit Nullen aufgefüllt. Die restlichen 64 Bit der IPv6-Adresse entsprechen dem Interface Identifier für den die MAC-Adresse des Netzwerkadapters

herangezogen wird. Dabei wird die 48-Bit-MAC-Adresse in der Mitte mit einem "ff:fe" auffüllt, damit eine Länge von 64 Bit entsteht. Zusätzlich wird das zweite Bit im ersten Byte invertiert.
Dieses Verfahren gehört zur Stateless Address Autoconfiguration (SLAAC).

Windows bildet den konstanten Interface Identifier anders als hier beschrieben. Bei der Windows-Installation wird für jede Schnittstelle nicht die MAC-Adresse herangezogen, sondern ein zufälliger Interface Identifier erzeugt.
Das kann folgende Konsequenzen haben: Sind auf einer Hardware mehrere Betriebssysteme installiert (Virtualisierung), dann hat jede Windows-Installation einen anderen Interface Identifier.

Woher bekommt ein Host seine globale IPv6-Adresse?

Die globale IPv6-Adresse ist mit einer öffentlichen IPv4-Adresse vergleichbar, weil ein Host nur damit über das lokale Netz hinaus eine Verbindungen ins Internet aufbauen kann. Um eine globale IPv6-Adresse zu bekommen, benötigt der IPv6-Host die link-lokale IPv6-Adresse. Der hintere Teil der Adresse besteht aus dem Interface-Identifier und ist somit bei beiden Adressen gleich. Nur der vordere Teil, der Präfix, der muss für die globale Adresse noch ermittelt werden.

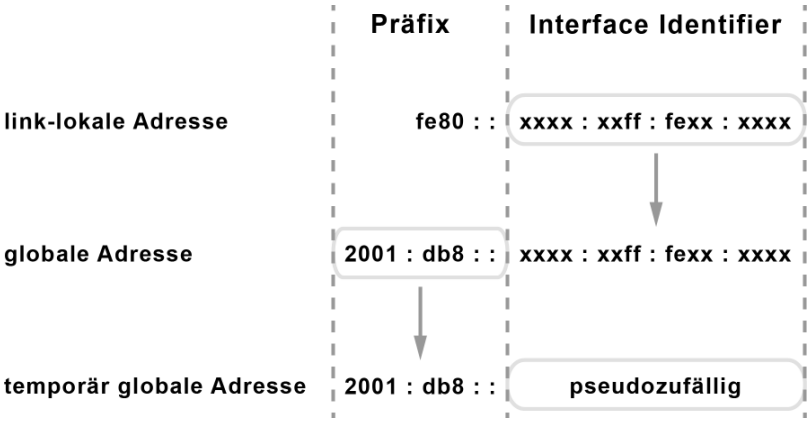
IPv6 kennt drei Wege, wie ein Host an eine globale IPv6-Adresse kommen kann. Entweder wird sie manuell konfiguriert, per Autokonfiguration (SLAAC) oder wie bei IPv4 per DHCP (DHCPv6) vergeben.

Mit SLAAC bezieht ein IPv6-Host nur den globalen Präfix per Router Advertisement und bildet sich zusammen mit dem bekannten Interface Identifier die globale IPv6-Adresse selber.
Sofern ein DHCPv6-Server eingerichtet ist, kann ein Host die globale IPv6-Adresse auch von dort beziehen, wie man es von IPv4 kennt. DHCPv6 läuft unter der Bezeichnung Stateful Address Autoconfiguration. Hierbei wird an zentraler Stelle festgelegt, welcher Host, welche IPv6-Adresse bekommt/hat.

Woher bekommt ein Host seine temporären globalen IPv6-Adressen?

Die temporäre globale IPv6-Adresse basiert auf den Privacy Extensions. Hierbei wird der globale Präfix verwendet und der ursprüngliche Interface Identifier, der aus der MAC-Adresse gebildet wird, wird durch einen pseudozufälligen Interface Identifier ersetzt. Der wird regelmäßig geändert, um den Datenschutz zu gewährleisten.

Zusammenfassung: IPv6-Adressen



Grundsätzlich gilt, dass ein IPv6-Host seine Adressen per SLAAC selber bilden kann. Er ist dabei nicht auf DHCPv6 angewiesen.

- Zuerst erzeugt sich ein Host eine link-lokale Adresse mit "fe80:..." und dem Interface Identifier, der in der Regel aus der MAC-Adresse gebildet wird.
- Damit ist der Host in der Lage im lokalen Netzwerk zu kommunizieren und besorgt sich damit einen globalen Präfix und bildet sich zusammen mit dem Interface Identifier eine globale IPv6-Adresse. Über diese globale IPv6-Adresse kann ein Host global kommunizieren und auch aus dem Internet erreichbar.
- Ist Privacy Extensions aktiviert, dann wird regelmäßig eine neue, temporär globale IPv6-Adresse mit dem globalen Präfix und einem zufälligen Interface Identifier für ausgehende Verbindungen erzeugt.

Woher bekommt ein Host die IPv6-Adresse des Standard-Gateways?

Im Rahmen der Router Advertisements wird nicht nur der globale Präfix, sondern auch die IPv6-Adresse des Standard-Gateways kommuniziert. Das ist ein Bestandteil von SLAAC.

Woher bekommt ein Host die IPv6-Adresse des DNS-Servers?

Es gibt zwei Möglichkeiten. Im Rahmen der Stateless Address Autoconfiguration (SLAAC) enthalten Router Advertisements die RDNSS-Option für Nameserver-Adressen. Alternativ kann die Bekanntgabe der Nameserver-Adresse über DHCPv6 erfolgen. Ursprünglich war die Verteilung von DNS-Server-Adressen über einen zusätzlichen DHCPv6-Server vorgesehen. Erst mit dem RFC 6106 wurde im Rahmen von SLAAC mit Router-Advertisements die RDNSS-Option (Recursive DNS-Server) definiert. Mit der RDNSS-Option erfolgt die IPv6-Autokonfiguration zusammen mit den IPv6-Adressen eines oder mehrerer DNS-Server. Weitere Parameter einer Netzkonfiguration erfordert dann DHCPv6.

Beide Verfahren, SLAAC und DHCPv6, haben den Nachteil, dass sie für sich alleine nicht gut funktionieren. Das liegt daran, weil in älteren Betriebssystemen IPv6 nur unzureichend implementiert ist.

Leider fehlt in manchen Betriebssystemen die RDNSS-Option. Dazu gehören zum Beispiel Windows 7 und 8, sowie einige ältere Linux-Distributionen. Bei anderen Betriebssystemen und Geräten ist es womöglich ebenso.
Ein DHCPv6-Server ist deshalb für die vollständige IPv6-Konfiguration dringend notwendig, weil die Unterstützung der RDNSS-Option oftmals fehlt. Wenn die Betriebssysteme aber keinen DHCPv6-Client haben, wie zum Beispiel das veraltete Windows XP, dann ist es nur eingeschränkt IPv6-fähig. Es kann auf IPv6-Ebene keine Domain-Namen auflösen. Es sei denn man konfiguriert die IPv6-Adresse des DNS-Servers manuell.

Hinweis: Dass die RDNSS-Option bei manchen Clients fehlt, spielt in einer Dual-Stack-Umgebung (IPv4 und IPv6 im Parallelbetrieb) keine Rolle. Es ist ausreichend, wenn die Clients die IPv4-Adresse des DNS-

Servers über DHCPv4 bekommen. Zur Namensauflösung verwendet der Client dann IPv4 und bekommt darüber dann die IPv6-Adresse zu einem Domain- oder Computer-Namen zurück. Sofern der Client eine globale IPv6-Adresse hat wird er die Verbindung wahlweise über IPv4 oder IPv6 aufbauen.

Stateless oder Stateful Address Autoconfiguration

Die "stateless" Autokonfiguration bietet den gleichen Komfort wie beim Betrieb eines sehr einfach gehaltenen DHCP-Servers (stateful). Ohne einen dedizierten DHCP-Server für derartige Informationen bereitstellen zu müssen. In kleinen Netzwerk ist das ein Segen. In großen Netzwerken mag man sich darauf weniger gerne einlassen. Wenn man DHCP von IPv4 her kennt und dann mit SLAAC in den lokalen Netzen arbeiten muss, dann verliert man dabei an einigen Stellen auch Protokollierungs- und Kontrollmöglichkeiten. Davor graut es dem einen oder anderen Netzwerk-Administrator.

Prinzipiell muss man immer mit Router Advertisements arbeiten. Hierbei kann man sich überlegen, welche Informationen darüber verbreitet werden sollen und die fehlenden Teile der IPv6-Konfiguration per DHCPv6 angefordert werden müssen.

Momentan (Stand Anfang 2014) gibt es drei Szenarien die für eine IPv6-Autokonfiguration sinnvoll erscheinen:

1. IPv6-Autokonfiguration nur über Router Advertisement (stateless), ohne globale IPv6-Adresse.
2. Link-lokale und globale IPv6-Adresse und Default-Route über Router Advertisement, DNS-Adresse und weitere Parameter über DHCPv6 (stateless).
3. Globale IPv6-Adresse, DNS-Adresse und weitere Parameter über DHCPv6, die Default-Route über Router Advertisements (stateful).

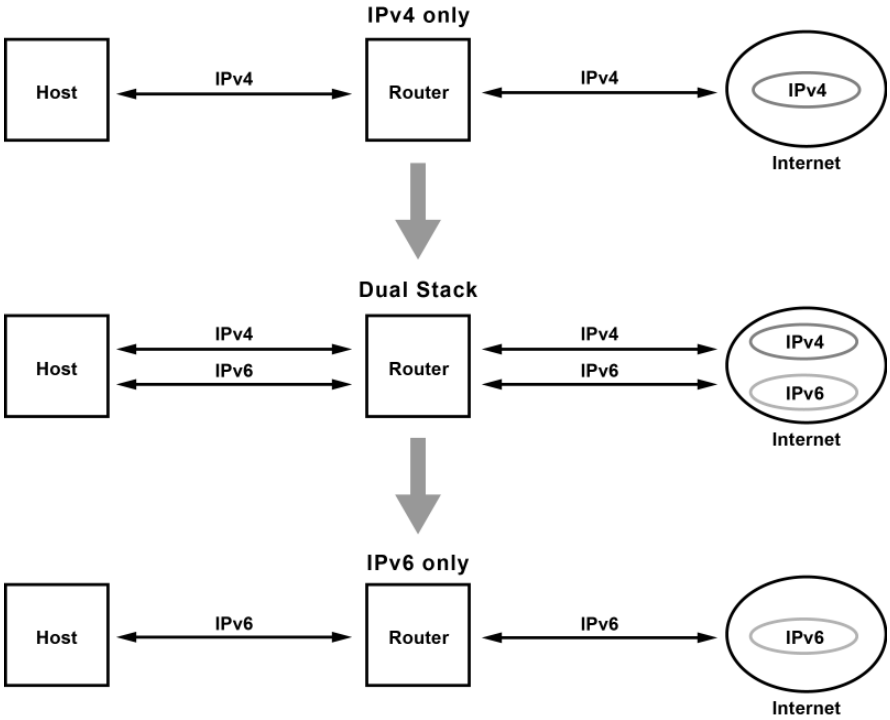
Alternativ besteht sogar die Möglichkeit, SLAAC und DHCPv6 simultan zu betreiben. Das heißt, dass die IPv6-Konfiguration über beide Verfahren verteilt werden. Sowohl per Router Advertisement als auch per DHCPv6. Die Clients erhalten dann zwei globale Adressen (RFC 4862).

Übergangsverfahren (Transition Strategy)

IPv6 ist in aller Munde. Denn der weltweite IPv4-Adresspool ist seit Anfang 2012 erschöpft. Wer öffentliche IP-Adressen braucht, der muss sich einen IPv6-Präfix besorgen. Leider hat man damit das Problem nicht gelöst. Mit der praktischen Umsetzung hapert es, weil es unmöglich ist alle Netzwerk-Geräte auf einmal IPv6-fähig zu machen. Damit der Wechsel leichter geht und Investitionen in alte IPv4-Technik nicht gleich für die Tonne sind, gibt es verschiedene Übergangsverfahren, die ein Teil einer "Transition Strategy" sein können.

- Tunneling (z. B. Teredo, 6in4, 6to4, 6over4, DS Lite)
- Parallelbetrieb (z. B. Dual-Stack)
- Protokollübersetzung (z. B. NAT64)

Transition Strategy



Das Hauptproblem bei der "Transition" ist, dass der Wechsel von IPv4 auf IPv6 nicht auf einen Schlag, sondern über Jahrzehnte erfolgt. Das bedeutet auch, dass auf der ganzen Welt von diesem Wechsel die Internet-Nutzer unterschiedlich stark betroffen sind. Das heißt, während in Europa nicht zwingend IPv6 eingeführt werden muss, und deshalb die Einführung etwas schleppend erfolgt, sieht das in Afrika und Asien ganz anders aus. Dort bleibt Netzbetreibern, Providern und Diensteanbietern nichts anderes übrig als ihre Server mit IPv6-only zu betreiben, weil es keine IPv4-Adressen mehr gibt.

Aber was macht man, wenn man in Europa als IPv4-only-Internet-Nutzer auf eine solche Webseite zugreifen möchte. Oder umgekehrt, ein asiatischer IPv6-only-Internet-Nutzer will auf eine IPv4-only-Webseite zugreifen? In beiden Fällen ist keine Verbindung möglich. Was macht man dann? Eine "Transition Strategie" sollte darauf eine Antwort geben können.

Wie sieht eine technische Lösung aus, wenn man nur IPv6 hat und auf eine Webseite zugreifen möchte, die nur IPv4-only erreichbar ist? Oder umgekehrt. Wie sieht eine technische Lösung aus, wenn da nur IPv4 ist, aber eine Webseite nur per IPv6 erreichbar ist?
Solche Szenarien scheinen heute vielleicht eher unwahrscheinlich. Aber niemand kann genau sagen, wann sich das ändert und wann diese Szenarien zum Problem werden. Wer dann kein IPv6 hat, der ist plötzlich von seinen Kunden abgehängt. Und dann ist die Frage, bis wann man IPv6 stabil eingeführt bekommt?

Für jedes Szenario gibt es unterschiedliche Mechanismen, die man teilweise nur aktivieren und teilweise von Hand konfigurieren muss. Übergangsverfahren spielen dabei eine wichtige Rolle. Da in Zukunft immer mehr Internet-Service-Provider und Unternehmen auf echtes IPv6 umstellen, dürften die Übergangsverfahren nicht ganz verschwinden, aber zumindest abnehmen. Generell sollten alle Übergangsverfahren als vorübergehende Lösung auf dem Weg zu IPv6-only gesehen werden. Bis zur vollständigen Nutzung von IPv6 werden noch einige Jahre ins Land gehen.

Tunneling / Tunnelung

Wenn ein Client kein IPv6 hat, der Server aber nur darüber erreichbar ist, dann kommen Tunneling-Verfahren, zum Beispiel Teredo (Microsoft) oder 6to4/6over4, zum Einsatz.
Wenn bereits das eigene Netzwerk IPv6 unterstützt, aber der Service-Provider am Internet-Anschluss noch nicht, können die IPv6-Clients über einen Tunnel durch das IPv4-Netz mit IPv6-Servern kommunizieren. Dafür benötigt man einen Tunnel-Provider, der die lokalen IPv6-Pakete über das IPv4-Internet ins IPv6-fähige Internet routet. Dafür gibt es verschiedene Tunneling-Verfahren.

- 4in6: Tunneling von IPv4 in IPv6
- 6in4: Tunneling von IPv6 in IPv4
- 6to4: Transport von IPv6-Datenpaketen über ein IPv4-Netzwerk
- 6over4: Transport von IPv6-Datenpaketen zwischen Dual-Stack Knoten über ein IPv4-Netzwerk
- Dual-Stack Lite: Dual-Stack mit globaler IPv6 und Carrier-NAT-IPv4
- Teredo: Kapselung von IPv6-Datenpaketen in IPv4-UDP-Datenpaketen

Parallelbetrieb von IPv4 und IPv6 (Dual-Stack)

Der Parallelbetrieb von IPv4 und IPv6 wird eine lange Zeit der Normalfall sein. Hierbei beherrschen alle Netzknoten sowohl IPv4 als auch IPv6.

Protokollübersetzung (DNS64 und NAT64)

Bei DNS64 und NAT64 geht es darum mit einem IPv6-Client auf einen IPv4-Server zuzugreifen. Es findet praktisch eine Übersetzung zwischen internen IPv6-Adressen und externen IPv4-Adressen statt. Dabei fragt der IPv6-Client einen DNS64-Server nach der IPv6-Adresse des IPv4-Servers. Weil der Server noch keine IPv6-Adresse hat konvertiert der DNS64-Server die IPv4-Adresse des Servers in eine IPv6-Adresse, in etwa wie bei 6over4 und 6to4. Anschließend teilt der DNS64-Server dem Client die IPv6-Adressse mit, der die IPv6-Pakete zum NAT64-Gateway schickt. Das NAT64-Gateway, im Dual-Stack-Betrieb, erkennt in der IPv6-Adresse die IPv4-Adresse, generiert ein neues IPv4-Paket und leitet

es an den IPv4-Server weiter. Die Antwort-Pakete nehmen den umgekehrten Weg zurück.
Der Vorteil der Protokollübersetzung mit DNS64 und NAT64 ist, dass der IPv6-Client nicht wissen muss, dass er eine Verbindung zu einem IPv4-Server unterhält.
Der Nachteil ist, dass man zwingend öffentliche IPv4-Adressen braucht, die unter Umständen nicht zur Verfügung stehen. Wie für NAT typisch werden mittels Portnummern die einzelnen internen IPv6-Clients unterschieden. Auf diese Weise kann man dann wiederum IPv4-Adressen einsparen.

Fazit

Momentan dominieren die Verfahren, die es ermöglichen IPv6-Pakete in IPv4-Netzen zu übertragen. Verfahren, die IPv4-Pakete über IPv6-Netze übertragen spielen eine immer größere Rolle.
Alle Übergangsverfahren von IPv4 auf IPv6 sind als Übergangslösung anzusehen. Beim Wechsel von IPv4 auf IPv6 ist eines entscheidend: Entweder man hat/bekommt vom Internetanbieter eine native IPv6-Verbindung (Dual-Stack) oder man realisiert es über einen IPv6-Tunnel.

Dual Stack

Mit Dual Stack bezeichnet man den Parallelbetrieb von IPv4 und IPv6. Da keine direkte Umstellung von IPv4 auf IPv6 möglich und auch nicht sinnvoll ist, sieht eine "Transition Strategy" vor, dass alle Netzknoten sowohl IPv4 als auch IPv6 beherrschen. Längerfristig würde man dann auf IPv4 verzichten können. Ausgenommen da, wo bereits heute kein IPv4 mehr möglich ist, weil keine öffentliche IPv4-Adressen mehr verfügbar sind. Hier fährt man bereits IPv6-only.

Die Migration zu Dual Stack ist vergleichsweise einfach. Viele Betriebssysteme können mit Dual Stack, also IPv4 und IPv6 gleichzeitig, umgehen. Alle bestehenden Dienste sind weiterhin unter ihrer gewohnten IPv4-Adresse erreichbar. Nach und nach kann man bestehende Dienste per IPv6 erreichbar machen.
Der Schritt zu IPv6 und damit Dual Stack, wird nur häufig deshalb nicht vollzogen, weil während des Parallelbetriebs der doppelte Administrationsaufwand anfällt. Beispielsweise müssen statische IP-

Konfigurationen und das Routing, Filterregeln und Access Control Lists doppelt geführt werden. Und das bedeutet auch, es gibt die doppelte Anzahl an Fehlerquellen.
Erschwerend kommt hinzu, dass man es in der Regel mit Mitarbeitern, Dienstleistern und Experten zu tun hat, die vor Jahren oder Jahrzehnten IPv4 gelernt und verinnerlicht haben. Die müssen IPv6 völlig neu lernen. Denn IPv4 und IPv6 sind in vielen Dingen vergleichbar, aber nicht identisch.
Das Problem der Adressknappheit bei IPv4 löst man aber nicht dadurch, dass man IPv6 ignoriert. Irgendwann kommt man an den Punkt, an dem neue Dienste per IPv6 erreichbar sein müssen, weil die Kunden nur noch eine eingeschränkte oder gar keine IPv4-Connectivity mehr haben.

Alle Lösungswege im Hinblick auf die aktuellen Probleme mit IPv4/IPv6 sollten in Richtung IPv6-only führen. Egal welche Erfahrungen der eine oder andere gemacht hat oder noch machen wird. An IPv6 führt kein Weg vorbei. Auf dem Weg Richtung IPv6-only wird Dual Stack, also der Parallelbetrieb von IPv4 und IPv6, der Normalfall sein. Auf Jahrzehnte gesehen. Wie genau das Dual Stack aussieht, hängt aber vom Provider ab.

Was ist Dual-Stack Lite (DS-Lite / DSlite)?

Oft wird im Zusammenhang mit Dual Stack zwischen Dual Stack und Dual Stack Lite (DS-Lite) unterschieden. Das macht allerdings wenig Sinn. "Dual Stack" ist die Bezeichnung für den IPv4/IPv6-Parallelbetrieb und "Dual Stack Lite" ist eine Tunnel-Technik. Das eine Tunneltechnik als Dual Stack Lite bezeichnet wird, ist eigentlich irreführend.

- Was ist Dual Stack? Bei Dual Stack wird jeder Netzknoten mit öffentlicher oder privater IPv4-Adresse zusammen mit einem globalen IPv6-Präfix, also IPv4 und IPv6 parallel betrieben.
- Was ist Dual Stack Lite? Dual Stack Lite ist eine Betriebsart für einen Breitband-Anschluss mit globalem IPv6-Präfix und Carrier-Grade-NAT-IPv4-Adresse, wobei der IPv4-Datenverkehr in IPv6-Paketen getunnelt wird.

DS-Lite wird oft als ein "IPv6 und mit privaten IPv4-Adressen" definiert. Also ein abgespeckter Dual Stack. Das ist so nicht richtig, weil Dual Stack Lite ein definierter Standard für eine Tunnel-Technik (IPv4 in IPv6) ist.

DS-Lite wird an Internet-Anschlüssen verwendet und auch nur dann, wenn eine globale IPv6-Adresse vorhanden ist und IPv4-Pakete in IPv6 getunnelt werden.
Ein Internet-Zugang ist auch dann Dual Stack, wenn eine private IPv4-Adresse verwendet wird. Das als Dual Stack Lite zu bezeichnen ist ein Irrtum. Dual Stack Lite wäre es nur dann, wenn der IPv4-Datenverkehr über IPv6 getunnelt werden würde.

TCP - Transmission Control Protocol

Das Transmission Control Protocol, kurz TCP, ist Teil der Protokollfamilie TCP/IP. TCP ist ein verbindungsorientiertes Protokoll und soll maßgeblich Datenverluste verhindern, Dateien und Datenströme aufteilen und Datenpakete den Anwendungen zuordnen können.

Das Transmission Control Protocol (TCP) im TCP/IP-Protokollstapel

<table>
<tr><td>Schicht</td><td colspan="4">Dienste / Protokolle / Anwendungen</td></tr>
<tr><td>Anwendung</td><td>HTTP</td><td>IMAP</td><td>DNS</td><td>SNMP</td></tr>
<tr><td>Transport</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td>Internet</td><td colspan="4">IP (IPv4 / IPv6)</td></tr>
<tr><td>Netzzugang</td><td colspan="4">WLAN, Ethernet, ...</td></tr>
</table>

Für die Anwendungen ist TCP transparent. Die Anwendungen übergeben ihren Datenstrom an den TCP/IP-Stack und nehmen ihn von dort auch wieder entgegen. Mit der für die Übertragung nötige TCP-Paketstruktur sowie die Parameter der ausgehandelten Verbindung haben die Anwendungen nichts zu tun.

Aufgaben und Funktionen von TCP

- Segmentierung (Data Segmenting): Dateien oder Datenstrom in Segmente teilen, Reihenfolge der Segmente wieder herstellen und zu Dateien oder einem Datenstrom zusammensetzen

- Verbindungsmanagement (Connection Establishment and Termination): Verbindungsaufbau und Verbindungsabbau
- Fehlerbehandlung (Error Detection): Bestätigung von Datenpaketen und Zeitüberwachung
- Flusssteuerung (Flow Control): Dynamische Auslastung der Übertragungsstrecke
- Anwendungsunterstützung (Application Support): Adressierung spezifischer Anwendungen und Verbindungen durch Port-Nummern

Segmentierung (Data Segmenting)

Eine Funktion von TCP besteht darin, den von den Anwendungen kommenden Datenstrom in Datenpakete bzw. Segmente aufzuteilen (Segmentierung) und beim Empfang wieder zusammenzusetzen. Die Segmente werden mit einem Header versehen, in dem Steuer- und Kontroll-Informationen enthalten sind. Danach werden die Segmente an das Internet Protocol (IP) übergeben.
Da beim IP-Routing die Datenpakete unterschiedliche Wege gehen können, entstehen unter Umständen zeitliche Verzögerungen, die dazu führen, dass die Datenpakete beim Empfänger in einer anderen Reihenfolge eingehen, als sie ursprünglich hatten. Deshalb werden die Segmente beim Empfänger auch wieder in die richtige Reihenfolge gebracht und erst dann an die adressierte Anwendung übergeben. Dazu werden die Segmente mit einer fortlaufenden Sequenznummer versehen (Sequenzierung).

Verbindungsmanagement (Connection Establishment and Termination)

Als verbindungsorientiertes Protokoll ist TCP für den Verbindungsaufbau und Verbindungsabbau zwischen zwei Stationen einer Ende-zu-Ende-Kommunikation zuständig.
Durch TCP stehen Sender und Empfänger ständig in Kontakt zueinander.

Fehlerbehandlung (Error Detection)

Obwohl es sich eher um eine virtuelle Verbindung handelt, werden während der Datenübertragung ständig Kontrollmeldungen ausgetauscht.

Der Empfänger bestätigt dem Sender jedes empfangene Datenpaket. Trifft keine Bestätigung beim Absender ein, wird das Paket noch mal verschickt.
Da es bei Übertragungsproblemen zu doppelten Datenpaketen und Quittierungen kommen kann, werden alle TCP-Pakete und TCP-Meldungen mit einer fortlaufenden Sequenznummer gekennzeichnet. So sind Sender und Empfänger in der Lage, die Reihenfolge und Zuordnung der Datenpakete und Meldungen zu erkennen.

Flusssteuerung (Flow Control)

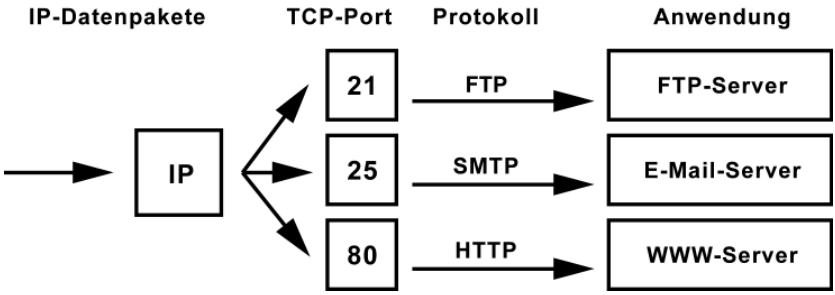
Bei einer paketorientierten Übertragung ohne feste zeitliche Zuordnung und ohne Kenntnis des Übertragungswegs erhält das Transport-Protokoll vom Übertragungssystem keine Information über die verfügbare Bandbreite.
Mit der Flusssteuerung werden beliebig langsame oder schnelle Übertragungsstrecken dynamisch auszulasten und auch auf unerwartete Engpässe und Verzögerungen reagiert.

Anwendungsunterstützung (Application Support)

TCP- und UDP-Ports sind eine Software-Abstraktion, um Kommunikationsverbindungen voneinander unterscheiden zu können. Ähnlich wie IP-Adressen Rechner in Netzwerken adressieren, adressieren Ports spezifische Anwendungen oder Verbindungen, die auf einem Rechner laufen.

TCP- und UDP-Ports

TCP- und UDP-Ports sind eine Software-Abstraktion, um parallele Kommunikationsverbindungen einer oder mehreren Anwendungen voneinander unterscheiden zu können. Ähnlich wie IP-Adressen zur Adressierung von Rechnern in Netzwerken dienen, adressieren Ports spezifische Anwendungen und ihre Verbindungen, die auf einem Rechner laufen.



Datenpakete, die über IP ihr Ziel erreichen, werden von TCP zusammengesetzt und an eine Anwendung übergeben. Da mehrere Anwendungen zugleich TCP-Verbindungen aufbauen können, muss eine Zuordnung zwischen Datenpaket und Anwendung erfolgen. Zu diesem Zweck wird eine Kennung zwischen Daten und Anwendung definiert, die als Port bezeichnet wird. Es handelt sich dabei um eine fortlaufende Nummer zwischen 0 bis 65.535. TCP-Pakete sind mit diesen Port-Nummern, jeweils eine für Sender und Empfänger, versehen. Mit den Ports ist es möglich, dass die Datenpakete mehrerer Verbindungen dem richtigen Datenstrom zugeordnet werden können.

Übersicht: Ports

Die Port-Nummern, die für TCP und UDP gleichzeitig gelten, werden von der IANA (Internet Assigned Numbers Authority) bzw. ICANN (Internet Corporation for Assigned Names and Numbers) verwaltet und vergeben.

Well Known Ports (0 - 1.023): Diese Port-Nummern sind einem Dienst oder einem Anwendungsprotokoll fest zugeordnet. Jeder Dienst hört standardmäßig auf einen solchen Port. Man bezeichnet sie auch als Standard- oder Default-Ports (Destination-Port). Um Fehler und die damit einhergehende Fehlersuche zu vermeiden sollte diese Zuordnung nicht verändert werden.

Registered Ports (1.024 - 49.151): Diese Port-Nummern sind zur Registrierung freigegeben. Im Prinzip kann sich jeder einen Port bei der IANA/ICANN für seine Anwendung reservieren, wenn er es begründen kann. Es ist durchaus möglich, dass diese Ports mehrfach belegt sind.

Dynamically Allocated Ports (49.152 - 65.535): Die darüberliegenden Port-Nummern, ab 49.152, können frei belegt werden bzw. werden dynamisch zugewiesen. Typischerweise nutzen Client diese Ports für ausgehende Verbindungen (Source-Port).

Wenn Anwendungen zu einem Server Kontakt aufnehmen wollen, dann vergibt TCP bzw. UDP den Standard-Port für den Empfänger-Port und vergibt einen freien Port ab 49.152 für den Sender-Port. Wenn der Server die Daten erhalten hat und eine Antwort zurückschickt, dann werden die Port-Nummern vertauscht. Damit wird sichergestellt, dass die Daten nicht an eine falsche Anwendung übergeben werden.

Beispiele für Standard-Ports (TCP)

Port	Protokoll	Anwendung
21	FTP	Dateitransfer (FTP-Server)
23	Telnet	Konsole (Server)
25	SMTP	Postausgang (SMTP-Server)
80	HTTP	World Wide Web (Webserver)
110	POP	Posteingang (POP-Server)
119	NNTP	Usenet (News-Server)

Beispiele für Standard-Ports (UDP)

Port	Protokoll	Anwendung
53	DNS	Domain Name Server
69	TFTP	Trivial File Transfer Protocol
137	NetBIOS	NetBIOS Nameserver
138	NetBIOS	NetBIOS-Datagramm-Dienst
161	SNMP	Simple Network Management Protocol

Port-Zustände

Ports können mehrere Zustände aufweisen. Der Zustand eines Ports definiert, ob eine Kommunikation über diesen Port zu einer dahinterliegenden Anwendung möglich ist, oder nicht. Vereinfacht gesehen gibt es drei Zustände.

- Open / Offen
- Closed / Geschlossen
- Filtered / Gefiltert (Blocked / Geblockt)

Open / Offen

Der Zustand "Open" oder "Offen" ist dann gegeben, wenn auf einem spezifischen Port eine Anwendung lauscht. Mit "Offen" ist gemeint, dass man zu einer Anwendung über diesen Port eine Verbindung aufbauen kann.

Closed / Geschlossen

Der Zustand "Closed" oder "Geschlossen" ist der Standardzustand eines Ports. Er ist dann gegeben, wenn auf einem spezifischen Port keine Anwendung lauscht. Der Host wird eine Verbindung zu diesem Port aktiv ablehnen. Mit "Geschlossen" ist gemeint, dass es keine Anwendung gibt zu der man eine Verbindung über diesen Port aufbauen kann. Zumindest gibt es auf TCP/UDP-Ebene keine Verbindungsmöglichkeit. Denn der Zustand "Geschlossen" kann auch dann gelten, wenn das kontaktierte System durch eine Firewall geschützt ist und die Verbindungsversuche auf einem bestimmten Port aktiv ablehnt. Das bedeutet aber auch, dass zu der dahinterliegenden Anwendung keine Verbindung aufgebaut werden kann.

Filtered / Gefiltert (Blocked / Geblockt)

Der Zustand "Filtered" oder "Gefiltert" ist dann gegeben, wenn der kontaktierte Port durch eine Firewall geschützt ist und auf Verbindungsversuche nicht antwortet. Das heißt, die Verbindung wird weder bestätigt (Offen), noch abgelehnt (Geschlossen). Man muss also annehmen, dass der Verbindungsversuch aktiv blockiert wird. Das gilt

aber nur dann, wenn der Host generell online ist, also auf mindestens einem anderen Port eine Verbindung zulässt.
Der Zustand "Gefiltert" drückt aus, dass der Port nicht erreicht werden kann, weil er zum Beispiel durch eine Firewall-Regel blockiert wird. Dieser Zustand kann aber auch dadurch entstehen, dass der kontaktierte Host gar nicht erreichbar ist.

UDP - User Datagram Protocol

UDP ist ein verbindungsloses Transport-Protokoll und arbeitet auf der Schicht 4, der Transportschicht, des OSI-Schichtenmodells. Es hat damit eine vergleichbare Aufgabe, wie das verbindungsorientierte TCP. Allerdings arbeitet es verbindungslos und damit unsicher. Das bedeutet, der Absender weiß nicht, ob seine verschickten Datenpakete angekommen sind. Während TCP Bestätigungen beim Datenempfang sendet, verzichtet UDP darauf. Das hat den Vorteil, dass der Paket-Header viel kleiner ist und die Übertragungsstrecke keine Bestätigungen übertragen muss. Typischerweise wird UDP bei DNS-Anfragen, VPN-Verbindungen, Audio- und Video-Streaming verwendet.

Das User Datagram Protocol (UDP) im TCP/IP-Protokollstapel

Schicht	Dienste / Protokolle / Anwendungen			
Anwendung	HTTP	IMAP	DNS	SNMP
Transport	TCP		UDP	
Internet	IP (IPv4 / IPv6)			
Netzzugang	Ethernet, ...			

Funktionsweise von UDP

UDP hat die selbe Aufgabe wie TCP, nur das nahezu alle Kontrollfunktionen fehlen, dadurch schlanker und einfacher zu verarbeiten ist.

So besitzt UDP keinerlei Methoden die sicherstellen, dass ein Datenpaket beim Empfänger ankommt. Ebenso entfällt die Nummerierung der Datenpakete. UDP ist nicht in der Lage die Datenpakete in der richtigen Reihenfolge zusammenzusetzen. Statt dessen werden die UDP-Pakete direkt an die Anwendung weitergeleitet. Für eine sichere Datenübertragung ist deshalb die Anwendung zuständig.
In der Regel wird UDP für Anwendungen und Dienste verwendet, die mit Paketverlusten umgehen können oder sich selber um das Verbindungsmanagement kümmern. UDP eignet sich auch für Anwendungen, die nur einzelne, nicht zusammenhängende Datenpakete transportieren müssen.

RTP - Realtime Transport Protocol

RTP (Realtime Transport Protocol) ist wie TCP und UDP ein Transport-Protokoll. RTP wurde von der IETF entworfen und gewährleistet einen durchgängigen Transport von Daten in Echtzeit. Speziell für Audio- und Video-Daten, bei denen je nach Codec 1 bis 20% Paketverlust tolerierbar sind. Allerdings garantiert RTP nicht die Dienstqualität der Übertragung (Quality of Service).

Bei RTP geht es darum, dass Paketverluste bis zu einem bestimmten Grad akzeptabel sind. UDP hat dazu leider keine Funktionen, um Paketverluste festzustellen. Und bei TCP muss jedes verlorene Paket erneut gesendet werden. RTP baut auf UDP auf, damit der Empfänger wenigstens die Möglichkeit hat, Paketverluste festzustellen.

NetBIOS - Network Basic Input/Output System

NetBIOS stammt aus dem Jahr 1983 und ist eine Entwicklung von IBM. Es steht für Network Basic Input/Output System und stellt auf der 5. Schicht des OSI-Schichtenmodells (Kommunikationsschicht) eine Schnittstelle für Anwendungen zum Windows-basierten Netzwerk zur Verfügung. Diese Schnittstelle dient als API (Application Programming Interface) zu den Protokollen die sich auf den unteren Schichten des OSI-Schichtenmodells befinden.

NetBIOS im OSI-Schichtenmodell

<table>
<tr><td>Schicht</td><td colspan="3">Dienste / Protokolle / Anwendungen</td></tr>
<tr><td>Anwendung (7)</td><td colspan="3">Anwendungen</td></tr>
<tr><td>Darstellung (6)</td><td rowspan="3">Dienste und Protokolle</td><td rowspan="2"></td><td>SMB / CIFS</td></tr>
<tr><td rowspan="3">Kommunikation (5)</td><td>NetBIOS</td></tr>
<tr><td>Transport (4)</td><td rowspan="2">TCP</td><td rowspan="2">IPX/SPX</td><td rowspan="2">NetBEUI</td></tr>
<tr><td rowspan="2">Internet (3)</td><td rowspan="2">IP</td><td>NDIS</td></tr>
<tr><td rowspan="2">Sicherung (2)</td><td colspan="3">LLC</td></tr>
<tr><td colspan="3">MAC</td></tr>
<tr><td>Netzzugang (1)</td><td colspan="3">Ethernet, WLAN, ...</td></tr>
</table>

Ursprünglich sollte NetBIOS die Kommunikation in kleinen Netzwerken mit maximal 80 Hosts ermöglichen. Später wurde NetBIOS als Protokoll definiert, das direkt auf der Ebene 2 des OSI-Schichtenmodells aufsetzt. Später wurde daraus NetBEUI, ein sehr einfaches Protokoll ohne Routing-Funktionen, das aber ausschließlich den Anforderungen kleiner Netze gewachsen war.
Doch weder NetBIOS noch NetBEUI haben je an die Funktionalität von TCP/IP heran gereicht.

NetBIOS-Dienste

- Name-Service (137/udp): Dienst zur Auflösung von NetBIOS-Namen
- Datagram-Service (138/udp): Statusmeldungen
- Session-Service (445/tcp und 139/tcp): Übertragung von Nutzdaten und Steuerungsinformationen mit SMB und CIFS

Zeroconf / Bonjour / Avahi

Zeroconf, Bonjour und Avahi sind selbstkonfigurierende Verfahren für Adhoc-Netze auf Basis von IPv4 und IPv6. Im Prinzip handelt es sich um eine Sammlung bestehender Protokolle auf Basis von IP, DNS und NAT, um Netzwerkdienste, die in einem IP-Netz bereitgestellt werden, automatisch erkennen zu können, ohne das der Anwender irgendetwas manuell konfigurieren muss.
Somit ist Bonjour auch im Embedded- oder IoT-Bereich interessant, wenn Sensoren und Aktoren sich vernetzen und im lokalen Netzwerk bekannt machen sollen.

Bonjour, dass auch als Zeroconf (Zero Configuration Networking) bezeichnet wird, ist der Nachfolger von AppleTalk. Bonjour wurde von Apple im Jahr 2002 mit dem Namen "Rendezvous" ins Leben gerufen und später umbenannt. Bonjour gibt es nicht nur für Mac OS X, sondern auch für Linux (Avahi) und Windows (Bonjour). Bonjour wurde von Apple unter der Apache-2.0-Lizenz als Open Source freigegeben.

Bonjour löst verschiedene Probleme, die in lokalen Netzwerken auftreten.

- IP-Adressen zuweisen
- Namen zuweisen
- Dienste bekannt machen

Immer dann, wenn ein Computersystem in ein Netzwerk eingebunden wird, müssen Adressen konfiguriert, Dienste, Verzeichnisse und Laufwerke freigegeben werden. Bei Bonjour teilen die Diensteanbieter ihre Dienste von sich aus mit (Annoncierung), so dass sie von anderen Stationen automatisch gefunden werden können. Dabei kommt man ohne zentralen Server aus, der die Adressen, Portnummern und Servernamen verteilt. Die Dienste melden sich dynamisch an und ab. Dabei bleibt Bonjour im Hintergrund, ohne dass für den Nutzer Konfigurationsaufwand entsteht.

Funktionsweise von Zeroconf / Bonjour / Avahi

Bonjour nutzt zum Informationsaustausch lediglich einzelne Multicast-DNS-Pakete (mDNS). Die Clients tauschen die Bonjour-Informationen über die Multicast-Adresse 224.0.0.251 (IPv4) bzw. ff02::fb (IPv6) an den Port 5353 aus. Die Bonjour-Pakete bleiben dabei im Subnetz. IP-Pakete aus dem Adressbereich zwischen 224.0.0.0 bis 224.0.0.255 dürfen IP-Router nicht über das eigene Subnetz hinaus übertragen. Hier gilt die Regel, dass Multicast-Pakete nicht zwischen den Subnetzen geroutet werden dürfen.
Ein Problem ist das dann, wenn man mehrere Subnetze im Netzwerk hat, dann kommen nicht alle Bonjour-Pakete überall an. Nur wenn alle Hosts im selben Subnetz arbeiten, dann ist die Kommunikation zwischen allen Geräten mit Bonjour möglich.
Damit Bonjour-Informationen auch über Subnetzgrenzen hinweg übertragen werden, setzt man DNS-übliche Unicasts ein. Das Verfahren nennt man Wide Area Bonjour (WAB) und setzt einen DNS-Server voraus.

Ursprünglich war Bonjour für Heimnetzwerke gedacht. Doch mit der Verbreitung von MacBooks, iPhones und iPads verbreitete sich Bonjour auch in größeren Netzwerkumgebungen. Doch je mehr Bonjour-Hosts im Netzwerk, desto mehr fluten mDNS-Pakete das Netzwerk mit An- und Abmeldungen von Diensten. Aus diesem Grund hat sich Apple mit einer Arbeitsgruppe der Internet Engineering Task Force (IETF) zusammengetan, um eine neue Spezifikation für größere Netzwerk-Umgebungen in Unternehmen und Universitäten zu schaffen.

Funktion: IP-Adressen zuweisen

Immer wenn man mehrere Geräte über einen Switch, mit einem Patchkabel, über einen WLAN-Access-Point oder Powerline-Adapter miteinander verbindet, dann stellt sich die Frage, wie die Geräte an ihre IP-Adressen kommen. Bei IPv6 ist es einfach. Hier gibt es die Autokonfiguration per SLAAC. Damit generiert sich jeder Host eine eigene IPv6-Adresse, die nur link-lokal gültig ist. Bei IPv4 kümmert sich Bonjour darum. Auch hier weisen sich die Geräte selber Adressen zu und Bonjour greift ein, wenn es zu Adresskonflikten kommt.

Während IPv6 hierfür den Adressbereich "fe80" hat, liegt der Adressbereich für link-lokale IPv4-Adressen bei "169.254.0.0/16".

Hat ein Host eine IPv4-Adresse für sich bestimmt, dann macht er diese im lokalen Netzwerk zusammen mit seiner Hardware-Adresse per Broadcast bekannt. Die anderen Netzwerk-Teilnehmer aktualisieren dann ihren ARP-Caches (Liste mit benachbarten Netzwerk-Teilnehmern).
Wird die IPv4-Adresse von einem anderen Teilnehmer bereits verwendet, dann muss dieses Gerät seine Adresse verteidigen. Dazu antwortet der Teilnehmer auf den Broadcast. Um zu verhindern, dass manuelles Eingreifen des Nutzers nötig wird, überlassen die Teilnehmer anderen Teilnehmern eine vergebene IP-Adresse, wenn die diese trotzdem haben wollen.

Funktion: Namen zuweisen

Bei Bonjour nennt sich diese Funktion Multicast DNS, kurz mDNS. Das ermöglicht die eigenständige Zuweisung von Namen in einem Netzwerk ohne Nutzereingriff und Unicast DNS innerhalb eines lokalen Netzwerks. Dazu weisen sich die Geräte selber Namen zu. Häufig Typenbezeichnungen, benutzerdefinierte Computernamen oder auch Teile aus Benutzernamen. Der dabei ablaufende Prüfprozess ähnelt der Zuweisung von link-lokalen IP-Adressen. Immer dann wenn ein Konflikt auftritt, wird der Name automatisch abgeändert und erneut geprüft.
Damit man bei den Namen zwischen mDNS und DNS unterscheiden kann, bekommen die Namen ein ".local" als Pseudo-Top-Level-Domain (TLD) angehängt. Das heißt, ".local" ist die TLD in einem lokalen Netzwerk.
Bei der Namensauflösung bedient sich mDNS dem gleichen Protokoll, wie beim Unicast DNS. Dabei stellt der Client einfach eine DNS-Anfrage an die Multicast-Adresse "224.0.0.251" und bekommt vom betreffenden Rechner eine Antwort zurück. Dabei muss man berücksichtigen, dass diese Adresse nur im jeweiligen Subnetz erreichbar ist.

Funktion: Dienste bekannt machen

Nicht alle Netzwerk-Teilnehmer sind Clients, die nur auf das Internet zugreifen. Es gibt auch Hosts, die Dienste anbieten. Beispielsweise ein Netzwerk-Drucker oder ein Media-Center. Solche Geräte machen ihre

Dienste über UDP bekannt. Weil es keinen speziellen Empfänger für die Bekanntmachungen/Annoncen gibt, gibt es die Multicast-Adressen für IPv4 "224.0.0.251" und IPv6 "ff02::fb" und den Port 5353. Auf diese Adressen lauschen alle kompatiblen Geräte auf Bekanntmachungen durch Dienste-Anbieter. Dabei muss man berücksichtigen, dass diese Adresse nur im jeweiligen Subnetz erreichbar ist.

Anwendungen und Dienste

World Wide Web E-

Mail

Namensauflösung

Verzeichnisdienste

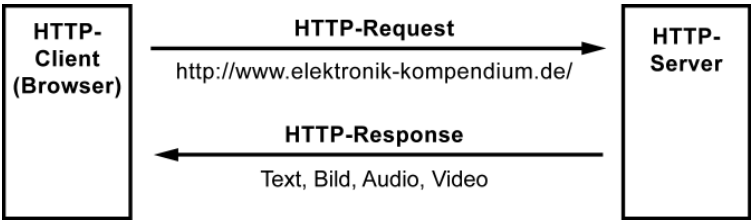
Voice over IP

WWW - World Wide Web

Das World Wide Web, kurz WWW oder Web, ist eine Sammlung von Servern, auf denen Informationen abgelegt sind. Auf die Informationen in Form von Text, Bild, Audio und Video greift man mit Hilfe eines Software-Clients (Browser) zu. Um die verfügbaren Informationen zugänglich zu machen, werden sie miteinander verknüpft. Man bezeichnet das als Verlinken.
Neben E-Mail und File-Transfer (FTP) ist das World Wide Web (WWW) der meistgenutzte Dienst des Internets. Aus diesem Grund wird der Begriff Internet synonym für WWW verwendet. Für den Zugriff auf das WWW ist ein Internet-Anschluss erforderlich. Im Gegensatz zum Internet, ist das World Wide Web erst seit 1992 öffentlich freigegeben.

Wie funktioniert das World Wide Web (WWW)?

Die Art und Weise wie man sich innerhalb der Informationsangebote bzw. einer Webseite bewegt wird als Surfen bezeichnet, womit der Vergleich mit dem Wellenreiten herangezogen wird. Beim Surfen im Wasser bewegt man sich von Welle zu Welle. Beim Surfen im Internet springt man über anklickbare Hyperlinks von Webseite zu Webseite, oder bewegt sich innerhalb einer Web-App.



Die Kommunikation im World Wide Web basiert auf HTTP, dem Hypertext Transfer Protocol. Auf dem HTTP-Server, den man allgemein als Webserver bezeichnet liegen Dateien in Text, Bild, Audio oder Video. Diese ruft man mit einem HTTP-Client ab, den man allgemein als Webbrowser oder auch nur als Browser bezeichnet. Die Informationen werden mit URLs adressiert und werden durch Eingabe in die Browser-Adresszeile oder per Klick auf einen Hyperlink (Link) vom HTTP-Server, auf dem die Ressource liegt, mit einem HTTP-Request abgerufen. Der

HTTP-Server liefert dann die aufgerufenen Dateien an den Browser mit einem HTTP-Response aus. Der Browser kümmert sich um die Darstellung und das Nachladen weiterer Ressourcen. Zum Beispiel Bilder, die ebenfalls dargestellt werden.

In den Anfangszeiten des Internets waren viele Nutzer noch mit analogen Wählmodems an das Internet angebunden. Aufgrund der Experimentierfreude mancher Webseiten-Gestalter (Webdesigner) mussten die überladenen Webseiten mit ihren großen Datenmengen über die Modem-Verbindung mit einer quälend langsamen Verbindung geladen werden. Außerdem war die Infrastruktur des Internets noch nicht so gut ausgebaut. Zu manchen Spitzenzeiten musste man dann einfach warten, bis die Dateien endlich übertragen wurden. Daher rührt auch der Spitzname für das WWW: World Wide Waiting.

Heute ist Dank DSL und anderen breitbandigen Zugangstechniken ein bequemes Surfen zu bezahlbaren Preisen mit hohen Übertragungsgeschwindigkeiten und geringer Wartezeit möglich.

HTTP-Client / Webbrowser / Browser

Der Browser ist der Client, der über HTTP eine Anforderung an einen Server schickt. Der Server liefert die Daten zurück. Der Browser stellt diese Daten dann auf dem Bildschirm dar.
Der Nutzer des World Wide Webs kann zwischen den verschiedenen Browsern (HTTP-Clients) auswählen:

- Edge (Microsoft)
- Firefox (Mozilla)
- Safari (Apple)
- Chrome (Google)
- Opera

HTTP-Server / Web-Server / WWW-Server

Es gibt auch verschiedene HTTP-Server, die auch als Webserver oder WWW-Server bezeichnet werden. Alle Bezeichnungen sind richtig. Sie meinen jeweils dasselbe.

- Apache
- Internet Information Server (Microsoft)
- Lighttpd
- nginx

Der HTTP-Server ist ein Server-Dienst, der ohne grafische Benutzeroberfläche auf einem speziellen Computer läuft. Die Ausstattung ist auf die Verarbeitung von Daten ausgelegt.
Um die enormen Datenmengen in das Internet zu übertragen, ist der Server über einen Breitband-Internet-Anschluss an das Internet angebunden.

HTML - Hypertext Markup Language

Das World Wide Web (WWW) basiert auf HTML (Hypertext Markup Language), das Text, Bilder Videos und Audio-Dateien strukturiert im Browser (HTTP-Client) darstellt. HTML ist eine Beschreibungssprache um plattformübergreifende Dokumente zu erstellen.

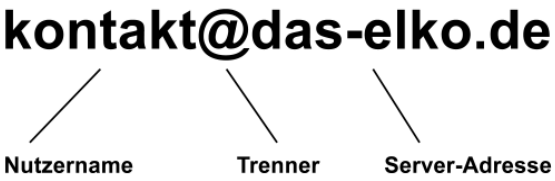
E-Mail

E-Mail ist die Abkürzung für Electronic Mail, was "Elektronische Post" oder "Elektronischer Brief" bedeutet. Bei einer E-Mail erfolgt das Erstellen, Versenden und Darstellen ausschließlich in elektronischer bzw. digitaler Form. E-Mail ist neben dem Telefon und Messaging ein zentrales Kommunikationsmittel in unserer Gesellschaft. Nachrichten, Diskussionen und Austausch von Dokumenten, das alles ist mit E-Mail möglich.

Das Bearbeiten von E-Mails durch den Benutzer findet auf einem elektronischen Gerät mit Internet-Zugang statt. Nach dem Absenden wird die E-Mail innerhalb eines Netzwerks oder über das Internet verschickt. Beim Empfänger wird die E-Mail wieder auf einem elektronischen Gerät mit Internet-Zugang angezeigt. Das Senden, Empfangen, Lesen und Schreiben von E-Mails erfolgt mit einer entsprechenden Software oder im Browser, in dem eine grafische Benutzeroberfläche zur Verwaltung von E-Mails abgebildet ist.

Im Jahr 1971 wurde erstmals eine E-Mail zwischen zwei Computern im damaligen ARPANET übertragen. Danach wurden E-Mails auf wissenschaftlicher Ebene zwischen den Mitarbeitern der Universitäten ausgetauscht. Im Zuge der kommerziellen Nutzung des Internets setzte sich E-Mail als Kommunikationsmittel im privaten und geschäftlichen Umfeld durch. E-Mail ersetzt bzw. ergänzt Telefon, Fax und Brief um eine schnelle Möglichkeit Nachrichten und Dokumente digital zu übertragen. In der heutigen Zeit ist die elektronische Post nicht mehr weg zu denken, und hat teilweise Brief und Fax als schnelle und direkte Kommunikation ersetzt.

E-Mail-Adresse



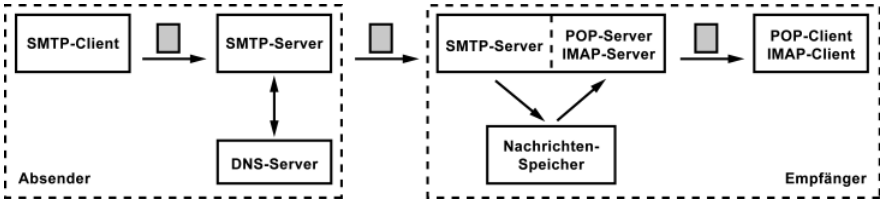
Wie beim Brief muss jede E-Mail mit einer Adresse für den Empfänger versehen werden. Die E-Mail-Adresse kennzeichnet das ungewöhnliche Zeichen "@" (Klammeraffe). Es wird als Trennzeichen zwischen Nutzername und dem Domain-Namen (Server-Adresse) verwendet. Darin unterscheidet sich die E-Mail-Adresse von anderen Internet- oder Netzwerk-Adressen.

Ablauf der E-Mail-Kommunikation mit Postausgang und Posteingang

Die E-Mail-Kommunikation erfolgt über einen Client und einen Server. Hier unterscheidet man zwischen dem Posteingangsserver und dem Postausgangsserver, wobei es sich um unterschiedliche Server handeln kann. Der Ablauf der Kommunikation zwischen den Clients und Servern erfolgt nach dem Client-Server-Prinzip.

Die Unterscheidung zwischen Posteingang und Postausgang liegt daran, weil man bei E-Mail davon ausgeht, dass der Nutzer nicht ständig online ist. Beispielsweise, weil der PC ausgeschaltet ist oder weil der Internet-Zugang über einen Dialup-Zugang hergestellt wird und dann eben nur

zeitweise eine Verbindung besteht. Wenn also der Empfänger einer E-Mail nicht online ist, dann kann man ihm auch keine E-Mail senden. Damit das trotzdem geht, bedarf es zweier Zwischenschritte. Einmal dem Senden von E-Mails über den Postausgangsserver. Und das Empfangen und Speichern von E-Mails über den Posteingangsserver. Die Kommunikation erfolgt über die Protokolle SMTP, POP und IMAP.



- MUA - Mail User Agent (E-Mail-Client)
- MTA - Mail Transfer Agent oder Message Transport Agent (Postausgangsserver)
- MDA - Mail Delivery Agent (Posteingangsserver)

Beim E-Mail-Versand schickt der sendende E-Mail-Client (Mail User Agent, MUA) die E-Mail per SMTP an seinen Postausgangsserver (Mail Transfer Agent oder Message Transport Agent, MTA). Von dort wird die E-Mail per SMTP an den MTA des Empfängers weitergeleitet. Da dieser Server die E-Mail nicht von sich aus an den Empfänger schicken kann, verschiebt er die E-Mails in den Posteingangsserver (Mail Delivery Agent, MDA). Von dort muss der empfangende E-Mail-Client (Mail User Agent, MUA) die E-Mails per POP oder IMAP abholen.

Welche Aufgabe hat der DNS-Server? Weil eine E-Mail-Adresse nicht den Domain-Namen des Mail-Server des Empfängers beinhaltet, wird die Mail-Server-Adresse im MX-Record des (autoritativen) DNS-Servers hinterlegt und kann per DNS-Request abgefragt werden.

SMTP - Simple Mail Transfer Protocol

Das SMTP-Protokoll ist für die Übertragung von E-Mails vom SMTP-Client des Absenders zum SMTP-Server (Postausgang) und von dort wiederum zum SMTP-Server des Empfängers zuständig. Dazu kontaktiert der E-Mail-Client des Absenders seinen eigenen SMTP-Server

(Postausgangsserver) und übergibt ihm die E-Mails, die zum Versand anstehen.

POP - Post Office Protocol

Da E-Mail-Nutzer in der Regel nicht ständig online sind, um immer E-Mails empfangen zu können, werden alle eingehenden Nachrichten zwischengespeichert. Um die E-Mails abzuholen kontaktiert der Empfänger seinen Posteingangsserver mit POP.
POP ist für den Zugriff von mehreren Geräten auf ein E-Mail-Postfach nicht geeignet, weil es die E-Mails aus dem Posteingang (Inbox) laden und löschen kann. Das Verwalten von E-Mails (Verschieben, Kopieren, Löschen) in Ordnerstrukturen kennt POP nicht. Außerdem kann der Client die Verbindung zum Server nicht aufrecht erhalten (Idle-Funktion), um neue eingehende Mails zum Client zu "pushen". Das geht nur mit IMAP.

IMAP - Internet Mail Access Protocol

IMAP hat vom Prinzip die selbe Aufgabe wie POP. Es bietet jedoch mehrere Vorteile. IMAP definiert Methoden zum Erstellen, Löschen und Umbenennen einer Mailbox sowie zum Prüfen, ob neue Nachrichten eingetroffen sind. Außerdem erlaubt IMAP das auszugsweise Laden einer E-Mail und Verzeichnisdienste innerhalb der Mailbox.
Im Gegensatz zu POP kann der Benutzer selber wählen, welche E-Mails er zum Lesen herunterladen will. Das ist vor allem bei der Benutzung einer Verbindung mit geringer Bandbreite ein Vorteil.

POP oder IMAP

Üblicherweise werden E-Mails vom Posteingangsserver mit POP heruntergeladen und anschließend auf dem Server gelöscht. Das bedeutet, POP eignet sich für die Offline-Bearbeitung von E-Mails in Zeiten von Internet-Zugängen über Wählleitungen. Doch im Zeitalter von "Always-on" ist diese Vorgehensweise alles andere als praktikabel. Da würde es sich anbieten die E-Mails auf dem Server zu lassen und nur die E-Mails herunterzuladen, die man lesen will. Auch wenn man von verschiedenen Computern und Endgeräten auf ein Postfach zugreifen will, ist POP ungeeignet. Überall hat man dann einen anderen Datenstand. Überall sind die E-Mails verteilt.

Doch es gibt das IMAP-Protokoll. Dieses Protokoll arbeitet im Online-Modus und hat auch die Möglichkeit Ordner auf dem E-Mail-Server anzulegen, um dort die E-Mails zu speichern und zu archivieren. Hat man ausreichend Speicherplatz kann man dort die E-Mails über mehrere Jahre kategorisieren und archivieren. Auch haben E-Mails mit IMAP verschiedene Kennzeichnungen. Zum Beispiel "gelöscht" oder "gelesen". Unabhängig vom Client hat man Zugriff aus seinen E-Mail-Bestand, ganz so, als wäre er lokal gespeichert.
IMAP arbeitet nach einem interaktiven Client-Server-Modell, bei dem die Nachrichten auf dem Server bleiben, bis sie endgültig gelöscht werden. So hat man von verschiedenen Geräten immer Zugriff auf die E-Mails, sobald man online ist.

POP ist ein altes Protokoll und entspricht nicht mehr dem modernen Umgang mit Daten. Bei POP müssen E-Mails lokal gespeichert werden. Und trotzdem hat sich IMAP nicht wirklich durchgesetzt. Viele private E-Mail-Nutzer verwenden lieber Webmail
Das einzige Manko ist der Speicherplatz für IMAP, der auf dem E-Mail-Server vorhanden sein muss. Für die Internet-Provider ist das natürlich nicht immer gewünscht, obwohl jeder Provider IMAP unterstützt. Meistens kann man wahlweise auf die eingerichteten Postfächer über POP oder IMAP zugreifen, ohne es auf Provider-Seite konfigurieren zu müssen. Auch alle gängigen E-Mail-Clients unterstützen IMAP für den Zugriff auf E-Mail-Postfächer.

Namensauflösung

In einem TCP/IP-Netzwerk, in der Regel im lokalen Netzwerk und im Internet, werden Hosts mit einer IP-Adresse adressiert. Darüber werden auch die Verbindungen aufgebaut. Eine IP-Adresse wird in einer binären Form elektronisch verarbeitet. Sie wird entweder in dezimaler (IPv4-Adresse) oder hexadezimaler Schreibweise (IPv6-Adresse) dargestellt. Leider sind Zahlen für das menschliche Gehirn schwer zu erfassen und zu merken. Deshalb verwendet der Mensch lieber Namen um eine Sache zu benennen und zu identifizieren. Diese Erkenntnis ist in den 1970er-Jahren bei der Entwicklung des ARPANETs, dem ursprünglichen Vorgänger des Internets, mit eingeflossen.

Deshalb werden zur Adressierung von Computern nicht nur IP-Adressen, sondern auch Namen verwendet. Die sind für Menschen leichter zu merken und zu verstehen. Bis heute ist es jedoch nicht möglich, einen Computer direkt mit seinem Namen über das Netzwerk anzusprechen. Diese Welt besteht immer noch aus 1en und 0en (binäre Adresse). Aus diesem Grund wurden Methode entwickelt, um eine Umwandlung bzw. Auflösung von Namen in numerische Adressen zu realisieren. Diesen Vorgang nennt man Namensauflösung.

Die Namensauflösung erfolgt typischerweise anhand eines Verzeichnisses oder einer Datenbank. Das kann im einfachsten Falle eine per Hand gepflegte Datei sein, in der IP-Adressen und Computername verzeichnet sind. Viel eher kommen dezentral verantwortliche Client-Server-Systeme zum Einsatz, die nach einer hierarchischen Abfragefolge mit unterschiedlichen Verantwortungsbereichen arbeiten.

hosts

Jedes TCP/IP-Betriebssystem hat eine Datei mit dem Namen "hosts". In dieser Datei sind IP-Adressen und Computernamen tabellarisch aufgelistet. Weil diese Datei händisch gepflegt werden muss, trägt man hier temporär nur die Adressen und Namen lokaler Systeme ein.

lmhosts

Die Datei "lmhosts" ist zusätzlich in Windows-Betriebssystemen zu finden. In dieser Datei sind speziell die für Windows-Netzwerke wichtigen NetBIOS-Namen für die Namensauflösung enthalten.

DNS - Domain Name System

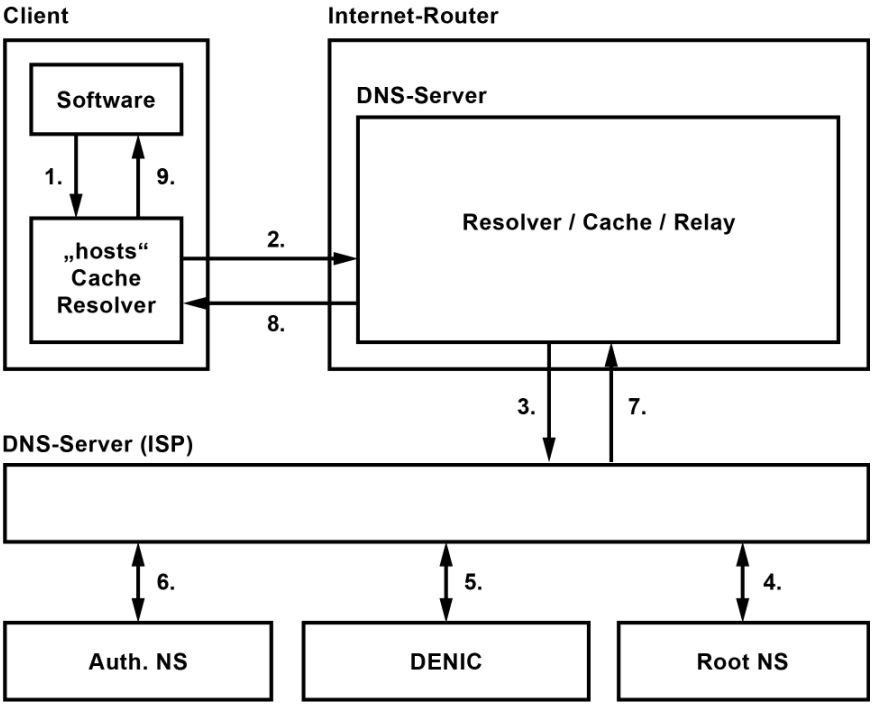
DNS ist ein dezentrales und hierarchisch angeordnetes System zur Auflösung von Domain-Namen in IP-Adressen. Ein Client, der einen Domain-Namen in eine IP-Adresse auflösen will, stellt eine Anfrage an einen DNS-Server. Kann dieser DNS-Server die Anfrage nicht beantworten, dann befragt er einen übergeordneten DNS-Server, bis eine IP-Adresse ermittelt und an den anfragenden Client zurück geliefert werden kann.

WINS - Windows Internet Name Service

WINS ist ein auf Windows basierendes System zur Namensauflösung. Es baut auf den NetBIOS-Dienst von Windows auf. WINS wurde eingeführt, um die NetBIOS-Rundsprüche, die zur Namensauflösung verwendet werden, zu reduzieren. Wie bei DNS greift der Client auf den WINS-Server zu, um die IP-Adresse zu einem Rechnernamen herauszufinden.

Schritt für Schritt: Ablauf einer Namensauflösung

Der folgende Ablauf soll eine mögliche Namensauflösung darstellen. In bestimmten Systemen und der praktischen Anwendung kann der Ablauf von diesem hier abweichen. Der Ablauf geht davon aus, dass die ursprüngliche Anfrage zur Namensauflösung erst vom verantwortlichen Nameserver (autoritativ) beantwortet werden kann. In der Praxis kommt es häufig vor, dass die Namensauflösung durch einen Resolver (Stellvertreter) erfolgreich beantwortet werden kann.



1. Der Client stellt seine Anfrage zur Auflösung eines Computer- oder Domain-Namens an seinen lokalen DNS-Resolver. Der schaut zuerst in die "hosts"-Systemdatei, ob sich dort ein statischer Eintrag für den Computer- oder Domain-Namen befindet. Danach schaut der Client in seinen eigenen Cache.
2. Ist der lokale Resolver nicht fündig geworden, befragt er den DNS-Server im lokalen Netzwerk. In der Regel ist das der Router für den Internet-Zugang. Bei diesem DNS-Server handelt es sich meistens um einen DNS-Resolver bzw. Proxy mit einem Zwischenspeicher (Cache) handelt. Manchmal ist er auch nur ein Relay.
3. Dieser DNS-Resolver befragt den DNS-Server beim Internet-Service-Provider (ISP). Wie ab hier die Abfragefolge aussieht hängt davon ab, wie ISP-Nameserver die die DNS-Hierarchie angebunden ist.
4. Denkbare wäre, dass der ISB-Nameserver den Root-Nameserver für die Verantwortlichkeit der Top-Level-Domain (.com, .net, .de, ...) befragt. Der Root-Nameserver delegiert die Anfrage an den für die Zone verantwortlichen NIC-DNS-Server. Für die TLD ".de" wäre das die DENIC.
5. Der ISP-Nameserver befragt dann den DENIC-Nameserver, der die Adresse des autoritativen Nameserver zurückliefert.
6. Der ISP-Nameserver befragt dann den für die Zone zuständigen autoritativen Nameserver, der die IP-Adresse zurückliefert.
7. Der ISP-Nameserver übergibt die IP-Adresse an den DNS-Server des Internet-Routers.
8. Von dort wird die IP-Adresse an den lokalen Resolver gegeben.
9. Ganz am Schluss landet die IP-Adresse bei der anfragenden Software.

Zusätzliche Namensauflösung in Windows

- Findet die Suche über den DNS-Server die IP-Adresse nicht, wird der WINS-Server befragt.
- Kennt auch dieser den Computernamen nicht, wird ein NetBIOS-Rundspruch abgesetzt.
- Als letzter Strohhalm bei der NetBIOS-Namensauflösung ist die lmhosts-Datei.

PNRP - Peer Name Resolution Protocol

PNRP ist ein Protokoll von Microsoft für die Namensauflösung in IPv6-Netzwerken. PNRP ermöglicht es, dass ein Rechner seine IP-Adressen mit einem Namen verknüpft und seine Dienste im lokalen Netzwerk anbietet. Damit hat es die gleiche Funktion, wie Bonjour (Zeroconf) von Apple.

DDNS - DynDNS - Dynamic Domain Name System

DynDNS oder DDNS ist ein System, das dynamische IP-Adressen von Domain-Namen aktualisieren kann. Unter DynDNS versteht man in der Regel einen DNS-Dienst, der die ständig wechselnden IP-Adressen an einem typischen Internet-Anschluss für einen festen Domain-Namen aktualisiert.

DNSSEC

Die Domain Name System Security Extensions (DNSSEC) sind eine DNS-Implementierung, für kryptografisch abgesicherte DNS-Anfragen. DNSSEC hat Funktionen, die prüfen, ob eine DNS-Auskunft von einem vertrauenswürdigen DNS-Server stammt und ob der Transport unverfälscht übertragen wurde.

DNS - Domain Name System

Das Domain Name System, kurz DNS, wird auch als "Telefonbuch des Internets" bezeichnet. Ähnlich wie man in einem Telefonverzeichnis nach einem Namen sucht, um die Telefonnummer heraus zu bekommen, schaut man im DNS nach einem Computernamen, um die dazugehörige IP-Adresse zu bekommen. Die IP-Adresse wird benötigt, um eine Verbindung zu einem Server aufbauen zu können, über den nur der Computername bekannt ist.

Das Domain Name System ist ein System zur Auflösung von Computernamen in IP-Adressen und umgekehrt. DNS kennt keine zentrale Datenbank. Die Informationen sind auf vielen tausend Nameservern (DNS-Server) verteilt.
Möchte man zum Beispiel die Webseite www.elektronik-kompendium.de

besuchen, dann fragt der Browser einen DNS-Server, der in der IP-Konfiguration hinterlegt ist. Das ist in der Regel der Router des Internet-Zugangs. Je nach dem, ob die DNS-Anfrage beantwortet werden kann oder nicht, wird eine Kette weiterer DNS-Server befragt, bis die Anfrage positiv beantwortet und eine IP-Adresse an den Browser zurück geliefert werden kann.

Wenn ein Computername oder Domain-Name nicht aufgelöst werden kann, dann kann auch keine Verbindung zu dem betreffenden Host aufgebaut werden. Es sei denn, der Nutzer verfügt über das Wissen der IP-Adresse. Das bedeutet, ohne DNS ist die Kommunikation im Netzwerk und im Internet praktisch nicht möglich. Deshalb existieren viele tausend DNS-Server auf der ganzen Welt, die zusätzlich hierarchisch angeordnet sind und sich gegenseitig über Änderungen informieren.

Namensauflösung vor DNS

DNS geht auf die Datei "hosts" zurück, deren Inhalt zur Namensauflösung im ARPANET (Vorgänger des Internets) diente und händisch gepflegt wurde. Mit zunehmender Anzahl der Hosts im ARPANET wuchs der Bedarf für ein verteiltes und hierarchisches System zur Auflösung von Computernamen in IP-Adressen und umgekehrt.

Ein weiterer Nachteil der Datei "hosts" ist die fehlende Eindeutigkeit. Gemeint ist, in der Datei kann alles drin stehen, was auch immer der Administrator für richtig hält. Der Inhalt könnte manipuliert sein. Um das zu vermeiden, sieht das DNS autoritative Nameserver vor und mit DNSSEC ein Verfahren mit der Möglichkeit zu prüfen, ob ein DNS-Response von einem vertrauenswürdigen DNS-Server stammt und ob der Transport unverfälscht erfolgt ist.

Domain oder Domain-Name

Ein Domain-Name, kurz Domain, dient dazu, um Computer, die mit kaum merkbaren IP-Adressen adressiert sind, richtige Namen zu geben und gleichzeitig in eine hierarchische Struktur zu unterteilen. Domain-Namen sind auch häufig Teil eines Uniform Resource Locator (URL). Der URL (nicht die) ist eine "einheitliche Angabeform für Ressourcen" in Netzwerken. Eine URL beginnt mit einem vorangestellten Kürzel, das den

verwendeten Dienst kennzeichnet (z. B. http:// oder ftp://). Es handelt sich dabei um eine optionale Angabe, die auch nur für Anwendungsprogramme wichtig ist und kein Teil des Domain-Namens ist.

Die für Domain-Namen verwendete Struktur besteht aus drei oder mehr Teilen. Die einzelnen Teile bzw. Ebenen werden durch Punkte voneinander getrennt.
Zu beachten ist, dass ein Domain-Name ganz rechts mit einem abschließenden Punkt beginnt. Dieser Punkt ist die Wurzel bzw. Root. In der Regel lässt man den Punkt einfach weg, weil er nur symbolischen Charakter hat.

Computername (Host oder Dienst)	Second-Level-Domain (SLD)	Top-Level-Domain (TLD)
www.	elektronik-kompendium.	de
ftp.	elektronik-kompendium.	de

Manchmal befindet sich zwischen der Second-Level-Domain (SLD) und dem Computernamen eine Sub-Level-Domain (Subdomain).

Computername (Host oder Dienst)	Sub-Level-Domain (Subdomain)	Second-Level-Domain (SLD)	Top-Level-Domain (TLD)
www.	dse-faq.	elektronik-kompendium.	de

Ein Domain-Name wird immer von hinten nach vorne gelesen. Dort beginnt die Adresse mit der Top-Level-Domain (TLD). Man unterscheidet zwischen zwei Typen von Top-Level-Domains. Geografische Top-Level-Domains, die Ländercodes die nach ISO 3166-1 definiert und als Country-Code Top-Level-Domains (ccTLD) bezeichnet werden. Dann gibt es noch die organisatorischen oder generischen Top-Level-Domains (Generic Top-Level-Domain, gTLD).

Die Second-Level-Domain kann von einer Person oder Organisation beantragt und eingesetzt werden. Die Second-Level-Domain bildet unter der Top-Level-Domain einen Domain-Namensraum, der es der

Organisation ermöglicht einen Server mit dem Namen "www" zu betreiben, der im Internet dann zum Beispiel unter "www.elektronik-kompendium.de" zu erreichen ist.
Für weitere Unterteilungen existiert noch eine Third-Level-Domain, die auch als Sub-Level-Domain oder Subdomain bezeichnet wird. Ganz am Ende der Kette (am Anfang des Domain-Namens) wird dann der optionale Hostname des Computers eingesetzt.

Eine so zusammengesetzte Adresse (zum Beispiel www.elektronik-kompendium.de) ist ein sogenannter Fully Qualified Domain Name (FQDN).

Organisatorische Top-Level-Domains (Auszug)

Domain (gTLD)	Organisationsform
.aero	Lufttransportindustrie
.arpa	Alte Arpanet Domäne
.biz	Business, für große und kleinere Unternehmen
.com	Kommerzielle Domain
.coop	Kooperationen, Genossenschaften
.edu	Schulen, Universitäten, Bildungseinrichtungen
.gov	Regierungsstellen der USA
.info	Informationsdienste
.int	International tätige Institutionen
.mil	Militär der Vereinigten Staaten von Amerika
.museum	Museen
.name	Privatpersonen
.net	Netzspezifische Dienste und Angebote
.org	Nichtkommerzielle Unternehmungen und Projekte
.pro	Professionals, spezielle Berufsgruppen
...	

Geografische Top-Level-Domains (Auszug)

Domain (ccTLD)	Land
.at	Österreich
.au	Australien
.cc	Kokos-Inseln
.ch	Schweiz
.de	Deutschland
.fr	Frankreich
.gb	Großbritannien
.ie	Irland
.it	Italien
.li	Lichtenstein
.nl	Niederlande
.no	Norwegen
.ru	Russland
.to	Tonga
.uk	Vereinigtes Königreich
...	

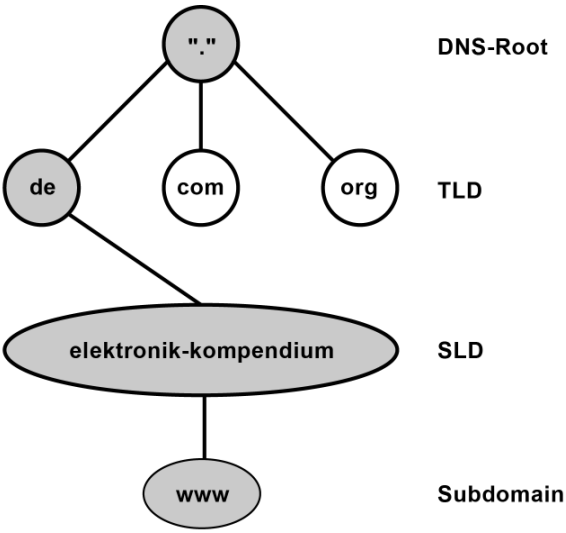
Nach der Top-Level-Domain (TLD) folgt die Second-Level-Domain (SLD), die einen beliebigen, aber unter der Top-Level-Domain einzigartigen Namen haben kann. Das jeweilige, für die Top-Level-Domain verantwortliche NIC verwaltet die Second-Level-Domains. Für .de (Deutschland) ist das die DENIC.

In einigen Ländern, wie beispielsweise Großbritannien, gibt es zur besseren Unterscheidung festgelegte Second-Level-Domains (zum Beispiel .co.uk., .ac.uk. oder .gov.uk.). Unterhalb der Second-Level-Domain können weitere Sub-Level-Domains (Subdomains) vorhanden sein, für die der Inhaber der Second-Level-Domain verantwortlich ist.

Aufgabenteilung im DNS

Eine Aufgabe im Domain Name System ist die Namensauflösung. Eine weitere Aufgabe ist die Verwaltung der DNS-Zonen. An der Spitze stehen die sogenannten Root-Server, die Informationen zu den Top-Level-Domains (TLD) speichern.
Auf den Ebenen darunter tummeln sich weitere Nameserver, die für Domains oder Subdomains zuständig und autoritativ auskunftsberechtigt sind.
Und dann gibt es DNS-Server, die sich nur mit der Namensauflösung beschäftigen und Anfragen weiterleiten und die Antworten erfolgreicher Anfragen zwischenspeichern.
Oder um es anders auszudrücken, ein DNS-Server ist nicht gleich DNS-Server. Jeder hat im DNS eine andere Aufgabe und Zuständigkeit.

DNS-Zonen



www.elektronik-kompendium.de.

Eine DNS-Zone ist ein Verantwortungsbereich oder eine Verwaltungseinheit, die in der Regel an einen Teil eines Domain-Namens gebunden ist. Ein autoritativer DNS-Server ist für eine oder mehrere

dieser DNS-Zonen verantwortlich. Das heißt, er ist derjenige, von dem eine DNS-Anfrage eindeutig und korrekt zu seiner Zone beantwortet werden kann.
Die Daten einer Zone liegen in einer lokalen Zonendatei, die vom zuständigen Administrator gepflegt werden muss.

Einträge in einer DNS-Zone bzw. Zonendatei

Die Einträge in einer DNS-Zone werden als Resource Records bezeichnet. Jeder Resource Record bezieht sich auf einen anderen Record-Type, der eine bestimmte Information enthält. Zum Beispiel eine IP-Adresse oder die Mailserver-Adresse eines Domain-Namens bzw. der Zone.

- Record-Type / Eintrag
- A / IPv4-Adresse
- AAAA / IPv6-Adresse
- CNAME / Verweis, Weiterleitung oder Alias
- MX / zuständiger Mailserver für die Zone (Mail Exchange)
- NS / zuständiger Nameserver für die Zone
- SRV / Server für einen Dienst im Windows-AD
- TXT / liefert einen Text zurück
- SOA / Ansprechpartner und Parameter zur abgefragten Zone (SOA: engl. für Start of Authority)

DNS-Server / Nameserver

Die Bezeichnungen DNS-Server und Nameserver benennen das gleiche. Während der Nameserver eine allgemeine Bezeichnung für einen Server ist, der für die Namensauflösung zuständig ist, bezeichnet der DNS-Server einen Nameserver im Domain Name System.

Den einen DNS-Server gibt es nicht. Man unterscheidet zwischen verschiedenen Arten von DNS-Servern, die unterschiedliche Verantwortungsbereiche, Aufgaben und Funktionen haben.

- DNS-Root-Server
- Autoritativer Nameserver (für eine DNS-Zone)
- Nicht-autoritativer Nameserver

- Cache
- Forwarder
- Resolver

DNS-Root-Server: DNS-Root-Server, Root-Name-Server oder auch nur Root-Server sind autoritative Nameserver für die Root-Zone. Sie beantworten Anfragen zur Root-Zone (".") oder geben eine Liste mit autoritativen Namenservern für eine bestimmte Top-Level-Domain (TLD) zurück (".de", ".com", ".org", etc.).
Um Manipulationen der Root-Zone zu verhindern gibt es weltweit über hundert Root-Name-Server, die dem DNS Root Server System Advisory Committee der ICANN unterstehen.

Autoritativer Nameserver: Ein autoritativer Nameserver ist für eine (oder mehrere) Zonen zuständig und beantwortet auch nur Anfragen für diese Zonen. Autoritativ bedeutet, dass die Informationen dieses Nameservers als verbindlich gelten.

Nicht-autoritativer Nameserver: Ein nicht-autoritativer Nameserver ist nicht selbst für eine DNS-Zone verantwortlich und muss deshalb die Informationen zu einer Zone aus zweiter oder dritter Hand mit einer rekursiven oder iterativen DNS-Abfrage ermitteln. Dieser Nameserver und seine DNS-Auskunft ist deshalb nicht-autoritativ.

In der Praxis unterscheidet man grob zwischen autoritativen und rekursiven DNS-Servern. Ein rekursiver DNS-Server ist dabei nur ein Proxy-Server. Er holt die angefragten Informationen ab und stellt das Ergebnis den Hosts zur Verfügung. Er hält die Informationen eine Zeit lang vor, damit bei einer erneuten Anfrage diese nicht noch einmal ins Netz geschickt werden muss. Von einem rekursiven DNS-Server erhält man immer "non-authoritative", also nicht autorisierte Antworten. Das bedeutet, dass der Inhalt der Antwort nicht richtig sein muss. Weil er im Prinzip nur das nachplappert, was er von woanders ermittelt hat.

Weitere Eigenschaften von Nameservern sind Caching (speichern) und Forwarding (weiterleiten).

Caching-Server: Ein Caching-Server erhält Informationen von einem anderen Nameserver und speichert die Auskünfte eine Zeit lang zwischen.

Dieser Server muss die Information erst dann wieder einholen, wenn sie nicht mehr zur Verfügung steht. Die Lebensdauer (Time-To-Live, TTL) bestimmt der autoritative Nameserver.

Forwarding-Server: Ein Forwarding-Server leitet alle DNS-Anfragen ausnahmslos an einen anderen Nameserver weiter.

Resolver: Die meisten DNS-Server sind keine autoritativen DNS-Server, sondern nur DNS-Resolver mit Caching- und/oder Forwarding-Funktion. Typischerweise sind DNS-Resolver in einem lokalen Netzwerk für die Namensauflösung der Clients zuständig. Ein als Resolver agierender DNS-Server befinden sich lokal auf einem Computer oder auch als Server-Funktion in einem Router im lokalen Netzwerk. Der in der IP-Konfiguration eingetragene DNS-Server ist demnach ein solcher DNS-Resolver. Wobei der lokale DNS-Client auch als Resolver bezeichnet wird.

Resolver (DNS-Client)

Ein Resolver ("to resolve", "auflösen") ist ein Programm, das Informationen aus dem Domain Name System besorgt. Das Programm ist eine Art Vermittlungsstelle zwischen einer Anwendungen und dem DNS. Der Resolver ist direkt in TCP/IP integriert und steht dort als Software-Bibliothek für die Namensauflösung zur Verfügung. Der Resolver wird mit den Funktionen "gethostbyname" und "gethostbyaddr" angesprochen. Er liefert die IP-Adresse eines Domain-Namens bzw. dem Haupt-Domain-Namen einer IP-Adresse zurück.
Damit der Resolver arbeiten kann benötigt er die IP-Adresse von einem, besser von zwei DNS-Servern, die in der IP-Konfiguration eingetragen sein müssen. In der Regel erhält ein IP-Host die IP-Adresse des oder der DNS-Server per DHCP oder die IP-Adresse muss manuell eingetragen werden.

Primärer und Sekundärer DNS-Server / Primary und Secondary Nameserver

Damit ein DNS-Server die ganze Last der DNS-Anfrage nicht alleine tragen muss, gibt es sogenannte Primary und Secondary Nameserver. Sie sind voneinander unabhängig und redundant ausgelegt, so dass

mindestens immer ein Server verfügbar ist. Der Secondary Nameserver gleicht in regelmäßigen Abständen seine Daten mit dem Primary Nameserver ab und dient so als Backup-Server. Ein zweiter Nameserver ist sinnvoll, weil ein Ausfall des primären Nameservers dazu führt, dass Internet-Verbindungen ohne Namensauflösung nicht mehr möglich sind. Um dann trotzdem Verbindungen aufbauen zu können, müsste man als Anwender die IP-Adressen der kontaktierten Server kennen. Was aber nicht die Regel ist.

URL - Uniform Resource Locator

Der URL ist ein wichtiger Bestandteil vieler Protokolle des Internets. URL gehört, wie HTTP und HTML, zum World Wide Web (WWW). Nahezu alle Programme, die auf Internet-Ressourcen zugreifen verwenden dazu URLs.
Obwohl es im eigentlichen Sprachgebrauch gerne als "die" URL bezeichnet wird, heißt es korrekterweise "der" URL, von "der" Uniform Resource Locator.

Aufbau eines URL

Ressourcentyp://User:Passwort@Host.Domain.TLD:Port/Pfad/Datei?Parameter

Der URL berücksichtigt sehr viele Adressierungsarten mit Benutzername, Passwort, lokale, nichtlokale Ressourcen und sogar Parameter. Der Aufbau kann deshalb äußerst komplex sein.

Ressourcentyp://

Der Ressourcentyp bezeichnet das Protokoll auf der Anwendungsebene. Mit diesem Protokoll wird die Ressource angesprochen. Protokolle wären z. B. HTTP, NNTP, FTP, etc.
Dem Protokoll folgt ein Doppelpunkt, der den Ressourcentyp vom restlichen Ressourcenzeiger trennt. Der Doppel-Slash (Schrägstriche) deutet auf eine nicht lokale Ressource hin, also außerhalb der eigenen Station (http://www.elektronik-kompendium.de/). Eine lokale Ressource führt meist zum Ausführen einer Aktion oder einer Anwendung. Z. B. wird bei mailto:kontakt@das-ELKO.de der E-Mail-Client aufgerufen.

Keine Ausnahme bildet der Ressourcentyp file: (z. B. file:///c:/windows/). Der Dritte Slash ist kein Fehler, sondern gehört bereits zum Ressourcenzeiger und kennzeichnet die höchste Ebene, über den Laufwerken, des Dateisystems.

User:Passwort@

Beide Werte enthalten einen Benutzername und Passwort, die durch einen Doppelpunkt voneinander getrennt sind. Diese Angaben sind erforderlich, wenn eine Ressource eine Authentifizierung erwartet. Selbige Schreibweise ist auch ohne Passwort möglich. Das führt dann zur Schreibweise einer E-Mail-Adresse, welche schon lange Zeit vor der URL bekannt war.
Alle weitere Angaben werden durch einen Klammeraffen (at, @) voneinander getrennt.
Vorsicht: Benutzername und Passwort werden in Klartext übertragen, wenn das Anwendungsprotokoll keine Verschlüsselung vorsieht.

Host.Domain.TLD

Dieser Teil besteht aus dem Host, der Domain und der Top-Level-Domain (TLD), die mit einem Punkt voneinander getrennt werden. Es handelt sich dabei um die Adresse des Computers, auf der sich die Ressource befindet. Alternativ ist hier auch die Angabe einer IP-Adresse möglich. Damit wird DNS umgangen.

:Port

Hierbei ist der Port von UDP und TCP gemeint. In der Regel ist jedem Kommunikationsprotokoll ein Port fest zugewiesen. Über diese Ports stellen die Protokolle die Verbindung her.
Wird der Port weggelassen, verwendet die Anwendung den Standard-Port des Ressourcentyps (Protokoll).

/Pfad/Datei

Diese Angabe verweist auf den Standort der Ressource des adressierten Zielsystems. Üblicherweise wird darin die teilweise identische Verzeichnisstruktur abgebildet.

Parameter

Enthält die Ressource ausführbare Bestandteile, so können diese mit Parametern gefüttert oder gesteuert werden. Auf diese Weise werden Benutzereingaben übermittelt, verarbeitet und sogar gespeichert. Die Parameter werden durch ein Fragezeichen (?) vom Rest der URL getrennt. Nicht jeder Ressourcentyp kennt Parameter. Außerdem gibt es unterschiedliche Verfahren und nicht alle Parameter sind für das entfernte Zielsystem bestimmt.

HTTP - Hypertext Transfer Protocol

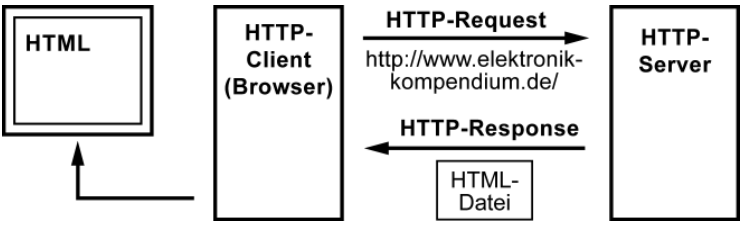
HTTP ist das Kommunikationsprotokoll im World Wide Web (WWW). Die wichtigsten Funktionen sind Dateien vom Webserver anzufordern und in den Browser zu laden. Der Browser übernimmt dann die Darstellung von Texten und Bilder und kümmert sich um das Abspielen von Audio- und Video-Daten.

Das Hypertext Transfer Protocol (HTTP) im Schichtenmodell

Schicht	Dienste / Protokolle / Anwendungen			
Anwendung	HTTP	IMAP	DNS	SNMP
Transport	TCP		UDP	
Internet	IP (IPv4 / IPv6)			
Netzzugang	Ethernet, ...			

Wie funktioniert HTTP?

Die Kommunikation findet nach dem Client-Server-Prinzip statt. Der HTTP-Client (Browser) sendet seine Anfrage (HTTP-Request) an den HTTP-Server (Webserver/Web-Server). Dieser bearbeitet die Anfrage und schickt seine Antwort (HTTP-Response) zurück. Nach der Antwort durch den Server ist diese Verbindung beendet. Typischerweise finden gleichzeitig mehrere HTTP-Verbindungen statt.



Die Kommunikation zwischen Client und Server findet auf Basis von Meldungen im Text-Format statt. Die Meldungen werden standardmäßig über TCP auf dem Port 80 (Richtung Server) abgewickelt. Die Meldungen werden Request und Response genannt und bestehen aus einem Header und den Daten. Der Header enthält Steuerinformationen. Die Daten entsprechen einer Datei, die der Server an den Client schickt oder im umgekehrten Fall Nutzereingaben, die der Client zur Verarbeitung an den Server übermittelt. Dateien kann der Server aber nur mit Hilfe eines zusätzlichen Programms oder Skriptes entgegennehmen.

HTTP-Adressierung

Damit der Server weiß, was er dem HTTP-Client schicken soll, adressiert der HTTP-Client eine Datei, die sich auf dem HTTP-Server befinden muss. Dazu wird vom HTTP-Client ein URL (Uniform Resource Locator) im HTTP-Header an den HTTP-Server übermittelt:

http://Servername.Domainname.Top-Level-Domain:TCP-Port/Pfad/Datei
z. B. http://www.elektronik-kompendium.de:80/sites/kom/0902231.htm

Der URL besteht aus der Angabe des Transport-Protokolls "http://". Dann folgt der Servername (optional) und der Domainname mit anschließender Top-Level-Domain (TLD). Die Angabe zum TCP-Port ist optional und nur erforderlich, wenn die Verbindung über einen anderen Port, als dem Standard-Port 80 abgewickelt wird. Pfade und Dateien sind durch den Slash "/" voneinander und von der Server-Adresse getrennt. Folgt keine weitere Pfad- oder Datei-Angabe schickt der Server die Default-Datei der Domain. Sind Pfad und/oder Datei angegeben, schickt der HTTP-Server diese Datei zurück. Ist diese Datei nicht existent, versucht er es mit einer Alternative. Gibt es keine, wird die Standard-Fehlerseite (Error 404) an den HTTP-Client übermittelt.

HTTP-Request

Der HTTP-Request ist die Anfrage des HTTP-Clients an den HTTP-Server. Ein HTTP-Request besteht aus den Angaben Methode, URL und dem Request-Header. Die häufigste Methoden sind GET und POST. Dahinter folgt durch ein Leerzeichen getrennt der URL und die verwendete HTTP-Version. In weiteren Zeilen folgt der Header und bei der Methode POST durch eine Leerzeile (!) getrennt die Formular-Daten.

HTTP-Methoden

Jeder HTTP-Request durch den Client wird durch die Angabe einer Methode eingeleitet. Die Methode weißt den Server an, was er mit dem Request machen soll. Die HTTP Version 1.1 sieht die folgenden Methoden vor:

GET
POST
HEAD
PUT
OPTIONS
DELETE
TRACE
CONNECT

HTTP-Response

Der HTTP-Response ist die Antwort des HTTP-Servers an den HTTP-Client. Der HTTP-Response besteht aus der verwendeten HTTP-Version, dem Status-Code der Responses und der Klartext-Meldung des Status-Codes. In den anschließenden Zeilen folgt der Header und durch eine Leerzeile (!) getrennt die HTML-Datei.

HTTP-Response-Codes / HTTP-Status-Codes

Die Antwort des HTTP-Servers an den HTTP-Client enthält in der ersten Zeile den Status-Code und die Klartext-Meldung des HTTP-Responses, verursacht durch den HTTP-Request. Der Status-Code ist eine 3stellige Nummer, die dem HTTP-Client Informationen über die Verfügbarkeit der

angeforderten Daten mitteilt. Z. B. wird über den Status-Code eine Fehlermeldung übermittelt.
Die Status-Codes sind in 5 Gruppen unterteilt, die über den HTTP-Response eine Grundaussage treffen.

Erläuterung der häufig auftretenden Status-Codes

Status-Code	Beschreibung
200	Dieser Status-Code wird bei jeder erfolgreich bearbeiteten Anfrage übermittelt.
401	Zugriffe auf passwortgeschützte Bereiche eines Servers werden dem Client mit diesem Code verwehrt. Nur wenn der Client sich nach diesem Code autorisiert, bekommt er Zugriff auf die Dateien und Verzeichnisse. (Siehe unter HTTP-Authentifizierung)
404	Immer dann, wenn keine HTML-Datei zurückgeliefert werden kann, dann erfolgt die Rückmeldung eines 404-Errors. Meistens liefert der Server eine Standard-Fehlerseite zurück.
500	Ein HTTP-Server kann nicht nur HTML-Dateien schicken, sondern auch Programme und Skripte ausführen, die HTML-Daten zurückliefern. Kommt es bei der Ausführung zu einem Fehler, bricht der Server den Vorgang ab und liefert diese Fehlermeldung zurück.

HTTP Version 2.0

Für HTTP 2.0 gibt es einen IETF-Entwurf, der auf dem von Google entwickelten Protokoll SPDY (Speedy) beruht. Beim zukünftigen HTTP geht es hauptsächlich darum, die HTTP-Datenübertragung zu beschleunigen.

Die wesentlichen Bestandteile von HTTP sollen dabei weiter verwendet werden. Es ändert sich lediglich die Art und Weise, wie die Daten zwischen einem Client und Server ausgetauscht werden.

- unbegrenzt viele HTTP-Requests über eine einzige TCP-Verbindung
- einzelne HTTP-Requests priorisieren, um bei knapper Bandbreite wichtige Daten zuerst zu laden
- Header komprimiert übertragen
- Daten vom Server zum Client ohne Request vom Client zu pushen

SPDY reduziert die übertragene Datenmenge im Header und verschlüsselt alle Verbindungen. Zudem transportiert SPDY mehrere Datenströme über eine TCP-Verbindung, priorisiert diese und somit das Laden einzelner Elemente einer Webseite und kann Daten vom Server zum Client pushen.

Der vorliegende HTTP-2.0-Vorschlag hat einige dieser Merkmale abgewandelt. So ist die Verschlüsselung optional und für die Kompression der Paket-Header kommt HPACK zum Einsatz.

WebDAV - Web-based Distributed Authoring and Versioning

WebDAV bedeutet Web-based Distributed Authoring and Versioning und ist eine Erweiterung von HTTP/1.1. Während das World Wide Web (WWW) mit dem Protokoll HTTP nur für den Informationsabruf auslegt ist, wandelt sich das Web mit WebDAV zu einem beschreibbaren Speichermedium. WebDAV eignet sich für das Hochladen und Herunterladen von Dateien. Denkbare Anwendungen sind virtuelle Festplatten auf Webservern im Internet.

WebDAV hebt die Einschränkungen von HTTP auf und erweitert es um Dateiverwaltungsfunktionen. WebDAV ist in der Lage Dateien entgegenzunehmen und auf einen Datenträger abzulegen. Diese Disziplin war lange Zeit dem FTP-Protokoll überlassen. Z. B. um Webseiten zu aktualisieren und zu verwalten. WebDAV-Zugänge lassen sich nahtlos in jedes Betriebssystem integrieren. Der Zugriff darauf ist so einfach, wie das Arbeiten mit Dateien auf dem lokalen System.
WebDAV ist darauf ausgelegt, Webseiten im Team zu entwickeln. Es stellt Funktionen für die Namens- und Versionsverwaltung zur Verfügung.

FTP - File Transfer Protocol

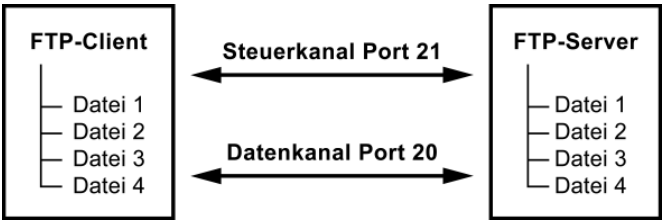
FTP ist ein Kommunikationsprotokoll, um Dateien zwischen unterschiedlichen Computersystemen zu übertragen. Die Übertragung findet nach dem Client-Server-Prinzip statt. Ein FTP-Server stellt dem FTP-Client Dateien zur Verfügung. Der FTP-Client kann Dateien auf dem FTP-Server ablegen, löschen oder herunterladen. Mit einem komfortablen FTP-Client arbeitet man ähnlich, wie mit einem Dateimanager.

FTP gibt es seit 1971 und ist damit das älteste und solideste Protokoll des Internets. Seit 1985 hat sich praktisch nichts mehr an den Übertragungsmechanismen geändert.

Das File Transfer Protocol (FTP) im Schichtenmodell

<table>
<tr><td>Schicht</td><td colspan="4">Dienste / Protokolle / Anwendungen</td></tr>
<tr><td>Anwendung</td><td>FTP</td><td>HTTP</td><td>DNS</td><td>SNMP</td></tr>
<tr><td>Transport</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td>Internet</td><td colspan="4">IP (IPv4 / IPv6)</td></tr>
<tr><td>Netzzugang</td><td colspan="4">Ethernet, ...</td></tr>
</table>

Wie funktioniert FTP?

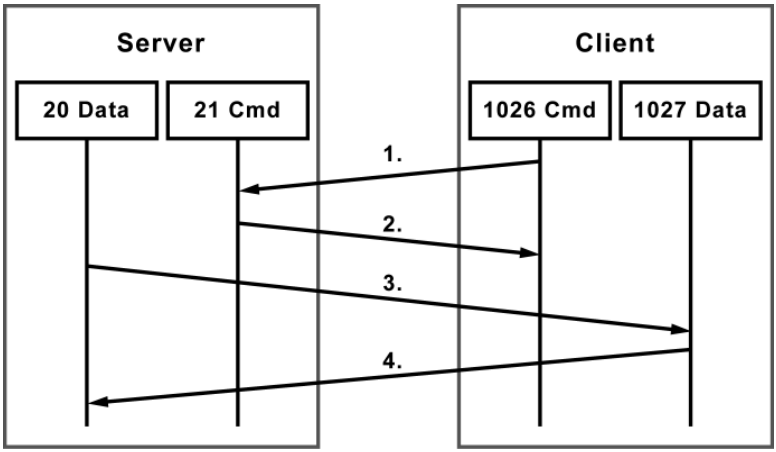


Die Kommunikation findet nach dem Client-Server-Prinzip statt. Wobei FTP zwischen Client und Server zwei logische Verbindungen herstellt. Eine Verbindung ist der Steuerkanal (command channel) über den TCP-Port 21. Dieser Kanal dient ausschließlich zur Übertragung von FTP-Kommandos und deren Antworten. Die zweite Verbindung ist der

Datenkanal (data channel) über den TCP-Port 20. Dieser Kanal dient ausschließlich zur Übertragung von Daten. Über den Steuerkanal tauschen Client und Server Kommandos aus, die eine Datenübertragung über den Datenkanal einleiten und beenden.

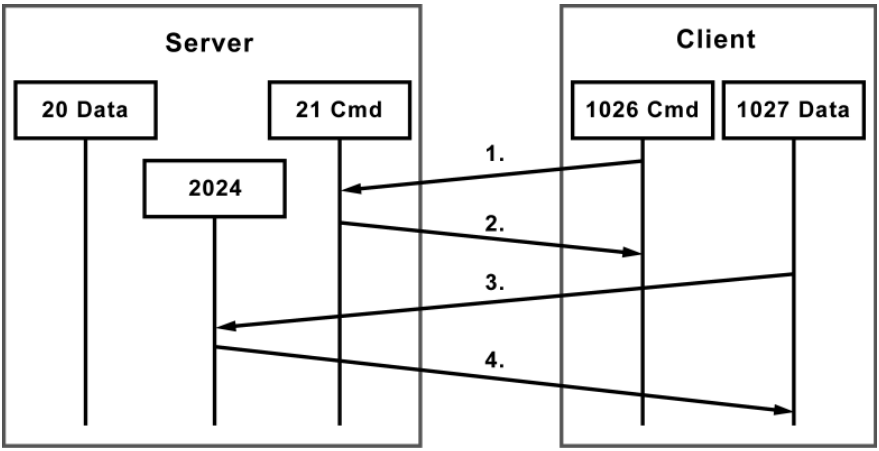
Der FTP-Verbindungsaufbau sieht vor, dass der Steuerkanal vom FTP-Client zum FTP-Server aufgebaut wird. Steht der Steuerkanal wird der Datenkanal vom FTP-Server zum FTP-Client initiiert (aktives FTP). Befindet sich der FTP-Client hinter einem NAT-Router oder einer Firewall und verfügt parallel dazu nur über eine private IPv4-Adresse, dann kommt die Verbindung nicht zustande. Die Verbindungsanforderung vom Server an den Client wird von der Firewall bzw. dem Router abgeblockt, bzw. kann wegen der privaten IPv4-Adresse gar nicht geroutet werden. Für diesen Fall gibt es das passive FTP, bei dem auch der Client den Datenkanal initiiert.

FTP Active Mode / Aktives FTP



Der FTP-Client kontaktiert den FTP-Server auf dem Port 21 (Command) und übermittelt die Port-Nummer, mit der der Server die Datenverbindung (Data) herstellen kann. Im Anschluss nimmt der FTP-Server auf diesem Port Kontakt mit dem FTP-Client auf. Die FTP-Verbindung ist hergestellt.

FTP Passive Mode / Passives FTP



Wenn ein FTP-Client hinter einem NAT-Router (mit privater IPv4-Adresse) oder hinter einer Firewall sitzt, kommt die vom FTP-Server initiierte Datenverbindung (Data) nicht zustande. Die Firewall verhindert alle aktiven Verbindungen, die von außerhalb initiiert werden. Aus diesem Grund wurde der Passive Mode eingeführt. Damit können auch FTP-Clients, die hinter einer Firewall sitzen FTP-Verbindungen herstellen. Nach dem die Verbindung auf Port 21 des Servers aufgebaut ist, bekommt der FTP-Client eine Portnummer vom Server, auf der die Datenverbindung aufgebaut werden kann. Der FTP-Client kontaktiert den Server dann auf diesem Port. Weil der Client die Verbindung initiiert, verhindert die Firewall diese Verbindung nicht mehr. Im Passive Mode wird dann der Port 20 des FTP-Servers nicht gebraucht.

NTP - Network Time Protocol

In Netzwerken und in Computern mit zeitkritischen Aufgaben ist eine genaue Zeit unerlässlich. Schon deshalb wurden sehr früh Mechanismen entwickelt, wie vernetzte Computer die Zeit untereinander austauschen können. NTP ist ein hierarchisches Protokoll über das Zeit-Server untereinander eine gemeinsame Zeit ermitteln können. Als Port wird 123 verwendet.
Auf Port 13 kann ein Server mittels "daytime" seine Zeit als ASCII-Klartext zur Verfügung stellen. Eine andere Möglichkeit ist der Port 37

über "time". Dieser liefert die verstrichenen Sekunden seit 1.1.1900 0 Uhr als 32-Bit-Binärwert zurück. Dieser Wert ist allerdings nur sekundengenau.
Diese beiden simplen Verfahren haben jedoch noch einen weiteren großen Nachteil. Sie berücksichtigen nicht die Datenpaketlaufzeit zum Ziel. Bis die Angabe der Zeit beim Empfänger "eintrifft" ist sie veraltet. Außerhalb von LANs sind diese Verfahren deshalb ungeeignet.
Die Mängel von "time" und "daytime" führten zur Entwicklung von NTP, das Paketlaufzeiten im Netz misst und ausgleicht. Der NTP-Dienst arbeitet parallel zur System-Uhr als eigenständige Uhr.

Verzeichnisdienste (X.500)

Ein Verzeichnisdienst ist ein Dienst zum Verwalten und Bereitstellen von Informationen über technische Ressourcen, Organisationseinheiten und Personen. Der Standard X.500 beschreibt, wie Verzeichnisdaten zur Verfügung gestellt und abgerufen, und wie die Authentifizierung der Zugriffe, die Replikation und Verwaltung der Verzeichnisdaten gehandhabt werden.

Je größer ein Netzwerk ist, umso wichtiger ist eine effiziente Verwaltung und Kontrolle aller darin enthaltenen Ressourcen (Server, Speicherplatz, Laufwerke, Drucker, Benutzer, etc.). Hierfür bietet sich die Nutzung eines Verzeichnisdienstes an.
Im Rahmen der X-Serie der ITU (International Telecommunication Union) wurde 1988 eine Empfehlung für Verzeichnisdienste unter der Bezeichnung X.500 veröffentlicht und als Standard von der ISO (International Standards Organization) aufgenommen.

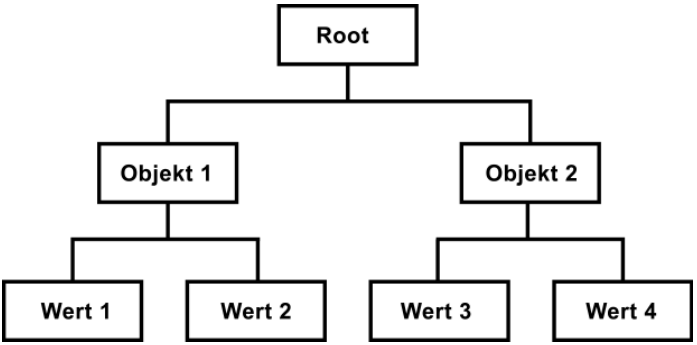
Beispiele für Verzeichnisdienste:

- LDAP - Lightweight Directory Access Protocol
- Microsoft Active Directory
- DNS - Domain Name System

Verzeichnis nach ISO 9594-1

Ganz allgemein ist ein Verzeichnis eine Sammlung von Informationen, die als Objekte in einer bestimmten Reihenfolge und Ordnung abgelegt

sind. Die Benutzeroberfläche (Interface), mit der der Zugriff auf die Informationen erfolgt (Suchen, Ändern, Hinzufügen, Löschen), nennt man Verzeichnisdienst.



Ein Verzeichnis nach ISO 9594-1 ist baumartig strukturiert. Dort sind die Daten statisch abgelegt. Jeder Eintrag kann beliebig viele Werte oder Attribute haben. Und jede Ebene kann beliebig viele Einträge haben. Das Verzeichnis selber ist eine spezielle Datenbank, in der die Benutzer, Anwendungen und Ressourcen und deren Eigenschaften und Standort gespeichert sind. Ein Benutzerverzeichnis enthält z. B. Anschrift, Telefonnummer und E-Mail-Adresse. Ein Druckerverzeichnis enthält z. B. Informationen über Standort, Druckerart, druckbare Seiten pro Minute und Qualität.

Verzeichnis nach X.500

Ein Verzeichnis nach X.500 ist ein verteiltes Verzeichnis auf das global zugegriffen werden kann. Die baumartige Struktur hat ein Wurzelobjekt mit dem Namen Root. Die Baumstruktur orientiert sich an den Regeln der objektorientierten Programmierung. Es gibt Objekte, Klassen, Vererbung und Polymorphie. Es geht darum, die einzelnen Teile einer Struktur in Objekten abzubilden und miteinander in Beziehung zu setzen. Die Objekte werden im Baum als Verzeichniseintrag bezeichnet.

Die Gesamtheit der Daten im Verzeichnis bezeichnet man als Directory Information Base (DIB). Mehrere Daten in einem Verzeichnis sind ein Verzeichnis-Baum, der als Directory Information Tree (DIT) bezeichnet wird.

Jeder Eintrag im Verzeichnisbaum gehört einer Objekt-Klasse an, in der Attribute definiert sind. Alias-Einträge (Verknüpfungen) ermöglichen einen Eintrag an mehreren Stellen im Verzeichnisbaum. Trotzdem muss dieser Eintrag nur an einer Stelle gepflegt werden.

Objekte (X.500)

Ein einzelnes Objekt wird über einen eindeutigen Namen, den Distinguished Name (dn), im Directory Information Tree (DIT) angelegt. Vergleichbar mit dem Namen einer Datei in einem Dateisystem.

Man unterscheidet zwischen zwei Objektarten. Die eine ist die Organisational Unit (OU), bei der es sich um ein Containerobjekt handelt. Container werden zum Aufbau der Struktur verwendet. Man kann darin weitere Objekte anlegen.
Und dann gibt es noch die Blattobjekte, die zum Beispiel mit Kennzeichnungcommonname (cn) und User-ID (uid) im DIT eingetragen sind. Ein solches Objekt dient zur Verwaltung einer Ressource.

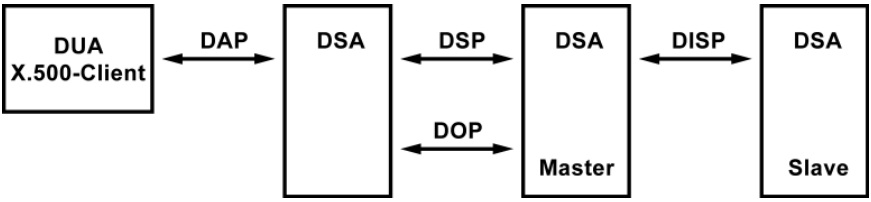
Attribute, Objektklassen und Schema (X.500)

Alle Objekte haben Eigenschaften, die Attribute genannt werden. Die Attribute unterscheiden sich je nach dem, um welche Art von Objekt es sich handelt. Ein Attribut hat einen Namen, mit dem das Attribut innerhalb eines Objekts eindeutig referenziert werden kann.
Weil unterschiedliche Objekte gleiche Arten von Attributen haben können, werden Attribute zu Objektklassen zusammengefasst. Objektklassen werden wiederum in Gruppen zu einem Schema zusammengefasst.

Aufgaben eines Verzeichnisdienstes (Auszug)

- Die Verzeichnis-Struktur auf mehreren Servern verteilen.
- Verwaltung in objektorientierten Datenmodellen.
- Vererbung von Eigenschaften auf andere Objekte.
- Verwaltung von Benutzern und Gruppen.
- Verwaltung von Weiterleitungen/Aliasen.
- Authentifizierung von Benutzern für die Anmeldung.

Zugriff auf ein Verzeichnis (X.500-Architektur)



Die X.500-Architektur folgt dem Prinzip der Client-Server-Architektur. Es gibt also eine X.500-Client-Komponente, die als Directory User Agent (DUA) bezeichnet wird. Damit erfolgt der Zugriff auf das Verzeichnis. Dafür stehen einige Operationen zur Verfügung. Z. B. lesen, vergleichen, suchen, hinzufügen, löschen und ändern.

Die Datenhaltung erfolgt auf einem oder mehreren Directory System Agents (DSA). Das entspricht einer X.500-Server-Komponente. Eine dezentrale Datenhaltung kann auf mehreren Servern realisiert werden. Diese kommunizieren miteinander, um Anfragen für einen anderen Datenbestand weiterzuleiten. Die einzelnen Server werden ebenfalls als Directory System Agents (DSA) bezeichnet.
Dazu wird ein Master-Server eingerichtet, auf dem der Datenbestand erstellt, gepflegt und bearbeitet werden kann. Auf einem oder mehreren Servern wird in regelmäßigen Abständen eine Kopie des Datenbestands gespeichert. Diesen Vorgang nennt man Replikation (Spiegelung). Dadurch erhöht sich auch die Ausfallsicherheit des Verzeichnisses.

Übersicht: X.500-konforme Verzeichnisdienste

Nahezu alle verfügbaren Verzeichnisdienste basieren auf X.500.

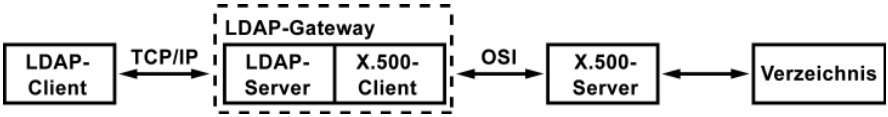
- Microsoft Active Directory
- LDAP - Lightweight Directory Access Protocol
- Novell eDirectory
- Siemens DirX

DNS ist zwar kein X.500-konformer Verzeichnisdienst, aber als solcher zu verstehen.

LDAP - Lightweight Directory Access Protocol

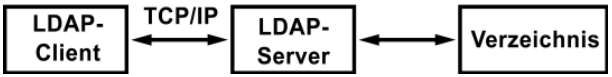
LDAP ist ein Protokoll, das für die Kommunikation zwischen einem Client und einem X.500-Verzeichnisdienst gedacht ist. X.500 ist ein Standard für DAP-Datenbanken bzw. Verzeichnisdienste. Leider gestaltet sich die Implementierung über verschiedene Systeme hinweg als sehr aufwendig. Deshalb wurde LDAP im Jahre 1993 entwickelt, um den Zugriff auf DAP-Datenbanken bzw. X.500-Verzeichnisdienste über TCP/IP zu erleichtern.
Ursprünglich war es nur ein Protokoll, das als Proxy für den Zugriff auf eine DAP-Datenbank diente, um zwischen X.500 und den verschiedenen Systemen zu vermitteln. Erst später wurde aus LDAP ein eigenständiger Verzeichnisdienst. LDAP bekam ein eigenes Datenbank-Backend, um unabhängig von einem DAP-Server zu arbeiten. Somit kann man mit einem LDAP-Server einen Verzeichnisdienst betreiben.

Wie funktioniert LDAP?



Der LDAP-Client greift über TCP/IP auf den LDAP-Server zu. Der LDAP-Server ist Teil eines LDAP-Gateways, in dem sich ein X.500-Client befindet, der über den OSI-Protokoll-Stack auf den X.500-Server zugreift.

Stand-alone-LDAP-Server



Anstatt eines LDAP-Gateways und der Umweg über einen X.500-Server kann der LDAP-Server auch direkt auf das Verzeichnis zugreifen. Man bezeichnet diese Konstellation auch als Stand-alone-LDAP-Server.
Für den LDAP-Client spielt es keine Rolle, ob der LDAP-Server direkt auf das Verzeichnis zugreift oder als LDAP-Gateway fungiert.
Greift der LDAP-Server direkt auf das Verzeichnis zu, kann man von

einem LDAP-Verzeichnisdienst sprechen. Die Architektur ist ein Client-Server-Modell das im Vergleich zu X.500 einfacher zu realisieren ist. Bei einem LDAP-Verzeichnisdienst stehen die X.500-Funktionen nicht mehr zur Verfügung. Es gilt nur ein eingeschränkter Funktionsumfang.

VoIP - Voice over IP

Voice over IP, kurz VoIP, ist die Übertragung und Vermittlung von Sprach-Kommunikation in einem IP-Netzwerk. Dieses Netzwerk kann sowohl lokal (LAN), ein Weitverkehrsnetzwerk (WAN) oder das ganze Internet sein. Voice over IP liegt in jedem Fall dem paketorientierten Internet-Protokoll (IP) zu Grunde.
Der Einsatz von Voice over IP ist darin begründet, dass es wesentlich Ressourcen-schonender mit dem zur Verfügung stehenden Übertragungsmedium umgeht. Insbesondere dann, wenn es sich um eine Breitbandverbindung handelt. So lassen sich über eine IP-gesteuerte Breitband-Verbindung mehr Sprachverbindungen realisieren als bei der klassischen Nutzung einer Telefonleitung.

Bestandteile von Voice over IP

Weltweit sind die Telefonnetze auf Zuverlässigkeit und höchste Verfügbarkeit optimiert. Die Technik ist ausgereift und stabil. Während die Festnetz-Telefonie aus möglichst wenigen Komponenten besteht, sind bei VoIP über das Internet sehr viele Komponenten im Spiel. Viele Faktoren spielen beim Verbindungsaufbau und auch danach eine große Rolle.

VoIP-Anwendungen	Call-Manager, Softphone, ...
VoIP-Protokolle	SIP, H.323, RTP, UDP, ...
unterstützende Dienste	DNS, NAT, QoS, AAA, ...
Betriebssysteme	Linux, Unix, Windows, ...
Hardware	Modem, Router, Server, IP-Telefon, Smartphone, ...
Netze	LAN, WAN, DSL, TV-Kabel, ...

Sprachqualität bei Voice over IP

Die Sprachqualität ist von der Verbindung und vom Codec abhängig, mit dem die Sprache digitalisiert wird. Wird der Codec G.711 verwendet, dann hat man Festnetz-Sprachqualität. Voraussetzung ist eine stabile Verbindung ohne Laufzeitschwankungen (Jitter) und Paketverluste. Bei der Festnetz-Telefonie wird vom Vermittlungssystem eine leitungsvermittelte Verbindungsqualität garantiert. Im Internet durchlaufen die Sprachdaten unterschiedliche Netze und Stationen. Wie schnell die Pakete weitergeleitet werden liegt in der Hand deren Betreiber. Nur mit einer durchgängigen Qualitätssicherung der Verbindung (Quality-of-Service, QoS) ist ein störungsfreies Telefongespräch über das Internet möglich.
Zur Zeit profitiert man im deutschen Internet von der großzügig vorhandenen Übertragungskapazität der Provider. Die Sprachpakete gelangen so ohne große Verzögerung durch das Internet. Die Sprachqualität ist mit der von Mobilfunkgesprächen vergleichbar. Hin und wieder hört man Knackser. Schwerer wiegt das Echo, das beide Teilnehmer zu hören bekommen können. In der Regel haben das die Anbieter im Griff. Ein leichte Zeitverzögerung der Übertragung lässt sich oftmals nicht vermeiden.

Protokolle und Standards

<table>
<tr><td>Call Control</td><td>Audio</td><td>Video</td></tr>
<tr><td rowspan="2">SIP
H.323

TCP</td><td>G.711
G.723
G.729</td><td>H.261
H.263</td></tr>
<tr><td colspan="2">RTP
RTCP

UDP</td></tr>
<tr><td colspan="3">IP</td></tr>
<tr><td colspan="3">LAN</td></tr>
</table>

Einheitliche Standards bei der Sprachübertragung über IP sind dünn gesät. Setzt man auf die Produkte eines einzigen Herstellers, so hat man keine Probleme. Versucht man jedoch die Produkte unterschiedlicher Hersteller zur Zusammenarbeit zu bewegen, muss man unter Umständen mit Einschränkungen leben.

Voice over IP im OSI-Schichtenmodell

Schicht		Protokoll
7.	Anwendung	VoIP-Anwendung Softphone / Call-Manager
6.	Präsentation	Sprachcodecs G.729 / G.723 / G.711
5.	Session	Signalisierung H.323 / SIP
4.	Transport	Transport-Protokolle RTP / UDP / RSVP
3.	Netzwerk	Netzwerk-Protokoll IP
2.	Verbindung	ATM / Ethernet
1.	Physikalische Ebene	DSL / Ethernet

Transport-Protokolle

Bei Voice over IP muss man zwischen den Datenpaketen zum Verbindungsauf- und -abbau (Signalisierung, Call Control) und den eigentlichen Sprachpaketen (Datenstrom) unterscheiden. Die Signalisierungsdaten müssen dabei möglichst sicher übertragen werden. Sie steuern die Verbindung. Sie dürfen länger unterwegs sein und einen größeren Protokoll-Overhead haben. Hauptsache die Verbindung kommt zu Stande. Dagegen müssen die Sprachpakete schneller und verzögerungsfrei unterwegs sein. Dabei kann man sich eine unsichere Übertragung leisten. Wenn mal ein Datenpaket verloren geht, dann ist das nicht so schlimm.

In der Praxis sieht das so aus, dass die Sprachpakete zuerst in RTP-Pakete und dann in UDP-Pakete verpackt werden und zur Adressierung zusätzlich mit einem IP-Header versehen werden. Die Übertragungstechnik auf dem physikalischen Medium fügt dann noch einen Paketrahmen hinzu, der vom jeweiligen Medium und Übertragungssystem abhängig ist. Dabei entsteht ein Overhead von 54 Byte pro Paket. Durch Kompression kann der Protokoll-Kopf von 40 Byte auf nur zwei bis drei Byte komprimiert werden.

Sprach-Codec / Audio-Codec

Bevor die Sprache übertragen werden kann, muss sie zuerst digitalisiert werden. In der Regel werden die Sprachdaten auch gleich komprimiert. Bei zunehmender Komprimierung nimmt die Sprachqualität ab. Die Dekomprimierungszeit und die Rechenleistung nehmen zu.

Abhängigkeit der Sprachqualität von Laufzeit, Jitter und Paketverlusten

Voice over IP ist nur dann in einem Netzwerk nutzbar, wenn die wichtigen Kennwerte, wie Bandbreite, Laufzeit und Jitter bei einem voll ausgelasteten Netzwerk einschließlich der Netzübergänge ausreichend sind. Dadurch wird im wesentlichen die Sprachqualität beeinflusst.
Die Hauptprobleme entstehen durch eine zu geringe Bandbreite und zu lange Distanzen. Paketverluste, hoher Jitter und große Verzögerungen reduzieren die Sprachqualität.

Delay - Verzögerung - Laufzeit

Die Laufzeit der Sprachpakete ist ein wichtiges Kriterium für die Sprachqualität. Dabei interessiert man sich für die Gesamtverzögerung zwischen dem Sprechen des Senders und dem Hören des Empfängers (Ende-zu-Ende-Verzögerung).
Laufzeitverzögerungen, auch Delay genannt, entstehen bei der Umwandlung der Datenformate und durch das Routing. Gerade beim Transport entstehen die größten Verzögerungen. Besonders in den Zwischenstationen (Switch, Router, Gateway, Firewall und Proxy) treten Verzögerungen auf. Dort werden die Pakete verarbeitet, was Zeit in Anspruch nimmt und zu Verzögerungen führt. Besonders das Routing ist

kritisch. Insbesondere dann, wenn ein Medienwechsel stattfindet. Eine Verzögerung entsteht auch bei der Digitalisierung und Komprimierung des Sprachsignals. Die Verzögerung ist dabei abhängig vom Codec und der zur Verfügung stehenden Rechenleistung. Der Codec hat nur einen geringen Anteil an der Gesamtverzögerung. Deshalb bringt es meistens sehr wenig am Codec selber zu optimieren.

Ursache	Laufzeit
AD-Wandlung	20 ms
Paketerstellung	30 ms
sonstige Servicezeiten	10 ms
Routing über 800 Kilometer	50 ms
Jitter Buffering	30 ms
D-A-Wandlung	20 ms
Laufzeit gesamt	160 ms

Die Gesamtverzögerung von Teilnehmer zu Teilnehmer sollte 150 ms nicht überschreiten. Eine Verzögerung unter 150 ms ergibt eine sehr gute Sprachqualität. Ab einem Delay von 250 ms wird ein Gespräch bereits negativ beeinflusst. Mit bis zu 400 ms gilt ein Gespräch noch als akzeptabel. Eine Verzögerung ab 400 ms ist als deutliche Gesprächspause hörbar. Man hört den anderen Teilnehmer noch, obwohl er schon zu Ende gesprochen hat. Das führt dazu, dass man dem Gesprächspartner zu oft ins Wort fällt. Dieses Problem kennt man bei Mobilfunkgesprächen, wenn der Empfang einseitig schlecht ist. Dann kommt es zu unangenehmen Verzögerungen und Unterbrechungen.

Jitter

Bei der Übertragung von Datenpaketen gibt es gewisse Verzögerungen bei der Laufzeit. Diese Verzögerungen können unterschiedlich ausfallen. Diese Unterschiede werden als Laufzeitschwankungen oder Jitter bezeichnet. Sie führen zu einer schlechten Sprachqualität. Um das zu vermeiden, bedient man sich eines Jitter-Buffers. Der Jitter-Buffer

speichert eingehenden Datenverkahr zwischen, um so ungleichmäßigen, wiederholten oder fehlerhaften Datenfluss auszugleichen. Es geht nicht um 10 ms mehr oder weniger, sondern darum, dass diese 10 ms stets konstant erreicht werden und es keinen Jitter gibt.
Je toleranter das System gegenüber Jitter ist, desto mehr erhöht sich das Delay (Verzögerung) durch den Codec. Man kann nur versuchen den Jitter in den eigenen Routern zu minimieren. Doch sobald die Datenpakete das Netzwerk verlassen hat man keinen Einfluss mehr auf den Jitter.

Paketverluste - Packet Loss

Für die Übertragung von VoIP-Sprachdaten wird UDP verwendet, das die Zustellung der Pakete nicht sicherstellen kann. Bei Sprachdaten macht das auch wenig Sinn. Ein Sprachpaket enthält nur etwa 20 bis 30 ms an Sprache, was in etwa einer Silbe entspricht. Eine Silbe nachzuliefern macht wenig Sinn und ist auch nicht notwendig. Sofern das nicht zu häufig auftritt, kann man den Verlust verschmerzen. Unregelmäßige Paketverluste kann man durchaus tolerieren. Unser Gehirn ist in der Lage, fehlende oder fehlerhafte, aber in einem logischen Satzzusammenhang stehende Worte bzw. Wortsilben selbständig richtig zu ergänzen. Doch wenn Datenpakete allzu oft fehlen, dann macht sich das durch Aussetzer und Ausfälle bemerkbar. Das reduziert die Sprachqualität. Sobald also aufeinanderfolgende Pakete verloren gehen, führt das dazu, dass ganze Wörter oder Satzbestandteile fehlen.

Die Angabe "Packet Loss" gibt Auskunft über die prozentuale Menge verlorengegangener Datenpakete. Dieser Wert liegt in der Regel bei einem Prozent. Bis zu 5% Datenverlust muss ein Codec ausgleichen können, was beim Telefonieren ungehört bleibt.
Die häufigste Ursache für Paketverluste ist die Überlastung des Netzwerks. Datenpuffer sind ein beliebtes Mittel um Paketverluste zu vermeiden und kurzzeitige Bandbreitenschwankungen durch das zwischenspeichern von Datenpaketen auszugleichen. Prinzipiell sollte man es vermeiden Sprachdaten bei der Übertragung zu puffern. Dadurch werden sie nur unnötig verzögert.

Quality of Service (QoS)

Für ein Telefongespräch mit Voice over IP in guter Qualität muss eine bestimmte Bandbreite für die Dauer des Gesprächs gewährleistet sein. Man spricht vom sogenannten Fernsprechkanal. In diesem Fernsprechkanal wird die Sprache isochron (gleich lang andauernd) übertragen. Die engen Grenzen bei der Verzögerung und den Laufzeitschwankungen lassen sich mit dem reinen Internet-Protokoll (IP) nicht realisieren.
Da Sprachübertragung von der Übertragungstechnik, in diesem Fall die paketorientierten Protokolle, besondere Eigenschaften fordern, lassen sich Übertragungsfehler, Verzögerungen und Laufzeitunterschiede nur durch eine ausreichende Bandbreite oder Protokollzusätze vermeiden. Man fasst diese Maßnahmen unter Quality-of-Service (QoS) zusammen.

Sicherheit

Sicherheits-Features für VoIP sind äußerst unpopulär. Als Grund wird der vergleichsweise hohe Aufwand für das Abhören oder Stören, im Vergleich zu ISDN oder analog, angeführt. Einen analogen Anschluss kann man abhören, in dem man ein Telefon oder Kopfhörer parallel zur Leitung schaltet. Bei VoIP ist das wesentlich komplizierter, weil die Daten auf mehreren Protokollschichten verteilt sind. Einen Datenverkehr mitzuschneiden ist sehr aufwendig und nur mit hochwertiger Hardware und Software möglich. Vorausgesetzt natürlich, man hat einen Punkt im Netz, an dem man Abhören kann.
Das Grundproblem bei VoIP ist die bidirektionale Datenverbindung. Die Datenpakete werden in beide Richtungen über die Firewall geschickt. Dafür werden Ports geöffnet, die wiederum als Angriffspunkt für Hacker dienen können. Solange die IP-Telefonie im lokalen Netzwerk und hinter einer Firewall arbeitet, ist das Risiko eines Angriffs von außen gering. Ist der Telefonie-Server über das öffentliche Netz zu erreichen, dann kann dessen Funktion beispielsweise durch Denial-of-Service-Attacken (DoS) gestört werden.

Bei SIP könnte die Authentifizierung mit PGP erfolgen. Der Datenstrom könnte auch mit SRTP verschlüsselt werden.
Damit die Sicherheitsmaßnahmen auch greifen, müssen alle an der Übertragung beteiligten Komponenten über genügend

Sicherheitsvorkehrungen verfügen. Es bringt nicht sehr viel, wenn die Signalisierung, aber nicht der Datenstrom verschlüsselt ist.

SIP - Session Initiation Protocol

Das SIP wurde entwickelt, um Teilnehmer zu Mehrpunktkonferenzen zusammen zu schalten. Schnell erkannte man die Eignung für die Punkt-zu-Punkt-Telefonie (Voice over IP). Genauso wie H.323 eignet sich SIP für den Aufbau, Betrieb und Abbau von Sprach- und Video-Verbindungen. Sowohl Punkt-zu-Punkt- als auch Multicast-Verbindungen lassen damit steuern.
SIP wurde 1996 von einer Arbeitsgruppe der IETF (Internet Engineering Task Force) entwickelt, 1999 veröffentlicht und genormt. Obwohl H.323 zuerst da war, war das Interesse an SIP gleich von Anfang an sehr groß. Schon 1999 war es beliebter als H.323.

SIP hat einem starken Bezug zu anderen Internet-Protokollen. Die Kommunikation ist von den TK-üblichen Mechanismen entlastet und auf das wesentliche beschränkt. Aufgrund seiner Einfachheit ist SIP leichter zu verstehen und der Aufwand für die Implementierung geringer. Die Vermittlung der Datenpakete folgt der Logik von IP-Anwendungen. SIP ist stark am HTTP (Hypertext Transfer Protocol) angelehnt. Somit lässt sich die SIP-Telefonie in Browser-Umgebungen, Webservices, Anwendungen und Geräte leicht integrieren.

Die Einfachheit von SIP stellt aber ein großes Sicherheitsproblem dar. Vor allem, weil die Informationen im Klartext übertragen werden. So einfach und flexibel es aufgebaut ist, so leicht lässt es sich manipulieren. Deshalb empfiehlt es sich, die verschlüsselte Variante SIPS zu verwenden.

SIP-Protokolle

SIP ist ein textbasiertes Protokoll, mit dem Clients und Server ihre Verbindungen steuern. Durch SIP wird eine verbindungsorientierte Kommunikation in einem paketvermittelnden Netz realisiert. Es arbeitet auf der 5. Schicht des OSI-Schichtenmodells. Dadurch ist es unabhängig von den darrunterliegenden Transportschichten. SIP verwendet die Transport-Protokolle TCP und UDP für die Übertragung. SIP beschreibt

nur die Signalisierung. Alles Weitere wird über SDP (Session Description Protocol) ausgehandelt. Mit SDP werden Medienbeschreibung, Codec, Ports und Senderichtung ausgetauscht. Der anschließende Datenstrom wird über RTP oder UDP übertragen. Mit RTP werden die Medienströme in Echtzeit übertragen. Parallel zu RTP wird RTCP dazu benutzt, um wichtige Kontrollinformationen über den RTP-Medienstrom zwischen Client und Server auszutauschen.

<table>
<tr><td colspan="3">Teilnehmer</td></tr>
<tr><td colspan="3">G.711 / G.729 / G.723 / ...</td></tr>
<tr><td>SIP</td><td>SAP
SDP</td><td>RTP</td></tr>
<tr><td colspan="2">TCP</td><td>UDP</td></tr>
<tr><td colspan="3">IP</td></tr>
<tr><td colspan="3">Data Link</td></tr>
<tr><td colspan="3">Physical Link</td></tr>
</table>

Adressierung

SIP ist für die weltweite Lokalisierung von Benutzern im ganzen Internet ausgelegt. Die Teilnehmer werden mit URL und DNS adressiert.
Jeder SIP-Teilnehmer hat eine Adresse, die einer E-Mail-Adresse ähnelt (UserID@Domain). Der vordere Teil ist entweder ein Benutzername oder eine herkömmliche Telefonnummer. Der hintere Teil adressiert das SIP-Netzwerk.

SIP-Systemarchitektur

SIP basiert auf einer kombinierten Client-/Server-Architektur. In SIP sind User Agent, Proxy Server, Redirect Server und der Registrator definiert. Der User Agent (UAC) ist der Client, der die Anrufe initiiert. Der User Agent Server (UAS) ist der Server, der die Anrufe vermittelt.

QoS - Quality of Service

Standardmäßig werden in einem Netzwerk alle Datenpakete nach dem Best-Effort-Prinzip gleich behandelt. In einem Paket-orientierten Netzwerk können die einzelnen Datenpakete unterschiedlich schnell unterwegs sein. So lange hauptsächlich Nachrichten und Dateien übertragen werden, kommt es hierbei selten zu Übertragungsproblemen. Werden jedoch Echtzeitanwendungen, wie Voice over IP oder Videostreaming genutzt, dann wirken sich Verzögerungen oder Paketverluste auf die Übertragungseigenschaften zwischen den Teilnehmern negativ aus. Beispielsweise durch abgehackte Sprache oder fehlende Bild-Fragmente in einem Video. Im Vergleich dazu fällt es kaum auf, wenn eine E-Mail ein paar Sekunden später beim Empfänger eintrifft.

Eine geringe Bandbreite, schlechte Übertragungseigenschaften und unterschiedliche Auslastung führen zum Verwerfen oder verzögerten Ausliefern von Datenpaketen. In der Konsequenz kommt es zu Störungen bei der Sprach- und Videoübertragung. Die Sprache wirkt verzerrt. Kratzen und knacken verschlechtert die Sprachqualität. Videobilder werden pixelig oder ruckelnd wiedergegeben.

Dadurch, dass TCP/IP die Anwendungsebene von der Übertragungsebene trennt und unabhängig macht, findet zwischen diesen Ebenen keine Kommunikation statt. Die Übertragungssysteme sind nicht in der Lage zwischen einem Sprachpaket und einem normalen Datenpaket zu unterscheiden. Das OSI-Schichtenmodell sorgt dafür, dass die Protokolle auf den unterschiedlichen Schichten unabhängig voneinander arbeiten. Was im Prinzip sinnvoll ist, verursacht bei der Audio- und Video-Übertragung Probleme.
Viele QoS-Maßnahmen versuchen diesen Mangel auszumerzen und Datenpakete mit Diensteklassen zu kennzeichnen, die bestimmten Anwendungen zugeordnet sind. Auf diese Weise wird versucht, auf Anwendungsebene Dienstmerkmale festzulegen und über die Protokolle hinweg nach unten durchzureichen.

QoS beschreibt in der TCP/IP-Welt die Güte eines Kommunikationsdienstes aus Sicht des Anwenders. Dabei wird häufig die Netzwerk-Service-Qualität anhand der Parameter Bandbreite, Verzögerung, Paketverluste und Jitter definiert.

Die Netzbelastung beeinflusst dabei die Qualität der Übertragung. Zum Beispiel, wie lange es dauert, bis ein Datenpaket beim Empfänger ankommt. Deshalb versucht man Datenpakete mit entsprechenden Diensteklassen zu kennzeichnen. Priorisierte Datenpakete werden in Routern oder Switche bevorzugt weitergeleitet. Das macht aber nur Sinn, wenn alle Netzkomponenten und Teilnetze die gleichen Verkehrsklassen und Priorisierungsregeln unterstützen. Damit QoS funktionieren kann muss auf der ganzen Übertragungsstrecke zwischen den Teilnehmern die notwendigen QoS-Mechanismen implementiert werden. Das geht natürlich nur, wenn das Netz einer einzigen Organisationseinheit gehört, was im Internet nicht der Fall ist.

Hinweis: QoS stellt keine zusätzliche Bandbreite zur Verfügung. Aus 2 MBit/s werden nicht mehr. Man kann mit QoS nur dafür sorgen, dass über die 2 MBit/s bestimmte Daten bevorzugt/priorisiert übertragen werden.

Qualität der Übertragung

Es reicht nicht aus, QoS-Merkmale einzuführen. Wer QoS-Maßnahmen einleitet, der sollte die Messbarkeit berücksichtigen. QoS ist Tuning im Netzwerk. Vergleichbar mit PC- und Auto-Tuning.
Qualitätsverbesserungen im Netzwerk sollten immer vorher und nachher gemessen werden. Wenn etwas verbessert werden soll, muss vor dem Tun festgestellt werden, was und wie es verbessert werden kann. Dazu muss die Qualität mit geeigneten Mess- und Monitoring-Werkzeugen überprüft werden. Zum Beispiel muss die verfügbare Bandbreite für bestimmte Anwendungen kontinuierlich überwacht werden.
Kriterien für die Qualität der Übertragung sind zum Beispiel Paket-Verzögerungen, Rate der Paketverluste und Jitter. Je nach Anwendung sind weitere Qualitätsmerkmale zu untersuchen und zu messen.

Typische QoS-Maßnahmen

Ein gutes Quality of Service ist eine Vielzahl von aufeinander abgestimmten Maßnahmen.

- Überdimensionierung der Netze (viel mehr Bandbreite als erforderlich)
- Reservierung von Bandbreite für bestimmte Anwendungen

- Priorisierte Übertragung bestimmter Datenpakete
- Verbindungsorientiertes Protokoll unterhalb der IP-Schicht

Überdimensionierung und damit mehr Bandbreite

In der Vergangenheit war es üblich auf Quality of Service zu verzichten und einfach viel mehr Bandbreite zur Verfügung zu stellen, als praktisch notwendig war. Doch mehr Bandbreite bringt nur dort etwas, wo zu wenige Bandbreite vorhanden ist. Dabei muss man die Engpässe auf der ganzen Übertragungsstrecke berücksichtigen.
Wenn der Bandbreiten-Bedarf mit der Zeit ansteigt, muss dem Rechnung getragen und noch mehr Bandbreite zur Verfügung gestellt werden.

Reservierung von Bandbreite

Um ein hohes QoS zu erreichen, ist es üblich die verfügbare Bandbreite für bestimmte Anwendungen zu reservieren. Andere Anwendungen werden dabei zurückgestellt und müssen mit weniger Bandbreite auskommen.

Priorisierung von Datenpaketen

Das Priorisieren von Datenpaketen setzt die Definition von Verkehrsklassen voraus. Die Verkehrsklasse ist nach einer Dienstgüte definiert und einer Anwendung zugeordnet. Datenpakete einer höheren Verkehrsklasse werden dann bevorzugt übertragen.
Allerdings funktioniert die Priorisierung nur dort, wo die Verkehrsklassen gelten. Verlassen priorisierte Datenpakete ein Netz, dann gelten hier unter Umständen andere Verkehrsklassen.

Verbindungsorientierte Protokolle

- MPLS - Multi-Protocol Label Switching
- VLAN - Virtual Local Area Network
- ATM - Asynchronous Transfer Mode

Mit VLAN, ATM und MPLS werden den Verkehrsquellen bestimmte Verkehrseigenschaften zugeordnet. Die Einhaltung dieser Eigenschaften werden ständig überwacht.

Jitter Buffer

Insbesondere Sprach- und Videoübertragungen (Echtzeitanwendungen) leiden an Laufzeitunterschieden der Datenpakete. Um Laufzeitunterschiede zu vermeiden, werden Jitter-Buffer eingesetzt. Ein Jitter-Buffer kann diese Unregelmäßigkeiten bis zu einem gewissen Grad ausgleichen. Er nimmt alle Echtzeit-Datenpakete auf und gibt sie in einem gleichmäßigen Fluss wieder ab.
Jitter ist die Bezeichnung für die Abweichung des Abstandes, wie die Pakete beim Empfänger ankommen.

CoS - Classes of Service

Klasse	Anwendung
1	Sprache
2	Video
3	VPN
4	WWW
5	Mail
6	Sonstiges

Classes of Service definiert Klassen von Datenübertragungen, denen Datenpakete zugeordnet werden. Jede Klasse entspricht einer Priorität, anhand der entschieden wird, welche Datenpakete bevorzugt übertragen werden. Dabei muss man beachten, dass die Datenmenge in den hohen Verkehrsklassen begrenzt werden muss, sonst ist auf überlasteten Verbindungen für gering priorisierte Datenpakete keine Übertragung möglich.

Die Umsetzung von CoS scheitert in der Regel an den unterschiedlich vergebenen CoS-Regeln in den verschiedenen Netzen der Netzbetreiber. Jeder Netzbetreiber kocht hier sein eigenes Süppchen.

DiffServ - Differentiated Services

DiffServ ist ein Verfahren zur Priorisierung von Datenverkehr für Echtzeitanwendungen über IP. Jedes Datenpaket wird einer Verkehrsklasse zugewiesen. Datenpakete einer höheren Verkehrsklasse werden gegenüber einer niedrigeren Verkehrsklasse bevorzugt behandelt.

Traffic-Shaping

Bei aktiviertem Traffic-Shaping werden Quittierungspakete im Uplink bevorzugt übertragen, damit parallel laufende Downloads nicht beeinflusst werden, deren Geschwindigkeit von der Schnelligkeit der Quittierungen abhängig ist.

MPLS - Multiprotocol Label Switching

MPLS wird häufig im Zuge von Quality of Service genannt. Allerdings ist das nur bedingt richtig. Zwar kommt MPLS einem Quality of Service gleich, aber nur dann, wenn man Quality of Service bei der Einrichtung berücksichtigt.
In MPLS-Routern werden Labels definiert anhand denen Datenpakete an vordefinierten Ausgänge weitergereicht werden. Auf diese Weise wird der Weg entsprechend markierter Datenpakete durch ein Netz vorgegeben. Wenn man MPLS als QoS nutzen will, dann bietet sich die Möglichkeit an, die Labels nach Merkmalen, wie Availability, Packet Loss, Latency, etc. auszuwählen.

Fazit

Solange sich die Kommunikationspartner im gleichen Netz befinden, können über ein entsprechendes Agreement Leitungsqualität und -verfügbarkeit zugesichert werden. Wie der Provider das dann in seinem Netz in die Praxis umsetzt, kann dem Kunden egal sein. Doch sobald die Pakete über fremde Netze laufen, wird es schwer die Vereinbarung einzuhalten, weil es keine einheitlichen Standards und Abkommen für zugesicherte Leitungsqualitäten gibt.
Und trotzdem funktioniert VoIP auch ohne MPLS, RSVP oder DiffServ recht gut. Bei den meisten Netzbetreibern wird QoS ganz einfach durch eine überdimensionierte Bandbreite umgesetzt.

Netzwerk-Sicherheit

Grundlagen

Kryptografie

Firewall

VPN – Virtual Private Network

Authentifizierung im Netzwerk

Grundlagen der Netzwerk-Sicherheit

Die globale, wie auch lokale, weltweite Vernetzung hat zu einer großen Bedeutung für die Computer- und Netzwerksicherheit geführt. Wo früher vereinzelt kleine Netze ohne Verbindungen nach außen für sich alleine standen, ist heute jedes noch so kleine Netzwerk mit dem Internet verbunden. So ist es möglich, dass aus allen Teilen der Welt unbekannte Personen, ob mit guter oder böser Absicht, eine Verbindung zu jedem Netzwerk herstellen können.

Die paketorientierte Protokoll-Familie TCP/IP ist speziell dafür ausgelegt, dass eine Ende-zu-Ende-Verbindung für alle am Netzwerk hängenden Stationen möglich ist. Die dabei vorherrschende dezentrale Struktur des Internets erlaubt jedoch kaum eine Kontrolle über den Weg den Datenpakete nehmen. Diese an sich vorteilhafte Eigenschaft, z. B. bei Ausfällen oder Überlastungen von Übertragungsstrecken, macht sich bei der Übertragung von sicherheitsrelevanten Daten und Anwendungen negativ bemerkbar.
Grundsätzlich kann man sagen, dass alle persönlichen und kritischen Daten, die über das unsichere Internet übertragen werden, immer mit einem sicheren Übertragungsprotokoll geschützt sein sollten (Authentifizierung und Verschlüsselung).

In diesem Zusammenhang steigen auch die Anforderungen an Unternehmensnetzwerke. Auf sie sollen externe Mitarbeiter von außen auf das Netzwerk zugreifen. Außendienst-Mitarbeiter, Home-Offices, entfernte Filialen und WLANs sind bereits Alltag in Unternehmen. Die neue Mobilität verbessert die Produktivität, fordert dafür die Auseinandersetzung mit völlig neuen Sicherheitsfragen.
Dabei stellt sich die Frage, welche Geräte werden mit welcher Applikation wo innerhalb und außerhalb des Unternehmens und wie und wann eingesetzt? Ein zentrales Problem ist dabei, dass viele mobile Geräte ursprünglich für den Privatgebrauch und nicht für Unternehmenszwecke entwickelt wurden. Das heißt, dass viele Sicherheitsverfahren in der Praxis mangels Software-Unterstützung nicht auf allen Geräten umgesetzt werden können.

Die 3 Pfeiler der Netzwerk-Sicherheit

Die Netzwerk-Sicherheit umfasst meist folgende drei Pfeiler: Integrität, Vertraulichkeit und Authentizität.

Zur Integrität zählen Mechanismen und Verfahren, die die Echtheit von Daten prüfen und sicherstellen können und somit auch vor Manipulation schützen.
Bei der Vertraulichkeit einer Kommunikation geht es darum dafür zu sorgen, dass niemand Einblick in die Daten und Kommunikation erhält.
Bei der Authentizität der Kommunikationspartner geht es darum festzustellen, ob der Kommunikationspartner auch tatsächlich der ist, für den er sich ausgibt.

Vereinfacht kann man sagen, dass es bei der Netzwerk-Sicherheit immer um die Authentifizierung der Kommunikationspartner und die Verschlüsselung der Kommunikation geht.

Authentizität: Authentifizierung und Autorisierung

Im echten Leben weisen wir uns durch Unterschriften, Pässe und Karten aus. Im Internet fällt dies durch die räumliche Trennung weg. Auf Sicherheit zu achten bedeutet auch, niemals die Authentifizierung und Autorisierung zu vernachlässigen. Authentifizierung ist der Vorgang, bei dem eine Person oder Maschine auf ihre Identität geprüft wird. Autorisierung ist der Vorgang, bei dem ermittelt wird, was die Person oder Maschine machen darf (Berechtigung).

Vertraulichkeit: Verschlüsselung

Übertragungen von Informationen in Klartext, womöglich Benutzername und Passwort, sind immer ein Problem. Werden die Datenpakete auf ihrer Reise zum Empfänger von einem Angreifer gesammelt, kann er die Informationen lesen. Ganz so wie der Empfänger es auch tut. Sind die Datenpakete verschlüsselt hat es der Angreifer schwerer Rückschlüsse auf die Original-Informationen zu ziehen.
Neben dem reinen Abhören, also einfaches Duplizieren von Informationen, besteht die Möglichkeit Datenpakete abzufangen, ihre Weiterleitung zu verhindern oder manipulierte Datenpakete zu versenden.

Besondere Gefahren

Eine besondere Gefahr geht von virtuellen Gewaltakten aus. Den Brute-Force-Attacken (z. B. DoS), die durch Überfluten der Zielstation mit Anfragen und so am Erledigen der eigentlichen Aufgaben zu hindern. Ein Ausfall von Software und Hardware wird auf diese Weise provoziert. Viele Anwendungen sind für solche Ereignisse nicht ausgelegt und in der Regel nicht geschützt.

Maßnahmen für die Netzwerk-Sicherheit

Ein Netzwerk auf Basis von TCP/IP teilt sich grob gesehen in die Anwendungsschicht, die Netzwerkschicht und Übertragungsschicht. Auf allen Schichten lassen sich Maßnahmen zur Verbesserung der Sicherheit einsetzen.

Sicherheitsverfahren auf den niederen Schichten sind flexibler einsetzbar, aber unsicherer. Sicherheitsverfahren auf den höheren Schichten sind an die Anwendung gebunden, aber sicherer und schneller umsetzbar.

	Schicht	Beispiele
7	Application Layer Anwendungsschicht	HTTPS S-MIME SSL/TLS SSH OpenVPN
6		
5		
4	Network Layer Netzwerkschicht	IPsec (AH/ESP)
3		
2	Data Link Layer Übertragungsschicht	PPTP L2TP PAP/CHAP IEEE 802.1x
1		

Maßnahmen auf der Übertragungsschicht (Data Link Layer)

In der Übertragungsschicht kommen meist Tunneling-Protokolle zum Einsatz, die beliebige Netzwerk-Protokolle übertragen können. Auch für die Anwendung, die eine solche Verbindung nutzt, spielt das Protokoll auf der Übertragungsschicht keine Rolle. Die hohe Flexibilität wird mit einem großen Verarbeitungsaufwand wegen mehrfacher Header erkauft.

Maßnahmen auf der Netzwerkschicht (Network Layer)

Auf der Netzwerkschicht werden häufig Paketfilter (Firewall) und Masquerading (NAT) verwendet. Das eine Verfahren um den Datenverkehr einzuschränken oder zu verhindern und das andere um Stationen gezielt zu verstecken. Diese Sicherheitsverfahren sind eng mit der Netzwerkschicht verwoben und funktionieren in diesem Fall nur mit TCP/IP. Auf der Netzwerkschicht arbeitet man auch gerne mit einer Firewall.
Welche Protokolle oder Verfahren hier verwendet werden sind für die Anwendungsschicht und die Übertragungsschicht unerheblich.

Maßnahmen auf der Anwendungsschicht (Application Layer)

Sicherheitsmechanismen auf der Anwendungsschicht sind direkt mit dem Dienst, einer Anwendung oder einer Sitzung gekoppelt. Sie können also nicht einfach so anderweitig genutzt werden. Das ist jedoch kein Nachteil, sondern mit einer hohen Sicherheit verbunden. Sofern Anwendungen Sicherheitsprotokolle unterstützen, sind sie bei kurzzeitigen Verbindungen das sicherste Verfahren. Meist ist eine komplizierte Konfiguration der Anwendungen nicht erforderlich. Die Gegenstellen auf beiden Seiten einigen sich vollautomatisch ohne Eingriff des Anwenders.

Kryptografie / Kryptographie

Kryptologie ist die Kunst und Wissenschaft, Methoden zur Verheimlichung von Nachrichten zu entwickeln. Die Kryptografie oder Kryptographie ist ein Teil der Krytologie und die Wissenschaft zur Entwicklung von Kryptosystemen, die die Geheimhaltung von Nachrichten zum Ziel haben. Auch ein Teil der Kryptologie ist die Kryptoanalyse, bei der es sich um die Wissenschaft zum Brechen von

Kryptosystemen handelt.
Kryptografie ist gleichzeitig auch ein Teilgebiet der Informatik. Meist spricht man von Computersicherheit oder IT-Sicherheit. Ein wichtiges Hilfsmittel der Kryptografie ist die Mathematik.

Bei der Kryptografie und den daraus entwickelten Kryptosystemen geht es im wesentlichen darum Daten, Nachrichten und die Kommunikation zu verschlüsseln, um sie vor der Einsicht und Manipulation Dritter zu schützen.

Kryptografie und die Geheimdienste

Kryptografie war ursprünglich eine Domäne der Geheimdienste und des Militärs. Denn bei der Übermittlung von Befehlen in elektronischer Form muss sichergestellt sein, dass der Gegner die Nachricht nicht abfängt oder sogar manipulieren kann.
Da sich die elektronische und digitale Verarbeitung, Übertragung und Speicherung von Daten und Informationen in der Wirtschaft und im Privatleben durchgesetzt hat, fand auch hier die Verbreitung von kryptografischen Verfahren statt.
Bis heute ist es jedoch so, dass die fähigsten Menschen, die sich mit Kryptografie und Kryptoanalyse auskennen den Geheimdiensten angehören. Besonders heikel ist, dass Geheimdienste die Ausarbeitung von Verschlüsselungstechniken unterwandert und Fehler einbauen, die sich wie Hintertüren auswirken und für die Überwachung genutzt werden.

Ziele der Kryptografie

- Zusicherung der Vertraulichkeit: Die Daten oder die Nachricht unterliegen der Geheimhaltung und können nur von den Personen gelesen werden, die den Schlüssel zum Entschlüsseln besitzen.
- Zusicherung der Integrität: Erbringt den Nachweis, dass Daten oder eine Nachricht auf dem Weg vom Sender zum Empfänger nicht verändert wurde.
- Zusicherung der Authentizität: Damit man erkennen kann, dass die Daten oder die Nachricht auch tatsächlich von demjenigen kommt, für den er sich ausgibt.

- Zusicherung der Verbindlichkeit: Der Urheber von Daten oder Absender einer Nachricht muss eindeutig nachweisbar sein (Nichtabstreitbarkeit).

Kryptografische Verfahren und Systeme müssen nicht zwangsläufig alle genannten Ziele unterstützen. Oft ist es so, dass in einem bestimmten Anwendungsfall drei oder auch nur zwei Ziele erreicht werden müssen.

Geschichte der Kryptographie

Monoalphabetische und polyalphabetische Verfahren (bis etwa 1900)
Mechanische und maschinelle Verfahren (ab etwa 1900 bis 1970)
Kryptografische Verfahren (ab etwa 1970)

Die Geschichte der Kryptografie beginnt mit einfachen Verfahren aus der Antike, um Nachrichten in eine unlesbare Form zu bekommen. Nur der Empfänger kennt den Trick, der angewendet werden muss, um die Nachricht wieder in eine lesbar Form zu bekommen. Zum Beispiel indem jeder Buchstabe einem festen Symbol zugeordnet ist (monoalphabetische Verfahren). Ein erweitertes Verfahren davon ist, dass Buchstaben mehreren Symbolen entsprechen (polyalphabetische Verfahren). Hier ist es so, dass man mit ein wenig Erfahrung (Häufigkeitsbetrachtungen oder Statistik) und herumprobieren relativ schnell auf den geheimen Text schließen kann. Im zweiten Weltkrieg wurden erstmals spezielle mechanische Maschinen verwendet.

Mit der Einführung von Computern wurde der Grundstein der heutigen Kryptografie gelegt. Mit der Bedeutung des Datenschutzes hat auch die Bedeutung der Kryptografie zugenommen und die Anwendung der Verfahren vereinfacht. Auf der anderen Seite bietet der Computer auch die Möglichkeit große Datenmengen zu analysieren und Schlüssel zu brechen.
Mit dem Aufkommen des Internets wurde die Kryptografie immer wichtiger. Früher hat man große Datenmengen noch auf externen Datenträgern ausgetauscht. Zum Beispiel auf Diskette, CD-ROM, später DVD. Hier war der Bedarf für Kryptografie gering, weil die Datenträger von Personen beaufsichtigt und nur selten per Post oder in einem Paket verschickt wurden. Doch im Internet werden Daten auf einem

unbekannten Weg übertragen. Das heißt, alles kann jederzeit abgehört werden.

Die moderne Kryptografie ist allerdings noch eine relativ junge Technik, die sich im Vergleich mit alltäglicher Technik noch im "Dampfmaschinenzeitalter" befindet. Das wird sich vermutlich erst dann ändern, wenn wir es im Alltag mit Quantencomputern zu tun haben.

Gute und schlechte Kryptografie

Was Wissen und Erkenntnisse um gute Kryptografie angeht stehen wir noch ganz am Anfang. Momentan müssen "harte" kryptografische Verfahren folgende Anforderungen erfüllen:

- kein Zusammenhang zwischen Verschlüsselung und Inhalt
- keine erkennbaren Abhängigkeiten zwischen dem Klartext und dem verschlüsselten Text
- Einsatz erprobter und über einen längeren Zeitraum getesteter Verfahren und Implementierungen

Harte und damit sichere Kryptografie braucht oft viel Rechenleistung, bedeutet erheblichen Aufwand bei der Entwicklung, Implementierung und Konfiguration und kostet deshalb auch viel Geld.
Kryptografie ist in den Details so kompliziert, dass man sie nicht selber implementieren sollte, sondern auf weit verbreiteten und geprüften Bibliotheken zurückgreifen sollte.
Eine nicht zu unterschätzende Gefahr geht von Krypto-Systemen und -Infrastrukturen aus, die schlecht oder nicht wirklich funktionieren. Denn viele Anwendungen vertrauen darauf, dass sie funktionieren. Wenn zum Beispiel eine Funktion in einem Kryptosystem die Authentizität der Kommunikationspartner nicht ausreichend überprüft, dann kann der Übertragungsweg zwischen den Kommunikationspartnern kompromittiert sein und somit abgehört und manipuliert werden.
Erschwerend kommt jedoch hinzu, dass man als Anwender das nur bedingt erkennen kann, wenn ein Sicherheitsproblem vorliegt. Der Anwender bekommt, wenn überhaupt, erst dann etwas mit, wenn das Kind schon in den Brunnen gefallen ist.

Usability als Sicherheitsfeature / Sicherheit vs. Einfachheit

In der Regel ist es so, dass Sicherheitssysteme oft komplex und schwierig zu bedienen sind. Die Nutzung einer Sache ist dann mit Hürden verbunden, die im Sinne der Sicherheit und des Datenschutzes akzeptiert und anerkannt werden wollen.
Unter Experten wird die Meinung vertreten: "Kryptografie muss umständlich sein, sonst ist es nicht sicher." Leider hat diese Einschätzung einen Haken. Scheitert eine verschlüsselte Verbindung, dann wechseln viele Benutzer ihre Programme und verschicken die Nachrichten und Daten einfach ungeschützt. Die Anwender agieren dabei noch nicht einmal böswillig, sondern wollen einfach nur die gewohnte Funktionalität herstellen.

Kryptografische Verfahren

Der Begriff Kryptografie wird oft mit Verschlüsselung gleichgesetzt. Allerdings gibt es viele unterschiedliche kryptografische Verfahren, die auf komplizierten mathematischen Verfahren beruhen und für die Durchsetzung der Ziele der Kryptografie entwickelt und verwendet werden. In der Literatur wird Kryptografie mit Verschlüsselung gleichgesetzt und alles andere als einheitlich und teilweise ungenau verwendet. So wird ganz allgemein von Verschlüsselungsverfahren gesprochen, wobei diese Verfahren nicht nur verschlüsseln, sondern zum Beispiel auch Authentifizierung und Integritätsprüfung enthalten.

Verschlüsselung / Chiffrierung

Unter Verschlüsselung versteht man Verfahren, die Daten mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich verändern, damit die Daten unlesbar werden. Gleichzeitig wird dafür gesorgt, dass nur mit dem Wissen des Schlüssels die geheimen Daten wieder entschlüsselt werden können.
Anstatt von Verschlüsselung spricht man auch von Chiffrierung, was das gleiche meint.

Kryptoanalyse

Die Kryptoanalyse gehört wie die Kryptografie zur Kryptologie. Zur Kryptoanalyse gehören Methoden um kryptografische Verfahren zu analysieren oder zu brechen. Das Brechen einer Verschlüsselung kommt einem ungewollten Entschlüsseln gleich. Hierzu wendet man oft mathematische und statistische Verfahren an, die auf Schwächen eines bestimmten kryptografischen Verfahrens beruhen.

Ein Problem und damit eine Schwachstelle für jedes Verschlüsselungsverfahren ist die endliche Zahl von verschiedenen Codes zum Verschlüsseln. In der Vergangenheit kam es immer wieder vor, dass nicht immer wieder neue Codes verwendet wurden, sondern nach einiger Zeit alte nochmals eingesetzt wurden. Durch diese Wiederholung wurden Ansatzpunkte geschaffen, die Verschlüsselung zu entziffern.

Durch die stetige Verbesserung der Kryptoanalyse werden auch die Angriffe auf Verschlüsselungsverfahren mit der Zeit immer besser. Ist man den Schwächen eines Verschlüsselungsverfahrens auf der Spur, dann dauert es nur noch wenige Jahre, bis jemand einen weiteren Trick findet oder genug Rechenleistung zur Verfügung steht, um ein Verschlüsselungsverfahren zu knacken.

Wie sicher ist Kryptografie?

Die Kryptografie basiert auf mathematischen Verfahren. Die Sicherheit eines Kryptosystems lässt sich also mathematisch beweisen und berechnen. Die mathematische Beweisführung einer gewissen Sicherheit beruht jedoch oft nur auf Annahmen. Zum Beispiel: "Solange diese Bedingung erfüllt ist, ist dieses Verschlüsselungsverfahren sicher."
Das hat Konsequenzen. Denn ein ungeschickt implementiertes Kryptosystem kann ein eigentlich sicheres Verschlüsselungsverfahren unsicher machen.
Wie sicher ein kryptografisches Verfahren ist, ist zu allen Zeiten immer zu optimistisch gewesen. Prinzipiell neigen wir zur Selbstüberschätzung, was die Sicherheit einer Technik angeht. Dabei zeigt die Erfahrung, dass kein Aufwand zu groß ist, um ein Verfahren zu brechen. Die Fragestellung ist nur, ob sich der Aufwand, in Erwartung des Inhalts verschlüsselter Daten, lohnt.

Verschlüsselung / Chiffrierung

Unter Verschlüsselung versteht man Verfahren und Algorithmen, die Daten mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht lesbare Form umwandeln. Diesen Vorgang bezeichnet man als Verschlüsseln. Gleichzeitig wird dafür gesorgt, dass nur mit dem Wissen eines Schlüssels die geheimen Daten wieder entschlüsselt werden können.
Anstatt von Verschlüsselung spricht man auch von Chiffrierung, was das gleiche meint.

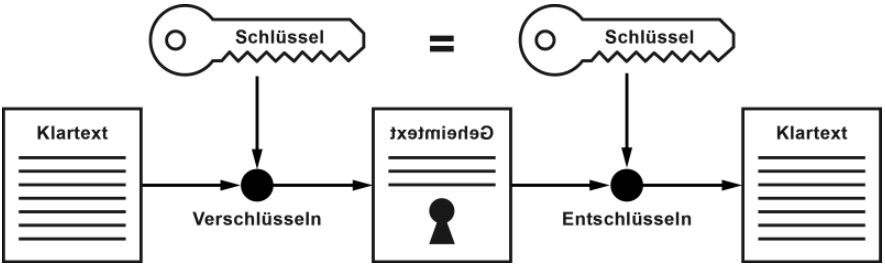
Verschlüsselungsalgorithmus

Ein Verschlüsselungsalgorithmus ist eine mathematische Funktion, der man den Klartext und einen Schlüssel übergibt. Die Ausgabe ist ein Geheimtext, der keinen Rückschluss auf den Klartext erlaubt. Nur mit Kenntnis des Schlüssels kann man mit der selben mathematischen Funktion den Geheimtext wieder in den Klartext umwandeln.
Von einem guten Verschlüsselungsalgorithmus weiß man, dass die Funktionsweise der mathematischen Funktion bekannt sein darf und die Daten nur mit Hilfe des Schlüssels entschlüsselt werden können. Und da das Verfahren bekannt ist, weiß man unter welchen Annahmen das Verfahren funktioniert und kann es überprüfen und auf Schwachstellen testen. Auf diese Weise kann man sicherstellen, dass ein Verschlüsselungsalgorithmus für einen bestimmten Anwendungsfall sicher genug ist.

Verschlüsselungsverfahren

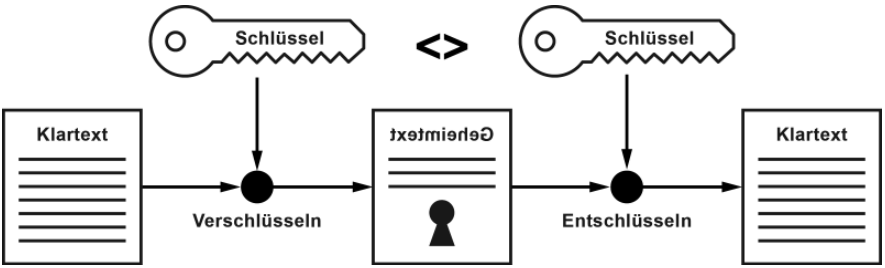
Ein Verschlüsselungsverfahren besteht aus einem Algorithmus zum Verschlüsseln und Entschlüsseln, sowie Verfahren zum Schlüsselaustausch, Prüfung der Authentizität und Integrität.
Die bekannten Verschlüsselungsverfahren teilen sich in symmetrische, asymmetrische und hybride Verschlüsselungsverfahren auf. Bei den hybriden Verschlüsselungsverfahren wird ein symmetrisches und asymmetrisches Verschlüsselungsverfahren miteinander kombiniert.

Symmetrische Verschlüsselung



Die symmetrische Verschlüsselung wird auch als Secret-Key-Verfahren bezeichnet. Es basiert auf einer mathematischen Funktion, die einen Klartext in Abhängigkeit eines Schlüssels (digitaler Code) in einen Geheimtext umwandelt. Beim Entschlüsseln wird der Geheimtext mit dem selben Schlüssel wieder in den Klartext umgewandelt.
Eine symmetrische Verschlüsselung eignet sich am besten für das Verschlüsseln von Dateien, Verzeichnissen und Laufwerken. Bei der Datenübertragung sind diese Verfahren weniger geeignet, weil man sich um einen sicheren Schlüsselaustausch und deren Verteilung kümmern muss.

Asymmetrische Verschlüsselung



Die asymmetrische Kryptografie wird auch als Public-Key-Verfahren bezeichnet. Der wesentliche Unterschied zur symmetrischen Kryptografie ist, dass die asymmetrische Kryptografie mit zwei Schlüsseln (unterschiedliche digitale Codes) arbeitet. Einen zum Verschlüsseln und den anderen zum Entschlüsseln. Wobei der Schlüssel zum Verschlüsseln öffentlich ist und der Schlüssel zum Entschlüsseln geheim bleiben muss. Man spricht auch vom Public-Key und vom Private-Key.

Beide Schlüssel sind ein Schlüsselpaar, dass dem Empfänger einer Nachricht gehört.
Damit ein Sender einem Empfänger eine verschlüsselte Nachricht schicken kann, muss der Empfänger seinen öffentlichen Schlüssel dem Absender bekannt machen.

Digitaler bzw. elektronischer Schlüssel

Man spricht von digitalen oder elektronischen Schlüsseln, wobei damit das selbe gemeint ist. Der digitale Schlüssel ist eine Bitfolge, deren Länge in Bit angegeben ist. Alle Verschlüsselungsverfahren benötigen den digitalen Schlüssel als individuellen Bestandteil der Verschlüsselung. Von einem guten Verschlüsselungsverfahren erwartet man, dass ein Angreifer ohne Schlüssel keine Chance hat, an den Klartext zu kommen. Gleichzeitig möchte man, dass der Sender mit Hilfe des Schlüssels schnell verschlüsseln und der Empfänger schnell entschlüsseln kann.

Ein Kriterium für die Sicherheit einer Verschlüsselung ist die Anzahl möglicher Schlüssel und eine möglichst überschaubare Anzahl schwacher Schlüssel. Ein Schlüssel mit einer Länge von 1.024 Bit, also eine Folge von 1.024 Nullen und Einsen, ist sicherer als ein Schlüssel mit nur 64 Bit. Selbst wenn man weiß, wie die Verschlüsselung arbeitet, müsste man alle möglichen Schlüssel durchprobieren, um irgendwann den richtigen Schlüssel zu bekommen. Selbst bei einem relativ unsicheren Schlüssel kann bei ausreichender Länge der Sicherheitspuffer groß genug sein. In der Regel gilt, je länger ein Schlüssel ist, desto schwieriger ist es an eine verschlüsselte Information ohne Schlüssel zukommen.

Stromchiffren und Blockchiffren

Bei Stromchiffren bzw. Stream-Cipher werden die Daten am Stück verschlüsselt. Diese Art und Weise der Verschlüsselung kommt aber nicht so häufig vor. Viel häufiger werden Blockchiffren bei der Verschlüsselung verwendet.
Bei Blockchiffren bzw. Block-Cipher werden die Daten blockweise zu einer festgelegten Größe einzeln und hintereinander verschlüsselt.

Kryptografische Protokolle / Verschlüsselungsverfahren

Um wirkungsvoll verschlüsseln zu können reicht es nicht aus, einen wirkungsvollen Verschlüsselungsalgorithmus zu haben, sondern man muss auch die verschiedenen Probleme bei der Übertragung von Daten und der Kommunikation lösen. Zu diesem Zweck fasst man verschiedene kryptografische Verfahren zusammen. Daraus entstehen dann standardisierte kryptografische Protokolle, auch Verschlüsselungsprotokolle genannt.

Bestandteile eines kryptografischen Protokolls oder einer Cipher-Suite

Die einzelnen Bestandteile der Kryptografie sind nicht in einem einzigen Verfahren und Protokoll umgesetzt, sondern verschiedene Algorithmen und Verfahren sind miteinander verwoben. Die einzelnen Verfahren sind teilweise austauschbar. Mehrere davon bilden eine Cipher-Suite oder ein Verschlüsselungsverfahren, was in seiner Gesamtheit einem Verschlüsselungsprotokoll oder einem kryptografischen Protokoll entspricht.

Die heute verwendeten kryptografischen Protokolle, die in der Kommunikations- und Netzwerktechnik eingesetzt werden, sind in der Regel eine Kombination aus Verfahren zur Schlüsselerzeugung, Schlüsselaustausch und Datenverschlüsselung. Häufig enthalten sie auch eine Integritätskontrolle und Authentifizierung. Die genau Zusammensetzung eines kryptografischen Protokolls hängt von den Anforderungen und dem Anwendungsfall ab.

- Funktion zur Schlüsselerzeugung mit einer kryptografischen Hash-Funktionen
- Schlüsselaustausch mit einem asymmetrischen Verfahren
- Algorithmus zur Verschlüsselung mit einem symmetrischen Verfahren
- Verfahren zur Integritätsprüfung mit einer kryptografischen Hash-Funktionen
- Authentifizierung mit einem asymmetrischen Verfahren

Bei der Betrachtungsweise von Verschlüsselungsprotokollen konzentriert man sich in der Regel auf den Schlüsselaustausch und die Verschlüsselung. Eine wirksame Verschlüsselung ist aber nur dann gut und gilt als sicher, wenn auch die Art und Weise der Schlüsselerzeugung nicht vorhergesagt werden kann und die Integrität und Authentizität der Daten und Kommunikationspartner geprüft wird. Die Verschlüsselung von Daten und der Kommunikation ist sinnlos, wenn nicht sichergestellt ist, dass der für den Schlüsselaustausch vorgesehene Kommunikationspartner der tatsächliche Empfänger des Schlüssels und der Daten ist.

Schlüsselerzeugung

Es gibt grundsätzlich drei Faktoren, die bei der Schlüsselerzeugung wichtig sind. Zum einen woraus der Schlüssel entsteht (Schlüsselmaterial), wie der Schlüssel entsteht (Verfahren) und wo er erzeugt wird (Hardware/System). Wobei das "Wo" auch darauf einen Einfluss hat, wie und woraus der Schlüssel entsteht.
Typischerweise werden digitale Schlüssel mit kryptografischen Hash-Funktionen erzeugt.

Schlüsselaustausch

Wenn man eine Kommunikation oder Datenübertragung verschlüsseln will, dann müssen sich die Kommunikationspartner überlegen, wie sie den oder die Schlüssel austauschen. Und das natürlich so, dass ein potentieller Angreifer den Schlüssel nicht abfangen kann.
Es ist eines der ungelösten Probleme der Kryptografie, den Schlüssel zu verteilen bzw. auszutauschen.

- RSA - Rivest, Shamir und Adleman
- Diffie-Hellman-Merkle-Schlüsselaustausch
- ISAKMP
- Needham-Schroeder-Protokoll

Verschlüsselungsverfahren

Der Begriff "Verschlüsselungsverfahren" wird immer dann verwendet, wenn es um Algorithmen, Mechanismen und Verfahren geht, die mit

Verschlüsselung zu tun haben. Da es bei der modernen Kryptografie und den meisten kryptografischen Verfahren hauptsächlich um Verschlüsselung geht, trifft der Begriff "Verschlüsselungsverfahren" in der Regel immer zu.
Es gibt kein allgemeingültiges Verschlüsselungsverfahren. Man unterscheidet in der Kryptografie grob zwischen symmetrischen und asymmetrischen Verfahren. Und dann gibt es noch hybride Verschlüsselungsverfahren, die Verfahren aus symmetrischen und asymmetrischen Kryptografie kombinieren.

Integritätsprüfung

Die Integritätsprüfung stellt fest, ob Daten verändert wurden. In Verschlüsselungsverfahren ist die Integritätsprüfung prinzipbedingt enthalten. Beim Verschlüsseln, wird nicht nur der Klartext, sondern auch eine Prüfsumme oder Hash verschlüsselt oder dem Geheimtext angehängt. Um nach dem Entschlüsseln festzustellen, ob man sinnvolle Daten bekommen hat, vergleicht man die Prüfsumme mit der aus dem Klartext gebildeten Prüfsumme. Stimmen beide überein, dann war die Entschlüsselung erfolgreich bzw. die Übertragung von Daten manipulations- und fehlerfrei.
In der Kryptografie bilden kryptografische Hash-Funktionen die Basis für die Integritätsprüfung.

Authentifizierung

Authentifizierung ist ein Vorgang bei dem festgestellt wird, wer eine Person oder eine Maschine ist. Im echten Leben weisen wir uns durch Unterschriften, Pässe und Karten aus. Im Internet ist die Authentifizierung durch die räumliche Trennung erschwert. Hier greift man auf Signaturen, Zertifikate und andere digitale Authentifizierungsmechanismen zurück.

- Digitale Schlüssel
- Digitale Signatur
- Digitale Zertifikate

Beispiele für eine Cipher-Suite (kryptografisches Protokoll)

Die Bestandteile eines kryptografischen Protokolls bzw. einer Cipher-Suite sind Schlüsselaustauschverfahren, Signaturverfahren, Verschlüsselungsverfahren und die kryptografische Hash-Funktion.

Die folgenden Zeilen zeigen die Ausgabe eines Servers, welche der üblichen Cipher-Suites für SSL/TLS-Verbindungen zur Verfügung stehen.

```
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES256-SHA384
ECDHE-ECDSA-AES128-SHA256
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-RC4-SHA
ECDHE-RSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA
ECDHE-RSA-AES128-SHA
ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-RC4-SHA
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA256
DHE-RSA-AES256-SHA
DHE-RSA-CAMELLIA256-SHA
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA256
DHE-RSA-AES128-SHA
DHE-RSA-SEED-SHA
DHE-RSA-CAMELLIA128-SHA
ECDH-RSA-RC4-SHA
ECDH-ECDSA-RC4-SHA
RC4-SHA
```

Nach unten werden die Cipher-Suites immer unsicherer. Für SSL/TLS-Verbindungen wird in der Regel die Kombination aus ECDHE, ECDSA oder RSA mit AES und GCM, sowie SHA256 oder SHA384 empfohlen. Die Cipher-Suites mit RC4 und/oder SHA gelten als hochgradig unsicher.

Hybride Verschlüsselungsverfahren

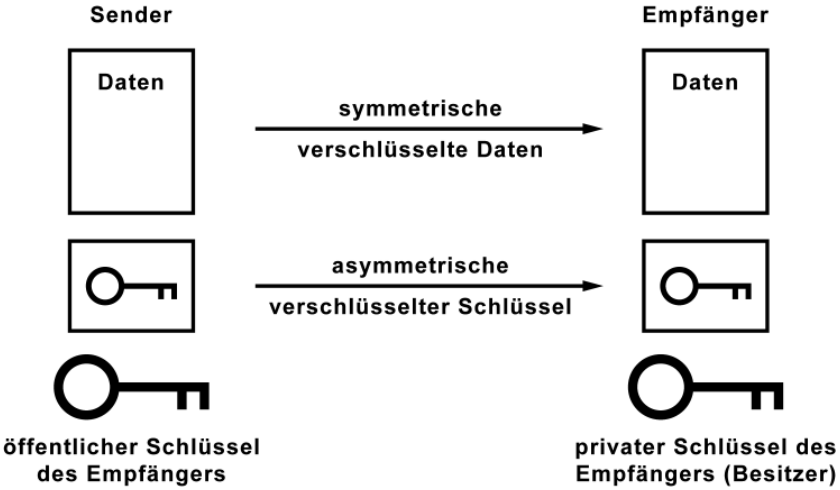
Viele kryptografische Protokolle und Krypto-Implementierungen arbeiten mit einem Hybrid-Verfahren, dass sich aus Verfahren der symmetrischen und asymmetrischen Kryptografie zusammensetzt.
Die Verfahren der symmetrischen und asymmetrischen Kryptografie erfüllen meist einen ähnlichen Zweck. Sie tun dies nur auf unterschiedliche Weise. Beide Verfahrensweisen ergänzen sich, weshalb sie häufig gemeinsam in einem kryptografischen Protokoll eingesetzt werden. Meist ohne, dass es Erwähnung findet.

Symmetrische Verfahren gelten allgemein als sicherer, weil deren Verschlüsselungsalgorithmen weniger Angriffsfläche bieten. Auf der anderen Seite hat man ein Problem den Sitzungsschlüssel sicher auszutauschen.
Asymmetrische Verfahren sind meist komplexer und langsamer bei der Verschlüsselung. Auf der anderen Seite lösen asymmetrische Verfahren das Problem mit dem Schlüsselaustausch.

Kombiniert man symmetrische und asymmetrische Verfahren löst man auf wunderbare Weise die Nachteile, die beide mit sich bringen. Hybride Verschlüsselungsverfahren setzen ein asymmetrisches Verfahren für den Schlüsselaustausch ein und verschlüsseln die Datenübertragung mit einem symmetrischen Verfahren.

Prinzip hybrider Verfahren

1. Zuerst wird ein zufälliger Sitzungsschlüssel für die symmetrische Datenverschlüsselung generiert.
2. Dann verschlüsselt der Sender diesen Sitzungsschlüssel mit dem öffentlichen Schlüssel des Empfängers (asymmetrische Verschlüsselung).
3. Der Sender schickt dann den asymmetrisch verschlüsselten Sitzungsschlüssel an den Empfänger.
4. Mit seinem privaten Schlüssel kann der Empfänger den Sitzungsschlüssel entschlüsseln (asymmetrische Verschlüsselung).
5. Danach werden die Daten mit Hilfe des Sitzungsschlüssels verschlüsselt übertragen (symmetrische Verschlüsselung).



Ein anderes hybrides Verfahren funktioniert so: Man denkt sich einen symmetrischen Sitzungsschlüssel, verschlüsselt die Daten damit und verschlüsselt den symmetrischen Schlüssel mit dem öffentlichen Schlüssel des Empfängers mit einem asymmetrischen Verfahren. Den verschlüsselten Sitzungsschlüssel hängt man für den Empfänger an. Der kann ihn mit seinem privaten Schlüssel entschlüsseln. Anschließend kann er mit dem symmetrischen Sitzungsschlüssel die Daten entschlüsseln.

Hybride Protokolle in der Praxis

In hybriden Protokollen wird bspw. RSA als asymmetrisches Verfahren und AES als symmetrisches Verfahren eingesetzt. Statt RSA kommt oft auch Diffie-Hellman oder ein anderes Verfahren auf Basis elliptischer Kurven zum Einsatz. Hierbei kommen RSA und Diffie-Hellman nicht für die Verschlüsselung in Frage, sondern nur für den Schlüsselaustausch. Dieser Schlüssel wird dann für die Verschlüsselung mit AES verwendet.

SSH - Secure Shell

SSH bzw. Secure Shell ist ein kryptografisches Protokoll mit dem man auf einen entfernten Rechner mittels einer verschlüsselten Verbindung über ein unsicheres Netzwerk zugreifen kann. Der Entwickler dieses Protokolls und der dazugehörigen Software ist der Finne Tatu Ylönen.

Die Shell (Kommandozeile) bietet vollen Zugriff auf das Dateisystem und alle Funktionen des Rechners. Dazu verwendet man in der Regel Telnet (TCP/Port 23) oder rlogin/rsh. Diese Programme und dazugehörigen Protokolle sind jedoch unsicher, weil das Zugangspasswort im Klartext übertragen wird. Das sollte innerhalb eines unsicheren Netzwerks, z. B. dem Internet, nicht passieren, da man nicht weiß, wo der Datenverkehr verläuft und ob er abgehört wird.
Die Funktionen der Secure Shell beinhalten den Login auf entfernte Rechner, die interaktive und nicht interaktive Ausführung von Kommandos und das Kopieren von Dateien zwischen verschiedenen Rechnern eines Netzwerks. SSH bietet dazu eine kryptografisch gesicherte Kommunikation über das unsichere Netzwerk, eine zuverlässige gegenseitige Authentisierung, Verschlüsselung des gesamten Datenverkehrs auf Basis eines Passworts oder Public/Private-Key-Login-Methoden.
In den meisten Fällen ist Secure Shell in der Lage die Protokolle und Anwendungen von Telnet, FTP und die r-Utilities zu ersetzen.

SSH 1.x und SSH 2.x

Das SSH-Protokoll existiert in den Versionen SSH 1.x und SSH 2.x. Beide Versionen sind inkompatibel zueinander. Das SSH-Protokoll 1.x ist nicht international standardisiert und unterliegt einiger konzeptionellen Schwächen, die in SSH 2.x nicht vorhanden sind.
Im Juni 1995 hat Tatu Ylönen SSH 1.0 unter Unix freigegeben und bis zur Version 1.2.12 als beliebig nutzbar freigegeben. SSH Version 1 sollte man nicht mehr einsetzen.

SSH 2.x wurde durch eine Arbeitsgruppe der IETF erarbeitet. Unter SSH 2.x gibt es außerdem das Protokoll SFTP (Secure File Transfer Protocol), das für den Dateitransfer zuständig ist. Es basiert auf dem bereits existierenden FTP. Es empfiehlt sich die Version 2 von SSH zu verwenden.

OpenSSH

OpenSSH ist eine Implementierung auf Basis von SSH 1.2.12. Im Gegensatz zum Original wird OpenSSH aktiv gepflegt und enthält neben einigen Erweiterungen und Verbesserungen auch das SSH-Protokoll 2.x.

SSL - Secure Socket Layer

SSL ist ein Protokoll, das der Authentifizierung und Verschlüsselung von Internetverbindungen dient. SSL schiebt sich zwischen die Anwendungs- und Transportprotokollen. Ein typisches Beispiel für den Einsatz von SSL ist der gesicherte Abruf von vertraulichen Daten über HTTP und die gesicherte Übermittlung von vertraulichen Daten an den HTTP-Server. In der Regel geht es darum, die Echtheit des kontaktierten Servers durch ein Zertifikat zu garantieren und die Verbindung zwischen Client und Server zu verschlüsseln.
SSL ist äußerst beliebt und das Standard-Protokoll bzw. die Erweiterung für Anwendungsprotokolle, die keine Verschlüsselung für sichere Verbindungen mitbringen.

Hinweis: Das ursprüngliche SSL ist inzwischen veraltet und in TLS aufgegangen. Obwohl man heute in der Regel TLS verwendet spricht man trotzdem immer noch von SSL. Teilweise tragen Software-Produkte und -Bibliotheken historisch bedingt "SSL" im Namen, obwohl sie TLS beherrschen.

SSL oder TLS?

SSL wurde ursprünglich von Netscape in den 90er Jahren für den Browser "Netscape Navigator" entwickelt und war lange Zeit "der Standard" für die Verschlüsselung von Internet-Verbindungen. Die Weiterentwicklung von SSL wurde mit der Version 3 beendet. Die IETF hat SSL 3.0 übernommen, ein paar Änderungen vorgenommen und als neuen und zu SSL inkompatiblen Standard mit der Bezeichnung TLS spezifiziert (SSL Version 3.1).

Vielfach haben bis heute Funktionen in Software und Bibliotheken immer noch die Bezeichnung SSL im Namen, obwohl sie TLS verwenden. Deshalb ist es heute immer noch üblich von SSL zu sprechen, obwohl man eigentlich die technische Implementierung von TLS meint.
In der Praxis ist es aber völlig unerheblich ob man SSL oder TLS sagt.

SSL/TLS im OSI-Schichtenmodell

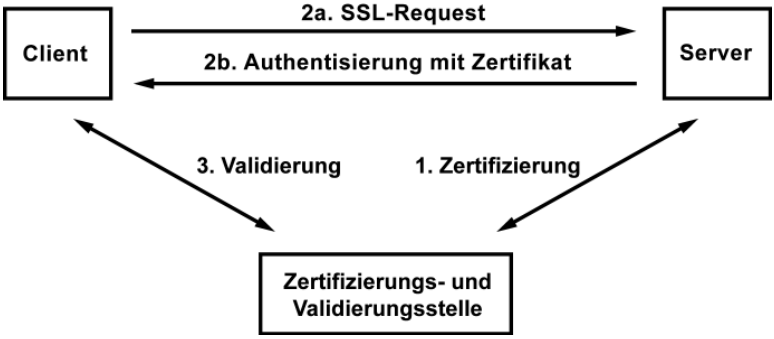
Anwendung	HTTP, FTP, SMTP, POP, IMAP, ...
Transport	SSL/TLS
	TCP / UDP
Vermittlung	IPv4 / IPv6
Netzzugang	Ethernet (LAN), IEEE 802.11 (WLAN), ...

Im OSI-Schichtenmodell ist SSL bzw. TLS auf Schicht 5, der Sitzungsschicht angeordnet. Im DoD-Schichtenmodell, das für TCP/IP verwendet wird, ist SSL/TLS auf der Transportschicht als Transportverschlüsselung über TCP und unterhalb der Anwendungsprotokolle zugeordnet. Dabei arbeitet SSL/TLS völlig transparent. So können theoretisch alle denkbaren Anwendungsprotokolle SSL zum Verschlüsseln benutzen. Dabei muss aber jedes Anwendungsprotokoll SSL bzw. TLS explizit beherrschen.
So wird beispielsweise aus dem unverschlüsselten HTTP (Hypertext Transfer Protocol) das verschlüsselte HTTPS (Hypertext Transfer Protocol Secure). Ebenso ist es möglich E-Mails über SSL beim POP-Server verschlüsselt abzurufen oder an den SMTP-Server verschlüsselt zu übermitteln. Auch hier bekommen die Protokolle einen "Secure"-Zusatz (SMTPS, POPS, IMAPS).
SSL ist inzwischen nicht nur auf HTTPS oder andere Kommunikationsprotokolle beschränkt. Verfahren wie EAP-TLS, EAP-TTL, PEAP und auch das LDAP-Protokoll verwenden SSL.

Anwendungsbeispiel: HTTPS

SSL ist eine optional aktivierbare Sicherheitskomponente für HTTP und ist somit für Webseiten gedacht, die vertrauliche Daten verarbeiten. Zum Beispiel beim Online-Banking oder Online-Shopping. Diese Webseiten bauen in der Regel automatisch eine verschlüsselte Verbindung zwischen Browser und Webserver auf. Der User bekommt das nur mit, wenn ein Schloss- oder Schlüssel-Symbol in der Statusleiste eingeblendet wird oder die Adresszeile ihre Farbe ändert.

Funktionsweise von SSL/TLS



Bestandteil von SSL ist die Zertifizierung (1.) des öffentlichen Schlüssels, die Authentifizierung des Servers (2.), die Validierung des übermittelten Zertifikats (3.) und die anschließende verschlüsselte Übertragung von Daten zwischen Sender und Empfänger.
Für die Authentifizierung werden Zertifikate verwendet. Unter anderem um das Verteilungsproblem von Authentifizierungsinformationen zu beheben und um Identitäten zu authentifizieren. Hierbei geht es darum, die Authentizität der Gegenstelle zweifelsfrei feststellen zu können, um nicht mit einer falschen Gegenstelle eine Verbindung einzugehen.

Zertifikate

Eine Verschlüsselung besteht aus der Verschlüsselung der Daten beim Sender und der Entschlüsselung der Daten beim Empfänger. Bei SSL bzw. TLS arbeitet man mit zwei unterschiedlichen Schlüsseln zur Ver- und Entschlüsselung. Das sogenannte Schlüsselpaar besteht aus einem privaten (Private Key) und einem öffentlichen Schlüssel (Public Key). Der öffentliche Schlüssel des Empfängers ist dem Sender bekannt. Er benutzt ihn zum Verschlüsseln der Daten. Anschließend können die verschlüsselten Daten aber nicht mehr mit dem öffentlichen Schlüssel entschlüsselt werden. Dafür braucht es den privaten Schlüssel, der nur dem Empfänger bekannt sein darf und deshalb zwingend geheim gehalten werden muss. Nur der Server mit dem passenden privaten Schlüssel ist in der Lage die verschlüsselten Daten zu entschlüsseln (asymmetrisches Verschlüsselungsverfahren bzw. Public-Key-Verfahren).

Bevor nun der Sender Daten verschlüsseln darf, muss er jedoch zweifelsfrei feststellen, ob der öffentliche Schlüssel, den er vom Empfänger mitgeteilt bekommt, auch tatsächlich dem Empfänger gehört, dem er die Daten verschlüsselt schicken will. Eine per SSL verschlüsselte Verbindung bietet keinen Schutz, wenn nicht sichergestellt ist, dass der öffentliche Schlüssel von dem Server kommt, zu dem eine verschlüsselte Verbindung hergestellt werden soll.
An der Stelle kommt jetzt das Zertifikat ins Spiel, mit dem sich ein Server und sein öffentlicher Schlüssel authentisieren. Um die Gültigkeit des öffentlichen Schlüssels zu unterstreichen, lässt sich der Server-Betreiber und Domain-Inhaber ein Zertifikat ausstellen, in dem unter anderem Domainname, der öffentliche Schlüssel, ein Ablaufdatum enthalten sind und welche Instanz die Vertrauenswürdigkeit bestätigt hat.
Durch das Zertifikat authentisiert sich der Empfänger gegenüber dem Sender bzw. der Server gegenüber dem Client. Gleichzeitig kann der Client das Zertifikat überprüfen (Validierung) und somit die Vertrauenswürdigkeit feststellen (Authentizität).

SSL bzw. TLS arbeitet mit PKIX-Zertifikaten bzw. mit einer Public Key Infrastructure nach X.509v3. Die Zertifikate koppeln eine Identität an einen öffentlichen Schlüssel, der zur Authentifizierung und Verschlüsselung verwendet wird.
Es gibt insgesamt drei Zertifikatstypen, die sich durch einen unterschiedlichen Prüfaufwand bei der Zertifizierung unterscheiden und so eine entsprechend unterschiedliche Echtheitsstufe garantieren.

- Domain-Validated-Zertifikat (DV-SSL)
- Organisation-Validation-Zertifikat (OV-SSL)
- Extended-Validation-Zertifikat (EV-SSL)

Die häufigsten Zertifikate sind DV- und EV-Zertifikate. Während man DV-Zertifikate schon für wenige Euro oder sogar kostenlos bekommen kann, kommen wegen des erheblichen Prüfaufwands bei EV-Zertifikaten mehrere hundert oder sogar tausend Euro zusammen. Allerdings kann man bei EV-Zertifikaten von einer höheren Vertrauenswürdigkeit ausgehen.

Welches Zertifikat bei einer verschlüsselten Verbindung zum Einsatz kommt, ist als Nutzer nicht so leicht zu erkennen. Meist ist eine

verschlüsselte Verbindung in einem Client nur an einem Schloss-Symbol zu erkennen. Aber nicht, um was es sich für ein Zertifikat handelt. Zertifikate werden von einer Zertifizierungsstelle bzw. Certification Authority (CA) ausgestellt und beglaubigt.

Certificate Authority (CA) / Zertifizierungsstelle

Weltweit gibt es weit über 700 Zertifizierungsstellen. Im Englischen auch Certificate Authority oder Certification Authority genannt. Meist mit CA abgekürzt.
Die Certificate Authorities (CA) sind ein wichtiger Pfeiler für die Sicherheit im Internet. Jeder, der sichere Dienste im Internet anbietet, lässt sich die Echtheit von digitalen Schlüsseln und Signaturen von einer Certificate Authority bestätigen.

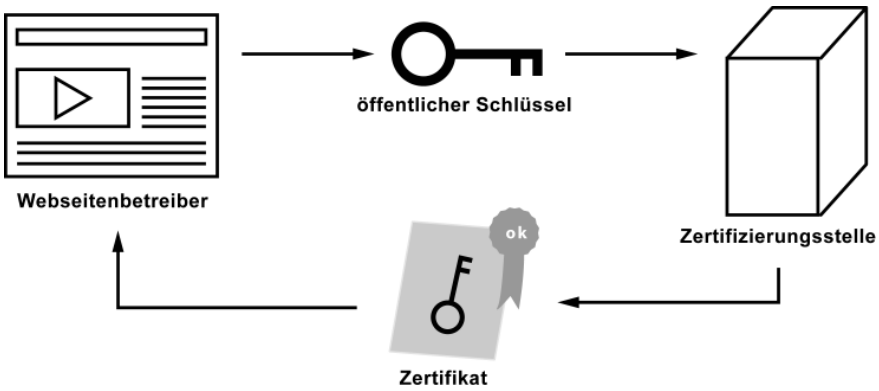
Dazu lässt sich ein Unternehmen oder eine Organisation von einer Certificate Authority nach einer Überprüfung ein digitales Zertifikat ausstellen. Das kann dann zum Beispiel auf einem Webserver hinterlegt werden. Mit diesem Zertifikat weist sich die Webseite gegenüber den zugreifenden Browsern als Eigentümer aus. Der Browser des Besuchers überprüft die Angaben im Zertifikat und fragt bei Bedarf bei der ausstellenden Zertifizierungsstelle nach, ob das Zertifikat gültig ist.
Auf diese Weise können zum Beispiel die Kunden einer Bank davon ausgehen, dass sie tatsächlich mit dem Server der Bank verbunden sind und das der Datenaustausch verschlüsselt erfolgt, wenn sie Online-Banking betreiben.

Auch die Zertifizierungsstelle besitzt ein Zertifikat, indem sich deren öffentlicher Schlüssel befindet. Dabei handelt es sich um ein Wurzel- bzw. Stammzertifikat, das in Browsern und Betriebssystemen hinterlegt ist. Diesen Stammzertifikaten wird in der Regel bedingungslos vertraut. Anhand der Signatur der Zertifizierungsstelle und dem Stammzertifikat kann ein Browser feststellen, ob das Zertifikat einer Domain wirklich von der angegebenen Zertifizierungsstelle ausgestellt wurde.

Das Geschäftsverhältnis zwischen Zertifizierungsinstanz und den Unternehmen, aber auch zu den Internet-Nutzern, beruht auf Vertrauen. Daher muss eine CA alles dafür tun, dass die Prüfprozesse ordnungsgemäß funktionieren und sicher vor Manipulationen sind.

Leider ist es schon vorgekommen, dass Eindringlinge auf interne Server von Zertifizierungsstellen zugegriffen und sich dort Zertifikate generiert haben. Wird ein solches Zertifikat verwendet, kann ein Internet-Nutzer einen Betrug nicht überprüfen. Und ein Unternehmen, dass Dienste im Internet anbietet, kann genauso wenig feststellen, ob eine Zertifizierungsstelle unberechtigt Zertifikate ausgestellt hat. Höchstens die CA kann betrügerische Zertifikate feststellen.
CAs sind also Treuhänder, die nur von ihrem guten Ruf leben. Sobald bekannt wird, dass eine CA Schindluder betreibt oder gehackt wurde, kann sie den Laden schließen.

SSL-Zertifizierung

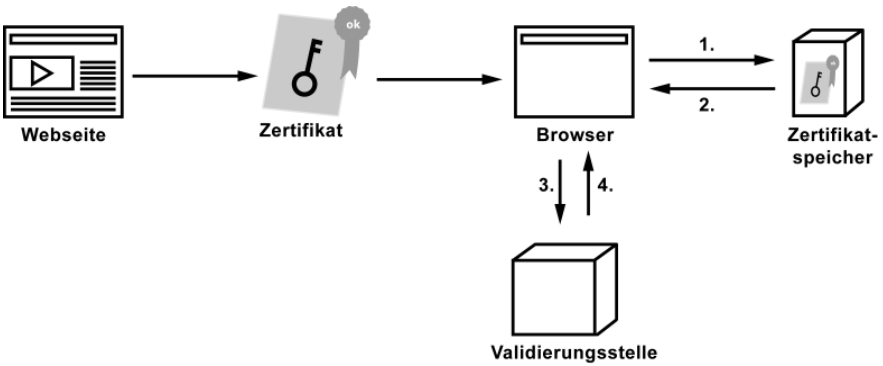


Das Zertifikat wird von einer Zertifizierungsstelle, auch Certificate Authority (CA) genannt, ausgestellt. Die Zertifizierungsstelle signiert das Zertifikat mit ihrem eigenen privaten Schlüssel, womit die Echtheit der Daten bestätigt sind. Im Vorfeld prüft die Zertifizierungsstelle die Informationen im Zertifikat und die Identität des Antragstellers. Dafür gibt es verschiedene Verfahren. Beispielsweise den Certificate Signing Request (CSR).

Validierung eines Zertifikats

Bekommt ein Client oder Server von einem anderen Server ein Zertifikat, dann muss er sich von dessen Echtheit überzeugen. Also, ob das Zertifikat wirklich von dem Server kommt, der kontaktiert wurde.

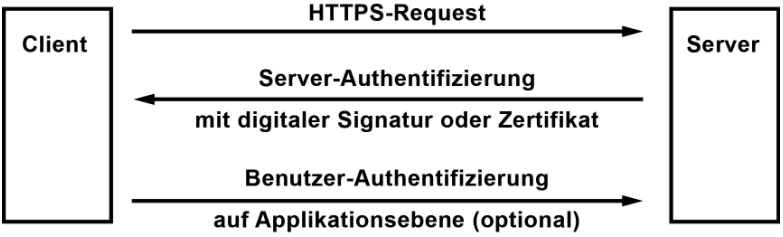
Mit der Validierung eines Zertifikats wird die Identität bestätigt, ohne dass die beteiligten Kommunikationspartner vorab Authentifizierungsinformationen, wie zum Beispiel Schlüssel, austauschen müssen.



Im folgenden Beispiel wird die Validierung exemplarisch für eine verschlüsselte HTTPS-Verbindung beschrieben. Grundsätzlich funktioniert die Validierung bei anderen Protokollen genauso.
Nachdem der Browser vom Webserver ein Zertifikat bekommen hat, beginnt er mit der Validierung. Der Browser prüft zuerst, ob er dem Aussteller des Zertifikats, der Zertifizierungsstelle oder Certificate Authority (CA), vertraut. Dazu muss das entsprechende Wurzelzertifikat der Zertifizierungsstelle im Browser hinterlegt sein (1. und 2.). Der Browser hat dazu eine Liste mit Zertifizierungsstellen, denen er per Default vertraut.
Im zweiten Schritt kontaktiert der Browser die angegebene Validierungsstelle bzw. Zertifizierungsstelle (3. und 4.). Diese prüft, ob das Zertifikat gültig ist und meldet das Ergebnis an den Browser zurück. Sofern das Zertifikat bereits bekannt ist, ist eine Validierung über die Zertifizierungsstelle nicht mehr zwingend erforderlich.

Ablauf der Authentifizierung

Beim ersten HTTPS-Request durch den Browser (Client) nutzt SSL die asymmetrische Verschlüsselung. Der Server schickt als erste Antwort seinen öffentlichen Schlüssel (Public Key) und ein Zertifikat. Auf diese Weise authentisiert sich der Webserver gegenüber dem Client. Schlüssel und Zertifikat werden vom Client auf Glaubwürdigkeit überprüft.



Je nach Einstellung des Clients muss der Benutzer zuerst die Glaubwürdigkeit bestätigen.
Nach erfolgreicher Authentifizierung des Servers, generiert der Browser einen symmetrischen Schlüssel, den er mit dem öffentlichen Schlüssel des Servers verschlüsselt. Den symmetrischen Schlüssel schickt der Browser dann an den Server. Der Server kann das verschlüsselte Paket mit seinem privaten Schlüssel öffnen. Der darin enthaltene Schlüssel des Browsers nutzt der Server für die symmetrische Verschlüsselung der darauf folgenden Verbindung. Eine sichere Übertragung ist gewährleistet. Die Inhalt der HTTPS-Pakete sind gegen Belauschen und Veränderung geschützt.
Während der Datenübertragung zwischen Client und Server wird immer wieder ein neuer Schlüssel ausgehandelt, so dass ein möglicher Angreifer nur für eine kurze Zeit die Verbindung stören kann.

In der Regel authentifiziert sich der Client nicht. Die Möglichkeit der beiderseitigen Authentifizierung per Signatur ist als Option in der SSL-Spezifikation enthalten. In der Regel muss nur bei einem SSL-VPN auch der Client seine Identität mit einem Zertifikat ausweisen.
Die Benutzerauthentifizierung, sofern erforderlich, findet in der Regel auf der Anwendungsebene statt. Konkret bedeutet dass, der Kunden würde sich in einem Online-Shop registrieren und anmelden oder im Online-Banking mit Pin, Passwort und TAN identifizieren.

Wie sicher ist SSL/TLS?

Seit den Enthüllungen im Rahmen des NSA-Skandals im Sommer 2013 ist bekannt, dass SSL/TLS definitiv unsicher ist und eine unsichere Authentifizierung enthält, was zu einer nur bedingt wirksamen Verschlüsselung führt. Das Problem dabei ist nicht die Verschlüsselung an sich, sondern das Vertrauenskonzept, welches hierarchisch angeordnet ist.

Ein Geheimdienst, wie die NSA, der Google, Microsoft, Yahoo und Apple zur Zusammenarbeit zwingen kann, kann das auch bei einer Zertifizierungsstelle, wie sie bei SSL/TLS die zentrale Instanz für die Zertifizierung und Validierung von Identitäten bildet. Und deshalb gelten Zertifizierungsstellen, denen man bedingungslos vertrauen muss, als kompromittiert.

SSL/TLS ist also nicht wirklich sicher! Trotzdem kann man SSL/TLS als sicher ansehen. Doch das bedeutet nicht, dass es für alle Anwendungen und in Zukunft sicher genug ist. Das bedeutet, trotz Authentifizierung und Verschlüsselung muss man als Nutzer mit einer gewissen Unsicherheit leben.

SSL/TLS sicherer machen

Hinweis: Mit dem aktuellen Vertrauensmodell (Certificate Authority) ist es unmöglich die Authentifizierung und Verschlüsselung für alle Anwendungen sicher zu machen. Die einzige Möglichkeit besteht darin, Workarounds zu bauen, also Teilprobleme von SSL/TLS und dessen kaputtes Vertrauensmodell zu lösen, um die Sicherheit des System einigermaßen glaubhaft am Laufen zu halten.

Weil die Authentifizierung grundsätzlich defekt ist, versucht man wenigstens die Verschlüsselung so weit hinzubekommen, dass die Kommunikation rückwirkend nicht entschlüsselt werden kann. Diese Maßnahmen sind erforderlich, weil man weiß, dass Geheimdienste (bspw. die NSA) verschlüsselten Datenverkehr aufzeichnet. Anschließend versuchen Geheimdienste über offizielle Anordnungen die Herausgabe der Schlüssel zu fordern oder sich den Zugang zu den Schlüsseln anderweitig zu beschaffen.
Mit dem Einsatz von Perfect Forward Secrecy in Kombination mit Diffie Hellman kann man die Kommunikation rückwirkend nicht entschlüsseln. Deshalb wird für die verschlüsselte Übertragung von personenbezogenen oder anderen sensiblen Daten mit SSL bzw. TLS Perfect Forward Secrecy und Diffie-Hellman empfohlen.

Um TLS/SSL sicherer zu betreiben führt ebenfalls kein Weg an TLS Verion 1.2 vorbei.

TLS - Transport Layer Security

TLS ist ein Protokoll, das der Authentifizierung und Verschlüsselung von Internetverbindungen dient. TLS schiebt sich als eigene Schicht zwischen TCP und den Protokollen der Anwendungs- und Darstellungsschicht. In der Regel geht es darum, die Echtheit des kontaktierten Servers durch ein Zertifikat zu garantieren und die Verbindung zwischen Client und Server zu verschlüsseln.

TLS (Version 1.0) hat seinen Ursprung in SSL, das von Netscape in den 1990er Jahren für den Browser "Netscape Navigator" entwickelt wurde. Die Weiterentwicklung von SSL wurde mit der Version 3 beendet. Danach übernahm die IETF (Internet Engineering Task Force) die Weiterentwicklung und Normierung. Daraus entstand 1999 der Standard TLS (Transport Layer Security).
TLS ist bis auf ein paar Details mit SSL identisch. Die Unterschiede zwischen TLS Version 1 und SSL Version 3 reichen jedoch aus, dass beide zueinander inkompatibel sind. TLS verwendet zur Authentifizierung der Daten HMAC und erzeugt die Schlüssel mit der Funktion PRF.

Obwohl man in der Regel TLS verwendet, ist die Bezeichnung SSL immer noch üblich. Häufig werden beide Bezeichnungen synonym verwendet.

Sichere E-Mail

Als die Protokolle und Programme für E-Mail entwickelt wurden, waren weder IT-Sicherheit noch Anonymität ein Thema. Deshalb sind bis heute die Übermittlung und der Inhalt von E-Mails während der Übertragung einsehbar.

- Postkarte : E-Mail
- Brief : verschlüsselte E-Mail

Eine E-Mail ist keine elektronische Variante des Papierbriefs. Beim Papierbrief ist die Nachricht durch den Umschlag nicht einsehbar. E-Mail funktioniert eher wie eine Postkarte. Neben Absender und Empfänger ist

auch die Nachricht für jeden, der die Postkarte in die Hand bekommt bzw. die E-Mail überträgt, einsehbar.

Wie geht sichere E-Mail?

Wenn es um sichere E-Mail geht, dann sind zwei Dinge von Bedeutung. Einmal die Verschlüsselung der Nachricht und zweites die Überprüfung der Identität des Absenders. Es muss also nicht nur die Nachricht vor fremden Blicken geschützt werden, sondern auch sichergestellt werden, dass die Nachricht tatsächlich von der Person kommt, die als Absender angegeben ist.

Verschlüsseln und signieren von E-Mails

Es gibt im Prinzip nur zwei Verfahren, die sich für die Verschlüsselungen von E-Mails eignen.

- S/MIME (nicht sicher, aber überall integriert)
- PGP - Pretty Good Privacy (sicher, muss nachträglich installiert werden)

Beide Verfahren bauen auf einer Public-Key-Infrastruktur (PKI) auf. Darin gibt es für jeden Teilnehmer einen öffentlichen (public) und einen geheimen (private) Schlüssel. Mit dem öffentlichen Schlüssel des Empfängers wird verschlüsselt und mit seinem geheimen Schlüssel kann der Empfänger die Nachricht entschlüsseln.

Bei der Verschlüsselung von E-Mails wird nur die Nachricht verschlüsselt. Nicht die Meta-Daten mit Absender und Empfänger. Auch nicht der Betreff, Datum und Uhrzeit der E-Mail. Einige Sicherheitsexperten kritisieren, dass eine Verschlüsselung ohne Einbeziehung der Meta-Daten sinnlos ist. Denn genau DAS sind die wichtigen Daten. Wer mit wem wann kommuniziert hat. Denn daraus lassen sich den Inhalt der E-Mail erraten oder nachvollziehen. Insbesondere Geheimdienste und Strafermittler reicht es aus, wer mit wem und wann Kontakt hatte, um weitere Ermittlungen anzustellen. Der ungefähre Gesprächsinhalt ist dann schon bekannt.

Verfahren für die Verbindungssicherheit

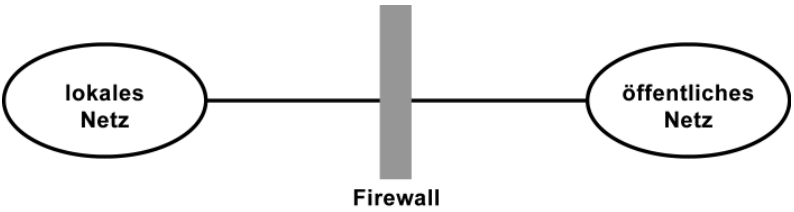
Die Meta-Daten sind nur dann vor fremden Blicken geschützt, wenn der Transport zwischen Mail-Client und Mail-Server sowie zwischen den Mail-Servern verschlüsselt ist. Doch spätestens im Posteingang beim Provider liegen die Meta-Daten der E-Mails wieder offen.

- STARTTLS
- SSL/TLS

Authentisierungsmethoden

- verschlüsseltes Passwort
- Kerberos, GSSAPI
- NTLM
- TLS-Zertifikat

Firewall



Eine Firewall ist eine Schutzmaßnahme gegen fremde und unberechtigte Verbindungsversuche aus dem öffentlichen (Internet) ins lokale Netzwerk. Mit einer Firewall lässt sich der kommende und gehende Datenverkehr kontrollieren, protokollieren, sperren und freigeben. Dabei ist die Firewall genau zwischen dem öffentlichen und dem lokalen Netzwerk platziert. Meist ist die Firewall Teil eines Routers. Sie kann aber auch als externe Komponente einem Router vor- oder nachgeschaltet sein.

Firewall als Sicherheitsstrategie

Eine Firewall ist keine Blackbox, die Sicherheit für das lokale Netzwerk vor dem öffentlichen Netzwerk vorgaukelt. Eine Firewall ist eine

technische Einrichtung, die eine Sicherheitsstrategie umsetzt, um unerwünschte, unsichere und schädigende Verbindungen zu verhindern. Ohne ständige Überwachung und Pflege bleibt nach einiger Zeit keine Schutzwirkung übrig.

Vor dem Einsatz einer Firewall ist die Akzeptanz und aktive Mitarbeit aller Beteiligten innerhalb eines lokalen Netzwerks zu gewährleisten, damit die Firewall effektiv funktionieren kann.
Am Anfang steht die Entscheidung zur Grundhaltung gegenüber Datenverbindungen. Die Firewall kann zunächst alle Verbindungen erlauben und nur bekannte und gefährliche Datenverbindungen unterbinden. Oder sie sperrt alles und alle erwünschten Datenverbindungen müssen explizit freigegeben werden.

Firewall-Strategie: Alles sperren

Alles ist gesperrt. Bekannte sichere und erwünschte Vorgänge werden freigegeben.

Diese Variante ist sehr sicher. Allerdings erfordert sie eine aufwendige Konfiguration der Firewall.

Firewall-Strategie: Alles freigeben

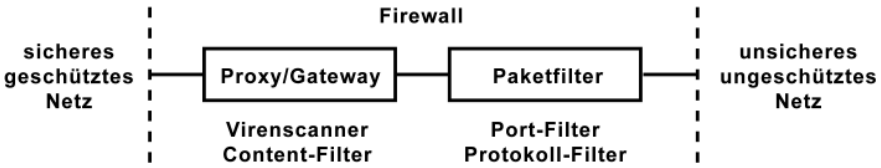
Alles ist freigegeben. Bekannte unsichere und unerwünschte Vorgänge werden gesperrt.

Diese Variante ist relativ komfortabel. Bei der Einführung ist mit keinerlei Problemen zu rechnen. Allerdings ist sie nur so sicher, wie Gefahren und Sicherheitslöcher bekannt sind und gesperrt werden.

Elemente einer Firewall

Grundsätzlich gibt es zwei verschiedene Ansätze für ein Firewall-Konzept:

- passiver Paketfilter mit Port- und Protokoll-Filter
- aktives Gateway (Proxy) mit Virenscanner und Content-Filter



Ein Paketfilter (TCP/IP) kontrolliert die Quell- und Ziel-IP sowie die dazugehörigen Portnummern (TCP). Neben der Filterfunktion ist die Protokollierung abgelehnter Pakete für spätere Analysen wichtig.
Das Gateway ist ein Proxy, der die Datenpakete der Internet-Dienste (HTTP, FTP, ...) zwischenspeichert. Dadurch lässt sich eine inhaltsbezogene Filterung der Daten vornehmen. Für ein LAN mit viel E-Mail-Verkehr ist ein Virencheck für E-Mails besonders empfehlenswert. Einen optimalen Schutz erreicht man durch eine Kombination aus Paketfilter und Proxy. Vorzugsweise sollte der Paketfilter dem Proxy vorgeschaltet sein, um unnötigen Datenverkehr über den Proxy zu vermeiden. Inhaltsbezogene Filterungen benötigen deutlich mehr Rechenleistung. Der Proxy sollte deshalb mit viel Rechenleistung und Arbeitsspeicher ausgestattet sein.

Eine Firewall kann ein einzelner Computer oder eine Kombination aus Proxy und einem Router sein. Praktikabel ist es, wenn der Paketfilter ein Router mit Firewall-Funktionen ist.

Hauptproblem beim Einrichten einer Firewall ist das Überprüfen der Filterregeln und Beschränkungen. Nur wenige Firewall-Produkte bieten diese Möglichkeit. Sich auf die einwandfreie Funktion der Firewall zu verlassen wäre fatal. Entweder man beauftragt eine externe Firma, die Firewall zu testen oder man beschafft sich einschlägige Software-Tools und testet die Firewall selber. Aber über einen anderen Internet-Zugang, nicht über das eigene lokale Netz!

Next Generation Firewall

Die Bezeichnung "Next Generation Firewall" wurde von Gartner Research (Marktforschungsinstitut im Bereich IT) definiert. Diese Firewall der nächsten Generation kann im Datenstrom Anwendungen und Benutzer erkennen. Dazu gehört ein integriertes Intrusion Prevention System (IPS), die Identifikation von Anwendungen und Protokollen

unabhängig vom genutzten Port und die Berücksichtigung externer Datenquellen, wie zum Beispiel Verzeichnisdienste mit Benutzerdaten. Next Generation Firewalls gehen also über die üblichen Fähigkeiten einer Firewall, wie Paketfilter, Network Address Translation (NAT) und Stateful Inspection hinausgeht.

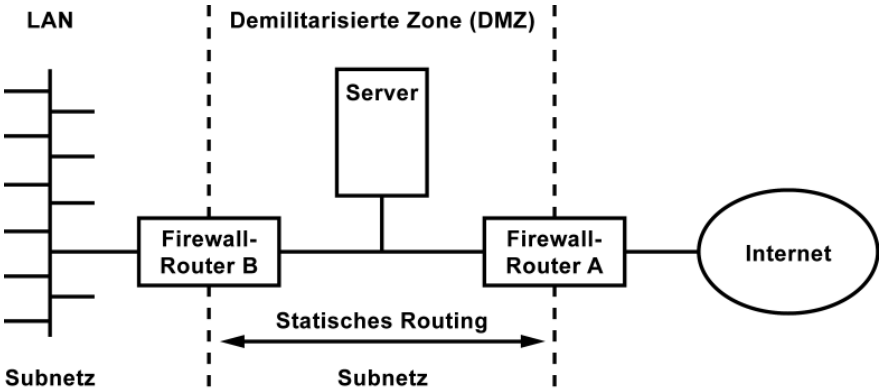
Insbesondere die Benutzer- und Anwendungserkennung ist für die zukünftige Sicherheit von Netzwerk extrem wichtig. Seit sich HTTP als Universalprotokoll entwickelt hat, müssen nicht mehr nur ein Browser und Webserver die Endpunkte einer HTTP-Verbindung sein. Grundsätzlich kann man mit HTTP alles transportieren. Aus Sicherheitsgründen darf man HTTP nach außen hin nicht mehr generell freigeben.

Hier setzt die Anwendungserkennung an, die versucht zu erkennen, was das System gerade überträgt. Die Anwendungserkennung übernimmt die Fähigkeiten eines Proxys bzw. Content-Filters. Aber sie muss weit mehr als das leisten. Um Anwendungen zu erkennen, bedarf es einen Abgleich mit Erkennungsmustern, ähnlich wie bei einem Virenscanner. Dabei ist es notwendig, dass diese Muster regelmäßig aktualisiert werden.

Typischerweise versucht man Google, Facebook, Youtube, Chats und Peer-to-Peer-Anwendungen zu erkennen. Wobei die meisten Anwendungen eher privater Nutzung zuzuordnen sind. Hierbei besteht der Irrweg darin, die Benutzer zu kontrollieren, anstatt Sicherheitslücken zu schließen. Sicherlich sinnvoll, wenn man bedenkt, dass der Mensch das größte Sicherheitsrisiko darstellt. Viel wichtiger wäre jedoch, dass die Firewall Anwendungen erkennt, vor denen das Unternehmensnetz tatsächlich geschützt werden muss.

Eine Firewall sollte im Optimalfall auch der VPN-Endpunkt sein. Damit können die Firewall-Regeln auch für die VPN-Daten gelten.

DMZ - Demilitarisierte Zone

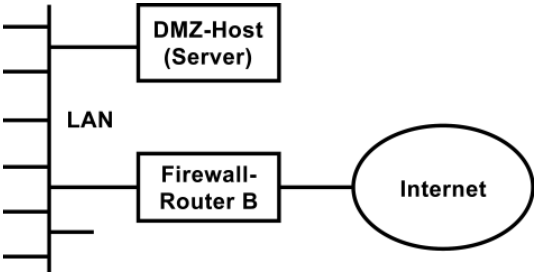


Die Demilitarisierte Zone ist ein eigenständiges Subnetz, welches das lokale Netzwerk (LAN) durch Firewall-Router (A und B) vom Internet trennt. Die Firewall-Router sind so konfiguriert, dass sie Datenpakete, für die es keine vorhergehenden Datenpakete gab, verwerfen. Wird also aus dem Internet ein Datenpaket an den Server geschickt, wird es vom Firewall-Router A verworfen. Sollte ein Hacker doch auf einen Server innerhalb DMZ Zugriff erhalten und Datenpakete in das LAN zum Schnüffeln oder Hacken schicken wollen, werden diese vom Firewall-Router B verworfen.
In beiden Firewall-Routern müssen statische Routen konfiguriert werden, damit die eingehenden Datenpakete an die richtige Station im LAN geschickt werden. Dieses Vorgehen hat den Vorteil, dass es den Datenverkehr vom Internet kommend aus dem LAN fern hält und deshalb im LAN nur der interne Datenverkehr und die Internet-Verbindungen ablaufen. Das LAN ist dann weniger anfällig für Überlastungen, die durch den Datenverkehr aus dem Internet kommen.

DMZ-Host (Exposed Host)

Die Kosten für einen zweiten Router und der Konfigurationsaufwand sind nicht unerheblich. Wer hier sparen will, kann auch einen DMZ-Host im LAN einrichten. In vielen einfachen Routern wird das als DMZ bezeichnet. Es handelt sich aber um keine echte Demilitarisierte Zone,

sondern um einen "Exposed Host" der alle eingehenden Daten erhält, was als sicherheitskritisch anzusehen ist.



Diese Sparlösung einer Demilitarisierten Zone (DMZ) sieht die Konfiguration eines Standard-Empfängers im Firewall-Router vor. Dabei gibt es zwei Ansätze. Die intelligente Lösung leitet alle Pakete mit einer festen NAT-Vorgabe (Port-Forwarding bzw. DNAT) zum DMZ-Host (Exposed Host). Dabei wird das Datenpaket abhängig vom TCP-Port an den DMZ-Host weitergeleitet oder verworfen.
Eine ungünstige Lösung ist es, alle von außen initiierte Verbindungen an den DMZ-Host weiterzuleiten. Dadurch kann der DMZ-Host mit Datenpaketen überschwemmt und ein Ausfall provoziert werden. Diesen Vorgang nennt man Denial-of-Service (DoS). In einem solchen Fall empfiehlt sich zumindest die Installation einer Software-Firewall (z. B. Pesonal-Firewall) auf dem DMZ-Host und das Aktivieren von Stateful Packet Inspection (SPI) im Firewall-Router.
In jedem Fall muss der Router das Network Address Translation (NAT) beherrschen, damit eine Verbindung in das Internet möglich ist. Da der Router im Internet mit einer eigenen IP-Adresse erreichbar ist und im LAN der private IP-Adressraum verwendet wird, übernimmt NAT die Umsetzung von öffentlicher IP-Adresse in die privaten IP-Adressen. Anhand der Sender-IP-Adresse kann NAT eingehende Datenpakete dem richtigen Empfänger zuordnen.
Vorteil des DMZ-Hosts: Er lässt sich als Proxy-Server (Vermittler) zwischen lokalem Netz und den Servern im Internet nutzen. Den Hosts im lokalen Netz tritt er als zuständiger Server auf. Den Servern im Internet spielt er einen Client vor. Auf diese Weise lässt sich die Kommunikation zwischen den Stationen und dem Internet protokollieren und filtern.

VPN - Virtual Private Network

VPN ist ein logisches privates Netzwerk auf einer öffentlich zugänglichen Infrastruktur. Nur die Kommunikationspartner, die zu diesem privaten Netzwerk gehören, können miteinander kommunizieren und Informationen und Daten austauschen.

Eine allgemein gültige Definition für VPN gibt es allerdings nicht. Der Begriff und die Abkürzung VPN stehen für eine Vielzahl unterschiedlicher Techniken. So wird manche Technik, Protokoll oder Produkt zu VPN zugeordnet, obwohl Aspekte wie Verschlüsselung oder Authentifizierung völlig außen vor gelassen sind.

VPN - Virtual Private Network		
Authentizität	Vertraulichkeit	Integrität

VPNs müssen Authentizität, Vertraulichkeit und Integrität sicherstellen, damit ein sicherer Betrieb mit Datenschutz möglich ist. Authentizität bedeutet die Identifizierung von autorisierten Nutzern und die Überprüfung der Daten, dass sie nur aus der autorisierten Quelle stammen. Vertraulichkeit und Geheimhaltung wird durch Verschlüsselung der Daten hergestellt. Mit der Integrität wird sichergestellt, dass die Daten von Dritten nicht verändert wurden. Unabhängig von der Infrastruktur sorgen VPNs für die Sicherheit der Daten, die darüber übertragen werden.

VPN-Typen

- End-to-Site-VPN (Host-to-Gateway-VPN / Remote-Access-VPN)
- Site-to-Site-VPN (LAN-to-LAN-VPN / Gateway-to-Gateway-VPN / Branch-Office-VPN)
- End-to-End-VPN (Host-to-Host-VPN / Remote-Desktop-VPN)

End-to-Site-VPN / Remote-Access-VPN

End-to-Site-VPN beschreibt ein VPN-Szenario, bei dem Heimarbeitsplätze oder mobile Benutzer (Außendienst) in ein

Unternehmensnetzwerk eingebunden werden. Der externe Mitarbeiter soll so arbeiten, wie wenn er sich im Netzwerk des Unternehmens befindet. Man bezeichnet dieses VPN-Szenario auch als Remote Access.
Die VPN-Technik stellt eine logische Verbindung, den VPN-Tunnel, zum entfernten lokalen Netzwerk über ein öffentliches Netzwerk her. Hierbei muss ein VPN-Client auf dem Computer des externen Mitarbeiters installieren sein.
Im Vordergrund steht ein möglichst geringer, technischer und finanzieller Aufwand für einen sicheren Zugriff auf das entfernte Netzwerk.

Site-to-Site-VPN / LAN-to-LAN-VPN / Branch-Office-VPN

Site-to-Site-VPN und LAN-to-LAN-VPN, oder auch Branch-Office-VPN genannt, sind VPN-Szenarien, um mehrere lokale Netzwerke von Außenstellen oder Niederlassungen (Filialen) zu einem virtuellen Netzwerk über ein öffentliches Netz zusammenzuschalten.
Netzwerke, die sich an verschiedenen Orten befinden lassen sich über eine angemietete Standleitung direkt verbinden. Diese Standleitung entspricht in der Regel einer physikalischen Festverbindung zwischen den beiden Standorten. Bei Festverbindungen, Frame Relay und ATM kommen je nach Anzahl, Entfernung, Bandbreite und Datenmenge sehr schnell hohe Kosten zusammen.
Da jedes Netzwerk in der Regel auch eine Verbindung zum Internet hat, bietet es sich an, diese Internet-Verbindung zur Zusammenschaltung von zwei oder mehr Netzwerken mit VPN-Technik (LAN-to-LAN-Kopplung) zu nutzen. Bei VPNs über das Internet entstehen einmalige Kosten für die Einrichtung und laufende Kosten nur die, die für den Internet Service Provider zu bezahlen sind.

Virtuelle private Netze (VPN) werden immer öfter über das Internet aufgebaut. Das Internet wird so zur Konkurrenz zu den klassischen WAN-Diensten der Netzbetreiber. VPNs lassen sich über das Internet billiger und flexibler betreiben.

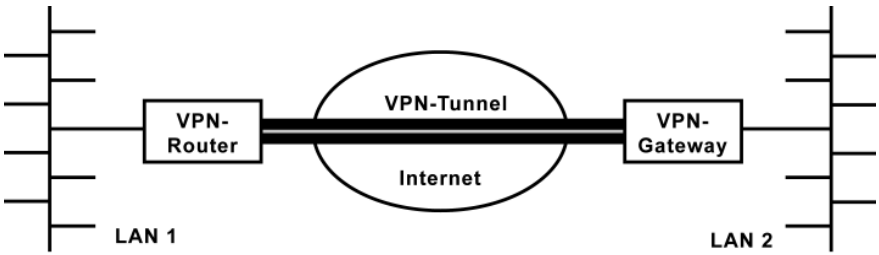
Eine Variante von Site-to-Site-VPN ist das Extranet-VPN. Während ein Branch-Office-VPN nur mehrere lokale Netzwerke einer Firma verbindet, ist ein Extranet-VPN ein virtuelles Netzwerk, das die Netzwerke unterschiedlicher Firmen miteinander verbindet. In der Regel geht es darum bestimmte Dienste fremder Unternehmen ins eigene Netzwerk zu

integrieren oder Dienste für fremde Unternehmen anzubieten. Zum Beispiel für Geschäftspartner, Lieferanten und Support-leistende Unternehmen. Dabei gewährt man dem externen Unternehmen Zugriff auf Teilbereiche des eigenen Netzwerks. Die Zugriffsbeschränkung erfolgt mittels einer Firewall zwischen dem lokalen Netzwerk und dem Dienstenetzwerk. Extranet-VPNs ermöglichen eine sichere Kommunikation bzw. einen sicheren Datenaustausch zwischen den beteiligten Unternehmen.

End-to-End-VPN / Host-to-Host-VPN / Remote-Desktop-VPN

End-to-End-VPN beschreibt ein VPN-Szenario, bei dem ein Client auf einen anderen Client in einem entfernten Netzwerk zugreift. Hierbei deckt der VPN-Tunnel die gesamte Verbindung zwischen zwei Hosts ab. Auf beiden Seiten muss eine entsprechende VPN-Software installiert und konfiguriert sein. In der der Regel ist der Verbindungsaufbau nur durch die Unterstützung einer zwischengeschalteten Station möglich. Das bedeutet, eine direkter Verbindungsaufbau von Host zu Host ist nicht möglich. Statt dessen bauen beide Seiten eine Verbindung zu einem Gateway auf, dass die beiden Verbindungen dann zusammenschaltet. Typische Anwendung eines End-to-End-VPN ist Remote-Desktop über öffentliche Netze. Während RDP und VNC sich wegen der fehlenden Verschlüsselung nur für den Einsatz in lokalen Netzwerken eignet, gibt es für Remote-Desktop-VPNs meist nur propritäre und kommerzielle Lösungen. Zum Beispiel Teamviewer und GotoMyPC.

Tunneling / Tunnelmodus / Transportmodus



Um eine gesicherte Datenübertragung über das unsichere Internet zu gewährleisten, wird mit einem Tunneling-Protokoll eine verschlüsselte Verbindung, der VPN-Tunnel, aufgebaut. Der Tunnel ist eine logische

Verbindungen zwischen beliebigen Endpunkten. Meist sind das VPN-Clients, VPN-Server und VPN-Gateways. Man nennt diese virtuellen Verbindungen Tunnel, weil der Inhalt der Daten für andere nicht sichtbar ist.
Einzelne Clients bindet man in der Regel per Tunnelmodus an. Für LAN-to-LAN-Kopplungen setzt man in der Regel den Transportmodus ein.

VPN-Endpunkt

Ein VPN-Endpunkt ist die Stelle an der der VPN-Tunnel endet bzw. beginnt. Der Endpunkt ist der Host, der für die Einhaltung von Authentizität, Vertraulichkeit und Integrität zuständig ist.
Ein VPN-Endpunkt kann ein Router, Gateway oder auch ein Software-Client sein.

VPN-Router / VPN-Gateway / VPN-Server

VPN-Lösungen gibt es als Hardware (VPN-Router), Software (VPN-Server) oder auch als Service (Layer-2-VPN vom Netzbetreiber). Typischerweise setzt man an VPN-Endpunkten einen VPN-Router oder ein VPN-Gateway ein. Es gibt aber auch Server, auf denen VPN-Dienste oder VPN-Software installiert sind. Diese VPN-Server dienen dann als VPN-Endpunkte. Ein eigenständiger VPN-Server ist eher selten nötig. VPN-Gateway-Funktionen finden sich auch in Routern und Firewalls. VPN-Gateways und -Router können VPN-Verbindungen und normale Verbindungen verarbeiten. Die VPN-Verbindungen erkennen sie am Header der Datenpakete oder an der IP-Protokollnummer.
Eine Sonderform sind VPN-Services von Netzbetreibern, die keine Installation zusätzlicher Hardware notwendig macht.

VPN-Protokolle

- IPsec
- PPTP
- L2TP
- L2TP over IPsec
- SSL-VPN
- Hamachi
- OpenVPN (Software, kein Protokoll)

Systemanforderungen

- Sicherheit
- Datenvertraulichkeit
- Schlüsselmanagement
- Paketauthentisierung
- Datenintegrität
- Benutzerauthentifizierung und Benutzerautorisierung
- Schutz vor Sabotage und unerlaubtem Eindringen

Durch die Verschlüsselung der Daten innerhalb eines VPNs entsteht eine zusätzliche zeitliche Verzögerung, die ein längere Paketlaufzeit zur Folge hat. Bei der Planung eines VPNs ist deshalb auf ein gute Ausstattung des gesamten Systems zu achten. Generell sollte man Hardware-Lösungen vorziehen. Sie arbeiten oftmals schneller und zuverlässiger als Software-Lösungen.

IPsec - Security Architecture for IP

IPsec ist eine Erweiterung des Internet-Protokolls (IP) um Verschlüsselungs- und Authentifizierungsmechanismen. Damit erhält das Internet-Protokoll die Fähigkeit IP-Pakete kryptografisch gesichert über öffentliche und unsichere Netze zu transportieren. IPsec wurde von der Internet Engineering Task Force (IETF) als integraler Bestandteil von IPv6 entwickelt. Weil das Internet-Protokoll der Version 4 ursprünglich keine Sicherheitsmechanismen hatte, wurde IPsec für IPv4 nachträglich spezifiziert.

Bestandteile von IPsec-VPNs

- Interoperalitität
- kyptografischer Schutz der übertragenen Daten
- Zugangskontrolle
- Datenintegrität
- Authentisierung des Absenders (Benutzerauthentisierung)
- Verschlüsselung
- Authentifizierung von Schlüsseln
- Verwaltung von Schlüsseln (Schlüsselmanagement)

Hinter diesen Bestandteilen stehen Verfahren, die miteinander kombiniert eine zuverlässige Sicherheit für die Datenübertragung über öffentliche Netze bieten. VPN-Sicherheitslösungen mit hohen Sicherheitsanforderungen setzen generell auf IPsec.

Einsatz-Szenarien

- Site-to-Site-VPN / LAN-to-LAN-VPN / Gateway-to-Gateway-VPN
- End-to-Site-VPN / Host-to-Gateway-VPN / Remote-Access-VPN
- End-to-End-VPN / Host-to-Host-VPN / Remote-Desktop-VPN / Peer-to-Peer-VPN

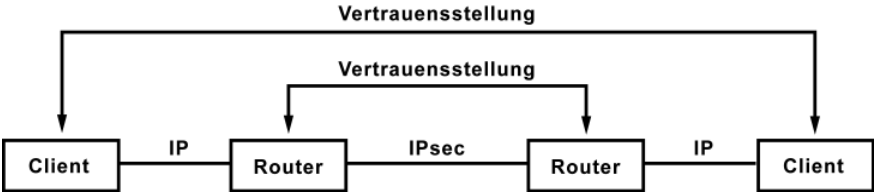
Prinzipiell eignet sich IPsec für Gateway-zu-Gateway-Szenarien. Also die Verbindung zwischen Netzen über ein drittes unsicheres Netz. Ebenso denkbar ist das Host-zu-Gateway-Szenario, dass dem Remote-Access-Szenario entspricht. Wobei die Komplexität von IPsec und einige Unzulänglichkeiten von TCP/IP hier gelegentlich Probleme bereiten können. Eher untypisch ist das Host-zu-Host-Szenario, aber ebenso möglich.

IPsec hat den Nachteil, dass es nur IP-Pakete tunneln kann. Außerdem ist es ohne zusätzliche Protokolle eher ungeeignet für Remote Access, da die Funktionen zur Konfiguration von IP-Adresse, Subnetzmaske und DNS-Server fehlen. Deshalb macht es Sinn, zur Realisierung eines VPNs außer IPsec auch SSL-VPN oder andere Lösungen und Protokolle in Betracht zu ziehen.

IPsec: Vertrauensstellungen / Security Association

Hauptbestandteil von IPsec sind die Vertrauensstellungen (Security Association) zwischen zwei Kommunikationspartnern. Eine Vertrauensstellung muss nicht zwangsläufig zwischen den Endpunkten (Client) einer Übertragungsstrecke liegen. Es reicht aus, wenn z. B. bei der Kopplung zweier Netze die beiden Router über eine Vertrauensstellung verfügen. Selbstverständlich dürfen auch mehrere Vertrauensstellungen für eine Verbindung vorhanden sein.

Die Vertrauensstellungen regeln die Kommunikation von IPsec. Die relativ flexiblen Kombinationen von Vertrauensstellungen erfordern einen sehr hohen Konfigurationsaufwand.



Um eine gesicherte Verbindung zwischen zwei Stationen aufbauen zu können, müssen auf beiden Seiten einige Parameter ausgetauscht werden:

- Art der gesicherten Übertragung (Authentifizierung oder Verschlüsselung)
- Verschlüsselungsalgorithmus
- Schlüssel
- Dauer der Gültigkeit der Schlüssel

Vertrauensstellungen werden durch den Austausch vorab definierter Schlüssel hergestellt. Eine andere Form ist die Vergabe von Zertifikaten durch ein Trust-Center oder einen installierten Zertifikate-Server. Schlüssel und Zertifikate sollen sicherstellen, dass derjenige welcher einen Schlüssel oder ein Zertifikat besitzt, auch derjenige ist, für den er sich ausgibt. Ähnlich wie bei einem Personalausweis, mit dem sich eine Person gegenüber einer anderen Person ausweist.

- PSK - Pre-Shared Keys
- X.509-Zertifikate

Schlüssel oder Zertifikate, ganz egal, beide Methoden benötigen viel Zeit und Sorgfalt bei der Einrichtung. Die einfachere Variante ist der geheime Schlüssel (Passwort bzw. Passphrase). Wichtig ist, dass die beiden Endpunkte über IP-Adresse, Subnetzmaske, Tunnelname und den geheimen Schlüssel informiert sind. Zusätzlich gibt es Parameter, die die Details der Authentisierung, Verschlüsselung und die Länge des Schlüssels festlegen.

Bei der Authentifizierung mit Pre-Shared Key muss ein Identifier konfiguriert werden. Der Identifier ist zusätzliche Angabe, anhand der sich die Gegenstellen (Gateway und Client) identifizieren können. Häufig werden dafür IP-Adressen, DNS-Namen (FQDN) oder E-Mail-Adressen (FQUN) verwendet.

Tunneling und Verschlüsselung

Die zentralen Funktionen in der IPsec-Architektur sind das AH-Protokoll (Authentification Header), das ESP-Protokoll (Encapsulating Security Payload) und die Schlüsselverwaltung (Key Management). Authentizität, Vertraulichkeit und Integrität erfüllt IPsec durch AH und ESP.
Für den Aufbau eines VPN gibt es in IPsec den Authentication Header (AH) und den Encapsulating Security Payload (ESP). Beide können gemeinsam oder eigenständig genutzt werden. In beiden Verfahren findet eine gesicherte Übertragung statt.
Das AH-Protokoll sorgt für die Authentifizierung der zu übertragenen Daten und Protokollinformationen. Das ESP-Protokoll erhöht die Datensicherheit in Abhängigkeit des gewählten Verschlüsselungsalgorithmus.

- Authentication Header (AH)
- Encapsulation Security Payload (ESP)

IPsec setzt kein bestimmtes Verschlüsselungs- und Authentifizierungsverfahren voraus. Deshalb entstehen häufig Probleme, wenn unterschiedliche VPN-Produkte zusammenarbeiten müssen.

Schlüsselverwaltung mit IKE - Internet Key Exchange Protocol

Es gibt zwei Wege für die Verwaltung und Verteilung der Schlüssel innerhalb eines VPNs. Neben der reinen manuellen Schlüsselverwaltung, kann auch das Internet Key Exchange Protocol (IKE) eingesetzt werden. Vor der geschützten Kommunikation müssen sich die Kommunikationspartner über die Verschlüsselungsverfahren und Schlüssel einig sein. Diese Parameter sind Teil der Sicherheitsassoziation (Vertrauensstellungen) und werden von IKE/IKEv2 automatisch ausgehandelt und verwaltet.

Das Internet-Key-Exchange-Protokoll dient der automatischen Schlüsselverwaltung für IPsec. Es verwendet das Diffie-Hellman-Verfahren zum sicheren Erzeugen von Schlüsseln über ein unsicheres Netz. Auf Basis dieses Verfahren wurden einige Schlüsselaustauschverfahren entwickelt, die zum Teil die Grundlage für Internet Key Exchange bilden.
IKE basiert auf dem Internet Security Association and Key Management Protocol (ISAKMP). ISAKMP ist ein Regelwerk, das das Verhalten der beteiligten Gegenstellen genau festlegt. Wie das zu erfolgen hat, legt IKE fest. Die Flexibilität von IKE äußert sich in seiner Komplexität. Wenn unterschiedliche IPsec-Systeme keine Sicherheitsassoziationen austauschen können, dann liegt das meistens an einer fehlerhaften IKE-Implementierung oder fehlende Verschlüsselungsverfahren.

Version 2 des Internet-Key-Exchange-Protokolls (IKEv2) vereinfacht die Einrichtung eines VPNs. Es ist wesentlich einfacher, flexibler und weniger fehleranfällig. Insbesondere soll das Mobility and Multihoming Protocol (MOBIKE) dafür sorgen, dass IPSec-Tunnel in mobilen Anwendungen erheblich zuverlässiger funktionieren.
IKEv2 korrigiert einige Schwachstellen bzw. Probleme der Vorgänger-Version. Die Definition wurde in ein Dokument zusammengefasst, der Verbindungsaufbau vereinfacht und viele Verbesserungen hinzugefügt. Insgesamt ist IKEv2 weniger komplex als die Vorgänger-Version. Das erleichtert die Implementierung, verringert Fehler und erhöht somit die Sicherheit.
IKEv2 ist allerdings nicht abwärtskompatibel zu IKE. Beide Protokolle werden aber über denselben UDP-Port betrieben.

Im Zusammenhang mit IPsec werden häufig die Begriffe Main Mode und Aggressive Mode verwendet. Es handelt sich dabei um unterschiedliche Verfahren zur Schlüsselaushandlung.

VPN mit IPsec in der Praxis

Die Netzwerkteilnehmer im LAN 1 können auf das LAN 2 zugreifen bzw. umgekehrt die Teilnehmer aus LAN 2 auf das LAN 1. Die Verbindung über das Internet läuft über einen verschlüsselten Tunnel ab.
Die beiden Firewalls müssen beim Verbindungsaufbau ihre Identität eindeutig nachweisen. Somit ist unberechtigter Zugang ausgeschlossen.
Die Kommunikation über das Internet erfolgt verschlüsselt. Sollte ein Dritter die Datenpakete protokollieren erhält er nur Datenmüll.

Damit beide Netze eine Verbindung zueinander aufbauen können muss die IP-Adresse des jeweiligen anderen Netzes bekannt sein. Für einen Verbindungsaufbau ist deshalb eine feste IP-Adresse notwendig, sonst wird der Verbindungsaufbau kompliziert. Ändert sich die IP-Adresse eines Netzes, z. B. beim Verbindungsaufbau zum Internet-Provider oder Zugangsnetzbetreiber, dann müssen die Adressen gegen neue ausgetauscht werden. Entweder manuell oder per dynamische DNS-Einträge mit DDNS.

Damit das Routing zwischen den Netzen funktioniert müssen die Adressbereiche innerhalb der Netze unterschiedlich sein. Da die Netze sich nach der Zusammenschaltung wie eines verhalten, dürfen IP-Adressen nicht doppelt vorkommen. Deshalb muss vorab auf beiden Seiten ein eigener Adressbereich, also unterschiedliche Subnetze, konfiguriert werden.

Probleme mit NAT

Ist sichergestellt, dass die VPN-Gegenstellen die gleichen Verschlüsselungsverfahren unterstützen und die IKE-Implementierung fehlerfrei ist, dann kann der Schlüsselaustausch mit IKE noch an den beteiligten NAT-Routern scheitern.

Wenn Netzwerk-Stationen in lokalen Netzen (LAN) private IP-Adressen haben und per NAT-Router ins Internet gehen, dann hat IPsec Probleme mit NAT. Durch NAT erhält ein IPsec-Paket eine neue IP-Adresse und einen anderen Quell-Port. Das Problem dabei, wird ein IPsec-Paket verändert, dann wird es ungültig. Durch die Änderung ist die Integrität des Pakets nicht mehr sicher gestellt. Es muss verworfen werden. So kann natürlich keine Verbindung aufgebaut werden.
Ein weiteres Problem ist, dass Original-IP-Adressen und TCP-Ports

verschlüsselt sind. So kommt der NAT-Router nicht an sie heran. Und so ist eine Zuordnung der IP-Pakete zu einer Netzwerk-Station nicht möglich. Die dafür erforderliche Information wird während des gesicherten Schlüsselaustauschs übertragen. Und da hat der NAT-Router keinen Einblick. Die Information wird im SPI-Wert (Security Parameters Index) mitgegeben. Somit könnte der VPN-Tunnel einem Host zugeordnet werden. Doch wegen der verschlüsselten Übertragung des SPIs kann der NAT-Router diesen Wert nicht mitlesen.

Um beide Probleme zu umgehen, beherrschen manche Router das IPsec-Passthrough-Verfahren, bei dem die Ports nicht verändert werden. Leider funktioniert Passthrough nur mit einem einzigen Client im Netzwerk.

IPsec-Passthrough (veraltet)

Bei IPsec-Passthrough wird die Port-Zuordnung (IKE) nicht verändert. Die IP-Adresse der ESP-Pakete wird dabei für einen Client umgeschrieben. Das bedeutet, die mit ESP behandelten Pakete können nur einer Verbindung und einem Client zugeordnet werden. Deshalb funktioniert IPsec-Passthrough hinter einem NAT-Router nur mit einem einzigen Client.
Weil in der Regel immer mehr als ein Client eine IPsec-Verbindung betreiben möchte, ist IPsec-Passthrough kaum noch in Gebrauch. Man setzt auf die IPsec-Erweiterung NAT-Traversal. Dabei werden die ESP-Pakete in UDP-Pakete verpackt und über den Port 4500 verschickt. Dann können NAT-Router IP-Adressen und Ports umschreiben.

IPsec mit NAT-Traversal

Weil das ursprüngliche IPsec über NAT-Router nicht funktioniert setzt man es in der Regel mit der IPsec-Erweiterung NAT-Traversal ein. In diesem Szenario tauschen beide Kommunikationspartner über das NAT-Traversal-Protokoll verschiedene Informationen aus. Im Anschluss werden die ESP-Pakete in UDP-Pakete verpackt und über Port 4500 verschickt. Dann können die NAT-Router ohne Probleme IP-Adressen und Ports umschreiben.
NAT-Traversal ist im IKE-Protokoll integriert (Negotiation of NAT-Traversal in the IKE). Während des Aufbaus einer IKE Security Association, wird versucht zu erkennen, ob sich ein NAT-Router

zwischen den Gegenstellen befindet. Wenn ja, dann wird die Einkapselung der IPsec-Pakete in UDP-Pakete ausgehandelt. Das bedeutet, das zwischen IP-Header und ESP-Header ein UDP-Header eingefügt wird. Die vollständige Bezeichnung dafür ist UDP Encapsulation of IPsec ESP Packets. In der Regel bezeichnet man diesen Vorgang als IPsec-NAT-Traversal.
Damit das funktioniert muss der Responder den Port 4500 (UDP und TCP) geöffnet haben. Der Responder ist derjenige, der auf die Initialisierung der IKE Security Association antwortet.

IPsec wird in der Regel immer mit der Erweiterung NAT-Traversal verwendet. Es funktioniert praktisch mit jedem NAT-Router.

Ablauf zum Aufbau eines VPNs mit IPsec und NAT-Traversal (vereinfacht)

1. Zuerst wird ermittelt, ob die Gegenstelle die notwendigen Verfahren überhaupt beherrscht.
2. Dann wird versucht die NAT-Router auf dem Übertragungsweg zu erkennen.
3. NAT-Keep-Alive wird auf der richtigen Seite aktiviert. Das sorgt dafür, dass die Einträge in der Tabelle der beteiligten NAT-Router nicht aufgrund von Timeouts gelöscht werden.
4. Bei Bedarf, wird NAT-Traversal aktiviert.
5. Danach beginnt die Aushandlung der Vertrauensstellungen. Dazu generiert das eine Ende von zwei VPN-Endpunkten eine Anfrage an das Zielsystem. Das Zielsystem antwortet und leitet den Schlüsselaustausch per Internet Key Exchange (IKE) ein. Beide Endpunkte handeln dabei Verschlüsselungs- und Authentisierungsverfahren aus. Über einen Schlüssel oder ein Zertifikat, das beide System kennen, wird eine Vertrauensstellung zueinander hergestellt. Für beide Seiten wird dann der digitale Master-Schlüssel erzeugt.
6. Beide Seiten legen dann die Verschlüsselungs- und Authentisierungsverfahren für die Datenübertragung fest. Mit dem Master-Schlüssel wird der Schlüssel für die Datenübertragung erzeugt.
7. Die Daten werden dann ausgetauscht und die Verbindung hergestellt.

Probleme mit einer Firewall bei NAT-Traversal

Damit IPsec-Verbindungen mit NAT-Traversal möglich sind, müssen die Firewalls auf beiden Seiten die verschlüsselten Datenpakete durchlassen. Die Authentifizierung erfolgt über den UDP-Port 500 oder 4500. In der Regel müssen diese Ports in der Firewall geöffnet werden.
Die verschlüsselten Datenpakete werden über das IP-Protokoll 50, dem ESP (Encapsulated Security Payload), oder dem IP-Protokoll 51, AH (Authentication Header), verschickt. Der sichere Transport von UDP-Paketen wird durch geeignete Maßnahmen im ISAKMP erreicht. So kann man auf das verbindungsorientierte TCP verzichten. Auf diese Weise haben auch viele Angriffsversuche keine Chance.

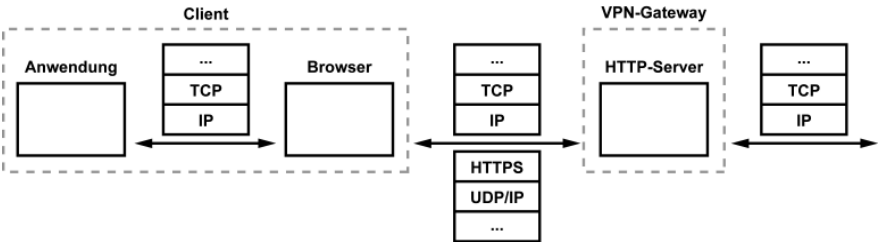
Wie sicher ist IPsec?

VPNs auf Basis von IPsec gelten als die sichersten VPNs. Allerdings ist IPsec vergleichsweise schwer zu konfigurieren. Der Aufbau eines IPsec-VPNs ist komplex und fehleranfällig. Damit ein IPsec-VPN funktioniert müssen viele Dinge reibungslos zusammenspielen. Wobei es dabei nicht nur um technische, sondern auch um organisatorische Dinge geht. Wenn mal auf der technischen Seite etwas nicht funktioniert kommt man nur sehr schwer hinter das Problem und muss per Trial & Error eine Lösung finden.
IPSec hat seit der Einführung von IKEv2 in der Handhabung und Flexibilität enorm aufgeholt. Ein weiterer Vorteil ist die Standardisierung. Durch spezielle Prozessoren haben VPN-Gateways sehr viel Leistung, können viele parallele Verbindung bedienen, sind dadurch skalierbar und zukunftssicher.
IPsec gilt im Bereich VPN als der Standard, an dem man nicht vorbei kommt. Weil IPsec eine lange Entwicklungszeit hinter sich hat, gilt es als sehr sicher. Vor allem auch deshalb, weil die Sicherheit immer wieder verbessert wurde. Aber, bei IPsec hat man es mit den Produkten unterschiedlicher Hersteller, die trotz Standard untereinander nicht oder nur begrenzt kompatibel sind.
Zudem gelten kommerzielle Implementierungen von IPsec angesichts der Enthüllungen um die NSA-Geheimdienstaktivitäten nicht mehr als vertrauenswürdig. Mit kommerziellen IPsec-Lösungen und -Produkten erwirbt der Kunde eine Black-Box, die er nicht überprüfen kann. So kann er nicht prüfen, ob das Produkt eventuell Hintertüren enthält.

SSL-VPN

SSL-VPN ist eine Art Remote-Access-VPN, das eine Alternative zu IPsec darstellt. Während die meisten VPN-Techniken relativ komplex und fehleranfällig sein können, kommt SSL-VPN durch jede Firewall und durch jedes Netzwerk hindurch. Weil SSL-VPN auf die Standards SSL bzw. TLS baut hat sich daraus der Begriff SSL-VPN gebildet.
SSL bzw. SSL-VPN beherrscht kein Tunneling und eignet sich deshalb ausschließlich für Remote-Access- oder Extranet-Anwendungen. Um Standorte zu vernetzen ist SSL-VPN eher ungeeignet. Es wäre sehr umständlich einzurichten.

Funktionsweise von SSL-VPN



Bei einem SSL-VPN ist in der Regel ein Browser der VPN-Client, der auf dem Client-Rechner läuft. Dabei werden die Daten mittels HTTPS vom Browser zu einem HTTP-Server (Webserver), der als VPN-Gateway dient, übertragen. HTTPS ist in jedem Browser eingebaut und funktioniert praktisch überall. Auch durch eine Firewall oder einen NAT-Router hindurch.
Um auch Daten von außerhalb des Browsers übertragen zu können, wird innerhalb des Browsers ein Plugin, Java-Applet oder eine ActiveX-Komponente ausgeführt, die als Gateway dient und die die Daten über die verschlüsselte Verbindung umleitet.

Browser-based

Ein typisches SSL-VPN ist ein Browser-basiertes SSL-VPN. Alles was man braucht ist ein Browser, der SSL/TLS beherrscht und einen Webserver mit der dazu passenden Implementierung. Die Verbindung wird dabei über HTTPS-Requests und -Responses zwischen Browser und

Server abgewickelt. Im Gegensatz zu HTTP ist die Verbindung bei HTTPS verschlüsselt.
Allerdings hat diese Art von VPN keine Vorteile. Es können keine Dienste außerhalb des Browsers, wie E-Mail oder File-Server benutzt werden. Es bräuchte dazu ein Web-Frontend, wie zum Beispiel ein Webmailer, der im Browser ausgeführt wird.
Im Prinzip handelt es sich beim Zugriff auf einen Webmail-Dienst, wie er von verschiedenen Internet-Service-Providern angeboten wird ein Browser-based SSL-VPN.

Client-based

Es gibt VPN-Clients, die auch SSL-VPN beherrschen. Häufig als Backup-Lösung, wenn keine Verbindung mit IPsec oder anderen VPN-Protokollen möglich ist. Beispielsweise weil eine Firewall den Verbindungsaufbau blockiert.
Nach einem erfolgreichen Verbindungsaufbau mit SSL-VPN klingt sich der VPN-Client wie üblich als zusätzliche Netzwerkschnittstelle ins Betriebssystem ein.

Enhanced Browser-based

Bei Client-basierten SSL-VPNs muss man auf alle Fälle einen Client installieren, wobei die Vorteile eines Client-losen VPNs nicht mehr gegeben sind. Im Vergleich ist mit einem rein Browser-basierte SSL-VPN vieles nicht möglich. Deshalb kombiniert man Client-basiertes und Browser-basiertes SSL-VPN miteinander.
Dazu stellt man per Browser eine HTTPS-Verbindung zu einem Server oder Gateway her. HTTPS ist in jedem Browser eingebaut und funktioniert praktisch überall. Auch durch eine Firewall oder NAT-Router hindurch. Vom Server oder Gateway lädt sich der Browser automatisch eine Java- oder ActiveX-Applikation herunter. Diese Applikation wird vom Browser ausgeführt und arbeitet als TCP/UDP-Gateway, um die VPN-Verbindungen über den Browser umzuleiten.
Dieses Verfahren funktioniert auf mobilen Geräten nur eingeschränkt, weil externe Applikationen in deren Browser nicht ausgeführt werden können.

Wie sicher ist SSL-VPN?

SSL ist für Online-Banking und eCommerce gemacht. Hier profitiert man von der Nutzung unabhängig von Ort und Software-Ausstattung. Die Kunden brauchen nur einen SSL/TLS-fähigen Browser. SSL-VPN funktioniert also von fast jedem Computer, der Internet-Zugang hat. Und das auch, bei einem unsicheren Rechner. Für manche Anwendungsfälle ist das nicht sicher genug. So unterstützt SSL/TLS keine Tunnel, was aber für ein sicheres VPN eigentlich eine Voraussetzung ist.

An der Absicherung von VPN-Verbindungen durch SSL/TLS kann man grundsätzlich nichts aussetzen, wenn man berücksichtigt, dass die Authentifizierung von SSL/TLS mangelhaft ist. Sicherer wird es, wenn man sich nicht auf das vorherrschende fehlerhafte CA-Modell verlässt, sondern selbst ausgestellte Zertifikate verwendet. Wobei man hier mit dem Aufwand der Zertifikatsverwaltung leben muss.
Außerdem muss man berücksichtigen, dass die Browser, die als VPN-Clients "missbraucht" werden unter Umständen Sicherheitslücken aufweisen oder eine fehlerhafte SSL-Implementierung enthalten.
Ein weiterer, unter Umständen kritischer Punkt, SSL verschlüsselt nur die Daten auf der Anwendungsebene, aber nicht die gesamte Kommunikation. Damit ist gemeint, dass der Aufbau der Verbindung unverschlüsselt ist, die Verschlüsselung ausgehandelt wird und erst dann die Daten verschlüsselt werden. Mit der Sicherheit, die eine IPsec-Lösung verspricht, ist das nicht vergleichbar. Allerdings kommen in SSL viele Verschlüsselungs-, Schlüsselerzeugungs- und Hash-Verfahren zum Einsatz, die auch im IPsec- und IKE-Protokoll Anwendung finden.

Vor dem Einsatz von SSL-VPN ist also zu prüfen, ob SSL/TLS für den gewünschten Anwendungsfall sicher genug ist. Gegebenenfalls muss der SSL-Datenverkehr zusätzlich durch eine Firewall kontrolliert und die Verbindungsmöglichkeiten eingeschränkt werden.

Vergleich: IPsec und SSL-VPN

IPsec und SSL kann man nicht direkt miteinander vergleichen. Dafür ist deren Ausrichtung und Einsatzzweck zu unterschiedlich.
IPsec arbeitet infrastruktur- und anwendungstransparent auf der Netzwerkebene. Dagegen arbeitet ein SSL-VPN ebenso

infrastrukturtransparent aber anwendungsbezogen zwischen Transport- und Anwendungsebene. In der Regel ist ein SSL-VPN schneller eingerichtet. Im laufenden Betrieb gibt es weniger Verbindungsprobleme.

Der große Vorteil von SSL-VPN ist, dass die Installation eines VPN-Client nicht zwingend notwendig ist. Es reicht ein SSL-tauglicher Browser und die Unterstützung von Java oder ActiveX. Eines von beiden sollte auf einem Standard-PC kein Problem darstellen. Insbesondere Java-Applets funktionieren Browser- und Betriebssystem-unabhängig.
SSL-VPN hinterlässt auch auf dem Rechner keine Spuren. Trotzdem sind bei hohen Sicherheitsanforderungen fremde Rechner tabu. Dann sollte man kein SSL-VPN zur Verfügung stellen. Bei veralteten Browsern kann niemand wirklich eine hohe Sicherheit gewährleisten.

IPsec schützt die gesamte Verbindung und erlaubt den Zugriff nur von Geräten und Netzen, die sich dafür autorisieren. Mit IPsec lassen sich Sicherheitsrichtlinien leichter durchsetzen und Angriffsversuche besser verhindern, als mit SSL-VPN. IPsec eignet sich für die Vernetzung und SSL/TLS für sichere Internet-Transaktionen.
Allerdings bietet sich SSL als Ergänzung zu IPsec an. Eine VPN-Lösung mit IPsec UND SSL, am besten mit einer einzigen Benutzerverwaltung, bietet die größtmöglichste Flexibilität und kann damit jedes Einsatz-Szenario abdecken. Die Schwächen der beiden Protokolle werden in einer Gesamtlösung sehr gut ausgeglichen.

Eine IPsec-Installation durch SSL-VPN ablösen zu wollen ist in den seltensten Fällen eine gute Idee. SSL-VPN kann IPsec in der Regel nicht ersetzen, aber auf Applikationsebene mit vergleichbaren Sicherheitsfunktionen ergänzen.

OpenVPN

OpenVPN ist eine betriebssystemübergreifende Open-Source-Software, die es für Linux, MacOS, Windows und Unix gibt, mit der man VPN-Verbindungen aufbauen kann. OpenVPN eignet sich für die Anbindung von Clients und zur Kopplung entfernter Netze. Seit PPTP als unsicher gilt, hat OpenVPN deutlich an Aufmerksamkeit gewonnen.

OpenVPN ist Dank seiner Flexibilität und hohen Sicherheit äußerst beliebt. Mit OpenVPN kann man schnell und einfach ein verschlüsseltes virtuelles privates Netzwerk (VPN) einrichten. Zum Beispiel, um externe Mitarbeiter über das Internet auf den Firmenserver zugreifen zu lassen. Um eine Verbindung per OpenVPN aufzubauen, muss man auf beiden Seiten die OpenVPN-Software installieren und zueinander passend konfigurieren. Ein OpenVPN-Server kann auch auf einem Router installiert sein. Nur dann stehen unter Umständen nicht alle Optionen zur Verfügung.

Neben Anwendungsdaten kann OpenVPN auch IP-Pakete und Ethernet-Frames übertragen. Das bedeutet, dass TCP-Pakete ineinander verschachtelt werden. Um zu vermeiden, dass es wegen der Datenflusskontrolle von TCP zu hohen Latenzen oder sogar Verbindungsabbrüchen kommt, nutzt OpenVPN zur Übertragung UDP. UDP verzichtet auf die Datenflusskontrolle.

NAT-Router stellen für OpenVPN-Verbindungen kein Problem dar, weil OpenVPN weder die IP-Adresse noch die Portnummern des Pakets authentisiert.

Verschlüsselung

OpenVPN nutzt SSL bzw. TLS zur Verschlüsselung. OpenVPN schiebt sich zwischen die nicht TLS-fähigen Anwendungen und dem TCP/IP-Protokollstack. Dazu muss der OpenVPN-Client auf der einen und auf der anderen Seite ein OpenVPN-Server installiert sein. Der OpenVPN-Server ist für den Betrieb auf einem Router ungeeignet.

OpenVPN setzt durchgängig auf SSL-Zertifikate. Sowohl auf der Seite des Servers als auch bei den Clients. Jeder Client bekommt ein eigenes Zertifikat. Das hat den Vorteil, wenn ein Client in falsche Hände gerät. So ist nicht das ganze VPN in Gefahr, sondern nur die Gültigkeit dieses einen Zertifikats zu entziehen.
Dazu muss man eine eigene Certification Authority (CA) betreiben, um Zertifikate und Schlüssel zu erzeugen und zu verwalten. Theoretisch wäre das auf einem Router möglich, aber auf einem PC unter Windows, Mac OS oder Linux ist das viel einfacher. Man muss nur darauf achten, dass der PC nicht für Dritte zugänglich ist.

Betriebsarten: Routing und Bridging

Um zwei Rechner miteinander zu verbinden (Host-to-Host-VPN), eignet sich die Betriebsart Routing. OpenVPN agiert dabei als Router, der auf IP-Ebene arbeitet. Soll im Rahmen eines Site-to-Site- oder Site-to-End-VPN auf ein lokales Netz zugegriffen werden, ist Bridging die bessere Wahl.

Authentifizierung im Netzwerk

Authentifizierung im Netzwerk ist ein Vorgang bei dem festgestellt wird, wer eine Person oder eine Maschine ist. Im echten Leben weisen wir uns durch Unterschriften, Pässe und Karten aus. Im Internet ist die Authentifizierung durch die räumliche Trennung erschwert. Hier greift man auf symmetrische Schlüssel, Zertifikate und andere Authentifizierungsmechanismen zurück.

Im Zusammenhang mit der "Authentifizierung" tauchen auch häufig die Begriffe "Autorisierung" und "Authentisierung" auf. "Autorisierung" ist der Vorgang, bei dem ermittelt wird, welche Berechtigung die Person oder Maschine hat und was sie machen darf.
"Authentisierung" bedeutet, dass eine Person oder Maschine sich gegenüber einem Kommunikationspartner identifizieren muss.

Die Authentifizierung erfolgt zum Beispiel mit Benutzername und Passwort. Knackpunkt bei jeder Authentifizierung ist die Übertragung von Benutzername und Passwort. Erfolgt die Übertragung unverschlüsselt, dann kann ein Angreifer die Zugangsdaten abhören und für seine Angriffsversuche missbrauchen. Der sichere Betrieb von VPNs und Zugang zu Netzwerken ist nur mit einer guten und verschlüsselten Authentifizierung möglich. Um Sicherheit in einem Netzwerk herzustellen sollte man niemals die Authentifizierung vernachlässigen.

Übersicht: Authentifizierung

- Pre-Shared-Key
- Zertifikat
- Kerberos und SecurI

Pre-Shared-Key

Ein Pre-Shared-Key ist ein symmetrischer Schlüssel (Passwort), der vor einer Verbindungsaufnahme ausgetauscht werden muss. Es handelt sich dabei um einen unsignierten Schlüssel, der frei wählbar ist.
Damit ein unsignierter Schlüssel ein wenig Sicherheit verspricht, sollte es sich dabei um ein sehr schwer zu erratendes Passwort handeln.
Wer den Schlüssel kennt, bekommt Zugang zu einem Netzwerk. Das bedeutet auch, wer ungewollt an den Schlüssel gelangt, der kann auch eine Verbindung belauschen. Sobald auch nur der Verdacht besteht, dass der Schlüssel Dritten bekannt sein könnte, muss er ausgetauscht werden. Vorsichtshalber sollte der Schlüssel regelmäßig ausgetauscht werden, was natürlich aufwendig ist. Sicherer ist der Einsatz von Zertifikaten, durch die auch der vorherige Schlüsselaustausch entfällt.

Zertifikat

Bei der Authentifizierung mit Zertifikaten kommt ein asymmetrischer Schlüssel zum Einsatz. Nach der erfolgreichen Authentifizierung wird der Schlüssel für die symmetrische Verschlüsselung berechnet.
Bei X.509v3-Zertifikaten wird ein öffentlicher Schlüssel an eine Identität gekoppelt und durch eine Certification Authority (CA) beglaubigt.
Der Einsatz von Zertifikaten zieht einen hohen Verwaltungsaufwand nach sich. Es ist eine Organisation und Infrastruktur notwendig, die Zertifikate beantragt, ausstellt und verteilt.
Zertifikate werden nicht nur bei der Authentifizierung, sondern auch bei der gesicherten Übertragung von E-Mails, dem Webseiten-Abruf (SSL/TLS) oder dem Code-Signing verwendet.

Protokolle für die Authentifizierung

- PAP - Password Authentication Protocol
- CHAP - Challenge Handshake Authentication Protocol
- MS-CHAP - Microsoft CHAP
- EAP - Extensible Authentication Protocol

Authentifizierungsverfahren

- IEEE 802.1x / RADIUS

IEEE 802.1x / RADIUS

IEEE 802.1x ist ein sicheres Authentifizierungsverfahren für Zugangskontrollen in lokalen Netzwerken (LAN). Im Zusammenhang mit IEEE 802.1x werden auch häufig EAP und RADIUS genannt.
Das Protokoll EAP (Extensible Authentication Protocol), das ursprünglich als Erweiterung für PPP-Verbindungen entwickelt wurde, ist der Kern von IEEE 802.1x. IEEE 802.1x beschreibt die Einbettung von EAP-Datagrammen in Ethernet-Frames. Das ermöglicht den Austausch von Authentifizierungsnachrichten auf der Schicht 2 des OSI-Schichtenmodells.
EAP beschreibt ein einfaches Frage-Antwort-Verfahren, bei dem die Authentifizierungsdaten vom Benutzer zum Authentifizierungs-Server und dessen Antworten ausgetauscht werden.
RADIUS kann bei der Anbindung einer zentralen Benutzerverwaltung eine wichtige Rolle spielen. Aber, IEEE 802.1x schreibt keinen RADIUS-Server vor. Doch in der Regel wird beim Einsatz einer Zugangskontrolle mit IEEE 802.1x auch ein RADIUS-Server eingesetzt.

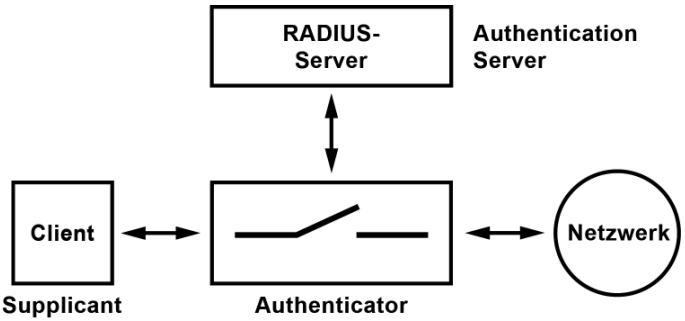
Im Zusammenhang mit WLAN wird die Authentifizierungsmethode IEEE 802.1x auch als WPA2-Enterprise, WPA2-1x oder WPA2/802.1x bezeichnet.

Funktionen von IEEE 802.1x

- Zugangskontrolle
- Authentifizierung, Autorisierung und Accounting (AAA)
- Bandbreitenzuweisung (QoS)
- Single Sign-on (SSO)

Wie funktioniert IEEE 802.1x?

Bestandteil eines Authentifizierungsverfahrens wie IEEE 802.1x ist der Supplicant (Antragsteller), der Authenticator (Beglaubigter) und ein Authentication Server, der den Antrag des Supplicant überprüft und seine Entscheidung dem Authenticator mitteilt. Der Authenticator schaltet den Zugang zum Netzwerk für den Supplicant frei oder verweigert ihn.



- Authenticator (Beglaubigter/Unterhändler): WLAN-Access-Point oder Switch mit IEEE 802.1x
- Authentication Server: RADIUS-Server, LDAP-Gateway/-Server, WLAN-Access-Point
- Supplicant (Antragsteller): WLAN-Client, LAN-Station

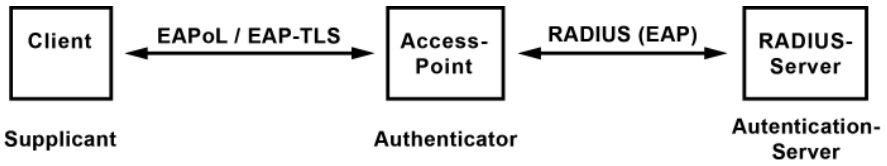
Anmeldungen vom Supplicant (Client) werden vom Authenticator zuerst an den Authentication Server weitergeleitet. Der entscheidet, ob der Supplicant Zugang bekommt. In Abhängigkeit einer erfolgreichen Authentifizierung wird der Zugang zum Netzwerk über einen bestimmten Port freigeschaltet. Wegen dem Bezug auf einen Port wird IEEE 802.1x auch als "Port-Based Network Access Control" bezeichnet.

Für IEEE 802.1x kann ein Port eine Buchse an einem Switch oder eine logische Assoziation sein. Denkbar ist hier die Zugangsmöglichkeit zum Netzwerk für einen WLAN-Client an einem WLAN-Access-Point. Mit IEEE 802.1x/EAP wird dem WLAN-Client zu Beginn einer Sitzung die dafür gültigen WPA2-Schlüssel mitgeteilt.

Wichtig bei WLAN, der WLAN-Access-Point muss auf WPA2-Enterprise eingestellt sein. Dabei hinterlegt man die IP-Adresse des RADIUS-Servers und ein Passwort, mit dem der RADIUS-Server und der WLAN-Access-Point ihre Kommunikation verschlüsseln und sichern.

Prinzipiell kann ein RADIUS-Server auch zur Verwaltung von Zugangsdaten dienen. Es gibt Architekturen bei denen der RADIUS-Server die Benutzer-Zugangsdaten nicht verwaltet, sondern zum Beispiel ein LDAP-Server (Verzeichnisdienst). In diesem Fall leitet der RADIUS-Server die Authentifizierung an den LDAP-Server weiter.

EAP - Extensible Authentication Protocol



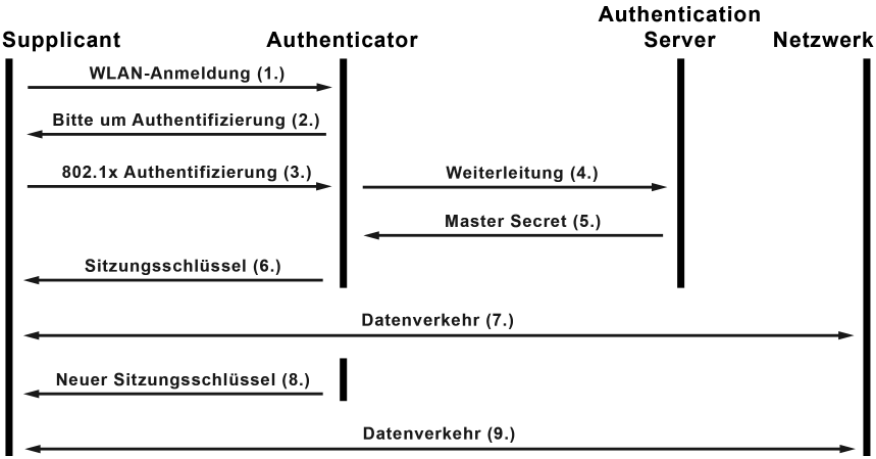
Die Kommunikation zwischen Supplicant und Authenticator erfolgt über das Extensible Authentication Protocol over LAN (EAPoL). Die Kommunikation zwischen Authenticator und Authentication Server erfolgt über in RADIUS-Paketen gekapselte EAP-Pakete.

Beispiel für die Anwendung von IEEE 802.1x, EAP und RADIUS

Beim Zugriff auf ein lokales Netzwerk eines Unternehmens über WLAN reicht die einfache Authentifizierung über ein gemeinsames Passwort (WPA2-PSK) nicht aus. Wenn das Passwort die Runde macht, dann ist das WLAN praktisch offen.

Mit RADIUS werden serverseitig Passwörter zugeteilt, was dem Administrator Arbeit erspart und für die Nutzer vergleichsweise einfach ist. In dieser Konstellation kommt WPA2-Enterprise zum Einsatz, bei dem die WLAN-Basisstation die Zugriffe der WLAN-Clients über das Protokoll IEEE 802.1x mit einem RADIUS-Server aushandeln.

Ein RADIUS-Server ist nicht immer zwingend erforderlich. Manche WLAN-Router enthalten bereits einen RADIUS-Server, der für kleine Netzwerke eine Alternative ist.



1. Zuerst meldet sich der WLAN-Client (Supplicant) am WLAN-Access-Point (Authenticator) an. Beide Geräte sind entsprechend auf WPA2-Enterprise konfiguriert.
2. Der Access-Point (Authenticator) fordert den Client (Supplicant) zur Authentifizierung auf. In der Regel folgt hier die Eingabe von Benutzername und Passwort durch den Nutzer.
3. Der Client (Supplicant) authentisiert sich nach IEEE 802.1x.
4. Der Access-Point (Authenticator) leitet die Authentifizierung an den RADIUS-Server (Authentication Server) weiter.
5. Bei erfolgreicher Authentifizierung gibt der RADIUS-Server das Master Secret zurück.
6. Der Access-Point generiert den Sitzungsschlüssel und teilt diesen dem Client mit.
7. Durch den Sitzungsschlüssel bekommt der Client Zugriff auf das Netzwerk.
8. In regelmäßigen Abständen bekommt der Client einen neuen Sitzungsschlüssel mitgeteilt.
9. Damit ist weiterhin der Zugriff auf das Netzwerk durch den Client möglich.

RADIUS - Remote Authentication Dial In User Service

Innerhalb eines großen Netzwerks findet die Verwaltung und Speicherung von Benutzerdaten an einer zentralen Stelle statt. Diese Daten dienen auch zur Authentifizierung von Benutzern, die sich am Netzwerk anmelden.

Kommt es zu einem Zugriff von außen auf das Netzwerk wird eine RAS- oder VPN-Verbindung hergestellt. Über diese Verbindung muss der Benutzer authentifiziert werden, bevor er Zugriff auf das Netzwerk bekommt.
Das Bindeglied zwischen der zentralen Benutzerverwaltung und dem RAS ist der RADIUS. Obwohl IEEE 802.1x keinen RADIUS-Server vorschreibt, sind die meisten Authenticatoren in der Praxis RADIUS-Clients. Das RADIUS-Protokoll übernimmt die Authentifizierung und Verschlüsselung, sowie das Accounting. Vom RADIUS-Server wird der Anfang und das Ende der Benutzung einer Leistung protokolliert und kann zu Abrechnungszwecken herangezogen werden.

Radius kennt drei Pakettypen, deren Namen so lauten, wie ihre Funktion:

- Access-Request (Bitte um Freigabe des Zugriffs)
- Access-Accept (Annahme für die Freigabe des Zugriffs)
- Access-Reject (Ablehnung der Freigabe)

Die RADIUS-Nachrichten werden auf IP-Ebene mit UDP-Paketen versendet. Die Informationen stecken in Attribute-Value Pairs (AVP).

Stichwortverzeichnis

A

Aktives FTP 231
Anwendung 36
Anycast 20
ARP 165
Asymmetrische Verschlüsselung 264
Authentifizierung 308
Authentizität 255
Avahi 198

B

Backbone 22
Baum 40
Beamforming 120
Bitübertragung 34
Blockchiffren 265
Bonjour 198
BOOTP 151
Brechungsindex 62
Bridge 17
Broadcast 21
BSS 109
Bus 38

C

Category 6 50
ccTLD 216
Chain 38
Chiffrierung 263
CIDR 146
Cipher-Suite 269
Client 16
Client-Server 13
Codec 241
CSMA/CA 104
CSMA/CD 75

D

Darstellung 36
Datagramm 19
Datastream 19
Datenpaket 18
Datenstrom 19
Datenübertragung 12
DDNS 214
Delay 241
DFS 118
DHCP 156
DHCPv6 182
DiffServ 251
Dispersion 63
DMZ 288
DNAT 163
DNS 214
DNSSEC 214
DNS-Server 220
DNS-Zonen 219
DoD 31
Domain 215
Domäne 18
DS-Lite 188
Dual-Stack 186

E

EAP 312
EIA 43
E-Mail 206
ESS 109

Ethernet....73

F

Fabric....41
Fast-Ethernet....83
Firewall....284
Flow Control....83
FQDN....217
Frame....19
FTP....56, 230

G

Gateway....17
Gigabit-Ethernet....85
Gigabit-WLAN....117
Glasfaser....59
gTLD....217

H

Halbduplex....79
HomePlug....130
Host....16
HTML....206
HTTP....225
Hub....64
Hybride
Verschlüsselungsverfahren
....270

I

IANA....22
IBSS....108
ICANN....22
ICMP....166
IEEE....23
IEEE 802....72
IEEE 802.11ac....117
IEEE 802.11ax....122
IEEE 802.11n....113
IETF....23
IKE....297
IMAP....209
Integrität....255
Internet....26
IP-Routing....153
IPsec....294
IPsec-Passthrough....300
IPv4....140
IPv4-Adressen....141
IPv4-Konfiguration....149
IPv4LL....147
IPv6....167
IPv6-Address-Scopes....175
IPv6-Adressen....172
IPv6-Autokonfiguration....179
ISO....23

J

Jitter....242

K

Knoten....16
Koaxialkabel....57
Kollisionen....76
Kommunikation....36
Kryptoanalyse....262
Kryptografie....257

L

LAN....24
Layer-3-Switch....67
LDAP....237
Lichtwellenleiter....59

Localhost 147
LWL 59

M

MAC-Adresse 80
Mainframe 14
MAN 26
Mesh 40
MIMO 117
Moden 62
MPLS 251
Multicast 21
MU-MIMO 120

N

Namensauflösung 210
Nameserver 220
NAT 159
NAT-Traversal 300
NBase-T 86
NetBIOS 196
Netzklassen 144
Netzwerk 10
Netzwerk-Kabel 46
Netzwerkkarte 63
Node 15
NTP 232

O

OpenVPN 306
OSI 32

P

Paket 18
Paketfilter 286
Passives FTP 232
Peer-to-Peer 13
PNRP 214
PoE 90
POP 209
Port 19
Powerline 130
Power-over-Ethernet 90
Privacy Extensions 176
Protokolle 11

Q

QoS 247
Quality of Service 247

R

RADIUS 310
RDNSS 182
Remote-Access 290
Resolver 222
Ressourcen 18
Ring 38
RJ45 53
Router 16, 66
Routing 17
RTP 196

S

Schichtenmodelle 28
Secure Shell 271
Server 16
Sicherung 35
SIP 245
SLAAC 180
SMTP 208
SNAT 161
Spleiß 62
SSH 271

SSL 273
SSL-VPN 303
Star 39
Stern 39
Stream 19
Stromchiffren 265
Subnetting 145
Switch 65
Switching 18
Symmetrische Verschlüsselung 264

T

TCP 189
TCP/IP 136
TIA 43
TLD 216
TLS 282
Topologie 37
Traffic-Shaping 251
Transport 35
Tree 40
Tunneling 21
Twisted-Pair 46

U

UDP 195
Unicast 20
URL 223
UTP 55

V

Vermittlung 35
Verschlüsselung 263
Vertraulichkeit 255
Verzeichnisdienste 233
VoIP 238
Vollduplex 79
VPN 290
VPN-Router 293

W

WAN 25
WDS 110
WebDAV 229
WINS 212
Wireless Gigabit 122
WLAN 93
WLAN-Frequenzen 97
WLAN-Sicherheit 123
WPA 125
WPA2 126
WPS 127
WWW 204

X

X.500 233

Z

Zeroconf 198
Zertifikate 275

Elektronik-Fibel

- Elektronik, einfach und leicht verständlich
- Nachschlagewerk für den Unterricht und die Ausbildung
- zum Lernen auf Klassenarbeiten, Klausuren und Prüfungen

Elektronik muss nicht schwer sein. Ziel der Elektronik-Fibel ist es, Elektronik allgemein verständlich zu beschreiben, so dass der Einstieg in die Elektronik so einfach wie möglich gelingt.

Durch die vielen grafischen Abbildungen, Formeln, Schaltungen und Tabellen soll es dem Einsteiger, wie auch dem Profi, immer und überall als unterstützende und nützliche Lektüre dienen.

Was andere über die Elektronik-Fibel sagen:

„Die Elektronik-Fibel ist einfach nur genial. Einfach und verständlich, nach so einem Buch habe ich schon lange gesucht. Es ist einfach alles drin was man so als Azubi braucht. Danke für dieses Schöne Werk."

„Vor allem gefällt mir, dass die Formulierungen einfach und gut verständlich sind. Das macht die Elektronik-Fibel für mich als Anfängerin zugänglicher."

„Für mich als Schüler, der nicht gerade sehr viel Ahnung von der Elektrotechnik hat, ist dieses Buch sehr hilfreich. Was mir vor allem zusagt, ist diese leichtverständliche Sprache mit der das Buch verfasst ist. Ein wirklich sehr gutes Buch, das ich jederzeit ohne Einschränkungen weiterempfehlen würde."

http://www.elektronik-fibel.de/

http://www.elektronik-kompendium.de/

Kommunikationstechnik-Fibel

Die Themen dieses Buches sind Grundlagen der Kommunikationstechnik, Netze, Mobilfunk, Breitband und Next Generation Network.

Die Kommunikationstechnik-Fibel ist kein Lehrbuch im klassischen Sinne. Es ist als Ergänzung zu einer schulischen oder betrieblichen Ausbildung gedacht. Es soll Lücken schließen und Verständnis für komplexe Sachverhalte in der Kommunikationstechnik bringen.

Die Arbeit mit diesem Buch soll dem Schüler oder Azubi ein klareres Verständnis und eine deutlich bessere Leistung ermöglichen.

Was andere über die Kommunikationstechnik-Fibel sagen:

„Die Bücher Kommunikationstechnik-Fibel und Netzwerktechnik-Fibel sind sehr informativ und verständlich. Genau das habe ich schon seit langem gesucht. Endlich mal ein Buch, das kurz und bündig die moderne Informationstechnik beleuchtet."

„Als Ausbilder im Bereich Elektronik und Telekommunikation bin ich über den Inhalt sehr begeistert."

„Meinen Glückwunsch. Die Kommunikationstechnik-Fibel übertraf bei weitem meine Vorstellung. Sogar die Beschreibung des alten analogen Telefonapparates mitsamt Nummernscheibe ist enthalten, was ich nicht erwartet hätte. Einfach Klasse und umfassend. Das Buch "hat etwas"! Ich werde es weiterempfehlen."

http://www.kommunikationstechnik-fibel.de/

http://www.elektronik-kompendium.de/

Computertechnik-Fibel

Die Computertechnik-Fibel ist ein Hardware-Buch über die Grundlagen der Computertechnik, Prozessortechnik, Halbleiterspeicher, Schnittstellen, Datenspeicher und Komponenten.

Durch die Computertechnik-Fibel ist es möglich, die grundlegenden Kenntnisse über Computertechnik zu erwerben und somit ein besseres Verständnis für Computertechnik und die Zusammenhänge zu bekommen.

Dieses Buch ist eine Ergänzung für die schulische und betriebliche Aus- und Weiterbildung. Mit Hilfe über 100 grafischer Abbildungen und Tabellen ist dieses Buch vor allem für den Einsteiger, aber auch für den Profi, ein treuer Begleiter durch das Thema Computertechnik.

Was andere über die Computertechnik-Fibel sagen:

> „Ich mache gerade eine Umschulung zur Informationselektronikerin und hatte vorher leider keinerlei Vorkenntnisse. Dabei ist mir dieses Buch und auch die anderen Bücher eine sehr gute Unterstützung.Ich lese lieber in diesen Büchern als in meinen Aufzeichnungen, da ich in der Computertechnik-Fibel alles sofort finde."
>
> „Die Computertechnik-Fibel ist wirklich verständlich geschrieben, frei von Ballast und ein tolles Nachschlagewerk. Man muss nicht alles wissen, man muss nur wissen, wo es steht. Insgesamt ein sehr empfehlenswertes Buch."
>
> „Ich empfinde diese Art der Wissensvermittlung als angenehm und einleuchtend. Nur sehr selten kommt mir ein so leicht verständliches Buch unter."

http://www.computertechnik-fibel.de/

http://www.elektronik-kompendium.de/

ElektronikQuest

ElektronikQuest ist ein webbasiertes Lernsystem. Es stellt Fragen, wie sie in Klassenarbeiten und Prüfungen gestellt werden. Wenn jemand die gestellte Frage nicht beantworten kann, also das nötige Wissen fehlt, dann kann er sich Hinweise und Links einblenden lassen unter denen er Erläuterungen zum Thema findet.

ElektronikQuest ist kein Ersatz für den Unterricht in der Schule oder in der Ausbildung. Viel mehr ist es eine Ergänzung, um Themen zu wiederholen und zu festigen. Und natürlich, um festzustellen, ob man das Thema begriffen hat oder nicht. Das ElektronikQuest wiederholt ganz automatisch die Fragen, die falsch beantwortet werden.

Kostenlos anmelden und testen

http://www.elektronik-quest.de/